AN INFORMATION SECURITY FRAMEWORK FOR WEB SERVICES IN ENTERPRISE NETWORKS

A THESIS SUBMITTED TO

THE GRADUATE SCHOOL OF INFORMATICS

THE MIDDLE EAST TECHNICAL UNIVERSITY

BY

BAHADIR GÖKHAN SARIKOZ

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

IN THE DEPARTMENT OF INFORMATION SYSTEM

JANUARY 2015

AN INFORMATION SECURITY FRAMEWORK FOR WEB SERVICES IN ENTERPRISE NETWORKS

Submitted by **Bahadır Gökhan Sarıkoz** in partial fulfilment of the requirements for the degree of **Master of Science in Information Systems, Middle East Technical University** by,

Prof. Dr. Nazife Baykal
Director, Informatics Institute _____

Prof. Dr. Yasemin Yardımcı Çetin
Head of Department, Information Systems _____

Assoc. Prof. Dr. Banu Günel
Supervisor, Information Systems, METU _____

Examining Committee Members:

Prof. Dr. Nazife Baykal
IS, METU _____

Assoc. Prof. Dr. Banu Günel
IS, METU _____

Prof. Dr. Şeref Sağıroğlu
CENG, Gazi University _____

Assist. Prof. Dr. Pekin Erhan Eren
IS, METU _____

Dr. Buğra Karabey
META, Microsoft _____

Date: June 21, 2015

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Surname: Bahadır Gökhan Sarıkoz

Signature:_____

ABSTRACT

AN INFORMATION SECURITY FRAMEWORK FOR WEB SERVICES IN ENTERPRISE NETWORKS

Sarıkoz, Bahadır Gökhan

M.S., Department of Information Systems

Keywords: Web Services, Cyber Security, Security Modeling, Security Controls, Security Measurement.

Supervisor: Assoc. Prof. Dr. Banu GÜNEL

January 2015, 197 pages

Web Service, an open standard based on existing Internet protocols, provides a flexible solution to web application integration. It provides faster, more practical and more effective way of solutions for the organizational structures. Online shopping, billing, reservation and other way of standards provided to people mostly depend on web services. On the other hand, it provides corporate identity and functionality of an organization. Since the importance and the necessity of the web services increase day by day, the level of criticality also increases in the same level. In the meanwhile, the necessary measurements are to be taken into account in order to provide 7/24 productivity. Such measurements include several subjects from the load testing to effective coding for best service. However, cyber security attacks, one of the most important issues nowadays are the root cause in order to take vital measurements. Preventing web services from these cyber security attacks requires several aspects from different perspectives including network-based security, protocol-based security, signature-based security and other types of control mechanisms. In this study, an information security framework has been proposed in order to define the complete security aspects of a web service of an enterprise network. Within this framework, a sample information security modeling for a web service has been presented with

respect to the several types of attacks. The mentioned modeling has been tested and measured for pre-defined and specified scenarios.

ÖZ

KURUM AĞLARINDA WEB SERVİSLERİ İÇİN BİR BİLGİ GÜVENLİĞİ ÇERÇEVESİ

Sarıkoz, Bahadır Gökhan

Yüksek Lisans, Bilişim Sistemleri Bölümü

Anahtar Kelimeler: Web Servisleri, Siber Güvenlik, Güvenlik Modellemesi, Güvenlik Kontrolleri, Güvenlik Ölçümleri.

Tez Yöneticisi: Doçent Dr. Banu GÜNEL

Ocak 2015, 197 sayfa

Varolan internet protokolleri bazlı web servisi web uygulama entegrasyonuna esnek bir çözüm sağlamaktadır. Bu da organizasyonel yapılarda daha hızlı, daha pratik ve daha efektif çözüm yolları sağlamaktadır. İnsanlara sağlanan çevrimiçi alışveriş, fatura ödeme, rezervasyon ve diğer standartlar neredeyse tamamen web servislerine dayanmaktadır. Diğer taraftan kurumsal kimlik, organizasyon fonksiyonalitesini sağlar. Web servislerinin önemi ve gerekliliği gün geçtikçe arttığı için, aynı şekilde kritikliği de artmaktadır. Bu arada, 7/24 üretimin sağlanabilmesi açısından gerekli önlemler göz önünde bulundurulmaktadır. Bu önlemler en iyi hizmet açısından yük testinden efektif kodlamaya kadar bir çok konuyu içermektedir. Buna rağmen, günümüzün en önemli konularından biri olan siber saldırılar hayati önlemlerin alınması için kök nedendir. Siber saldırılardan web servislerini korumak ağ bazlı, protokol bazlı, imza bazlı güvenliği ve diğer kontrol mekanizmalarını içeren birçok durumu gerektirmektedir. Bu çalışmada, bir işletme ağında bulunan web servisinin bütün güvenlik durumunun sağlanılması için bir bilgi güvenliği çerçevesi önerilmiştir. Bu çerçevede bir çok çeşit siber saldırı göz önünde bulundurularak bir bilgi güvenliği modellemesi sunulmuştur. Belirtilen modelleme önceden belirlenmiş spesifik senaryolara istinaden test edilmiş ve sonuçları paylaşılmıştır.

DEDICATION

To my wife, and daughter

ACKNOWLEDGEMENTS

First of all, I would like to thank my supervisor Assoc. Prof Dr. Banu Günel for her extensive support, guidance and patience throughout the thesis studies. I am grateful for what she has done for me so far.

I would like to express my gratitude to Murat Hüseyin Candan, Dr. Okan Yücel and all my colleagues in Barikat Information Security for their support, patience and encouragement for my studies.

I am also grateful to Volkan Ertürk for his valuable suggestions and contributions in this study.

I owe special thanks to my older brother Serdar Kürşat Sarıkoz for his valuable suggestions.

Finally, I would like to thank my beloved wife Ayşegül Sarıkoz and my little daughter Nil Şevval Sarıkoz for their boundless love, patience and support during the thesis period.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ANCRONYMS

B2B:	Business to Business
B2C:	Business to Consumer
CAPTCHA:	Completely Automated Public Turing test to tell Computers and Humans Apart
CIA:	Confidentiality, Integrity and Availability
COTS:	Commercial off-the-shelf
CSRF:	Cross-Site Request Forgery
CVE:	Common Vulnerabilities and Exposures
CWE:	Common Weakness Enumeration
DB:	Database
DBF:	Database Firewall
DLP:	Data Loss Prevention
DMZ:	Demilitarized Zone
DNS:	Domain Name System
DoS:	Denial of Service
DDoS:	Distributed Denial of Service
DTLS:	Datagram Transport Layer Security
DUNS:	Data Universal Numbering System
EAI:	Enterprise Application Integration

FTP:	File Transfer Protocol
HIPS:	Host Intrusion Prevention System
HTTP:	Hypertext Transfer Protocol
HTTPS:	Hypertext Transfer Protocol Over TLS
ICA:	Independent Computing Architecture
ICMP:	Internet Control Message Protocol
ICP:	Internet Caching Protocol
IDE:	Integrated Development Environment
IIS:	Internet Information Services
IP:	Internet Protocol
IPS:	Intrusion Preention System
IS:	Information Systems
ISMS:	Information Security Management System
ISO:	International Organization for Standardization
ISP:	Internet Service Provider
IT:	Information Technologies
MOM:	Message Oriented Model
MSADC:	Microsoft Active Directory Connector
NAC:	Network Access Control
NETBIOS:	Network Basic Input/Output System
NIST:	National Institute of Standards and Technology
NTP:	Network Time Protocol
OS:	Operating System
OSI:	Open Systems Interconnection Model

OWASP:	Open Web Application Security Project
PHP:	Personal Home Page
PM:	Policy Model
RAM:	Read Access Memory
REST:	Representational State Transfer
RDP:	Remote Desktop Protocol
ROM:	Resource Oriented Model
RPC:	Remote Procedure Call
SANS:	SysAdmin, Audit, Networking, and Security
SDL:	Security Development Lifecycle
SMB:	Server Message Block
SMTP:	Simple Mail Transfer Protocol
SOAP:	Simple Object Access Protocol
SOM:	Service Oriented Model
SNMP:	Simple Network Management Protocol
SQL:	Structured Query Language
SSI:	Server-side Includes
SSL:	Secure Socket layer
STM:	Synthetic Transaction Monitoring
TCP:	Transmission Control Protocol
TLS:	Transport Layer Security
UDDI:	Universal Description, Discovery and Integration
UDP:	User Datagram Protocol
URL:	Uniform Resource Locator

VLAN:	Virtual Local Area Network
WAF:	Web Application Firewall
WSDL:	Web Services Definition Language
W3C:	World Wide Web Consortium
WMI:	Windows Management Instrumentation
WWW:	World Wide Web
XML:	Extensible Markup Language
XPATH:	XML Path Language
XSS:	Cross-site Scripting

CHAPTER 1

1. INTRODUCTION

This introductory chapter states the general content of this study which includes the statement of the problem, related work, objectives and importance of this study and addresses the outline implemented throughout this thesis.

1.1. STATEMENT OF THE PROBLEM

Number of information systems that rely on web services increases day by day. Many organizations receive support from their information systems department in order to provide their web-based services. These web services vary from identifying corporate identity, to online business actions. Due to its nature, internet is an untrusted networks of networks. Most of the web services belong to the organizations and security of web services is a growing concern as each day more controversial issues arise. Recently, eBay Inc. (2014) has announced that an unauthorized access occurred to eBay systems which may result in customer information exposure. eBay Inc. has also added that there is no evidence that PayPal or their customers have been affected by the unauthorized access to eBay systems. However, one day later eBay Inc. (2014) has announced that the recent attack compromised a database that includes eBay user passwords and had recommended the users to change their passwords as soon as possible. Another sample is web defacement of Republic of Turkey Ministry of Foreign Affairs. Hurriyet Planet (2012) announced on September 3, 2012 that the website of Ministry of Foreign Affairs had been hacked by RedHack Team. The

website was out of service for twenty five minutes. The RedHack team also compromised the information of the officers that work in the foreign missions in Turkey.

As a result of technological improvements in computer science, new ways to publish and obtain information have been developed recently. Client – server software, web applications, database applications and other type of applications also bring vulnerabilities that can be exploited with an aim of harming the individuals and organizations. Imperva's hacker intelligence report (2012) cites that Anonymous hackers use many of the same tools for hacking, such as Havij, an SQL injection tool (probably invented in Iran) designed to penetrate applications and steal data. In other words, they are able to take advantage of common application vulnerabilities found in many websites, the same thing that fuels today's black market, data-driven cyber-crime economy. In order to satisfy the necessities of new protocols and applications, infrastructure of the organizations and also internet need to be enhanced. Each new technology has its own properties and challenges to overcome and make themselves secure. Security of information systems, and especially web services is becoming a debatable issue day by day because of these facts.

In order to provide the security requirements of the web services, the amount of resources that are spent and the work done are at the highest level during these days and if we take a look at the near future, it is not difficult to predict that the trend will be increasing gradually. To illustrate, in the past, a simple firewall solution was sufficient to make a web service system secure with respect to a certain level. However, the more technology is developed, the more sophisticated attacks become. Namely, limiting the access to any web service by a firewall is not sufficient since new attack libraries use legitimate services and formats that are already allowed and also must remain open in the firewall. As a result of this, extra security measures and protections such as web application firewalls, intrusion prevention systems and also DDoS protectors should be used to support and prevent relevant assets.

Although several measures and tools exist in order to provide the security requirement of web services, it seems that the staff responsible may be unaware of what is going on. In order to measure the information level of the IT stuff, a questionnaire was

prepared and 25 staff in IT departments of the governmental institutions in Ankara filled out this questionnaire. The questionnaire consisted of four different parts, which aimed to collect the information levels about the institution infrastructure, web service management, web services security and measures for the web services security, respectively.

In the first part of the questionnaire, we see that 20% of the IT staff have extensive information, 48% have sufficient information, 24% have little information and 8 people have no information about the infrastructure.

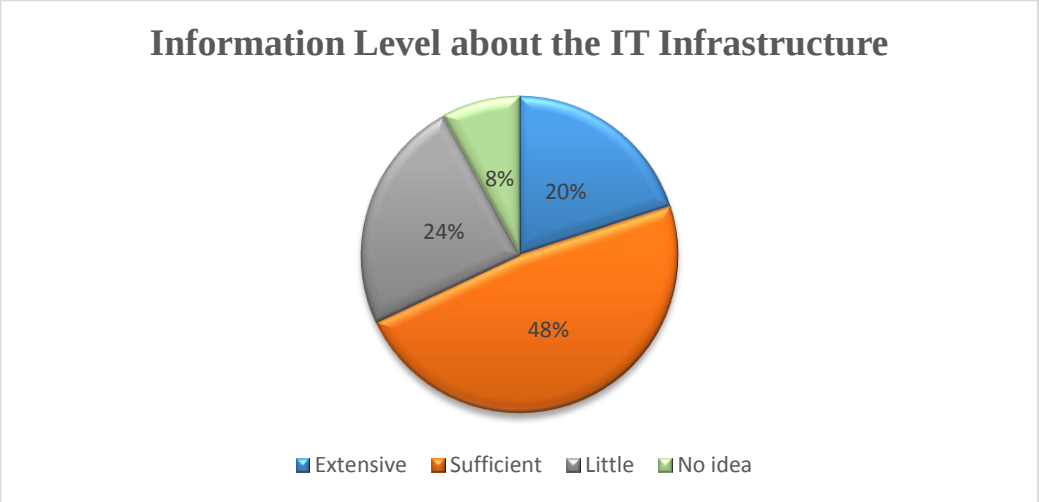


Figure 1-1: Information Level about the IT Infrastructure

In the second part of the questionnaire, we see that 16% of the IT staff have extensive information, 36% have sufficient information, 24% have little information and 24% have no information about the web service management.

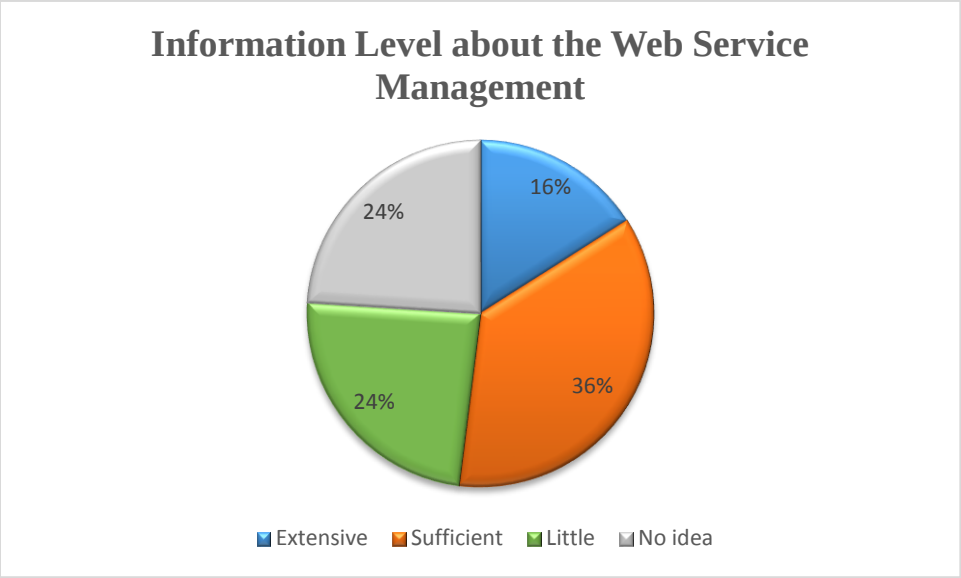


Figure 1-2: Information Level about the Web Service Management

In the third part of the questionnaire, we see that 16% have extensive information, 40% have sufficient information, 16% have little information, and 28% have no information about the web service security.

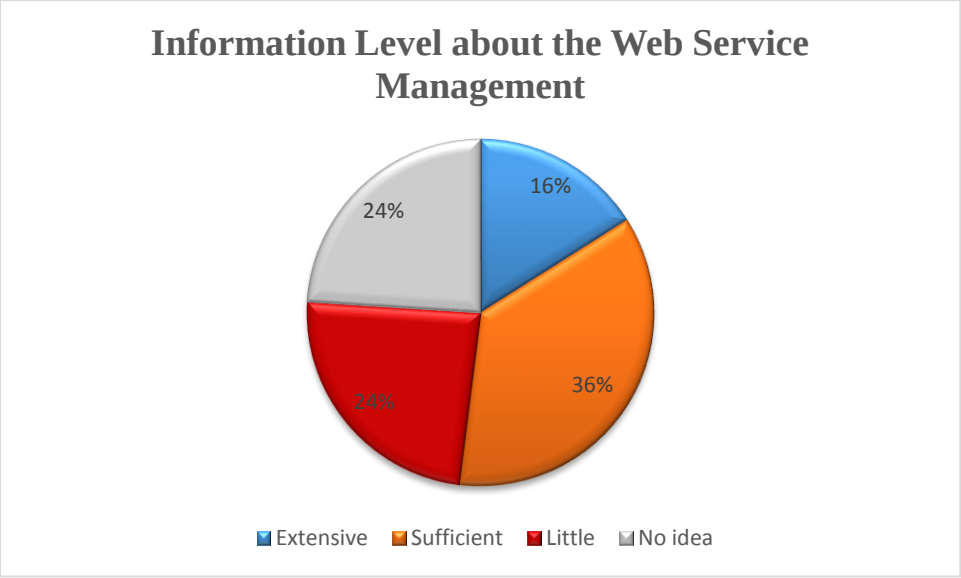


Figure 1-3: Information Level about the Web Service Management

In the last part of the questionnaire, we see that 28% have extensive information, 12% have sufficient information, 32% have little information and 28% have no information about the measures for the web service security.

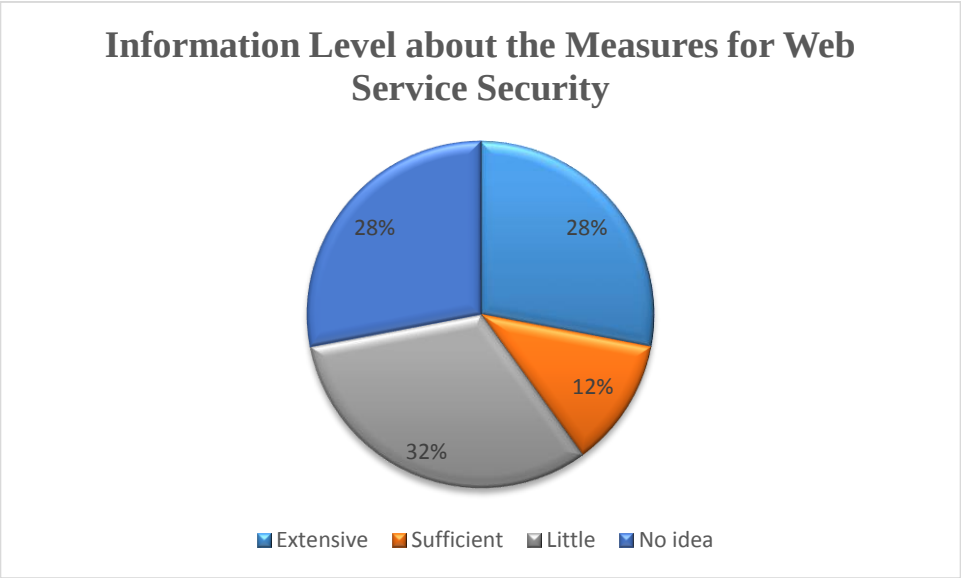


Figure 1-4: Information Level about the Measures for Web Service Security

Such illustrations show us that the security level and measurement of any web service which is one of the most important parts in the information systems should not be underestimated. It is of paramount importance in order to maintain a corporate's production environment and corporate identity. As a result, this goal can be achieved by providing a stable web service environment. Because of this, providing a secure environment for the web services is inevitable. In this study, therefore, typical security architecture of a web service in the organizations will be given according to the most common attributes and a framework will be provided on a fictitious organization to demonstrate security issues.

1.2. RELATED WORK

In this field, so many work has been done, so many papers have been published so as to provide and construct the initial state of security essentials of the web services and to underline specific issues and problems. Publications deal with this problem from several perspectives and some publications concentrate on specific areas of security of web services and give in depth knowledge about how to secure web services accordingly.

Uma and Kannan (2014) focus on web service attacks and propose solutions for detecting and filtering various types of web service attacks. In this proposed system, the requests to the original web server are received and a suitable response from a dummy server page is generated in order to analyze the nature of attack. With respect to the policies created, the responses are analyzed and the legitimate requests are forwarded to the original web server accordingly. All possible attacks have been tested in this proposed system in order to verify the robustness of filtering policies.

Hong and Kim (2014) concentrate on uncontrollable encrypted web traffic, especially, web mail traffic. In their study, they propose a system that controls encrypted web mail traffic by utilizing a proxy server and distributes the Secure Socket Layer (SSL) certificates to both client and server side in order to intercept and control the content of the web traffic.

Barna, Shtern, Smit, Tzerpos and Litoiu (2014) aim to provide a model-based adaptive architecture and algorithm in order to detect DoS attacks at the web application level and mitigate them. In this study, via a performance model to predict the impact of arriving requests, a decision engine adaptively generates rules for filtering traffic and sending suspicious traffic for further review, where the end user is given the opportunity to demonstrate they are a legitimate user. If no legitimate user responds to the challenge, the request is dropped.

Antunes and Vieira (2014) emphasize penetration testing for web services. In their study, it is stated that Web services are often deployed with critical software security faults that may result in malicious attacks. Penetration testing using commercially available automated tools can help avoid such faults, but new analysis of several popular testing tools reveals significant failings in their performance.

Munadi, Fajri, Meutia and Elizar (2013) also states the importance of SQL injection attacks on the web services. In their study, the security issues based on a variety of attacks that occur by the method of the SQL injection attacks are examined and a case study of a website is analyzed in order to establish some preventive measures to be understood and implemented.

Masood (2013) also focuses on various security issues pertaining to service oriented architecture by indicating that application layer security is not always a part of the discussion whereas there is an excessive focus on network layer security. In the study, he describes the application layer based attacks in details.

Zhang, Hou and Ma (2013) also states securing web services by deploying a wide range of third party security products already in use as part of the corporate infrastructure and also adds that a full end-to-end security solution is essential in order to avoid security gaps.

Berger, Sohr and Koschke (2013) touch on the issue with a different perspective by stating code analysis of the web service with the help of static analysis. As a result of this, a security architecture is extracted in order to detect and defend vulnerabilities. It is simply stated that the security issue starts from static code analysis that may result in common low-level security bugs, such as buffer overflows and cross-site scripting vulnerabilities.

Petukhov and Kozlov (2008) also state that the number of reported web application vulnerabilities is increasing gradually and most of the vulnerabilities come from improper input validation. In their study, extensions to the Tainted Mode model which allows the detection of intermodal vulnerabilities. Also a new approach to vulnerability analysis involving penetration testing and dynamic analysis is presented.

1.3. OBJECTIVE OF THIS STUDY

Objective of this study is to state security requirements of a web service of a typical organization. In order to specify such requirements, a typical security framework is developed in this thesis. Throughout the framework, all the basic steps in order to cover all the security gaps will be provided. With respect to the wide spectrum of the title, in

the thesis, technical details of every subject are not given; instead a higher level of view, which is logical one, is aimed. Hence, organizations that consider security design for the web services can get benefit from this study as a first step of a guidance.

1.4. OUTLINE OF THE THESIS

In Chapter 1, the current situation of the security of web services and studies performed on this subject are stated. The importance of the study is briefly explained. In Chapter 2, web service, the types and the importance of it are explained. Common examples about web services are given briefly in this chapter. In Chapter 3, general information about security engineering, basic terminology and essential security controls and measurement are defined.

In Chapter 4, the main purpose of this study, information security framework for a web service is explained in detail. In order to clarify this framework, a fictitious web service architecture is defined. In this framework, all the steps from penetration testing to third-party industry security solutions are explained. In Chapter 5, sample attack scenarios are defined and the role of the parts that establish this security framework are clearly explained.

Finally, in Chapter 6, summary of the work done and contributions of this study are presented. Some thoughts about the future work and directions are explained.

CHAPTER 2

2. BASIC CONCEPTS OF WEB SERVICES

This chapter commonly deals with the Web Services. The main purpose of this chapter is to give the common expression about the web services. Definition, information and types of the web services and web service architectures are addressed briefly in this chapter.

2.1. DEFINITION OF THE WEB SERVICE

Some of the materials in this chapter are based on Newcomer, and World Wide Web Consortium.

Fifteen years ago, web service seemed to be a luxuries part of our lives since the internet usage was not so common. However, today people perform nearly all the things from the internet environment. In other words, we nearly do everything by using web services.

Here is the definition for the web service from W3C Working Group (2002): "A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards."

To put it simply, a requester intends to use the provider's web service in order to utilize the function of the relevant web service. In order to utilize the relevant web service the

requester is supposed to use an agent; a web browser such as Mozilla Firefox, Google Chrome, etc. The type of the requester and provider may vary with respect to the functionality to be utilized.

In general view, web services are only considered as a special web application differing at the presentation layer of OSI layer. We may separate the web services into two parts as business to consumer (B2C) which consumer gets information from the business web services and business to business (B2B) which the web service of a business gets information from the web application of another business. Web services also provide enterprise application integration (EAI), supplying multiple integration from a single point (Newcomer, 2002).

2.2. IMPORTANCE OF THE WEB SERVICE IN ENTERPRISE NETWORKS

Since internet was discovered, the types and approaches of the operations and the purpose of internet usage have changed so many times. Developments were made with respect to needs and requests of the computer users. Now, computer users give more value to the effective online communication, information exchange and easier and faster access to the information. In this manner, interactive services through the web or internet are the key elements why today's computer users pay more attention to online communication, information exchange and easier and faster access to the information, especially.

In today's world, people do nearly everything through the internet. We purchase the flight tickets, meal, clothes. Furthermore, estate, renting, bill payments, and e-government projects are performed through the internet. All of these things seemed to be luxurious approximately fifteen years ago. However, for the time being, all of these services are the vital elements of our lives, and make our lives easier.

For all the things mentioned above, individuals or business organizations that publish their services need a way to provide these opportunities to the other individuals or organizations. In order to achieve this, internet-based applications should be used so that applications can find, access and have interactive communication with other internet-based applications. Within the extensive implementation web services,

individuals, organizations, and applications are able to connect, and interact with each other (World Wide Web Consortium, 2004).

As a result of this, web services are the vital part of the internet and have a crucial role in today's world. Just like water, electricity and other necessary utilities, internet has become an essential part of our lives and behind of this essential part, we should not forget the importance of the web services.

2.3. WEB SERVICE ARCHITECTURE

With the help of web services, different software applications that run on different platforms or frameworks can interact with each other. A web service architecture provides a general description for the web services and defines the place of the web service in a large-scale environment. A conceptual model and content in order to understand the web services and the communication between them is yielded by the web service architecture (Newcomer, 2002).

Web services architecture is an interoperable environment identifying the key elements of the web services network, which is necessary to interoperate between the web services.

There are certain elements that play an important role in a web service communication. These are agents, services, requester and providers. A requester uses an agent in order to access a web service which is provided by a provider with the help of a provider agent. Within this communication, both sides agree with the communication type, the type of the input and output messages, namely semantics of the web service.

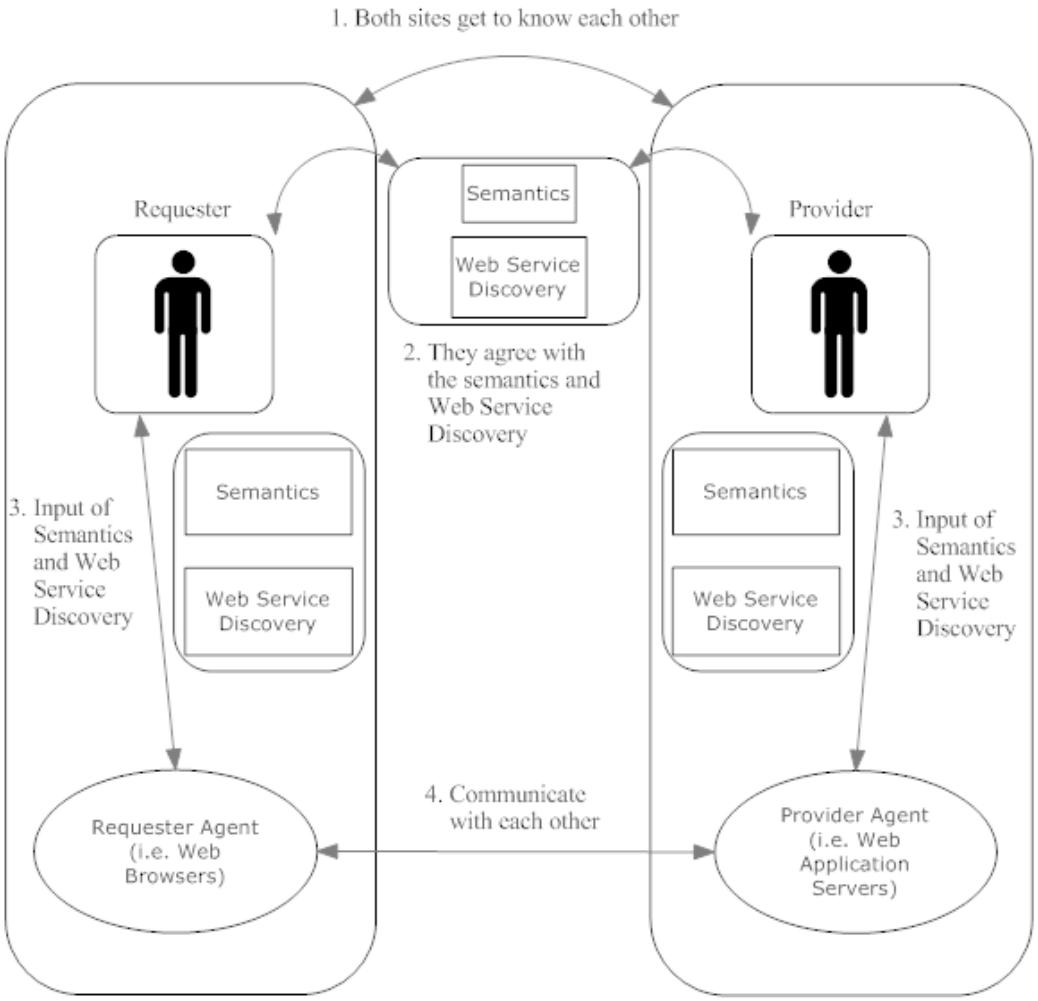


Figure 2-1: The Relationship Between the Requester, Provider and Agents That Are Used

The simple scenario mentioned above defines a web service architecture in a common format. However, the web service type or model differs with respect to the data type and communication methods. As a result of this, four different models exist in the web services architecture (Booth et al, 2004). Following are the models:

1) Message Oriented Model: It is the model based on the messages, message structure and message transfer.
2) Service Oriented Model: It is the model based on the aspects of the service and actions.
3) Resource Oriented Model: It is the model based on the resources existing and having owners.

4) Policy Model: It is the model based on the key parameters related to the behavior of agents and services.

Following is the meta-model of the web services architecture that defines the place and the role of each model that implements the web service hierarchy.

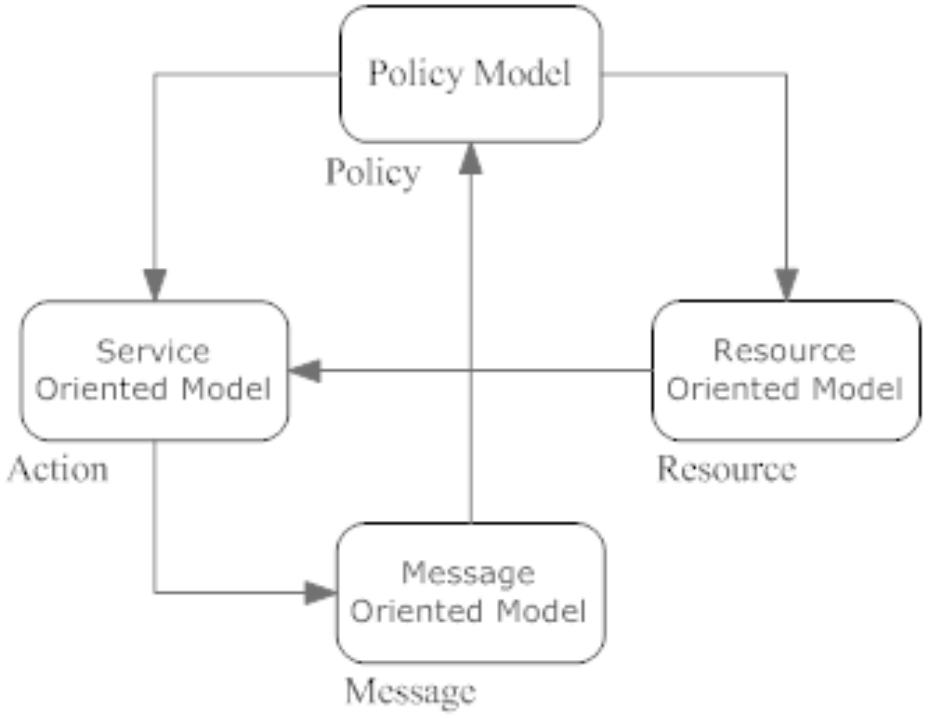


Figure 2-2: The Meta-Model of the Web Services Architecture

2.3.1. The Message Oriented Model

The Message Oriented Model (MOM) aims to focus on only the aspects of the message in the web service and process of the messages. As can be guessed, the semantic of the message in the web service is not a focusing subject. The main focus object is the structure and transmission of the message and the relationship with the sender and receiver. The Message Oriented Model is simply illustrated below:

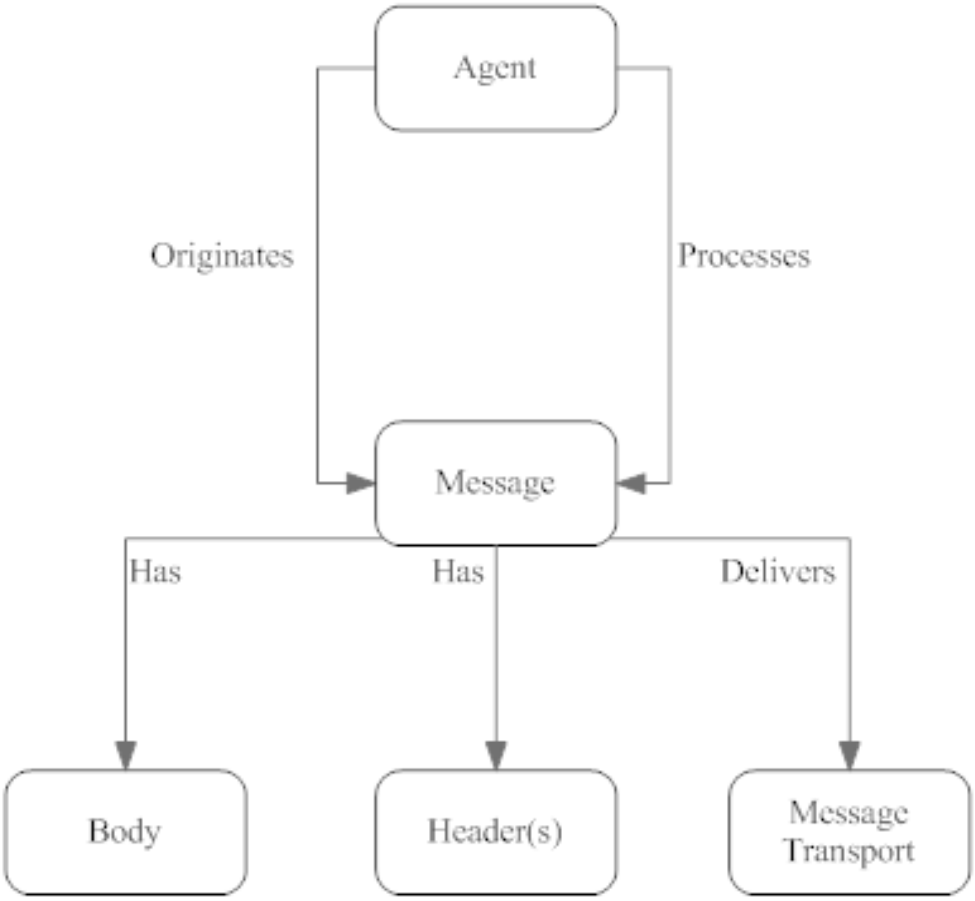


Figure 2-3: Simplified Message Oriented Model

2.3.2. The Service Oriented Model

The Service Oriented Model only focusses on the service and action in the web service architecture. The main goal of this model is to give the explanation of the agent, the web service and the communication between them. This model is built on The Message Oriented Model. Though MOM only focusses on the message itself, this model focusses on the action. The Service Oriented Model is simply illustrated below:

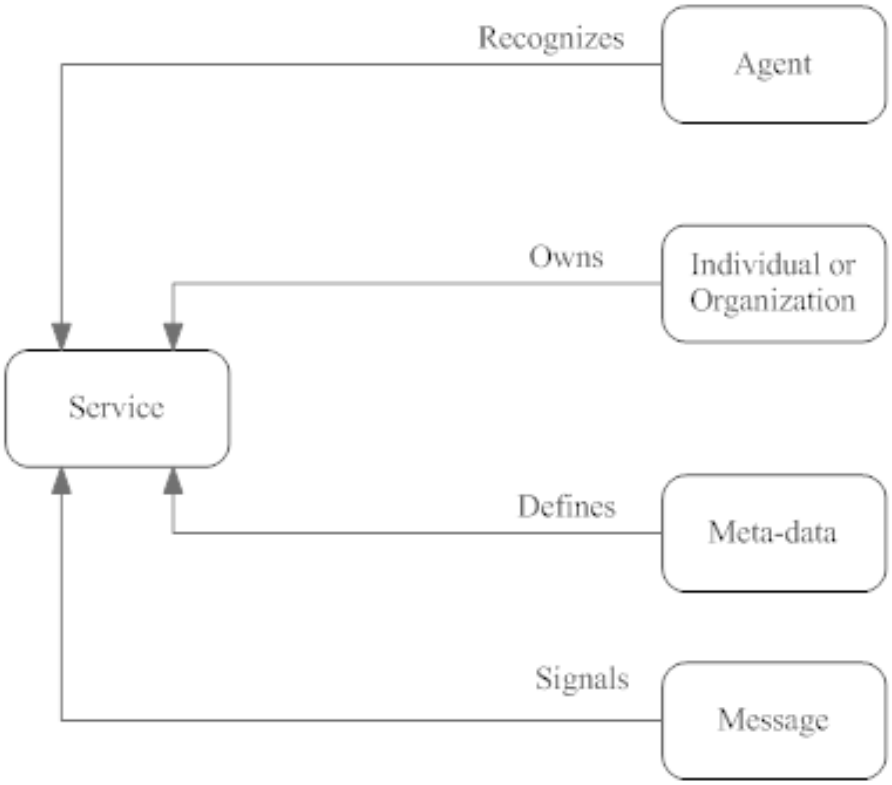


Figure 2-4: Simplified Service Oriented Model

2.3.3. The Resource Oriented Model

The Resource Oriented Model focuses on the web service architecture in the basis of resources that are the fundamental parameters issuing details about the web services. A web service can be given as a specific illustration of the resource with a paramount role in the web services architecture.

The main focus area of the Resource Oriented Model is the fundamental characteristics of the resources themselves but not the content of the web services. Therefore, the issues such as the ownership of the resources, policies associated with the resources, etc. will be the main concept. Following is the illustration of the Resource Oriented Model:

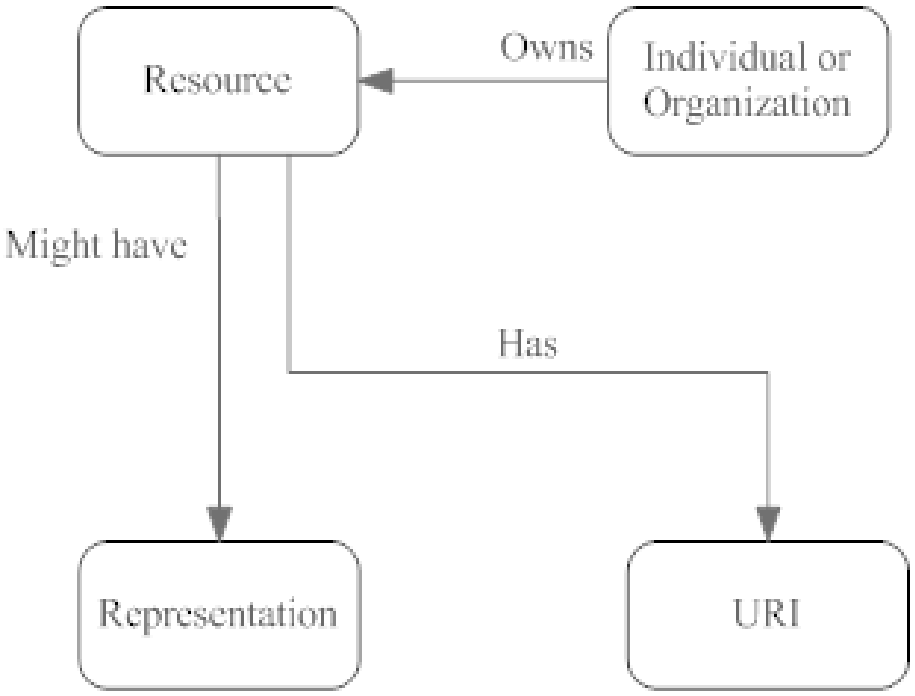


Figure 2-5: Simplified Resource Oriented Model

2.3.4. The Policy Model

In the Policy Model, the main focus area is the policies with respect to the extensions, security issues and the quality of the service. By means of security quality of service, the restriction of the behavior of the action and the restriction of the service is considered, respectively.

These restrictions are modeled on the main concept of policy and other elements constructing the relevant web services architecture. As a result of this, the Policy Model can be considered as a framework where security concept can be implemented.

The following is the simplified form of the Policy Model:

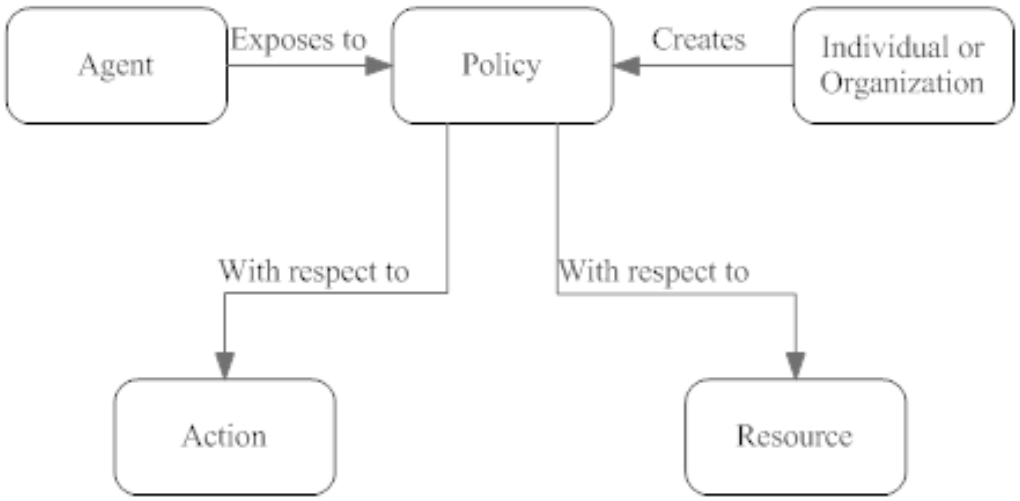


Figure 2-6: Simplified Policy Model

2.4. TYPE OF WEB SERVICES

When the operating mechanism of the web services are asked to the IT staff, they may give different answers than expected. The main reason behind this is the technique, or the technology they use for their web services. As can be guessed, there are several types of web services and all the web application technologies can use any of these types in order to cover web service functionalities. Following are the main web service types used for nowadays technology:

1) **Extensible Markup Language (XML):** represents a general form of specifications provided by the World Wide Web Consortium (W3C) and others.
2) **Web Services Definition Language (WSDL):** is the technology based on XML and clarifies communication patterns and protocol mappings for the web services.
3) **Simple Object Access Protocol (SOAP):** is a collection of the XML-based services. It is used for exchanging structured information in the implementation of a web application in a network.
4) **Universal Description, Discovery and Integration (UDDI):** is a record and discovery mechanism for the web services.

General definition and usage methodologies of these types will be given below. The detailed information will not be covered since we will be mainly focusing on the security of the web services.

2.4.1. Extensible Markup Language (XML)

XML which stands for Extensible Markup Language and designed by World Wide Web Consortium, is a flexible, extendible and easy text format. With the help of XML, a software engineer can create his own system, define his own tags. He can easily and effectively perform his own programming with the help of these tags and standardize these tags in his program.

XML can hold several different types of the data in a single repository. It provides easy and environment-independent access to the data. It can provide the opportunity to combine with the different formats of the data such as PDF, voice, image in a hierarchical structure. It aims to make the data transfer easier and provide the data integrity. In the meanwhile, it separates the content and presentation data. That's why XML differs from Hypertext Transfer Protocol (HTTP).

The XML format utilized in the Web services provides specifying how the data is represented typically, defining how and with what qualities of the service where the data is exchanged and detailing in what way the services are given. The implementation of web services parse multiple XML formats in order to perform required communication with the various software or any other services.

There are two types for the XML usage; which are representation and format of a data storage and specifying the web service which processes the data. Because of this, XML users are separated into two parts:the ones that are interested in text formatting and the ones interested in data formatting.

Considering the statements mentioned above; followings are the general concepts of the XML:

1) It is used for structuring and defining the data.
2) It is a technology used for defining the structure of the information.
3) It is the universal format of configured document and data.

4) It is a language that defines the markup languages.
5) It is a text-based markup language and used for the data exchange.
6) It is a standard format that defines the information and used for the information exchange between different assets.

2.4.2. Web Services Definition Language (WSDL)

Web services are used in order to deliver the business or consumer needs in predefined formats. However, in order to perform a successful delivery, the relevant web service format should be described and explained to its consumer. Moreover, the consumer should know how to communicate with the web service, the data to be received, the results, communication ports and the supported transfer format.

In order to perform a data exchange, a simple search parameter may be appended to the URL. However, this methodology may be useless and limited considering the limit of URL size and the usability of the URL for the data exchange. Furthermore, it may be cumbersome to perform required programming and understanding for such a kind of web service type.

WSDL which stands for Web Service Description Language is aimed to provide required description and publication of the formats and protocols of a web service between businesses or consumers. As a result of this, the requester knows how to send a search parameter and in what format he gets the data.

By using some of the XML schemas, the WSDL elements provide a definition for the data provided. With the help of this, both the requester and the provider can clarify the data being exchanged. These elements also include the description of the operation which is performed on the data, a binding to a port so that the requester can understand the process of the data and transport of the data, respectively. Usually, WSDL is used with SOAP and its specification also includes a SOAP binding (Newcomer, 2002).

WSDL was developed by Microsoft, Ariba and IBM and later submitted to the W3C with v1.1 version and it was accepted as WSDL and thereafter announced. Twenty two other companies joined to this submission in order to support WSDL (Newcomer, 2002). That’s why WSDL is offered for the web service integrations.

As mentioned before, the sites integrated with each other should have the same WSDL to achieve the ability to understand each other. In other words, both of the sites should have the same XML schema. Both the sender and requester are supposed to know how to format the output data and parse the input data, respectively. Consequently, both sites can have any type of web services with the help of WSDL file.

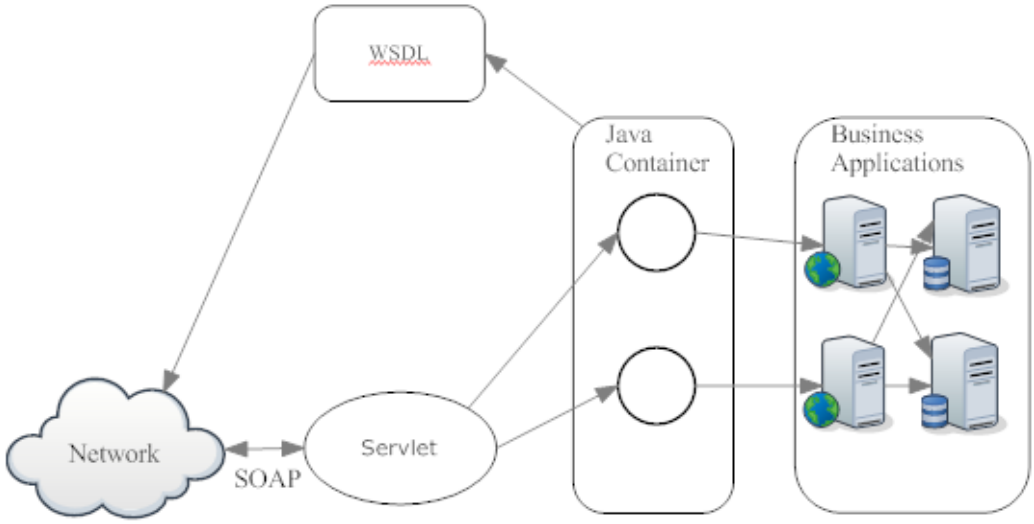


Figure 2-7: WSDL-Based Web Service Integration

Considering the operating mechanism of WSDL, it can be understood that WSDL separates the web service into three parts; which are determining the content and the data types of the message, the operations performed for the message and the specific communication criteria including protocol bindings and transports. Within these elements, we may also state sub-elements:

1) **Data types:** the data used in the message.
2) **Message:** brief definition of the data to be exchanged.
3) **Operation:** brief definition of the operation of the message.
4) **Port type:** brief set of operations mapped to the end points.
5) **Binding:** the protocol and the data formats for the operations and messages for a specific port.
6) **Port:** a combination of a socket and IP address
7) **Service:** a set of relevant hosts having the service definitions.

2.4.3. Simple Object Access Protocol (SOAP)

SOAP which stands for Simple Object Access Protocol is an XML-based web service technology in order to use the functions utilized over the networks. In other words, SOAP determines the relation between the requester and provider. With the help of SOAP, different software architectures using different programming languages, such as Java and C# can run the methods of another and use the response of the method in intended format.

SOAP is a kind of extension of Hypertext Transfer Protocol (HTTP) which supports XML messaging. Instead of HTTP method, SOAP sends an XML message by using an HTTP request and receives a reply by using an HTTP response. In order to cover XML message, there should be an XML processing capability in the HTTP listener, such Apache or Microsoft Internet Information Services.

SOAP communications are performed between the SOAP nodes which are SOAP message, senders, receivers and both. A SOAP node can support more than one SOAP processors and SOAP nodes handle the SOAP blocks when a message is received.

There are three major part of SOAP messages; which are the envelope, the header, and the body. The envelope is necessary and used for making the start and end of the envelope message. The header part may include one or more header blocks that contain the attributes of the message or the qualities of the service. Because of this, the header part is optional. The body is necessary and it contains the message itself with the body blocks.

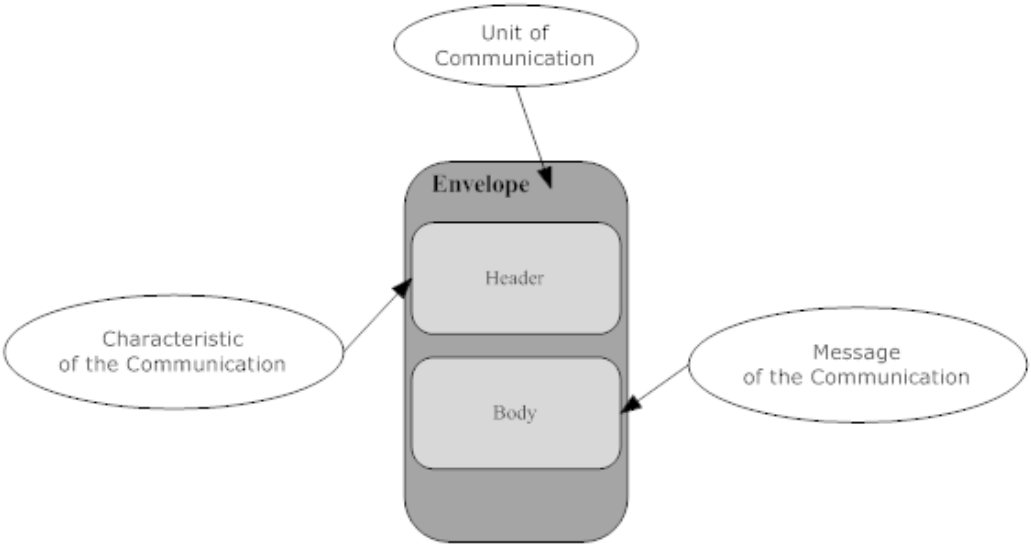


Figure 2-8: Three Main Parts of the SOAP Messages.

In order to reach a determined web service, SOAP transfers an XML-formatted document across the web or most probably the other types of networks. A SOAP message understands how to interpret the message but does not know the message itself. SOAP messages clarify the way to recognize the SOAP message itself. However, the web service implementation should know how to interpret the data and so as to implement the data for the back-end software.

With the help of SOAP and WSDL, an enterprise business platform can clarify how to expose the business data by using web services, interfaces that exchange the data at the specified format, such as method names, and input and output arguments.

2.4.4. Universal Description, Discovery and Integration (UDDI)

UDDI which stands for Universal Description, Discovery and Integration is an XML-based registry platform that provides listing the web services themselves and discovering these web services and mechanisms in order to locate any of the web applications being listed and discovered.

Nowadays, in our lives, in order to book a lunch or dinner, we simply look for restaurants to call or send an e-mail in order to purchase. In order to call or send an e-mail, we simply try to obtain the contact information via a business card or a list from the web. In the similar way, UDDI provides required information for a program running on your computer or any other resource to communicate with a program running outside.

The technology vendors, such as IBM, Microsoft, SAP, and others publish UDDI services. With the help of these publishments, each vendor share an accessible database that contains specific business-related data. The data shared by the vendor itself is replicated by using SOAP requests.

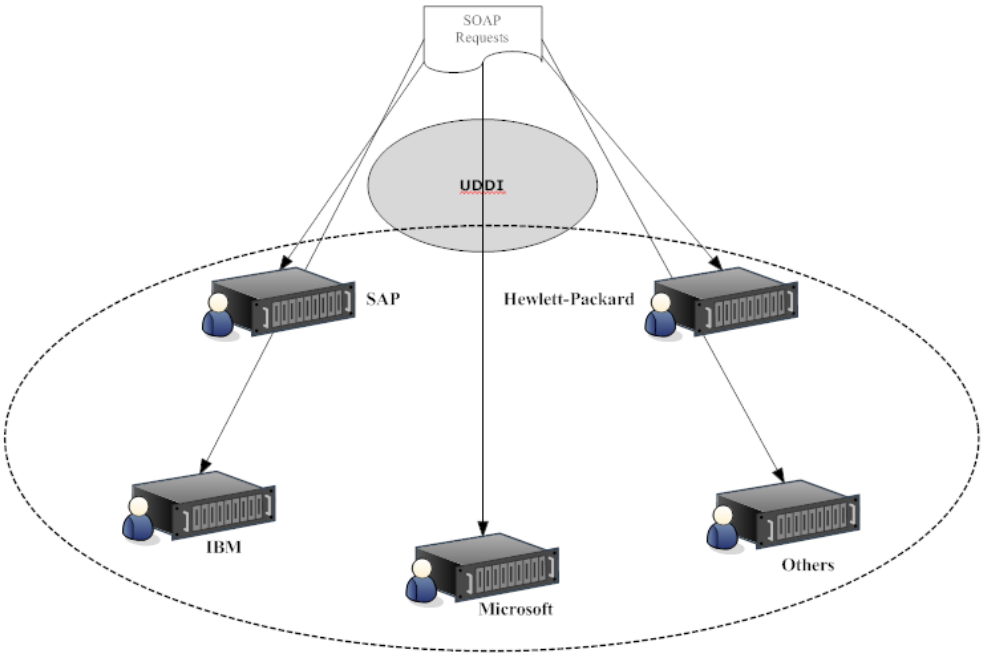


Figure 2-9: Replicated Registry Databases by the UDDI Operators.

These database sites hosted are called operator sites and these sites communicate with each other with the help of SOAP Application Programming Interfaces (API) used by the UDDI programmers. There may be business data pointers in order to address web service interface specifications, such as WSDL.

There are three main categories of business information in order to describe UDDI information:

1) **White pages:** Business name and address, contact information, web site name, and Data Universal Numbering System (DUNS) or other identifying numbers.
2) **Yellow pages:** Type of business, location, and products, including various categorization taxonomies for geo-graphical, industry type, business ID, and other identifying parameters.
3) **Green Pages:** Technical details about the business services.

Registration information for UDDI consists of five different data structure types. These data structures are identified by a unique key assigned by the UDDI operator whenever the data is submitted for the first time.

1) **businessEntity:** is top-level structure that defines what kind of information is registered for the business or other entity.
2) **businessService:** is the type of the service that is published.
3) **bindingTemplate:** is the information of the service that includes a pointer address to access the service.
4) **tModel:** is a collection of information that identifies the service specification in a unique format.
5) **publisherAssertion:** is a relational structure that associates two or more top-level structures with respect to relationship type.

CHAPTER 3

3. SECURITY CONCEPTS

This chapter provides a brief information about the concept of the security engineering. Basic principles, common definitions and terminologies of the security engineering and the relation of security engineering with this study are defined.

3.1 SECURITY ENGINEERING

Some of the materials in this chapter are based on Sommerville (2007).

The extensive use of the internet all around the world in the last two decades brought about a new challenge to the software engineers. This challenge was about designing and implementing the software based systems more secure. The more systems were connected to the internet, the more different external attacks occured in order to threaten the software based systems. As a result of this, the importace of providing trustworthy systems dramatically increased. Hence, both the software and the computer architectures had to take into consideration both the potential threats from malicious and intelligent attackers and problems yielded from accidental faults in the preparation process.

In today's world, it is of paramount importance to design such systems which resist external attacks and also recover the assets from these attacks. Without security measures, it is nearly inevitable that attackers compromise an infrastructure. The system hardware may be misused, confidential data may be stolen or there may be denial of services. As a result of this, system security engineering is an increasingly crucial aspect of the software and computer engineering process. In this manner,

security engineering is related to how to develop and maintain systems, which are able to withstand malicious attacks intended to damage computer based systems or steal the confidential data. The more criminals give an effort to exploit the systems for the illegal purposes, the more security engineering is the part of the general field of the computer security, as well. Because of this, it is essential that software engineers should be aware of the cyber threats faced by the systems and the methodologies in which all the malicious activities can be neutralized.

Vacca (2013) claims that there are three distinguished elements of the information systems security, which is logical security, physical security, and premises security.

- **Logical Security** is the protection of computer based data from communication based threats.
- **Physical Security** is the protection of physical infrastructure which constructs information systems of the organizations.
- **Premises Security** is the protection of the physical facilities of the organizations.

Computer security is an enormous subject and has a big role on many areas that constitue the business and technical aspects of computer engineering. Because of this, this thesis mainly focuses on the logical security which protects web services from the software based and communication based threats. Physical security and premises security may be figured out as one.

Having considered the logical security, it has to be considered that both the application software (that controls the system, the information system, etc.) and the asset on which the system is built. As given in Figure 3-1 by Sommervile (2007), the infrastructure that includes complex applications include an operating system environment, such as Linux or Windows distributions and other generic applications running on the operating systems, such as browsers, e-mail agents, a database management system, middleware which supports distributed computing and database access and libraries of reusable components, which are used by the application software. Indeed, the big portion of the attacks mainly focuses on the system infrastructures since the components (i.e. Browsers) used are well known, available and easy to use.

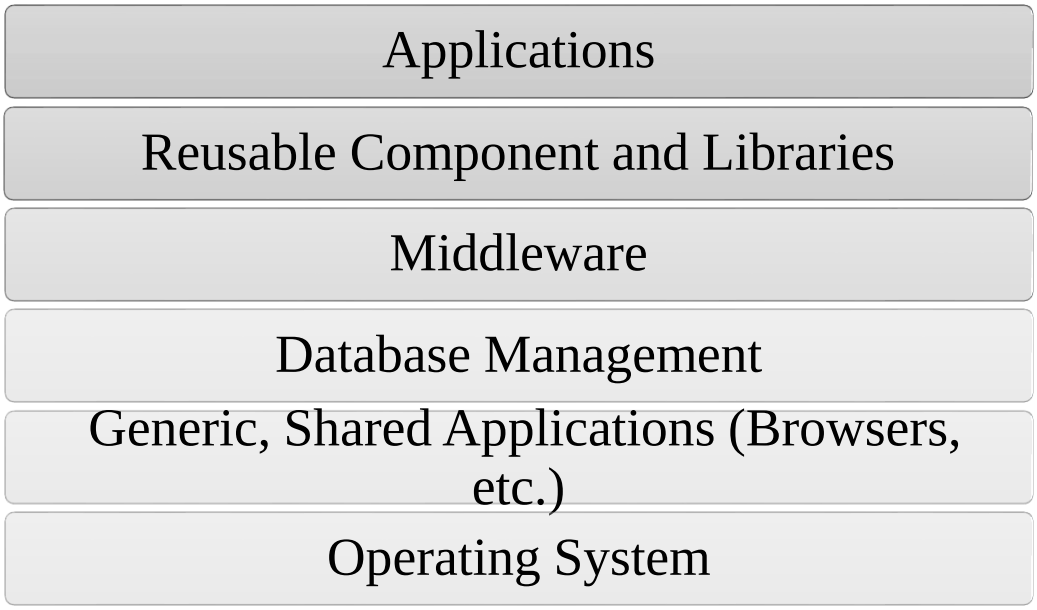


Figure 3-1: Security Wise Information System Layers

In practical terms, there is a serious distinction between application security and infrastructure security:

1. **Application Security** mainly focuses on the software engineering based problem where software engineers should guarantee that the system is implemented to withstand the attacks.
2. **Infrastructure Security** mainly focuses on a system management problem where the system managers should guarantee that the infrastructure is well configured to resist attacks. System managers should construct the infrastructure in order to provide the most effective use as much as infrastructure security provides available feautures. They also should mitigate infrastructure security vulnerabilities that have come to light since the software becomes essential.

As mentioned before, this study mainly focuses on the infrastructure security field of logical security rather than all the fields of the computer security. This does not mean that indepth security measures are considered separately. Some infrastructure security measures, such as web application or database security close the security breaches which may be introduced by weak, wrong or insufficient software design. In this

manner, infrastructure security measures should be implemented according to the software based systems used in an organization.

Sommerville (2007) approaches the information systems security from a software architect/developer point of view. However, evaluating the security level of IS in an organization requires a wider point of view. In his demonstration of IS, some essential layers are absent, such as the human factor, and detailed infrastructure layers. In order to establish a more generalized approach, IS layers of an organization are given in Table 3-1, within a prerequisite relationship between levels. Every level generally is prerequisite for the upper layer. There are also exceptions to this relationship such that operating systems can be used without a network connection or some networks are not accessible from the internet in any way. The purpose of this thought is so as to gain an extensively developed and applied IS in an organization.

Table 3-1: Detailed Layers of IS of An Organization

Application Security	IS Application, Provided Services
	Databases
	COTS Applications
Infrastructure Security	Operating Systems
	Internal Network
	Internet
Physical Security	Physical Equipment, Staff and Facilities

3.2. BASIC TERMINOLOGY IN SECURITY ENGINEERING

A few of the security concepts and terminology that are used in this thesis are given below:

Access: is a specific type of interaction between a source and a destination that results an information transfer.

Asset: is anything with a value to the organization, business operations and continuity, which includes information resources that complements the organization's objective.

Denial of Service: is an attempt in order to make services of the organization unavailable for the intended individuals.

Encryption: is the conversion of plaintext or data into scrambled form through a reversible translation.

Hacker: is the general nickname of an unauthorized person who detects a security gap of an information system and gives an effort to exploit.

Risk: is the probability that a special threat may exploit a vulnerability of the information system.

Vulnerability: is a weakness of an asset that may raise an exploitation to cause devastation.

Attack: An exploitation of a vulnerability that as asset has.

Threats: is the potential activity that the attacker may perform in order to successfully exploit vulnerabilities of an asset to cause devastation to the organization.

As shown in Figure 3-2 referring to Charles (2008), security threats may fail in three principal attributes of IS.

1. Threats aginst confidentiality of the system and its data. These may reveal information to people or programs that are not authorized to have access to the relevant information.
2. Threats against integrity of the system and its data. These threats may damage and corrupt the software based system or its data.
3. Threats against the availability of the system and its data. These threats may restrict access to the software based system or its data with regards to the authorized access.

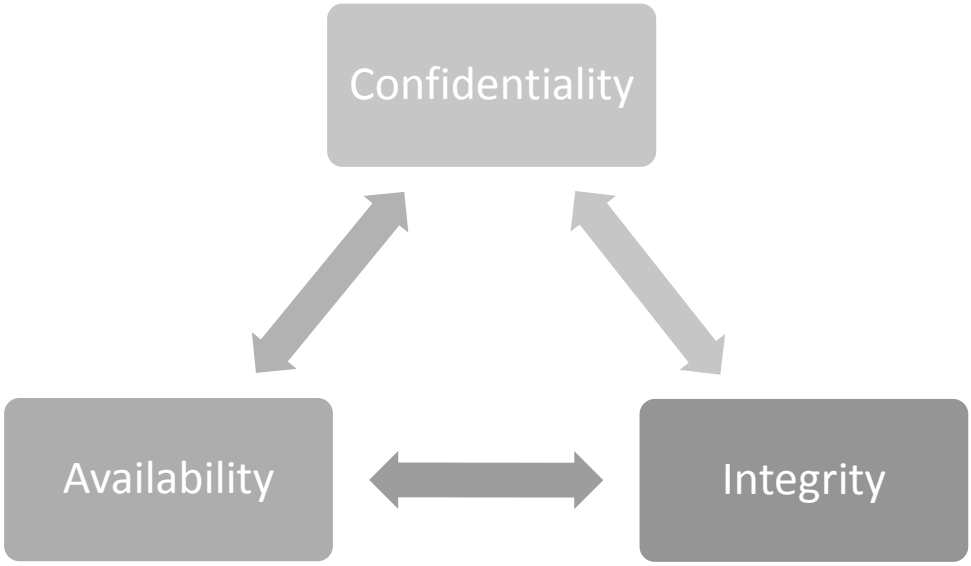


Figure 3-2: The CIA Triad

These attributes are, mutualist. If an attack causes a system to become unavailable, then it may not be updated with information that changes with time. That is to say, the integrity of the system may be compromised, and then it may have to be taken down to repair the problem. Therefore, the availability of the system is reduced.

3.3. SECURITY CONTROLS

A preventive precaution which mitigates the vulnerability of a system or blocks an attack is defined as a security control. In other words, security controls are the basic building blocks or functions in order to achieve security goals. To illustrate, applying at minimum level privilege access model is a security control in order to prevent unnecessary access to the assets.

There are variant methods in order to classify security controls. One method is to classify them with respect to what the control performs. If controls are classified in this method, they will be separated into the following three classes as referred by Sommerville (2007):

1) Controls which are preventive, and tries to make sure the existence of the attacks are unsuccessful. The purpose here is to design the system in order to avoid the security based problems. To illustrate, in order to make the external access to the sensitive military systems impossible, the sensitive military systems are not connected to the public networks. In the mean while, encryption can be figured out as a control based avoidance. Any unauthorized access to encrypted data means that it cannot be exploited by the attacker. Practically, it is very expensive and time wasting to descramble the strong encryption.
2) Controls which are intended to detect and block attacks. These controls include the functionality in a system which monitors ongoing operations and inspects for the aberrant patterns for activity. In the case of detection, an action, such as shutting down parts of the system, restricting access to the certain users may be taken.
3) Controls which contribute to the recovery procedure from problems. This may differ from an automated backup strategy and information mirroring to the insurance policies which involve costs along with a succeeding attack on the system if the recovery procedure is depended on financial issues.

It is a challenging issue in order to decide the separation of the security controls in classes since the control activity may differ with respect to the situation in most of the time. To illustrate, a security guard may be classified as a preventive control. However; assuming that an attacker performs an attack and the security guard notices the attacker and catches him, this makes the security guard control detective and corrective. In order to avoid such kind of confusions, security control categorization mentioned in this study will be based on who performs the control rather than what the control is about. National Institute of Standards and Technology (2009) adopts this approach and well organized security controls and families by considering the ease of the use in the control selection and specification process for the applications that consist of information system in an organization. By means of this, families form general classes of the security controls.

The main classes are as follows:

- Technical Controls,
- Operational Controls,
- Management Controls.

With respect to such a categorization, illustration of security guards belongs to an access control family and access control family belongs to the technical controls, as well.

Simply, management controls are techniques which are normally addressed by the management in the organizations' IT security program.

Technical controls indicate the security controls which the computer based system executes. As opposed to the technical controls, operation controls are those controls which are enforced by the people.

There are 17 families under the main three classes and their list is given in the Tables 3-2 and 3-3 as given by NIST (2009).

In order to acquire a well defined security posture, these three main classes of the security controls should be applied to the software systems developed within the organization and should be evaluated on the purchased security software and other software used in the organization. It is of paramount importance to pay attention to the fact that any system is as strong as its weakest component. Because of this, selected security controls should not be focused on a particular class. All essential technical, operational and management controls should be applied to obtain the expected level of security.

Table 3-2: Security Control Classes and Families #1

Class	Family	Example Security Controls
Management	Certification, Accreditation and Security Assessments	Security Assessments IS Connections Security Certification
	Planning	System Security Plan Rules of Behaviour Security Related Activity Planning
	Risk Assessment	Security Configuration Risk Assessment Vulnerability Scanning
	System and Services Acquisition	Allocation of Resources Life Cycle Support Software Usage Restrictions

Table 3-3: Security Control Classes and Families #2

Class	Family	Example Security Controls
Operational	Awareness Training	Security Awareness Security Traning Security Training Records
	Configuration Management	Baseline Configuration Configuration Change Control Access Restriction for Change
	Contingency Planning	Contingency Plan Contingency Training
	Incident Response	Incident Response Training Incident Response Training and Exercises Incident Handling
	Maintenance	Control Maintenance Maintenance Tools
	Media Protection	Media Access Media Labeling Media Sanitization
	Personal Security	Position Categorization Personal Screening Personal Termination
	Physical Environmental Protection	Physical Access Authoriations Monitoring Physica Access Visitor Control
	System and Information Integrity	Flaw Remediation Malicious Code Protection Information System Monitoring Tool and Techniques

Table 3-4: Security Control Classes and Families #3

Class	Family	Example Security Controls
Technical	Access Control	Access Control Policy and Procedures Account Management Remote Access
	Audit and Accountability	Audit and Accountability Policy and Procedures Audit Monitoring, Analysis and Reporting Time Stamps
	Identification and Authentication	User Identification and Authentication Device Identification and Authentication Identifier Management
	System and Communications Protection	Application Partitioning Security Function Isolation Denial of Service Protection

CHAPTER 4

4. AN INFORMATION SECURITY FRAMEWORK FOR THE WEB SERVICES

This chapter presents our proposed methodology for the information security framework. First the purpose, scope and assumptions of the information security framework is given. Second, a fictitious web service deployment in order to explain the information security framework is provided. Finally, the information security framework is explained in detail.

4.1. PURPOSE AND SCOPE

How would it be possible to make the web services secure? Assume that there is a web service which provides online shopping and there occurs a security incident that causes the outage of the registered users' credit card information. Due to this security breach, possible further research is most probable to analyze and learn the missed security gaps of the system. There may be several reasons for the security gaps. For example, unauthoritive access may accur or a security vulnerability may be exploited. After detecting and solving the issue, the IT security staff should take a lesson from this security breach and even accept the importance of the measurement which he does as a security methodology.

As mentioned in the Section 1.3, information security framework for the web services aims to determine the common criteria for the web services security, to detect technical issues on the web services, to clarify what should be done for the security of the web services and to validate the actions taken. Each of the activities stated requires

extensive work. Unfortunately, this is not one time action. Namely, it should be repeated periodically in order to maintain the web services security.

Information security framework proposes a security measurement, collection, reporting and mitigating framework. With the help of this framework, organizations will be able to prevent and recover from vital security violations and maintain a sustainable security level for the existing web services. The proposed framework covers a wide range of activities from the security administrator employment to validating security configuration checks.

The scope of the framework proposed is as follows:

1) Defining all the criteria and information security procedures for the web services,
2) Analyzing the web service architecture,
3) Analyzing software, performance and security metrics of the web services,
4) Performing and completing security requirements/metrics,
5) Analyzing the security level of the web service architecture,
6) Maintaining the security level of the web service architecture.

4.2. ASSUMPTIONS

In order to mention such a framework, any organization should have a remarkable web service environment. The main reason behind this is that the framework proposed may also require a remarkable cost for the organization. Because of this, an organization that has a narrow web service environment may outsource the security responsibility and maintenance of the assets they have to another company.

There are several examples in which the web server assets and also the security responsibility is outsourced to another ISP or security company (Amazon Web Services Inc., 2015). The main purpose is that the organization cannot fulfill the steps due to the financial situations and also should provide the security measurement for the web services. As a result of this, such kind of organizations may use the advantage of such kind of possibilities.

4.3. DEFINITION OF A FICTITIOUS WEB SERVICE DEPLOYMENT

Though the topic of this thesis is based on the web services security, the infrastructure that the web service will be deployed in is also important for the information security framework. In this chapter, we will be focusing on the framework steps. These framework steps also cover industry based solutions. As a result of this, the topology design of the infrastructure is going to be of paramount importance for all the components that consist of this infrastructure.

Web servers provide the web services access from both inside and outside the infrastructure. Hence, all the access to the web service should be tracked, inspected and filtered whenever required. In this manner, all the connections to the web services should pass through the firewall in order to track the connections, restrict the access or block whenever required. The main reason behind this is that we cannot restrict the accesses by the firewall policies if all the assets are in the same network. As of the web server's deployment, other types of the assets are deployed in different segments of the firewall. In other words, all the accesses from different assets to each other should be tracked, restricted and blocked whenever required. As a result of this, the firewall is located in the center of the infrastructure.

With the help of firewall technologies, any IT staff can track, restrict and block any Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) connections. In addition to this, network and system activities should be monitored in order to detect and prevent vulnerability exploits. These vulnerability exploits generally aim to interrupt or gain the control of a service or an asset. In this manner, intrusion prevention system (IPS) should monitor all the network traffic in order to drop or quarantine the malicious packets, block the traffic from the source or reset the connection whenever required. IPS inspects data link layer traffic of the network or assets.

Access to the web services and database services can be monitored and restricted by the firewall or intrusion prevention systems. However, for the protocol based network traffic such as HTTP, these solutions may be inadequate. For this reason, web application firewall (WAF) and database firewall (DBF) technologies are essential in order to protect web application and database assets. Protocol based attacks such as

SQL injection or cross-site scripting (XSS) can be blocked with the help of a web application firewall. On the other hand, all the SQL operations can be monitored, restricted or blocked with the help of a database firewall. The deployment of web application and database firewalls are restricted when compared to the firewall or IPS technologies. To illustrate, WAF and DBF can be deployed in front of the web application servers and database servers, respectively. WAF and DBF inspects data link layer traffic of web application servers and database servers, respectively.

Security measurement for the entire infrastructure may not be sufficient with the help of the firewall, and IPS technologies. The main reason is that the attacker is likely to saturate the internet bandwidth of the organization so that the organization cannot give any service to the world. In such a scenario, one can observe that all the web services are accessible from the local network. However, these services are not accessible from outside the infrastructure. Therefore, DDoS protection should be deployed outside the organization infrastructure. With the help of the DDoS protector, behavioral protection is performed. Advance challenge and/response techniques are used. DDoS protector automatically defends against network flood attacks and application layer attacks and quickly filters the traffic before it reaches the infrastructure. Hence, DDoS protector protects the networks and servers, blocks the exploits and prevents the bandwidth saturation.

For any of the internet access, the firewall can track of the network layer and the transport layer with respect to the Open Systems Interconnection Model (OSI). However, the inspection of the content-based accesses may be difficult for the firewall technologies. For this reason, URL based accesses should be filtered by the proxy servers in order to filter internet accesses and filter whenever required. With the help of proxy servers, the internet access, bandwidth utilization, security scanning and malicious activities can be filtered easily.

While mitigating these vulnerabilities by IPS, predefined customer attack signature sets or user defined signature sets should be used. However, for the zero day attacks for which there exist no customer attack signature database, IPS may not be adequate. As a result of this, zero day malware protection systems should be used in order to discover zero day attacks. This malware protection system runs virtual operating

systems on it so as to analyze the network traffic. With the help of these virtual operating systems, the malware protection system analyzes the network traffic, simulates the suspicious activity on the virtual operating systems and clarifies whether it is normal or abnormal.

Assume that there is only one asset for any of the web service in the infrastructure. In the case of a system down for this asset, the relevant web service cannot serve neither outside the organization, nor inside the organization. Because of this, the redundancy of the web servers are inevitable for such scenarios. In this manner, application delivery technologies of which load balancers consist should be used. With the help of load balancers, access to the web services can be performed in a redundant infrastructure, the response time of the web services can be minimized and the overload of the web services can be avoided. Furthermore, SSL Offload can be performed in the load balancer in order to avoid SSL load on the web servers. Additionally, HTTP compression, connection limiting feautures can be used in order to reduce the resource utilization of the web servers with the help of load balancers.

Other than these security concepts, we should consider endpoint security technologies in order to complete the security requirement from the initial point which are assets. Operating systems of the web servers or any other assets may be based on Microsoft, Linux, Mac OS X or other type of distributions. Considering the endpoint security gaps, such as a virus, or a Trojan; anti-virus agents should be deployed on all the assets in order to provide initial mitigation. To illustrate, most common vulnerability exploitation tools such as Mimikatz.exe can be blocked by the anti-virus agent. Additionally, access to the other assets cannot be tracked by the center firewall. For this manner, host IPS agent should also be deployed in order to block accesses on the assets themselves.

Performing the essential configuraton with respect to the antivirus software and host based IPS may not be sufficient. The main reason is that there may be a wrong configuration or deployment, misuses of these softwares, or other types of conditions. In such a case, network access control protection (NAC) mechanism should be considered in order to analyze the asset that is supposed to be a part of the system. In this manner, host based configuration such as being member of a domain, operating

system based configurations, antivirus and host IPS deployment and configuration should be controlled by an NAC. With the help of the NAC, the asset that is going to join the network is controlled with respect to the initial and essential configuration. It is allowed to join the network if all the configuration checklists performed by the NAC are provided.

As can be figured out, the management of all the security components have a vital role in the infrastructure. Any exception, or permission given in the security components may cause incredible security breaches. As a result of this, access to the management of the security components should also be restricted. Only authenticated IT staff should have access to the management.

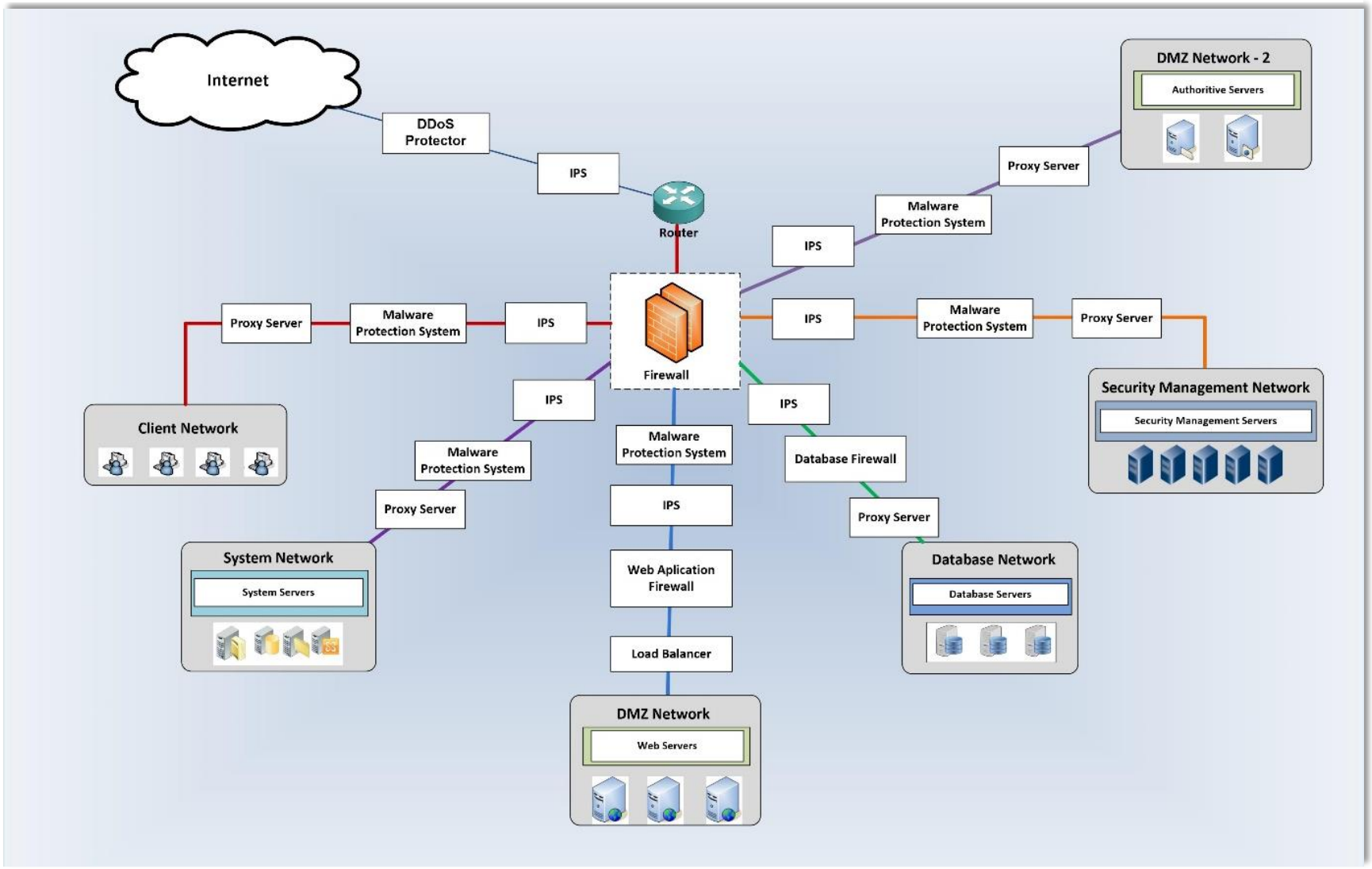
As can be understood from the topology given in Figure 4-1, all the assets should be sorted and deployed in the same networks. For this purpose, network segmentation should be performed on the firewall of the organization. By this way, the accesses from different assets can be tracked and restricted.

Industry-based security solutions should be deployed with respect to the type of the assets. For example, web application firewall deployment should be performed in the DMZ segment since the assets to be protected are in that network. IPS sensors should be deployed in all the networks in order to monitor all the traffic inside and outside the infrastructure. Malware protection system should be deployed in the networks where the probability of occurrence of the malware traffic is most probable. Load balancers should be deployed in the same network with web servers in order to share workload to the web servers efficiently. Email security solutions should be deployed as in the same way with web servers since the email traffic also comes from the outside network. Proxy servers should be deployed in the network where any asset must access to the internet.

Other than these security deployments, internet service provider of the organization also provides cloud DDoS and IPS protection over the internet. In some cases, this may be a vital step due to the conditions, such as bandwidth saturation.

This sample topology is just a logical view. That is to say, other network devices, except the router, are not determined since the main focus here is performed with respect to the security deployment.

Figure 4-1: A Fictitious Topology of an Enterprise Network



4.4. INFORMATION SECURITY FRAMEWORK

This section includes the detailed explication of the porposed information security framework. This framework has a systematic approach for the web services security in the enterprise networks. It is aimed to be easy to follow and apply in the production systems. Since the framework offers diverse implementation details, it establishes a well-defined reference for the web services security.

Information security framework is not a straight-forward subject which can be easily implemented in the organizations since it is supposed to be a continuous process which may have many fallacies that may cause the efforts to be failed. The implementation of the security solutions stated in the framework is world-wide agreed for the information security. However, combining each of these security steps may vary in terms of standards and guides. Hence, the implementation of the information security framework was taken as a goal. How to build a secure web services infrastructure via information security framework was clearly defined.

We have five separate steps which consist of this information security framework. In the framework, in order to start implementation of a step, the previous step is prerequisite. On the other hand, having completed the final step, the framework makes a new start. The main reason behind this is to provide a security cycle permanently.

In the first step of the information security framework, the activities to be performed in the following steps are clearly defined in a written format. With the help of this, all the activities are standardized in a formal structure. The activities shown in Figure 4-2 should be followed in this step so that the purpose of the framework can be fulfilled.

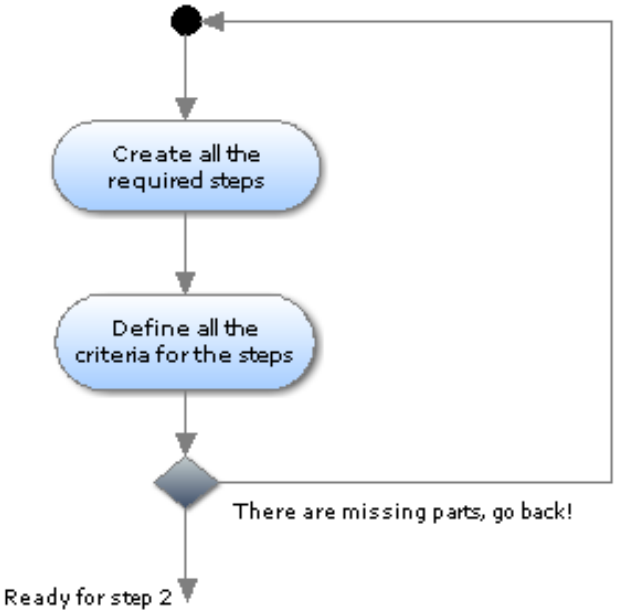


Figure 4-2: Creating All the Required Steps

In the second step, analysis of the web service structure in the organization is performed. The access method to the web services, the integration with the web services and administrative access to the web services are the main concept of this step. The main aim is to better understand the web service structure to be protected. By performing this aim, the actions to be taken in the next steps will be more clear and and easy to implement. Figure 4-3 shows the activities in this step.

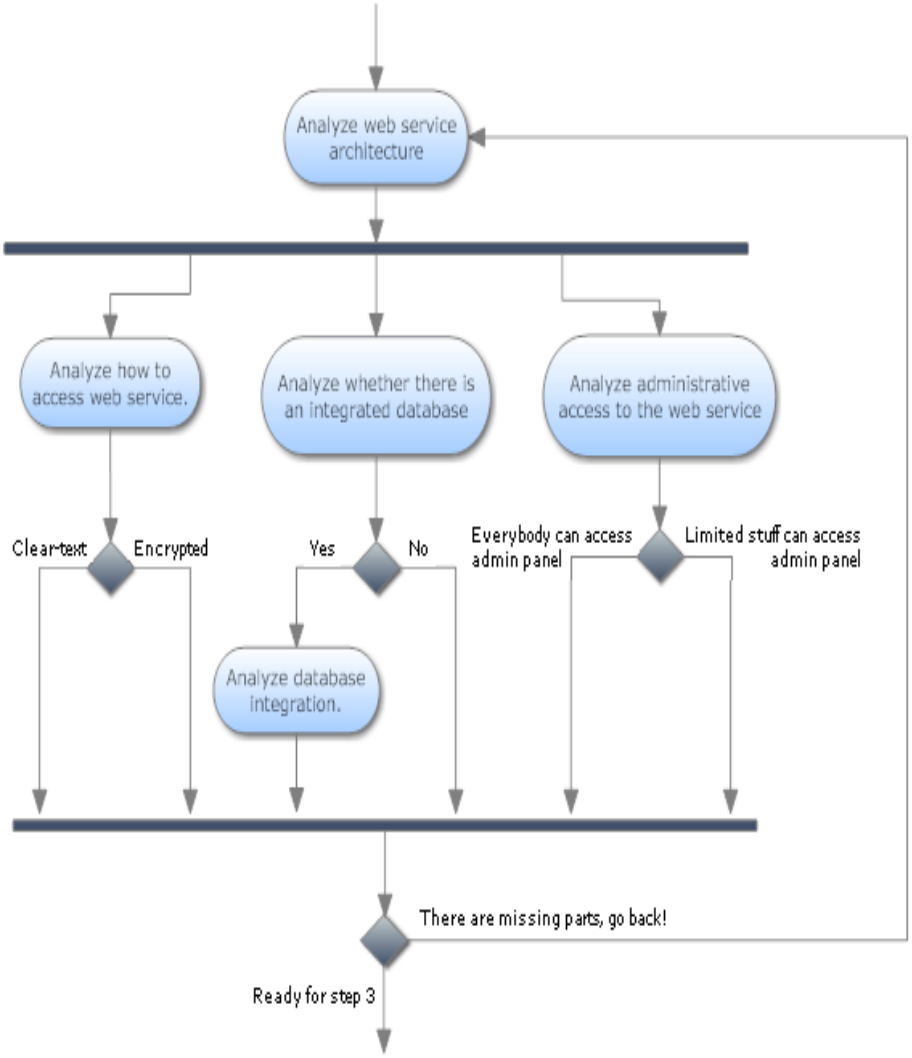


Figure 4-3: Analyzing Web Service Deployment

In the third step, the security and performance level of the web service environment is analyzed in detail. The main function is to determine the security and performance level of the web services. Code analysis, load test, penetration test and social engineering test are performed in order to clarify what should be done without industry based security solutions. With the help of this step, the main security requirements on the web server assets are fulfilled. Figure 4-4 shows the activities in this step.

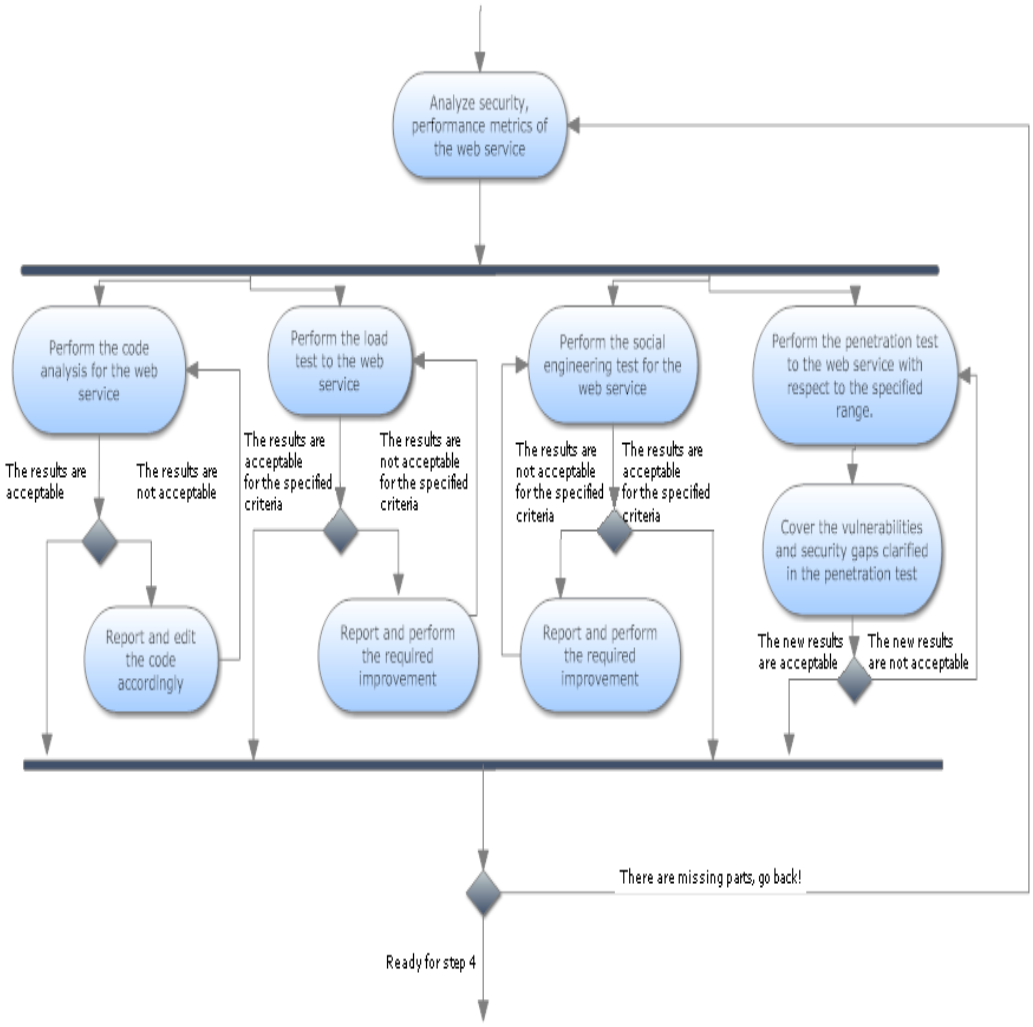


Figure 4-4: Analyzing Security/Performance Metrics of The Web Services

Coming to the fourth step, the implementation of the industry based solutions and web services are explicated in detail. The main role and the contribution of each industry based security solution is explained. On the other hand, the relation between web service environment and security components is considered. The main purpose of this section is providing more secure and granular infrastructure with the help both of the security and web server assets. Figure 4-5 shows the activities in this step.

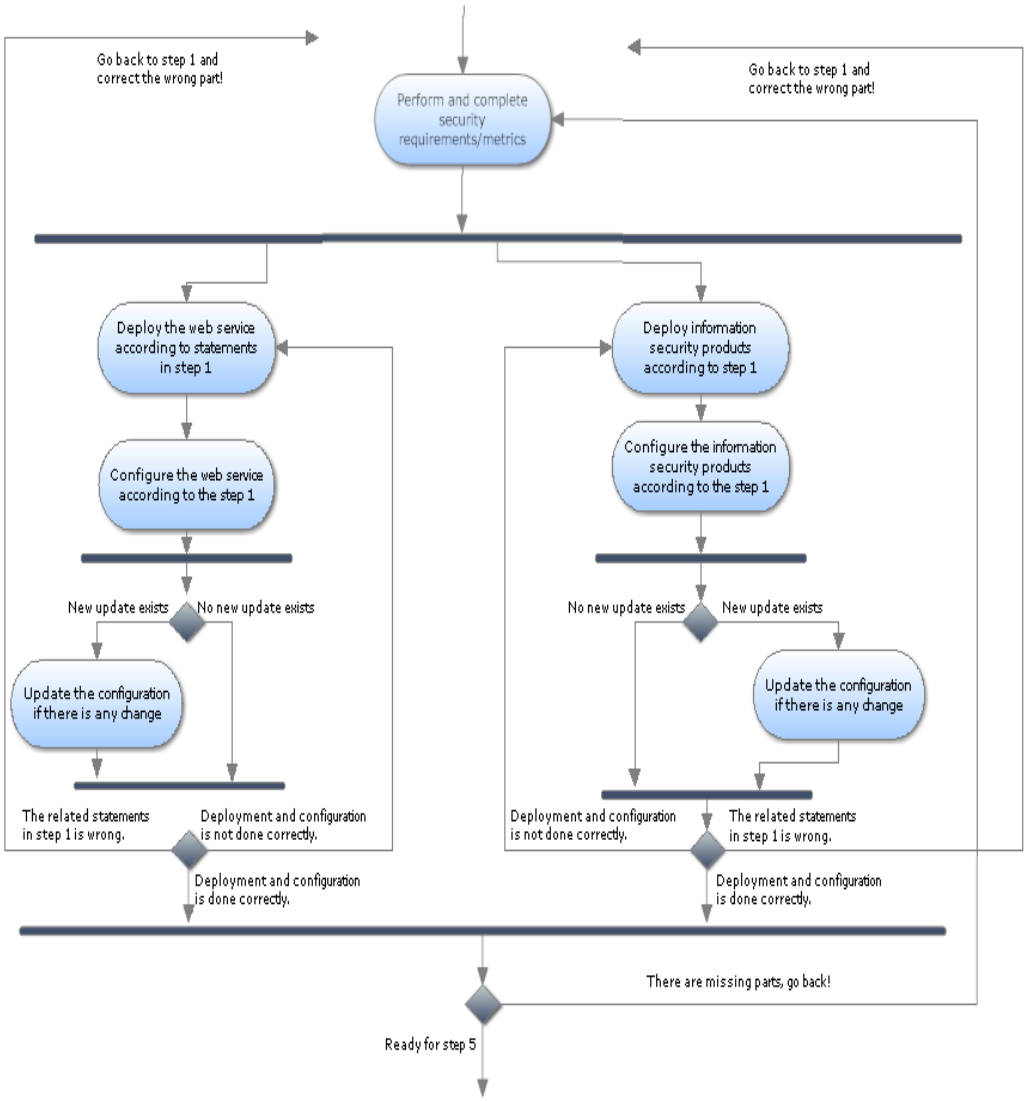


Figure 4-5: Performing and Completing Security Requirements/Metrics

In the final step, effectibility of the actions which have been performed so far are examined. With the help of this, any fallacies and or missing points are supposed to be detected in order to fulfill essential remediations on the information security framework. The effectibility of the information security framework is provided by performing attack simulations to the web servers. These attack simulations cover all the steps of the information security framework. Figure 4-5 shows the activities in this step.

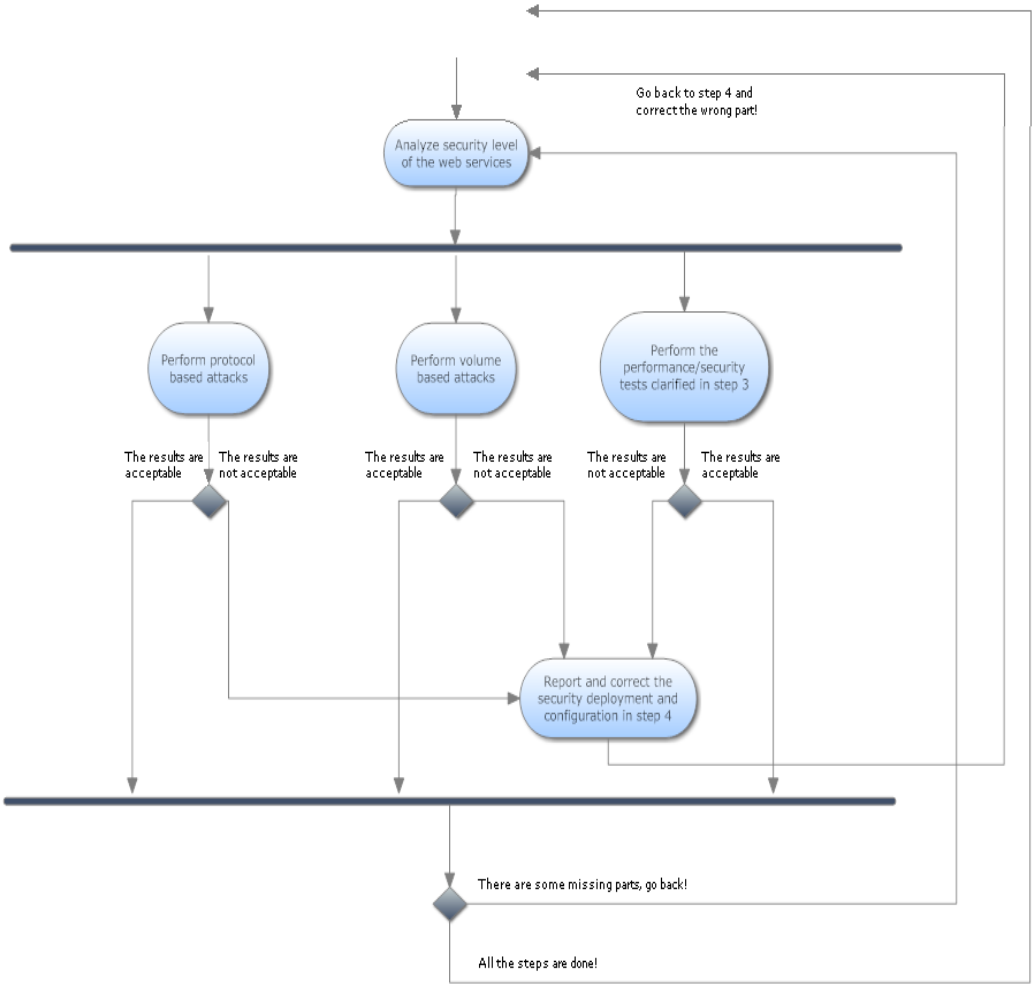


Figure 4-6: Analyzing Security Level of the Web Services

4.4.1. Step 1 – Defining All the Criteria and Information Security Procedures for the Web Services

In this step, what is intended is defining all the criteria and required steps for this framework. Namely, all the executive steps and actions are defined. It was aimed that all the actions were written in an easy to follow format so that whenever required, they can be used as a reference or as a first step of a guidance.

This step can be modelled as part of an Information Security Management System (ISMS), which aims to manage sensitive company information so that it remains secure and includes people, processes and IT systems by applying a risk management

process. An ISMS can help small, medium, and large businesses in any sector to keep information assets secure (ISO, 2014).

The main reason why it is a part of an ISMS is that an ISMS aims to cover all parts of IT systems. However, what is intended in this thesis is to cover only the information security of the web services.

As mentioned above, the first step includes both administrative and technical subjects. To illustrate; as a reference of an administrative subject, it can be stated that "the person who is no longer responsible from administration of web servers will no longer have administrative access to these assets by removing all the administrative accounts which he or she had in advance." As a reference of technical subject, it can be mentioned that "in order to inspect the encrypted HTTP traffic towards web servers, both the intrusion prevention system (IPS) and web application firewall (WAF) have to inspect the HTTPS traffic, so that they can identify and block security violations. In order to do this, the wildcard certificate used for the HTTPS service in the web services has to be imported to both IPS and WAF products."

In order to define all the criteria, checklist mechanism is recommended in order to follow the actions easily. The following is a list of the checklist:

1. **Identify the purposes of the web server:**
   I. Define the type of information which the web server provides,
   II. Define the web server integration with any other asset such as database,
   III. Define the integration method between the web server and database server,
   IV. Define the additional services on the web server if there is any,
   V. Define the requirements for the continuity of service provided by the web servers, such as the continuity of operations plans and disaster recovery plans.
2. **Determine what kind of web server applications satisfy the organization's requirements considering the servers that may offer greater security, but with less functionality or vice versa in some circumstances such as:**
   I. Cost,
   II. Compatibility with existing environment,
   III. Technical capability of IT staff,
   IV. Existing vendor relationship

V. Functionality.

3. **Define the location of a Web server, considering the following issues:**
   I. Define the appropriate physical security protection mechanisms in the physical place such as:
      - Locks,
      - Card reader access,
      - Security guards,
      - Physical IDs.
   II. Define an appropriate environmental control so that the necessary humidity and temperature are maintained,
   III. Define the location of the web servers with regards to the known natural disasters such as:
      - Determine whether the location is hardened against the relevant disasters,
      - Determine a disaster recovery site outside the potential disaster area.
4. **Identify the network services that is supposed to be provided such as:**
   I. Hypertext Transfer Protocol (HTTP),
   II. Hypertext Transfer Protocol Secure (HTTPS),
   III. Internet Caching Protocol (ICP),
   IV. Hyper Text Caching Protocol (HTCP),
   V. Database services.
5. **Identify any network based software, both client and server, to be installed on the web server or any other support servers if required.**
6. **Identify the users or categories of users of the web server and any support hosts.**
7. **Define and implement the privileges that each category of user will have on the web server and support hosts.**
8. **Define and implement the location of web service management such as:**
   I. Locally,
   II. Remotely from the internal network,
   III. Remotely from external networks.
9. **Determine and implement the authentication methods of the users.**
10. **Determine and implement an appropriate access to the information resources on the web server to be enforced.**

11. Define and implement an appropriate access and configuration methods that provides the following:

I. Restrict administrative access to the authorized users only,
II. Prevent unauthorized access to the web servers,
III. Control access to data on the server,
IV. Disable unnecessary network services that may be built into the OS or server software,
V. Control access to various forms of executable programs, such as Common Gateway,
VI. Log appropriate server activities to troubleshoot security or system based incidents.

12. Analyze and mitigate the security breaches on the web servers by performing the following actions:

I. Code analysis in order to clarify and identify software implementation problems with respect to the following:
   - Determine and perform data flow analysis in order to collect real time information about the data in the software,
   - Determine and perform control flow graph in order to perform compilation of the software,
   - Determine and perform taint analysis in order to detect the tainted variable in the software,
   - Determine and perform the lexical analysis in order to make the source code abstract and easy to manipulate,
   - Determine and perform the mitigation steps stated in the code analysis,
   - Determine and perform the security gaps which are stated but could not be mitigated in the following code analysis test.
   - Determine the reason of not mitigating the vulnerabilities and perform the following:
     - Correct the problems for the mitigation,
     - Repeat the mitigation process.

II. Load test in order to clarify maximum performance under the increasing load with respect to the following:
   - Determine the behavior of the web servers under the expected load,

- Determine the errors to be faced under the expected load,
- Determine the robustness of the web servers under the expected load.
- Determine and perform the mitigation steps stated in the load test,
- Determine and perform the improvements which are stated but could not be performed in the following load test,
- Determine the reason of not performing the improvements and cary out the following:
  - Correct the problems for the improvement,
  - Repeat the improvement process.

III. Social engineering in order to clarify the security awareness of the IT staff with respect to the following:
- Determine and perform the social engineering methods to the IT staff of the organization in order to collect organization based information,
- Determine and analyze the information obtained from the social engineering methods,
- Determine and perform security awareness education for the organization staff.

IV. Penetration test in order to clarify existing security vulnerabilities with respect to the following:
- Determine and define the information about the organization with respect to the following:
  - Determine and identify the information such as:
    - Internet service provider,
    - The authority of the organization domain name,
    - DNS records of the servers,
    - Autonomous system.
  - Determine and identify information from the serach engines over the internet,
  - Determine and identify the DNS records of the servers, hostname information, the detection of the accessible servers and access methods,
  - Determine and identify the open or filtered ports,
  - Determine and identify the IP address range and the controls of IP routing,
  - Determine and gather information by bypassing security measures,
  - Determine and identify the security products and security applications,

- Determine and identify the operating systems of the servers, version and release information,
- Determine and gather detailed information about the services running.

- Determine and identify the configuration of the DNS servers,
- Determine and perform the controls of the servers which is accessible from outside with respect to the following:
  - Determine and identify open ports of the servers and classify the unnecessary ports,
  - Determine and identify the security vulnerabilities of the operating systems,
  - Determine and identify the security vulnerabilities for the specified applications,
  - Determine and identify organizational applications,
  - Determine and perform user prediction and password control,
  - Determine and perform common controls and identify the vulnerabilities with respect to the leakage that may be caused by the commonly used services such SMTP, FTP, HTTP, HTTPS, TELNET, ICMP, RPC, NETBIOS, SNMP.
- Determine and perform the scanning of the services that are open to the internet with respect to the following:
  - Determine and perform the control of the security vulnerabilities that exist on the assets except the organization assets announced on the internet,
  - Determine and identify the accessible services and the security vulnerabilities of the unannounced assets.
- Determine and scan the organizational applications within and without authorized user with respect to the following:
  - Session management,
  - Input validation,
  - User validation,
  - Application waste,
  - Input/output management,
  - Integration with other assets and the security of data transfer,
  - Brute force,
  - Bypassing authorization,

- Accessibility control of the information and files which are not accessible,
- Database services,
- Unauthorized access to the database,
- Application server services,
- Command injection such as OS, SQL, SSI, XPATH,
- Modifying HTTP header,
- Modifying HTTP form,
- Cross site scripting,
- Buffer overflow,
- Cookie injection.

- Determine and perform the following criteria with respect to the penetration tests:
  - The integrity, confidentiality, and accessibility of the assets,
  - The importance and criticality of the assets,
  - The criticality of the vulnerabilities detected,
  - The effect of the exploitation of the vulnerabilities with respect to the security measures,
  - Determine and perform an emergency action report in order to mitigate emergent and privileged vulnerabilities. The report should contain the following:
    - The detailed information on the vulnerability,
    - The criticality and the possibility of the exploitation of the vulnerability,
    - The assets which are affected by the vulnerability,
    - The risk score of the vulnerability,
    - The possible effect of this vulnerability on the organization,
    - The solution details with respect to the vulnerability.
- Determine and perform mitigation procedure for the vulnerabilities stated in the report.
- Determine and perform the vulnerabilities which are stated but could not be mitigated in the following penetration test.
- Determine the reason of not mitigating the vulnerabilities and perform the following:
  - Correct the problems for the mitigation,

- Repeat the mitigation process.

13. Perform and complete security requirements of the web servers:

I. Perform the deployment of the web servers with respect to the following:
   - Deploy the web servers in the demilitarized zone (DMZ),
   - Deploy the web servers in a redundant environment,
   - Identify the integrations of the web servers such as:
     - Database servers,
     - System servers,
     - SMTP servers.
   - Separate the web servers from the other types of the servers.

II. Perform the deployment of the security solutions with respect to the following:
   - Determine and perform the firewall deployment with respect to the following:
     - Enable logging for the access rules of the web servers,
     - Optimize the access rules that may contain "any" option in source, destination, or service,
     - Determine the naming convention in the assets and network objects,
     - Perform the anti-spoofing configuration for all the interfaces in the firewall,
     - Restrict the access rules as much as possible in case of security breaches,
     - Determine the most used access rules and define them preferentially,
     - Determine the network address translation in order to access the web servers from both outside the network and inside the network,
     - Disable the inactive services in order to improve firewall performance,
     - Perform the stealth rule after defining all the access rules in the firewall,
     - Perform stateful inspection in order to capture the network traffic efficiently,
     - Determine and perform capacity optimization for the optimization of the memory allocation,
     - Determine and perform administrative access to the firewall management,
     - Determine and perform time synchronization in the firewall,
     - Determine and perform administrative auditing regularly,
     - Determine and perform backup mechanism periodically,
     - Determine and perform redundancy in the firewalls in case of disaster recovery.

- Determine and perform the IPS deployment with respect to the following:
  - Determine and perform the traffic inspection for all the firewall segments,
  - Determine and optimize the resource utilization for the best performance,
  - Determine and perform the fail open utility on the IPS sensors,
  - Determine and observe the real time network traffic on the IPS sensor,
  - Determine and perform IPS policies with respect to each network segment on the IPS sensor,
  - Determine and perform advanced features such as:
    - HTTP response scanning,
    - Advanced traffic inspection,
    - Reconnaissance policies.
  - Determine and perform DoS profile configuration for the internet segment,
  - Determine and perform HTTPS inspection in order to analyze encrypted web service traffic,
  - Determine and perform automatic attack signature and botnet databases in the IPS sensor,
  - Determine and optimize IPS policies with respect to the attack signature and botnet databases regularly,
  - Determine and perform system event policy for the system event,
  - Determine and perform reporting for the following:
    - Security violations,
    - System events.
  - Determine and perform administrative auditing regularly,
  - Determine and perform backup mechanism periodically,
  - Determine and perform redundancy in the IPS sensors in case of disaster recovery.
- Determine and perform the WAF and DBF deployment with respect to the following:
  - Determine and perform the service scanning regularly on the server networks,
  - Determine and perform data classification on the databases regularly,
  - Determine and perform user rights management on the databases regularly,
  - Determine and perform the operation mode of the active web server groups,

- Determine and perform the protected IP configuration on the web server groups,
- Determine and perform source restriction on the web server groups,
- Determine and perform active service ports with respect to the web services,
- Determine and perform character set configuration on the web services,
- Determine and perform HTTPS inpection in order to analyze encrypted web service traffic,
- Determine and perform web service plugins if available,
- Determine and perform error pages for the security vulnerabilities,
- Determine and perform the web error policies for the web servers,
- Determine and perform the web profile policies for the web servers,
- Determine and perform the web worm policies for the web servers,
- Determine and perform the universal user tracking and application user tracking with respect to the web server and database server integration,
- Determine and perform data masking in order to hide confidential data in the web server or database server,
- Determine and perform forwarded connections with respect to the connections coming from the load balancers,
- Determine and perform application mapping for the web services,
- Determine and perform limited access policies for the administrative access to the web servers,
- Determine and perform database table groups to be used in the WAF policies,
- Determine and perform stored procedure groups periodically,
- Determine and perform file extensions for the web services,
- Determine and perform the ignored file patterns for the web services,
- Determine and perform false positive signature reduction in the WAF policies,
- Determine and deploy database agents in case of DBF traffic inspection limitation,
- Determine and perform database monitoring for the performance monitoring,
- Determine and perform database assessment scanning,

- Determine and perform web service scanning or integration with a web application scanner,
- Determine and perform the database audit policies in order to monitor and store database traffic,
- Determine and perform archiving action for the database auditing,
- Determine and perform system event policy for the system event,
- Determine and perform reporting for the following:
  - Security violations,
  - Database auditing,
  - System events.
- Determine and perform administrative auditing regularly,
- Determine and perform backup mechanism periodically,
- Determine and perform redundancy in the WAF and DBF in case of disaster recovery.

- Determine and perform the DDoS protector deployment with respect to the following:
  - Determine and perform a port group in order to monitor the production network,
  - Determine and perform a forwarding table in order to use the pair of ports,
  - Determine and create a protected network in order to analyze what might be under attack,
  - Determine and create a DDoS profile in order to learn and simulate DDoS traffic,
  - Determine and create a behavioral DDoS profile in order to detect abnormal network traffic,
  - Enable the behavioral DDoS profile for the DDoS profile,
  - Determine and configure an HTTP mitigator profile for the web servers,
  - Determine and perform administrative auditing regularly,
  - Determine and perform backup mechanism periodically,
  - Determine and perform redundancy in the DDoS protector in case of disaster recovery.
  - Determine and perform the malware protection system with respect to the following:

- Determine and configure the security content for the infected hosts,
- Determine and configure the virtual machines in order to perform malware traffic simulations,
- Determine and configure the operational mode in order to inspect all the network traffic,
- Determine and configure the prevention mode in order to provide active protection,
- Determine and configure YARA rules in order to identify and classify malware types,
- Determine and configure IPS and WAF integration in order to identify and block immediately the assets which contain malware activity,
- Determine and perform administrative auditing regularly,
- Determine and perform backup mechanism periodically,
- Determine and perform redundancy in the malware protection system in case of disaster recovery.

- Determine and perform the load balancer with respect to the following:
  - Determine and perform the resource provisioning in order to optimize resource utilization,
  - Determine and create the following in order to perform server segments:
    - Virtual local area network (VLAN),
    - Routing,
    - Self-IPs.
  - Determine and create the following in order to perform load balancing:
    - Nodes for the web server,
    - Pools,
    - Virtual servers,
    - Pool assignment for the virtual servers.
  - Determine and perform routing domain in order to perform segmentation on the load balancer,
  - Determine, create and assign essential load balancing profiles for the virtual servers with respect to the following:
    - HTTP,
    - HTTP compression,

        - Web acceleration.
        - SSL.
    - Determine, create and assign specific profiles for the virtual servers such as:
        - Persistency,
        - HTTP class,
        - TCP or UDP.
    - Determine and enable packet filtering in order to analyze network traffic,
    - Determine, create and assign persistency profiles for the virtual servers,
    - Determine, perform and assign cipher suite configuration in the SSL offload in order to inspect encrypted traffic for the IPS and WAF,
    - Determine and perform connection limiting with respect to the performance of the web servers,
    - Determine and perform automap option for the load balancing methods,
    - Determine and perform connection optimization in order to enhance web service traffic,
    - Determine and perform load balancing policies in order to perform specific actions such as:
        - Virtual server restriction,
        - SSL redirection,
        - Remote logging.
    - Determine and perform administrative auditing regularly,
    - Determine and perform backup mechanism periodically,
    - Determine and perform redundancy in the load balancers in case of disaster recovery.
- Determine and perform the proxy deployment with respect to the following:
    - Determine and perform the assets to access the internet over proxy,
    - Determine and bypass the local connections from the proxy server,
    - Determine and create internet access policies in the proxy server,
    - Determine and configure HTTPS inspection in order to analyze encrypted traffic,
    - Determine and configure safe search with respect to the search engines,
    - Determine and configure logging for the internet access of the assets,

- Determine and configure SSL decryption bypass in order not to analyze the encrypted traffic which contains personal or financial information,
- Determine and configure domain based integration in order to identify user information in the traffic,
- Determine and assign domain based policies with respect to the content filtering,
- Determine and configure the proxy redirection in order to redirect internet accesses to the proxy server transparently,
- Determine and configure caching in order to optimize the internet accesses with respect to the most visited sites,
- Determine and perform reporting for the following:
  - The use of the internet by the assets,
  - The use of the bandwidth utilization by the assets,
  - The access to the risky sites by the assets,
- Determine and perform administrative auditing regularly,
- Determine and perform backup mechanism periodically,
- Determine and perform redundancy in the proxy servers in case of disaster recovery.

o Determine and perform the central endpoint protection deployment with respect to the following:

- Determine and perform platform integrations such as:
  - Anti-virus,
  - Host intrusion prevention (IPS),
  - Host data loss prevention (DLP),
  - Host encryption for files and folders.
- Determine and perform domain integration in order to identify and classify the assets registered to the domain,
- Determine and perform domain synchronization,
- Determine and create distributed repository in order to synchronize with the assets in the branch sites if available,
- Determine and perform agent deployment to the assets registered to the domain,
- Determine and perform periodic agent update on the assets,

- Determine and perform removal task for the assets that do not exist,
- Determine and perform scheduled tasks in order to deploy and run following components:
  - Anti-virus,
  - Host intrusion prevention (IPS),
  - Host data loss prevention (DLP),
  - Host encryption for files and folders.
- Deploy and perform scheduled tasks for the component updates,
- Determine and perform reporting for the following:
  - Security violations on the endpoints,
  - System events.
- Determine and perform administrative auditing regularly,
- Determine and perform backup mechanism periodically,
- Determine and perform redundancy in the central endpoint protection in case of disaster recovery.

- Determine and perform the email security gateway deployment with respect to the following:
  - Determine and perform mail server integration,
  - Determine and perform inbound and outbound email policies,
  - Determine and perform mail relay configuration and domain integration,
  - Determine and perform periodic anti-spam database updates,
  - Determine and perform custome whitelist and blacklists with respect to the senders, recipients and keywords,
  - Determine and perform reporting for the following:
    - Spam mail activities,
    - Inbound and outbound email traffic,
    - System events.
  - Determine and perform administrative auditing regularly,
  - Determine and perform backup mechanism periodically,
  - Determine and perform redundancy in the central endpoint protection in case of disaster recovery.
- Determine and perform the vulnerability management system deployment with respect to the following:

- Determine and perform vulnerability database update periodically,
- Determine and create the asset lists in order to scan,
- Determine and define accesses to the assets,
- Determine and perform the scanning policies periodically,
- Determine and perform reporting for the following:
  - Existing assets in the organization,
  - Existing vulnerabilities on the assets,
  - System events.
- Determine and perform administrative auditing regularly,
- Determine and perform backup mechanism periodically,
- Determine and perform redundancy in the central endpoint protection in case of disaster recovery.

- Determine and perform the risk management system deployment with respect to the following:
  - Determine and perform following integrations:
    - Firewall,
    - IPS,
    - Central endpoint management,
    - Load balancer,
    - WAF and DBF,
    - Network devices.
  - Determine and perform periodic analysis of integrated components,
  - Determine and create organization model,
  - Determine and create business units under organization model,
  - Determine and define the business assets under the business units,
  - Determine and assign business impacts for the business units,
  - Determine and define threat origins with respect to both outside and inside the organization,
  - Determine and perform vulnerability management integration in order to obtain vulnerability status of the assets,
  - Determine and obtain access compliance within the following:
    - Firewall,
    - IPS,

- WAF and DBF,
- Load balancers,
- Network devices.

➢ Determine and perform vulnerability import from the vulnerability management,

➢ Perform attack simulation with respect to the vulnerabilities imported,

➢ Perform key performance indicator and vulnerability level indicator in order to learn which vulnerabilities may be exploited,

➢ Determine and perform removal of outdated vulnerabilities,

➢ Perform the integrity of the organizational model predefined,

➢ Determine and perform administrative auditing regularly,

➢ Determine and perform backup mechanism periodically,

➢ Determine and perform redundancy in the central endpoint protection in case of disaster recovery.

○ Determine and perform the performance monitoring system deployment with respect to the following:

➢ Determine and perform the integration of the following assets in order to monitor organization infrastructure:

- All the system assets,
- All the database assets,
- All the web service assets,
- All the network assets,
- All the security assets.

➢ Determine and perform discovery tasks in order to identify and classify undetected assets,

➢ Determine and perform the communication methods such as simple network management protocol (SNMP), and windows management instrumentation (WMI),

➢ Determine and perform synthetic transaction monitoring (STM) in order to monitor specified services such as a web application,

➢ Determine and perform mail server or message integration in order to notify the system administrator timely in case of an incident,

- Determine and perform specific monitors that identifies and clarifies the current status of the organization specified assets,
- Determine and perform administrative auditing regularly,
- Determine and perform backup mechanism periodically,
- Determine and perform redundancy in the central endpoint protection in case of disaster recovery.

- Determine and perform the log management system deployment with respect to the following:
  - Determine and perform the integration of the following products in order to combine the logs of all the assets,
    - All the system assets,
    - All the database assets,
    - All the web service assets,
    - All the network assets,
    - All the security assets.
  - Determine and define the log format of all the assets to be parsed and formed as human readable,
  - Determine and define log correlation policies in order to detect suspicious events and incidents,
  - Determine and define the notifications and reports with respect to the log correlation policies,
  - Determine and perform administrative auditing regularly,
  - Determine and perform backup mechanism periodically,
  - Determine and perform redundancy in the central endpoint protection in case of disaster recovery.

14. Analyze the security level of the web services:

- Perform the protocol based attacks with respect to the followings:
  - Perform the vulnerability exploitable attacks in order to control the security configuration and deployment,
  - Review the response of the security configuration and deployment with respect to the vulnerability exploitable attacks,
  - Decide whether the results are acceptable ot not,
  - Determine and address the security vulnerabilities which are not blocked,

- Determine and report the missing or wrong security configuration or deployment,
- Determine and assign the responsibilities to the IT staff with respect to the report,
- Go back to the previous step and correct the security configuration and deployment or web server deployment.

- Perform the volume based attacks with respect to the following:
  - Perform the volume based attacks in order to control the security configuration and deployment,
  - Review the response of the security configuration and deployment with respect to volume based attacks,
  - Decide whether the results are acceptable ot not,
  - Determine and address the volume based attack types which are not blocked,
  - Determine and report the missing or wrong security configuration or deployment,
  - Determine and assign the responsibilities to the IT staff with respect to the report,
  - Go back to the previous step and correct the security configuration and deployment or web server deployment.
- Perform the risk assessment with respect to the following:
  - Perform the risk assessment in order to control the security configuration and deployment with respect to the following:
    - Code analysis,
    - Load test,
    - Penetration test.
  - Review the response of the security configuration and deployment with respect to the risk assessment,
  - Decide whether the results are acceptable ot not,
  - Determine and address the security gaps which are not mitigated,
  - Determine and report the unmitigated security gaps,
  - Determine and assign the responsibilities to the IT staff with respect to the report,
  - Go back to the previous step and correct security gaps.

4.4.2. Step 2 – Analyzing Web Service Architecture

In this step, what is going to be done is analyzing web service architecture in detail. To put it simply; access methods to the web service, web service integration with other components and administration of the web service will be analyzed.

Firstly, access methods of the web service will be considered. As can be figured out, a simple client is supposed to perform an HTTP request to the web server where the relevant web application runs. Web services include several access methods in order to perform their functionalities. The web services including static web page do not require any confidential data. That's because plain text traffic is sufficient. However, other type of web services such as online banking, shopping sites which include confidential data will require encrypted traffic in order to protect confidential data of the users. As a result, default access to the web services can be done via HTTP or HTTPS traffic.

Considering today's IT technology, a simple web service architecture including a few static web page is even integrated with a database service. With respect to the functionality of the web service, the database integration can be much more complex and advanced. In other words, there may be a database integration and the integration type can be more complex with respect to the functionality. As there is an integration, all the information served in the web services is stored in the database. Therefore, database services are also supposed to be deployed in the infrastructure accordingly and security concepts have to be considered and implemented.

Web services are administrated by limited staff in the relevant organization. As can be guessed, administrative access is supposed to be limited so that only authenticated staff can access. In this manner, the administrative accesses have to be limited. To illustrate, if the web service runs on the windows server, other types of the access methods such as remote desktop connection should be limited and be only available to web server administrators. Web service administration can also be performed via web graphical interface such as /admin.php. Such kind of access should be blocked to the outside of the organization network. Additionally, Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA), should be used in order to harden administrative access.

By performing all the analysis for the web service architecture, following steps will be clear enough to provide more secure and robust infrastructure.

4.4.3 Step 3 – Analyzing Software, Performance and Security Metrics of the Web Services

In this step, the main purpose is analyzing the current status and clarifing the missing parts of the web services. The step is separated into four parts, which are source code analysis, load test, social engineering testing and penetration testing. Each step can be considered as subsidiary part of each other. The main reason behind this is that performing only each part cannot define the current status of the web services.

The first part which is, source code analysis is supposed to be based on software-based status of the web services. To put it simply, the efficiency of the code is analyzed and evaluated. As mentioned in The Open Web Application Security Project (OWASP) (2013), Source Code Analysis is generally carried out within the context of a Code Review which is also known as white-box testing and is applied at the implementation phase of a security development lifecycle (SDL). Source Code Analysis commonly stands for the running of static code analysis tools which give an effort to address possible vulnerabilities in the static source code which is non-running via techniques such as taint analysis and data flow analysis. Preferably, such tools instinctively find out security flaws with a high level of confidence. However, this is far beyond the technological masterpiece with regards to the many types of application security flaws. By this way, such tools frequently assist analysts to help them on the security-related divisions of the code, so they can find flaws more efficiently, rather than a tool which basically finds flaws. Some tools are starting to move into the Integrated Development Environment (IDE). With respect to the types of problems that can be detected in the phase of the software development itself, this is a powerful step within the development lifecycle to implement such tools, since it provides simultaneous feedback to the developer about the issues they may be facing during the code development process. This simultaneous feedback is very helpful when compared to searching the security gaps in the development process.

The second part, which is load testing aims to provide a detailed information about the load capacity of the web services. As stated by Microsoft Patterns Practices (Meier et al., 2007), load testing provides detailed information about the maximum operating capacity of an application as well as any bottlenecks which may prevent its productivity. The general approach in order to perform load testing on a web application is as folows:

1) Identifying the specific scenarios that address the criticality of the performance.
2) Identifying the workload profile with respect to the distribution of the entire load considering the specific scenarios.
3) Identifying the metrics which are intended to be collected with the aim of verifying them against the performance objectives.
4) Designing tests in order to simulate the load to the web applications.
5) Using automated tools to employ the load with respect to the designed tests, and capturing the metrics.
6) Analyzing the metric data captured during the tests.

There are several factors in order to perform load testing to the web applications. The most basic one is utilized to determine the web application's behavior with regards to both normal and expected peak load conditions. It is recommended to start with a small number of virtual users and then gradually increase the load from normal to peak for a load testing. How the application performs during this gradually increasing load condition can be observed in this manner. Finally, a threshold limit will be crossed for the performance objectives. To illustrate, increasing the load can be performed until the server resource utilization reaches 75 percent, or the response time for the end-point connections exceed 8 seconds.

Coming to the third part, which is social engineering testing, it is one of the basic hacking methods. Basically, social engineering is performed in order to gather and use organization based information by manipulating human relations or inattention of the humans in the organization. The main purpose of the social enginerring is gathering all the material about the targeted organization or person, the information system of

the organization, personal information of the organization staff in case of any attack scenario (Social Engineer, Inc., 2014).

Malicious social engineering activities are separated into three parts as follows:

1) Phishing: is the method of effecting and gathering personal information of a staff in an organization by sending emails from so-called valid and reputable sources.
2) Vishing: is the method of giving an effort to impress the activity or gathering personal information of a staff in an organization by using telephone, which may also include phone spoofing.
3) Impersonation: is the method of gathering the information or accessing to a person, organization or a computer system by pretexting as another person.

Social engineering tactics are considered to be the greatest risk towards information security. According to the statistics which is obtained by the social engineering organization, there is an important impact, which can be considered as a remarkable risk factor (Social Engineer, Inc., 2014):

1) 90 percent of the people they asked provided their names and email addresses without any identity confirmation.
2) 67 percent of the people they asked provided the social security numbers, birthdates or employee numbers.
3) There was 100 percent success ratio in physical breach they performed.

With the help of social engineering tests, personal and organizational awareness is supposed to be gained and other security precautions go for nothing.

Coming to the last part, which is penetration testing, it is intended to identify and clarify security gap of a system. As clarified in Technical Guide to Information Security Testing and Assessment by National Institute of Standards and Technology (2008), penetration testing is security testing where investigators simulate real world attacks to detect and identify methods in order to bypass the security measures of an application, system, or network. Real time attacks that use automated tools or techniques used by the attackers are included for the penetration testing. Most of the penetration tests search for the set of vulnerabilities on one or more systems in order

to gain more access when compared to gaining access by a single vulnerability. Penetration testing can also be helpful for determining the following:

1) The toleration of the system with respect to the real work attack patterns.
2) The complexity level which is necessary for an attacker to successfully compromise the system.
3) Additional precauitons which can mitigate threats against the system.
4) The ability of the security components with regards to detecting attacks and responding properly.

Penetration testing may be priceless, however it is labour-intensive and high level expertise is essential in order to reduce the level of risk for targeted systems. Systems may be harmed or turned into inoperable during the process of penetration testing, contrary to the main purpose, which is to identify how a system can be exploited by an intruder. Despite the fact that professional penetration testers are likely to mitigate the risk, it can never be entirely suppressed. Penetration testing should be performed after careful planning, consideration, notification, and recovery scenarios are predefined.

4.4.4 Step 4 – Performing and Completing Security Requirements/Metrics

In this step, industry-based security solutions for the web services and the required configuration and implementation of the web services with the industry-based security solutions are performed.

Security requirements should be performed on both web service components and also the security components. Firstly, web service deployment and its integration with the database services should be performed accordingly. Web services are the assets that answer to outside the network. In other words, web services are open to the cyber-attacks from both sides of the network. That's why only required sockets should be allowed in order to access to the web services with respect to the functionality. As an example, a web service which contains a static web page should only be accessed via the HTTP port, which is TCP 80 for the clients. With regards to being either Windows or Linux based OS, remote desktop connection or secure shell access should be

limited. As a result of this, web services should be deployed in the demilitarized zone (DMZ) segment. The access from the web servers to the clients should not be allowed if there is no exceptional situation. As described in Guidelines on Securing Public Web Servers by National Institute of Standards and Technology (2007), DMZ prevents outside users who are connected to the web service from having a right of direct access to an organization's internal network (intranet). The risks of locating a web server on an internal network or exposing it directly to the internet can be mitigated by DMZ. It is a well advised solution which offers the most beneficial methods with the minimized level of risk for most organizations. At this point, next generation firewall technologies should be used in order to deploy the web services in a secure zone and obtain full visibility of the access towards the web services.

In the next generation firewall technologies, port-based limitation is provided. However, this may not be enough. Assuming that there may also be signature based attacks, we cannot prevent the relevant web service with the help of the next generation firewall. As a result of this, another way of security solution is required, which is an intrusion prevention system. With the help of intrusion prevention system, signature-based, anomaly-based and protocol-based prevention can be performed (NIST, 2007). Intrusion prevention systems typically prevent security violations that compromise the network infrastructure. In the intrusion prevention systems, there may also be firewall rule-based policies considering intrusion prevention systems do not perform any routing protocols or network address translation technologies. In addition to this, with the help of intrusion prevention systems, reconnaissance activities can be identified. Such kind of activities may include host sweep, which is determining the assets located inside the enterprise network and port scan, which is determining the open sockets of the relevant assets. Another example is TCP-UDP-ICMP volume too high. With this simple attack sample, the attacker aims to saturate internet bandwidth of the enterprise network or make the relevant web service unavailable. Only an intrusion prevention system can prevent such kind of attacks.

The deployment of intrusion prevention systems are typically, layer-2 inline mode or sniffing mode, which means no routing process will be performed. Generally, intrusion prevention systems are deployed outside the enterprise network, in front of the DMZ

network, and in front of the local network. In order to inspect encrypted traffic, the SSL certificate of the web service is supposed to be imported to the IPS sensors.

Outside the enterprise network we aim to prevent the web services from remote attackers by the help of intrusion prevention system initially. Assuming that there is another kind of attempt which aims to make the web server or the outside network unavailable, i.e., Distributed Denial of Service (DDoS) attacks, the intrusion prevention system will not be useful. The DDoS attacks typically cause (Glenn, 2003):

- Slow/saturated network performance,
- The service break of particular web site,
- The difficulty to access to a web site,

In order to prevent these attack types, DDoS protector is deployed outside the network, in front of the IPS sensors. The main reason for this is to compensate the bottleneck of the traffic flow in front of the outside network. With the help of the DDoS protector, behavioral protection base-lining multiple elements and blocking abnormal traffic is performed. Additionally, network flood and application layer attacks are blocked. Customized protection is provided with respect to the specific network environment.

Considering the security performance metrics of the intrusion prevention systems, it may be figured out that intrusion prevention system will not prevent such kind of attacks as SQL injection, cross-site scripting or directory traversal. Such kind of attacks might require specific protocol-based inspection, especially HTTP. Consequently, web application firewall technologies are supposed to be used in order to provide deep security for the web services.

With the help of web application firewall technologies, it is assumed to protect web services with respect to the web service level, namely protocol-based level (OWASP, 2014). Assuming when an attacker intends to perform a defacement to the main web service of an enterprise network, only the web application firewall can perform the required blocking. Commonly, unauthorized administrative access to the web services are blocked by the web application firewalls. Beside all these, other HTTP-protocol based attacks can be blocked by the web application firewalls. There are several deployment types for the web application firewalls, such as layer-2 inline mode, sniffing mode, reverse proxy mode. Considering all the deployments, typically, layer-

2 inline mode are preferred in order to inspect the HTTP traffic of the web service in the most efficient way. As described before, in order to inspect the encrypted web service traffic, SSL certificate of the web service is supposed to be imported to the web application firewall.

In addition to the web application firewall, assuming that there is a database integration of the web service, then another prevention solution, which is the database firewall will be required. The main reason behind this is to audit and control database operation activities either performed from the web service or any other source. Supposing that an attacker compromises the web service, with the open session the attacker can obtain access to the database tables which he is not supposed to access. He can get all the confidential information, insert new information or drop the table. For such kind of cases, database firewall is also necessary. With the help of a database firewall, all the database access is monitored, all the sessions are logged and via the database policies, access to the database can be limited (Imperva, 2014).

Assuming that there are several web servers which provide the relevant web service to the outside world, equal load distribution to the web servers are preferred. In addition to this, SSL offload and caching methodologies are required for the web servers. Load balancers act as virtual servers, receiving all HTTP requests to the Web site. These requests are forwarded, based on the load balancer's policy, to one of the servers that hosts the Web site. In order to implement all these criteria, application delivery center technologies are suggested. In this manner, load balancer should be used in order to perform load balancing to the web servers, SSL Offload, caching and determined distribution. With the help of a load balancer, load share to the web server is performed by considering the health level of the web server. With this aim, specific health monitor is performed, such as URL-based health monitoring. As a result of this, mainly web server redundancy, business continuity, and other aspects will be supplied by the load balancer (NIST, 2007).

In order to control malware threat mitigation technically on the operating system itself, antivirus solutions are the most commonly implemented software. With the help of antivirus software, operating systems and applications which are often targeted by the malware can be protected from such security incidents (NIST, 2005). Within the

capabilities which the antivirus software provides, the following are supposed to be performed:

- Scanning all the critical system components such as startup files and applications, registiries, and boot records.
- Monitoring the real time activities on the system in order to detect any suspicious activity,
- Monitoring the situation of the common applications such as browsers, e-mail agents, file transfer programs, etc.
- Scanning files and folders with respect to the known viruses,
- The capability of identifying common types of malware such as viruses, worms, Trojans, etc.
- Disinfecting files by removing the malware from the file where it exists and quarantining files in another isolated environment.

Considering the capabilities and features about the antivirus software stated above, it is recommended to deploy and configure antivirus software on all systems with any available types. The sooner the operating system installation finishes, the sooner the the deployment of the antivirus software should be performed with the latest antivirus signatures and patches. Thereafter, a complete scan should be performed in order to identify potential problems.

In order to monitor the characteristics of a single host and the threat events which occur in the host itself, host based intrusion prevention system mechanism should be deployed and configured in all the systems. With the help of host IPS, network traffic, system logs, running processes, file access and modification, and system and application configuration changes can be monitored. Host IPS software functions with a set of attack signatures and policies in order to identify known and unknown attacks from the asset itself similar to the antivirus software (NIST, 2005).

Beyond all these security solutions, also self-security level of the web servers should also be considered. The main reason behind this is assuming there is no such industry-based security solutions, security gaps should be covered. Like network port and service identification, vulnerability scanning can determine the assets and attributes of them but it also tries to identify vulnerabilities rather than relying on human

interpretation of the scanning results. Many vulnerability scanners are qualified to implement results from network discovery and port and service identification, which reduces the amount of work needed for vulnerability scanning. Also, some scanners can perform their own network discovery and network port and service identification. Vulnerability scanning can help identify outdated software versions, missing patches, and misconfigurations, and validate compliance with or deviations from an organization's security policy. This is done by identifying the operating systems and major software applications running on the hosts and matching them with information on known vulnerabilities stored in the vulnerability databases (Mell et al., 2005).

By managing vulnerability assessment, it is also necessary to perform a risk management process in order to evaluate current security status of the web service. In other words, by evaluating security components and web service architecture, all the risk assessment to the web service can be determined and the actions to be taken in order to cover the relevant risks can be performed. By combining and correlating firewall, IPS, WAF policies and load balance configuration, the measures to be taken can be identified in a big picture and with the help of these measures, the steps in order to cover security gaps of the web service can be clarified (NIST, 2010).

In order to improve the capability of identifying inappropriate or unusual activities, security information and event management (SIEM) tools can be utilized with the integration of vulnerability assessment, performance data, network monitoring, resource utilization and system logs. SIEM tools can be considered as a centralized logging software which performs aggregation and consolidation of the logs from several information system assets. SIEM tools can also perform log correlation and analysis, which is important in order to determine attack detection events (Dempsey et al., 2011). SIEM products commonly supports the integration with multiple information system assets in order to collect system logs (e.g, such as operating system logs and application server logs) of each asset such as system and security products. With the help of a SIEM solution, the log data coming from different assets are analyzed and events among the log files are correlated and significant events are prioritized. As a result of this, immediate response to such events can be configured to initiate.

Beyond all the measures stated above, performance monitoring is another essential component in order to pinpoint issues on the assets faster by managing all components of application specific performance across physical, virtual, wired and wireless infrastructures. By means of this, performance and availability metrics, application health and infrastructure resource usage can be monitored easily. Network and application behavior and baseline metrics can easily be tracked and abnormal activities can easily be detected (Chew et al., 2008).

4.4.5 Step 5 – Analyzing the Security Level of the Web Service Architecture

In the final step, all the security level that was designed and implemented for the web services are tested. With the help of these tests, the aim is to analyze, identify, and correct the missing parts or errors and maintain the security framework designed for the web services.

To put it simply, in order to test all the security measurements, separate tests are performed. With the help of all these tests, security configuration and tuning of the security components are controlled. If there is any missing or wrong configuration, the relevant security step is corrected and tested again. Via this methodology, this information security framework can br scheduled and performed periodically in order to achieve security continuity.

CHAPTER 5

5. EVALUATION OF THE FRAMEWORK AND CASE STUDIES

In this chapter, the information security framework presented in the previous chapter is evaluated. The evaluation methods are explained and the outcomes of the information security framework are provided in detail.

5.1. INTRODUCTION

In the previous chapter, the information security framework was defined in detail. In this chapter we try to examine the proposed framework. For this purpose, we use 2011 CWE/SANS Top 25 Most Dangerous Software Errors initially for the evaluation (Martin et al., 2011). The main purpose in covering these software errors is to evaluate our framework with respect to the well-known software errors. Thereafter, our framework is evaluated for the security vulnerabilities obtained in the risk analysis results of a special environment. Finally, the framework is explicated for the case studies that state the common security gaps of the web services in the enterprise networks. The results obtained in both parts are as expected. The methodologies provided in the framework cover all the security gaps stated.

5.2. FRAMEWORK VALIDATION

5.2.1. Validation for the Most Dangerous Software Errors

The reason why we choose the 2011 CWE/SANS Top 25 Most Dangerous Software Errors is that these are the world wide known software errors and these software errors are easy to be found and exploited. We considered the software errors with respect to the framework and found out how they are resolved and in which step of the framework they are resolved.

Table 5-1: Top 25 Most Dangerous Software Errors and Mitigation Steps #1

Rank	Definition	CWE ID	Score	Solution	Steps
1	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	CWE-89	93.8	Relevant code should be reviewed by filtering the relevant parameters or it can be mitigated by the IPS or WAF signature.	Step 3 or Step 4
2	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	CWE-78	83.3	Relevant code should be reviewed without using external input or it can be mitigated by the WAF signature.	Step 3 or Step 4
3	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	CWE-120	79.0	It can be mitigated by the IPS signature.	Step 4

Table 5-2: Top 25 Most Dangerous Software Errors and Mitigation Steps #2

Rank	Definition	CWE ID	Score	Solution	Steps
4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	CWE-79	77.7	Relevant code should be reviewed by not allowing any session cookies or custom cookies to access or it can be mitigated by the WAF signature.	Step 3 or Step 4
5	Missing Authentication for Critical Function	CWE-306	76.9	It can be mitigated by the WAF signature.	Step 4
6	Missing Authorization	CWE-862	76.8	Access control capabilities should be used	Step 3
7	Use of Hard-coded Credentials	CWE-798	75.0	Password storing options should be reviewed.	Step 3
8	Missing Encryption of Sensitive Data	CWE-311	75.0	Encryption algorithm should be reviewed or it can be handled by SSL offload option of Load Balancer or by the IPS or WAF signature.	Step 3 or Step 4

Table 5-3: Top 25 Most Dangerous Software Errors and Mitigation Steps #3

Rank	Definition	CWE ID	Score	Solution	Steps
9	Unrestricted Upload of File with Dangerous Type	CWE-434	74.0	File upload algorithm should be reviewed.	Step 3
10	Reliance on Untrusted Inputs in a Security Decision	CWE-807	73.8	Input validations should be reviewed or it can be handled by the WAF signature.	Step 3 or Step 4
11	Execution with Unnecessary Privileges	CWE-250	73.1	The code should be run by using lowest privileges required to perform the relevant task.	Step 3
12	Cross-Site Request Forgery (CSRF)	CWE-352	70.1	Captcha, or One time password should be used.	Step 3 or Step 4
13	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	CWE-22	69.3	Input validation should be performed or it can be mitigated by the WAF signature.	Step 3 or Step 4
14	Download of Code Without Integrity Check	CWE-494	68.5	Integrity check should be performed.	Step 3

Table 5-4: Top 25 Most Dangerous Software Errors and Mitigation Steps #4

Rank	Definition	CWE ID	Score	Solution	Steps
15	Incorrect Authorization	CWE-863	67.8	A proven authentication and authorization framework should be enforced.	Step 3
16	Inclusion of Functionality from Untrusted Control Sphere	CWE-829	66.0	A vetted library or framework should be used or it can be mitigated by the WAF signature.	Step 3 or Step 4
17	Incorrect Permission Assignment for Critical Resource	CWE-732	65.5	Access to the administrative panel should be prevented by the code review, firewall rules or WAF signature.	Step 3 or Step 4
18	Use of Potentially Dangerous Function	CWE-676	64.6	Prohibited functions and developers in order should be identified and avoided or it can be mitigated by the WAF signature.	Step 3 or Step 4

Table 5-5: Top 25 Most Dangerous Software Errors and Mitigation Steps #5

Rank	Definition	CWE ID	Score	Solution	Steps
19	Use of a Broken or Risky Cryptographic Algorithm	CWE-327	64.1	A well-known encryption algorithm should be used or it can be performed by the Load Balancer.	Step 3 or Step 4
20	Incorrect Calculation of Buffer Size	CWE-131	62.4	Enough memory should be provided for the memory allocation or it can be mitigated by the IPS signature.	Step 3 or Step 4
21	Improper Restriction of Excessive Authentication Attempts	CWE-307	61.5	Brute force should be used or it can be mitigated by the IPS or WAF signature.	Step 3 or Step 4
22	URL Redirection to Untrusted Site ('Open Redirect')	CWE-601	61.1	A valid input validation strategy should be used or it can be mitigated by the IPS or WAF technology.	Step 3 or Step 4

Table 5-6: Top 25 Most Dangerous Software Errors and Mitigation Steps #4

Rank	Definition	CWE ID	Score	Solution	Steps
23	Uncontrolled Format String	CWE-134	61.0	All format strings in the code should pass a static string that cannot be controlled by the user or it can be mitigated by the WAF signature.	Step 3 or Step 4
24	Integer Overflow or Wraparound	CWE-190	60.3	Input validation on any numeric input should be performed.	Step 3
25	Use of a One-Way Hash without a Salt	CWE-759	59.9	One way hashing techniques should be used or it can be mitigated by the WAF signature.	Step 3 or Step 4

As can be seen in the tables above, all the software errors stated by the Common Weakness Enumeration can be mitigated by the proposed framework. With respect to the steps for the solution procedure, 28 percent of the software errors are mitigated by the solution procedure in step 3 only, 8 percent of the software errors are mitigated by the solution procedure in step 4 only and 64 percent of the software errors are mitigated by the solution procedures in both steps 3 and step 4.

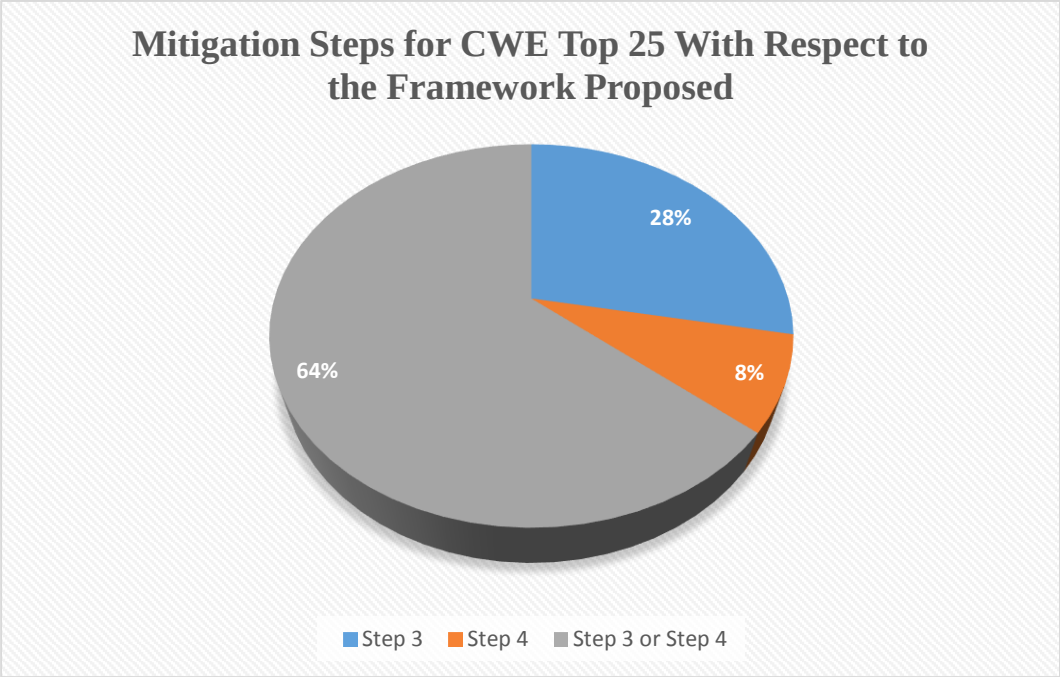


Figure 5-1: Mitigation Steps for CWE Top 25 With Respect to the Framework Proposed

5.2.2. Validation for the Security Vulnerabilities Obtained in An Enterprise Network

With respect to the security vulnerabilities of a special environment, the framework proposed was evaluated again. The security vulnerabilities were obtained as follows:

1) Initially, all the assets in an enterprise network are determined via vulnerability assessment tool.
2) Thereafter the security vulnerabilities on these assets are obtained via vulnerability assessment tool.
3) With respect to the security modeling created and attack simulations predefined in the risk management product, the security vulnerabilities are evaluated against threat models which are predefined.
4) These threat models are classified as either insider or outsider. In other words, the security vulnerabilities may be exploited from either inside or outside.
5) In order to perform these validation steps, McAfee Vulnerability Management and SkyBox Vulnerability Control and Threat Manager Products are used.

6) With respect to the security vulnerabilities obtained in the vulnerability management tool and threat models, and the attack simulations defined in the risk management tool, the solutions and the steps for the solution procedures are composed as follows:

Table 5-7: The Mitigation Steps and Solutions for the Security Vulnerabilities #1

ID	Definition	Solution	Steps
ID1	[cpujul2012-392727,cpujuly2013-1899826] Apache APR before 1.4.4 Remote DoS due to Infinite Recursion Condition in 'apr_fnmatch()'	Apache software version should be upgraded or it can be mitigated by the IPS signature.	Step 3 or Step 4
ID2	Apache HTTP Server 2.2.17 Through 2.2.21 Remote DoS via a Specially Crafted Cookie	Apache software version should be upgraded or it can be mitigated by the IPS signature.	Step 3 or Step 4
ID3	Allaire Jrun 2.3.x Sample Files Allows Files Disclosure and Code Execution	All sample code, example applications, tutorials, and documentation should be removed from the production servers or it can be mitigated by the IPS signature.	Step 3 or Step 4
ID4	Oracle 9iAS Allows Unauthenticated User Access To Sensitive Services	The Vulnerability should be mitigated by the IPS signature.	Step 4

Table 5-8: The Mitigation Steps and Solutions for the Security Vulnerabilities #2

ID	Definition	Solution	Steps
ID5	Apache HTTP Server 1.* and 2.* Remote Denial of Service via Partial HTTP Requests	Apache software version should be upgraded or it can be mitigated by the IPS signature.	Step 3 or Step 4
ID6	GoAhead WebServer Remote DoS Vulnerability via Partial HTTP Requests	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID7	Apache 2.2.11 and Prior mod_deflate Module Remote DoS Vulnerability	Operating system-based patch should be applied.	Step 3
ID8	PHP 5.2.11 and 5.3 Vulnerability Allows Remote Attackesr to Cause DoS via Multiple POST Requests	PHP version should be upgraded.	Step 3
ID9	PHP 5.3.x through 5.3.3 Remote Information Disclosure Vulnerability	PHP version should be upgraded.	Step 3
ID10	OpenSSL Remote DoS Vulnerability via a Malformed Record in a TLS Connection	OpenSSL version should be upgraded or it can be mitigated by the IPS signature.	Step 3 or Step 4
ID11	OpenSSL 1.0.1g and Earlier Remote DoS in do_ssl3_write Function - CVE-2014-0198	Operating system-based patch should be applied or it can be mitigated by the IPS signature.	Step 3 or Step 4

Table 5-9: The Mitigation Steps and Solutions for the Security Vulnerabilities #3

ID	Definition	Solution	Steps
ID12	PHP 5.2.11 and 5.3 Vulnerability Allows Remote Code Execution via LD_LIBRARY_PATH Crafted Value	PHP version should be upgraded.	Step 3
ID13	PHP 5.3.7 and 5.3.8 'is_a()' Remote File-Include Vulnerability	Operating system-based patch should be applied or it can be mitigated by the IPS signature.	Step 3 or Step 4
ID14	PHP 5.3.8 'zend_strndup' Function Flaw Allows Remote DoS via Crafted Input	Operating system-based patch should be applied.	Step 3
ID15	Apache Tomcat Before 5.5.35, 6.x Before 6.0.35, and 7.x Before 7.0.23 Hash Collision Remote DoS	Apache software version should be upgraded or it can be mitigated by the IPS signature.	Step 3 or Step 4
ID16	Apache Tomcat 7.0.* Allows Remote DoS via Partial HTTP Requests	The vulnerability should be mitigated by the IPS signature.	Step 4
ID17	PHP Prior to 5.3.6 Intl Extension Remote DoS Vulnerability via an Invalid Argument	PHP version should be upgraded.	Step 3
ID18	PHP 5.3.3 and Earlier NumberFormatter::getSymbol Integer Overflow Vulnerability	Operating system-based patch should be applied.	Step 3

Table 5-10: The Mitigation Steps and Solutions for the Security Vulnerabilities #4

ID	Definition	Solution	Steps
ID19	[cpujul2012-392727] PHP Before 5.3.9 Hash Collision Remote DoS Vulnerability	PHP version should be upgraded.	Step 3
ID20	FTP Server Accepts Anonymous Logins	Anonymous authentiation method should be disabled on the FTP server.	Step 3
ID21	Oracle Database XML DB Component Vulnerability	Relevant Oracle patch should be applied.	Step 3
ID22	[cpuapr2013-1899555, cpujuly2013-1899826] Apache HTTP Server mod_proxy_http Remote Information Disclosure Vulnerability via HTTP Requests	Apache software version should be upgraded.	Step 3
ID23	Oracle sqldemos Allows Access to the Demo Index Page	Access to the demo index page should be disabled.	Step 3
ID24	Apache HTTP Server Foreign Language Files Information Disclosure Vulnerability	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID25	Buffer Overflow in ApacheBench on Apache Web Server Enables Arbitrary Code Execution	Apache software version should be upgraded.	Step 3
ID26	Oracle Application Server SOAP Information Disclosure Vulnerability	The Vulnerability should be mitigated by the IPS signature.	Step 4

Table 5-11: The Mitigation Steps and Solutions for the Security Vulnerabilities #5

ID	Definition	Solution	Steps
ID27	[cpuapr2013-1899555] Apache Software Foundation 'mod_proxy' 2.2 through 2.2.11 Remote DoS Vulnerability	Operating system-based patch should be applied.	Step 3
ID28	PHP Prior to 5.2.10 JPEG Image Processing Remote DoS Vulnerability	PHP version should be upgraded.	Step 3
ID29	HTTP handlers in ASP.NET Remote Information Disclosure Vulnerability	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID30	PHP 5 Multiple Remote vulnerabilities Allows Information Disclosure, Code Execution and DoS	Operating system-based patch should be applied.	Step 3
ID31	PHP 5.3-5.3.3 Remote Information Disclosure or Arbitrary Code Execution Vulnerability	Operating system-based patch should be applied.	Step 3
ID32	PHP 5.2 - 5.2.13 and 5.3 - 5.3.2 Stack Consumption Vulnerability Allows Remote DoS	Operating system-based patch should be applied.	Step 3
ID33	PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3 Remote DoS Vulnerability via a Crafted ZIP Archive	Operating system-based patch should be applied.	Step 3
ID34	HP System Management Homepage before 6.3 Remote Privilege Escalation Vulnerability	The Vulnerability should be mitigated by the IPS signature.	Step 4

Table 5-12: The Mitigation Steps and Solutions for the Security Vulnerabilities #6

ID	Definition	Solution	Steps
ID35	PHP Remote Information Disclosure Vulnerability	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID36	OpenSSL 0.9.8 - 0.9.8y, 1.0.0 - 1.0.0l, 1.0.1 - 1.0.1g Remote Code Execution and DoS Vulnerability via Crafted DTLS ClientHello	OpenSSL version should be upgraded or it can be mitigated by the IPS signature.	Step 3 or Step 4
ID37	OpenSSL Before 1.0.0f GOST ENGINE Remote DoS Vulnerability via Crafted Data from a TLS Client	OpenSSL version should be upgraded.	Step 3
ID38	OpenSSL Before 0.9.8s and 1.x Before 1.0.0f Remote DoS Vulnerability via a Crafted X.509 Certificate	OpenSSL version should be upgraded.	Step 3
ID39	OpenSSL 0.9.8 - 0.9.8y, 1.0.0 - 1.0.0l, 1.0.1 - 1.0.1g Remote DoS Vulnerability with Anonymous ECDH Cipher Suite	OpenSSL version should be upgraded or it can be mitigated by the IPS signature.	Step 3 or Step 4
ID40	The substr_replace Function PHP 5.3.6 and earlier Remote Denial of Service Vulnerability	Operating system-based patch should be applied or it can be mitigated by the IPS signature.	Step 3 or Step 4

Table 5-13: The Mitigation Steps and Solutions for the Security Vulnerabilities #7

ID	Definition	Solution	Steps
ID41	Apache APR-util Before 1.3.10 Remote DoS Vulnerability via Unspecified Vectors	Operating system-based patch should be applied.	Step 3
ID42	HP System Management Homepage (SMH) Before 6.2 Remote Information Disclosure Vulnerability	HP SMH software version should be upgraded.	Step 3
ID43	Apache HTTP Server < 2.2.16 mod_cache and mod_dav Remote Denial of Service Vulnerabilities	Apache software version should be upgraded.	Step 3
ID44	[cpuapr2013-1899555] Apache HTTP Server 2.2.9 on Unix Remote Information Disclosure Vulnerability by Reading Responses	Apache software version should be upgraded.	Step 3
ID45	[cpujan2013-1515902] Apache Tomcat \ Oracle Fusion Middleware Inefficient Parameter Handling Allows Remote DoS	Apache software version should be upgraded.	Step 3
ID46	Buffer Overflow in OpenSSL Handling of ASCII Integer Representation Allows Arbitrary Code Execution	OpenSSL version should be upgraded.	Step 3

Table 5-14: The Mitigation Steps and Solutions for the Security Vulnerabilities #8

ID	Definition	Solution	Steps
ID47	PHP before 5.3.6 phar Extension Multiple Format String Vulnerabilities Allow Remote Code Execution	PHP version should be upgraded or it can be mitigated by the IPS signature.	Step 3 or Step 4
ID48	OpenSSL 0.9.8 - 0.9.8y, 1.0.0 - 1.0.0l, 1.0.1 - 1.0.1g Remote DoS Vulnerability via Crafted DTLS Handshake	OpenSSL version should be upgraded or it can be mitigated by the IPS signature.	Step 3
ID49	Apache Tomcat 7.0.0 - 7.0.27, 6.0.0 - 6.0.35 'parseHeaders()' Error Allows Remote DoS	Apache software version should be upgraded.	Step 3
ID50	[cpujul2012-392727] HP System Management Homepage (SMH) Before 7.0 Multiple Vulnerabilities	HP SMH software version should be upgraded or it can be mitigated by the IPS signature.	Step 3 or Step 4
ID51	OpenSSL Before 0.9.8s and 1.x Before 1.0.0f SGC Implementation Allows Remote DoS Vulnerability	OpenSSL version should be upgraded.	Step 3
ID52	[cpujul2009-091332] Jetty < 6.1.17 HTTP Server Remote Directory Traversal Vulnerability	Jetty software version should be upgraded.	Step 3
ID53	OpenSSL 0.9.8h-0.9.8q and 1.0.0-1.0.0c OCSP DoS Vulnerability via a Crafted 'ClientHello' Message	Operating system-based patch should be applied.	Step 3

Table 5-15: The Mitigation Steps and Solutions for the Security Vulnerabilities #9

ID	Definition	Solution	Steps
ID54	cURL libcurl Remote DoS Vulnerability via Crafted Compressed Data	cURL software version should be upgraded.	Step 3
ID55	PHP < 5.2.12 session.save_path Remote Arbitrary Code Execution Vulnerability	Operating system-based patch should be applied.	Step 3
ID56	OpenSSL Remote DoS and Database Write Vulnerability due to Use-After-Free in ssl3_release_read_buffer() - CVE-2010-5298	OpenSSL version should be upgraded.	Step 3
ID57	[cisco-sa-20030930-ssl] OpenSSL 0.9.6 and 0.9.7 ASN.1 inputs DoS	OpenSSL version should be upgraded or it can be mitigaetd by the IPS signature.	Step 3 or Step 4
ID58	OpenSSL 0.9.7 ASN.1 Encoding Allows DoS and Code execution	OpenSSL version should be upgraded it can be mitigated by the IPS signature.	Step 3 or Step 4
ID59	[cisco-sa-20030930-ssl] Integer Overflow in OpenSSL 0.9.6 and 0.9.7 ASN.1 Tag Values	OpenSSL version should be upgraded it can be mitigated by the IPS signature.	Step 3 or Step 4
ID60	DoS in Apache <=1.3.27 rotatelogs	Apache software version should be upgraded.	Step 3

Table 5-16: The Mitigation Steps and Solutions for the Security Vulnerabilities #10

ID	Definition	Solution	Steps
ID61	Oracle XSQL Servlet Sample Application Allows to Query the Database	Sample applications should be removed from the production servers or it can be mitigated by the IPS signature.	Step 3 or Step 4
ID62	BIND - Malicious modification of DNS records	The name server should be recompiled without - DALLOW_UPDATES option.	Step 3
ID63	Microsoft IIS Printers Virtual Directory Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID64	Microsoft Internet Information Services Scripts Virtual Directory Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID65	[cpujul2009-091332] Oracle Application Server and BEA Product Suite W3C XML Signature Syntax Remote Vulnerability	Relevant Oracle patch should be applied ot it can be mitigated by the IPS signature.	Step 3 or Step 4
ID66	SSL/TLS X.509 Self-Signed Certificate Obtained	The Vulnerability should be mitigated by the IPS signature.	Step 4

Table 5-17: The Mitigation Steps and Solutions for the Security Vulnerabilities #11

ID	Definition	Solution	Steps
ID67	[cpujul2009-091332] Oracle Database 10 - 10.1.8.3 Secure Enterprise Search Component Unspecified Vulnerability	Relevant Oracle patch should be applied it can be mitigated by the IPS signature.	Step 3 or Step 4
ID68	Oracle 9i Application Server Path Revealing Vulnerability	The product should be upgraded.	Step 3
ID69	Oracle 9i Application Server Allows Information Disclosure	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID70	OpenSSL <=1.0.0l ECDSA Remote Information Disclosure Vulnerability via FLUSH+RELOAD Cache	Operating system-based patch should be applied.	Step 3
ID71	[cpujul2012-392727] Apache HTTP Server 'mod_proxy' Remote Security Bypass Vulnerability	Operating system-based patch should be applied.	Step 3
ID72	SSL Certificate has Expired	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID73	TLS/SSL Server X.509 Certificate MD5 Signature Detected	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID74	Microsoft Internet Information Services was Detected on the Host	The Vulnerability should be mitigated by the IPS signature.	Step 4

Table 5-18: The Mitigation Steps and Solutions for the Security Vulnerabilities #12

ID	Definition	Solution	Steps
ID75	[cpujul2009-091332] Oracle Application Server 10 - 10.1.2.3 HTTP Server Component Unspecified Vulnerability	Relevant Oracle patch should be applied.	Step 3
ID76	SSL/TLS Server Preferred CipherSuite Detection	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID77	Oracle Application Server Oracle HTTP Server Component Unspecified Remote Vulnerability	Relevant Oracle patch should be applied.	Step 3
ID78	HTTP Version Obtained via Web Server	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID79	Web Server HTTP TRACE Method Enabled	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID80	FTP Server Detected on the Host	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID81	McAfee ePolicy Orchestrator is Running	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID82	Oracle Application Server Oracle Portal Component Unspecified Remote Vulnerability	Relevant Oracle patch should be applied.	Step 3

Table 5-19: The Mitigation Steps and Solutions for the Security Vulnerabilities #13

ID	Definition	Solution	Steps
ID83	TLS-SSL Server Untrusted X.509 Certificate Detection	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID84	Oracle Enterprise Manager Web Console Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID85	Microsoft Internet Information Services NTLM Authentication is Disabled on the Host	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID86	Siebel SimBuilder Component in Oracle Siebel Enterprise Multiple Vulnerabilities	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID87	Oracle Secure Enterprise Search or Ultrasearch Component Remote Unspecified Vulnerability DB04	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID88	[cpujan2008-086860] Oracle PeopleTools Critical Patch Jan. 2008: Unspecified Vulnerabilities [PSE01, PSE03, PSE04]	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID89	WWW Server Hidden Name Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID90	Oracle Database 9.0.1.5 FIPS+, 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.3 Multiple Vulnerabilities	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4

Table 5-20: The Mitigation Steps and Solutions for the Security Vulnerabilities #14

ID	Definition	Solution	Steps
ID91	Microsoft Internet Information Services Anonymous Access is Enabled	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID92	Oracle Application Express in Oracle Application Express 3.0.1 Unspecified Vulnerability APEX02	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID93	Oracle Application Server and Collaboration Suite Vulnerability in the Oracle Containers for J2EE	Relevant Oracle patch should be applied.	Step 3
ID94	SSL Certificates with a Short Public Key Are Used by the Web Server	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID95	Disabled Microsoft IIS Basic Authentication Scheme was Detected on the Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID96	[cpujul2010-155308] Oracle Database Server Application Express Component Remote Vulnerability via Unknown Vectors	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID97	Oracle Database Vault Component Unspecified Remote Vulnerability	Relevant Oracle patch should be applied.	Step 3
ID98	TLS/SSL Enumeration of X.509 Certificate Fields	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4

Table 5-21: The Mitigation Steps and Solutions for the Security Vulnerabilities #15

ID	Definition	Solution	Steps
ID99	Oracle Portal Component in Oracle Application Server Unspecified Vulnerability	Operating system-based patch should be applied or it can be mitigated by the IPS signature.	Step 3 or Step 4
ID100	SSL/TLS X.509 Certificate Server Name and Common Name Mismatch	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID101	Microsoft IIS "Use Host Header Name" Setting is Disabled on the Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID102	Oracle Database and Enterprise Manager Database Control component Unspecified Vulnerability	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID103	Web Server with Broken Links Has Been Detected	The Vulnerability should be mitigated by the WAF solution.	Step 4
ID104	Oracle E-Business Suite 11.5.10.2 , 12.0.4 Multiple Unspecified Vulnerabilities	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID105	SSL Server Information was Detected in the Host	The Vulnerability should be mitigated by the WAF solution.	Step 4

Table 5-22: The Mitigation Steps and Solutions for the Security Vulnerabilities #16

ID	Definition	Solution	Steps
ID106	Microsoft NetBIOS Names Information Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID107	Oracle E-Business Suite 11.5.10.2 Multiple Unspecified Vulnerabilities APP01, APP10, APP05	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID108	NetBIOS Null Session Enabled	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID109	SSL Supported Cipher Suite Has Been Detected on the host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID110	Oracle Dynamic Monitoring Service in Oracle Application Server Unspecified Vulnerability AS02	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID111	Web Server Redirection Status was Detected on the Host	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID112	Oracle Application Server and Collaboration Suite Oracle Portal Component Remote Vulnerability	Relevant Oracle patch should be applied.	Step 3

Table 5-23: The Mitigation Steps and Solutions for the Security Vulnerabilities #17

ID	Definition	Solution	Steps
ID113	Enumerated Microsoft IIS Server Extensions were Detected on the Host	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID114	Microsoft SQL Server Authentication Mode Is Reported	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID115	Microsoft IIS Script Mapping Configuration Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID116	A database service is running, e.g. a SQL server, Oracle, or MySQL.	The Vulnerability should be mitigated by the WAF solution.	Step 4
ID117	Oracle Portal Component in Oracle Application Server 9.0.4.3 Unspecified vulnerability AS03	The Vulnerability should be mitigated by the WAF solution.	Step 4
ID118	Enumerated Microsoft SQL Server Instances Detection	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID119	Oracle Application Server and Collaboration Suite Oracle Portal Component Unspecified Vulnerability	Relevant Oracle patch should be applied.	Step 3

Table 5-24: The Mitigation Steps and Solutions for the Security Vulnerabilities #18

ID	Definition	Solution	Steps
ID120	Anonymous Authentication is Enabled on the SSL Server	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID121	Testing, Temporary, or Default Web Server Welcome Page were Found on the Server	The default welcome and test pages should be removed.	Step 3
ID122	Oracle Application Server, Database and Enterprise Manager Vulnerability in Oracle Help for Web	Relevant Oracle patch should be applied.	Step 3
ID123	Clear-Text SSL Communication Support Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID124	[MS03-034] NetBT Name Service in Windows NT 4.0, 2000, XP, and Server 2003 Allows Information Disclo	Appropriate Microsoft patch should be applied.	Step 3
ID125	NetBIOS Bindings Information Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID126	Oracle Application Server and Collaboration Suite Portal Component Unspecified Vulnerability	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4

Table 5-25: The Mitigation Steps and Solutions for the Security Vulnerabilities #19

ID	Definition	Solution	Steps
ID127	SSH Protocol Supported Version Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID128	Apache htpasswd Buffer Overflow Vulnerability	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID129	WebDAV Extensions are Installed on Server	If the use of Webdav is not required, it should be disabled.	Step 3
ID130	Oracle 9i Application Server Multiple Sample Pages Remote Information Disclosure Vulnerability	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID131	Microsoft Windows IIS ASP.NET Product Version was Detected	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID132	SSL Web Server Version Information has been Obtained	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID133	PHP < 5.2.11 Unspecified Vulnerability Related to "Missing Sanity Checks around Exif Processing"	PHP version should be upgraded.	Step 3

Table 5-26: The Mitigation Steps and Solutions for the Security Vulnerabilities #20

ID	Definition	Solution	Steps
ID134	PHP enable_dl Option is Activated on the Remote Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID135	OpenSSL 0.9.8h-0.9.8j CMS_verify Function Security Bypass Vulnerability	OpenSSL version should be upgraded.	Step 3
ID136	The Session Extension feature of PHP Remote Security Bypass Vulnerability	PHP version should be upgraded.	Step 3
ID137	Apache HTTP Server OS Information Disclosure Vulnerability	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID138	PHP Display_Errors Directive Setting is "ON" on the Host	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID139	PHP File_Uploads Option is Enabled on the Host.	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID140	PHP Safe_Mode Option is Disabled on the Host	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4

Table 5-27: The Mitigation Steps and Solutions for the Security Vulnerabilities #21

ID	Definition	Solution	Steps
ID141	PHP file phpinfo.php Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID142	PHP < 5.2.11 Unspecified Vulnerability in the Imagecolortransparent Function	PHP version should be upgraded.	Step 3
ID143	SMTP Server Connection are Allowed on the Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID144	PHP before 5.2.11 php_openssl_apply_verification_policy Function Unspecified Vulnerability	PHP version should be upgraded.	Step 3
ID145	HP System Management Homepage (SMH) Before 7.3 Remote Information Disclosure Vulnerability	HP SMH software version should be upgraded.	Step 3
ID146	OpenSSL 0.9.8 - 0.9.8y, 1.0.0 - 1.0.0l, 1.0.1 - 1.0.1g Remote Man-in-the-middle Attack (CCS Injection Vulnerability)	Operating system-based patch should be applied or it can be mitigated by the IPS signature.	Step 3 or Step 4
ID147	Apache JServ Protocol Connector was Detected on the Host	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4

Table 5-28: The Mitigation Steps and Solutions for the Security Vulnerabilities #22

ID	Definition	Solution	Steps
ID148	SSL Server Supporting Weak Encryption Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID149	Microsoft SQL Server UDP 1434 Database Instance TCP Information Disclosure	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID150	Fopen_wrappers.c in PHP 5.3.0-5.3.3 Remote Open_basedir Restrictions Bypass Vulnerability	Operating system-based patch should be applied.	Step 3
ID151	The default Error Page Version for Apache Tomcat Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID152	SSL/TLS Supports DEFLATE Compression	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID153	Apache Tomcat Remote Security Bypass due to HTTP Digest Caching Information about Users	Operating system-based patch should be applied.	Step 3
ID154	Apache Tomcat Remote Security Bypass due to HTTP Digest Tracking cnonce Instead of nonce and nc	Operating system-based patch should be applied.	Step 3

Table 5-29: The Mitigation Steps and Solutions for the Security Vulnerabilities #23

ID	Definition	Solution	Steps
ID155	Apache Tomcat Remote Security Bypass due to HTTP Digest Improperly Checking for Stale Nonce Values	Operating system-based patch should be applied.	Step 3
ID156	SMTP Service Detection	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID157	HTTP Server that Handles Session using Set-Cookie Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID158	Default Installation Page Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID159	Microsoft Terminal Service Has Not Been Configured Network Level Authentication	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID160	SSL Certificate Key Length Less Than 1024 Bits	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID161	WebDAV Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4

Table 5-30: The Mitigation Steps and Solutions for the Security Vulnerabilities #24

ID	Definition	Solution	Steps
ID162	Service Location Protocol Service Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID163	Microsoft SharePoint Server Has Been Detected	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID164	Microsoft ASP.NET State Service Has Been Detected	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID165	Microsoft IIS Tilde Character Short File Name Disclosure (142982)	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID166	DNS Cache Snooping Vulnerability	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID167	DNS Server Cache Allows Snooping on the Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID168	DNS Server Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4

Table 5-31: The Mitigation Steps and Solutions for the Security Vulnerabilities #25

ID	Definition	Solution	Steps
ID169	DNS Spoofed Request Amplification Has Been Detected	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID170	DNS Server With DNSSEC Aware Resolver Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID171	Microsoft Windows NETBIOS Anonymous Accessible Shares Detected	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID172	Microsoft Internet Information Services IISADMPWD Virtual Directory Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID173	Microsoft IIS MSADC Virtual Directory Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID174	NTP <4.2.7p26 Remote DoS Vulnerability via Forged REQ_MON_GETLIST Request	NTP software version should be upgraded or it can be mitigated by the IPS signature.	Step 3 or Step 4
ID175	Remote FTP Server with Clear Text Authentication Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4

Table 5-32: The Mitigation Steps and Solutions for the Security Vulnerabilities #26

ID	Definition	Solution	Steps
ID176	Weak SSL Ciphers Detected	Support for the low encryption ciphers should be disabled.	Step 3
ID177	SSH2 Server Weak Key Exchange Algorithm or Symmetric Cipher	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID178	OpenSSL Before 0.9.8s and 1.x Before 1.0.0f DTLS Implementation Allows Remote Information Disclosure	Operating system-based patch should be applied.	Step 3
ID180	Check Point FireWall-1 with ICA Service Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID181	A NTP Server Has Been Detected on the Host	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4

As can be seen from the test results, there is no security vulnerability that the framework cannot cover. Of course, this does not mean that the framework can solve all the security gaps of the web service architecture. However, it is of paramount importance that the information security framework shows the essential methodology in order to cover security violations.

With respect to the test environment and test results, the solution steps are analyzed for all the security vulnerabilities obtained and a different result from the most dangerous software errors stated by Common Weakness Enumeration was obtained.

With respect to the steps for the solution procedure, 35 percent of the software errors are mitigated by the solution procedure in step 3, 8 percent of the software errors are mitigated by the solution procedure in step 4 and 12 percent of the software errors are mitigated by the solution procedures in both step 3 and step 4. These results show us that the real time environment may differ from the predefined software errors. Nevertheless, both of the results indicate that the information security framework proposed is apparently one of the best solutions for the web services security.

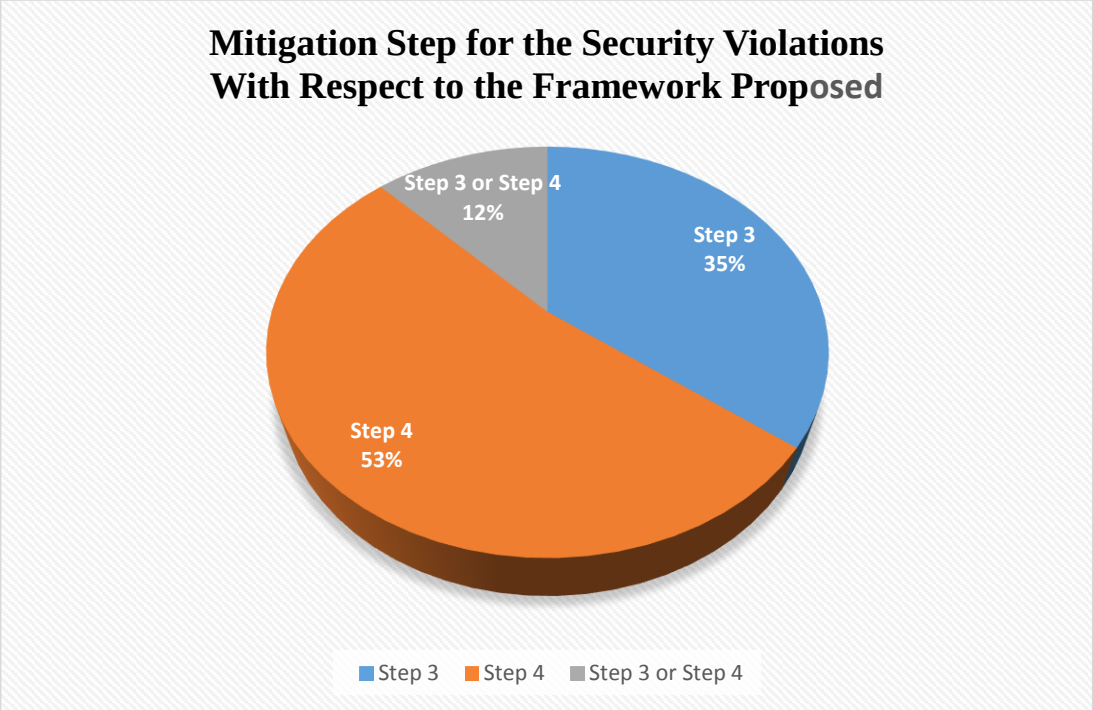


Figure 5-2: Mitigation Steps for the Security Violations With Respect to the Framework Proposed

5.3. CASE STUDIES

In this part, the main aim is to clarify the role of the information security framework proposed against sample scenarios. In this manner, 5 different case studies are considered. With regards to these case studies the results with and without the information security framework are evaluated.

5.3.1. Case Study 1

Assume that there is an institutional web page of a governmental institution, which is www.abc.gov.tr. There is administrative access through the web page that anyone can access from both outside the local network and inside the local network. In order to perform and attack, the user is supposed to get www.abc.gov.tr/admin.aspx. In this case, the main page of the web service was defaced with a note "It is too late for the security."

Table 5-33: Web Page Defacement

Case Study 1	
Attack Target:	Corporate Web Server
Attack Method:	Exploiting Administrative Console
Attack Result:	Web Page Defacement
Solution Stated In the Framework:	Restricting Administrative Access to Web Server
How the Solution is Provided:	Access Restriction by the Web Service Software, Access Restriction by the Firewall Rule, Blocking by the IPS policy, Blocking by the WAF policy.
Mitigation Steps	Step 3 or Step 4

In this case, since there is no protection provided for the administrative access, it is most probable that the attacker can exploit the administrative access and thereafter deploy the defacement content.

For such a case study, if administrative access is provided by a different port, firewall policy can be configured for only administrative staff to access from either outside the network or inside the network, initially. If the administrative access is provided with

the same port which provides the web service access, IPS policy or WAF policy can be configured for only administrative staff to access the relevant URI of the web service such as admin.php or ws-admin.html. In addition to this, administrative access can also be limited by the required configuration of the service provider such Microsoft Internet Information Services or Apache Tomcat. As can be understood, the framework covers this scenario within both step 3 and step 4 which are Analyze Security, Performance Metrics of the Web Service and Perform and Complete Security Requirements/Metrics, respectively.

5.3.2. Case Study 2

Assume that there is a company which serves online shopping from all around the world. The user access to the web service is performed via an HTTP connection, namely; plain-text traffic. It is supposed to perform penetration test in order to analyze and cover the current status of the web service but no penetration test has been performed so far. In this case, the information of all the users who are member of this company was obtained by the hacker group "BarikatPro".

Table 5-34: SQL Injection Attack

Case Study 2	
Attack Target:	Company Web Server
Attack Method:	SQL Injection Attack
Attack Result:	Exploiting Financial Information of Registered Users
Solution Stated In the Framework:	Blocking SQL Injection Attacks
How the Solution is Provided:	Parameter filter in the source code Blocking by the WAF policy.
Mitigation Steps	Step 3 or Step 4

In this case study, since there is no protection provided for the SQL injection attacks, it is most probable that the attacker can exploit the system by an SQL injection parameter and thereafter exploit all the user information including financial data from the database which was integrated with the web server.

For such a case study, since there has been no penetration test performed for the web services, the IT staff does not know any security vulnerability which the web server architecture has. In this case, if the relevant security vulnerabilities were known, then required security measurements and protections would have been taken in advance. In this manner, having considered such a scenario, the enterprise networks should perform penetration tests in order to determine their security vulnerabilities. Within the discovered security vulnerabilities, the relevant IT staff is supposed to know which actions should be taken. Firstly, parameter filtering in the source code and secondly activating web application security policies in the web application firewalls should be performed for such a scenario. As can be understood, the framework covers this scenario within both step 3 and step 4 which are Analyze Security, Performance Metrics of the Web Service and Perform and Complete Security Requirements/Metrics, respectively.

5.3.3. Case Study 3

Assume that there is an organization which provides weather information to the citizens. There is a 100 Mbps bandwidth for the organization provided by the internet service providers. Sometimes, bandwidth utilization reaches or exceeds 100 Mbps. In this case, the organization cannot provide weather information due to the high bandwidth utilization caused by Distributed Denial of Service (DDoS) attacks.

Table 5-35: Distributed Denial of Service (DDoS) Attacks

Case Study 3	
Attack Target:	Organization Web Server
Attack Method:	Distributed Denial of Service (DDoS) attacks
Attack Result:	Outage of the Weather Information
Solution Stated In the Framework:	Blocking DDoS-based Connections
How the Solution is Provided:	DDoS Service from Internet Service Provider, Activating Behavioral Protection by DDoS Protector, Activating and Tuning DoS protection by IPS policy, Connection Limiting by Firewall Configuration
Mitigation Steps	Step 4

This case study mainly focuses on the industry-based security solutions. The main purpose of this attack is to make the service unavailable. For this purpose, the attacker generates more traffic than the infrastructure of the organization can handle. The traffic may include SYN flood attacks, teardrop attacks, peer-to-peer attacks, etc.

For this case, only the security measurements or requirements performed inside the infrastructure may not be sufficient. The main reason is that the attacker intends to saturate the internet bandwidth of the organization so that the organization cannot give any service to the world. In such a scenario, one can observe that all the web services are accessible from the local network. However, these services are not accessible from outside the infrastructure. For this reason, mainly internet service provider (ISP) based protection is required. In today's world, internet service providers can provide this

security services. With the help of this security service, the internet bandwidth of the organization will not be saturated. Thereafter, further security measurements have to be taken in order to provide defense in depth. ISP based DDoS protection will not be under the control of the IT staff. In this manner, another DDoS protection can be handled by the organization. With the help of the DDoS protector the organization has behavioral protection can be performed. In other words, the DDoS protector analyzes the traffic of the organization and detects abnormal traffic in case of such a scenario. In order to detect such a traffic, pre-defined signatures or automatically generated signatures can be used. Moreover, IPS sensor can be deployed behind the DDoS protector. IPS sensor also performs DDoS protection against such kind of attacks. In this manner, required IPS policies are created and activated. Finally, connection limiting can be performed in the firewall so that the number of connection which such kind of attack causes can be limited. As a result of this, the traffic that includes the access to the web service passes through ISP DDoS protection, DDoS protector, IPS sensor and the firewall, respectively and layered security can be provided in this perspective. As can be understood, the framework covers this scenario within step 4 which is Perform and Complete Security Requirements/Metrics.

5.3.4. Case Study 4

Assume that there is a governmental institution where there is only one web service which provides institutional information. That is to say, there is a static web page. For the remote maintenance of the web page by the support company, the security administrator allows anyone outside the network access via the Microsoft Remote Desktop Connection and also SMB. It is also allowed to access local network from the web server. In this case, all the staff information of the institution was obtained due to the remote access to the web server.

Table 5-36: Operating System Based Access

Case Study 4	
Attack Target:	Corporate Web Server
Attack Method:	Operating System Based Access
Attack Result:	Outage of the Corporate Staff Information
Solution Stated In the Framework:	Blocking RDP and SMB Access
How the Solution is Provided:	Blocking RDP and SMB Access by the Firewall Policy, Deploying Anti-Virus Agent on the Web Server and Assigning Anti-Virus Policy, Deploying Host IPS Agent and Assigning Firewall Policy
Mitigation Steps	Step 4

This case is related to another type of administrative access. As can be understood from the scenario, this access was allowed for the purpose of remote maintenance. However, the attacker discovered this security vulnerability and obtained all the staff information. The attacker initially detected this access and uploaded a tool which was Mimikatz.exe to the web server in order get the logon information of the users who accessed to this web server.

First of all, there should be no such access from outside the organization infrastructure. If it is necessary, then there should be source IP restriction. In other words, only the source IP from which the access is required should be allowed. Furthermore, operating

system based activities should also be controlled in case of any harmful activity. The tool Mimikatz.exe is used to obtain the information stored temporarily to the read access memory (RAM) of the server. With the help of this tool, attacker obtains the logon information of the users. In this manner, anti-virus agent should deployed and essential anti-virus policies should be assigned. In this scenario, after the attacker obtains the logon information of the user, actually he gains access to the domain controller of the infrastructure by using the logon information of the staff who has administrative privileges. Now the attacker may access another server from this web server. Corporate firewall can block the traffic passing through itself. However, the firewall cannot block since the attacker access is in the same network. Because of this, detailed access lists can be created by the Host IPS agent. By means of this, the attacker access to another server on the same network can be blocked. Smooth firewall policies, anti-virus policies and host based IPS policies can prevent such a situation. As can be understood, the framework covers this scenario within step 4 which is Perform and Complete Security Requirements/Metrics.

5.3.5. Case Study 5

Assume that there is a revenue agency that governs and administers tax laws for the related country. In this agency, the web servers are not periodically maintained and also upgraded when necessary. In this case, the confidential information of taxpayers of the agency was obtained through the web server due to the Heartbleed attack.

Table 5-37: Heartbleed Vulnerability

Case Study 5	
Attack Target:	Corporate Web Server
Attack Method:	Heartbleed Bug
Attack Result:	Outage of the Confidential Information of the Taxpayers
Solution Stated In the Framework:	Mitigating the Heartbleed Vulnerability
How the Solution is Provided:	Applying Heartbleed Fix To the Relevant Systems
Mitigation Steps	Step 1, Step 3 or Step 4

In this case study, exploitation of the Heartbleed vulnerability occurs. All the assets in an infrastructure are supposed to be renewable. In other words, technological variations should be applied to all the systems.

The attacker detects Heartbleed vulnerability in the HTTPS connection which is contributed by the OpenSSL. Though the connection is secure, in other words, encrypted; the attacker can get the information of the existing connections. Shortly, attacker can get the logon information of the taxpayers including username and passwords. Such a case shows us that security concept is not steady. It should be updated and reviewed regularly with respect to today's growing cyber security threads. In this manner, for all the components that provides HTTPS service, HTTPS inspection should be applied for the Heartbleed fix. The components may be the web service itself, the load balancer that performs HTTPS service and application delivery service, IPS sensor or web application firewall that may perform HTTPS inspection. In order to perform such kind of mitigation, the IT staff should be informed by the IT vendors about the progress of information technologies and information technologies security. Otherwise, it seems impossible to perform required mitigations. As can be understood, the framework covers this scenario within step 1, step 3 and step 4 which are Create

All the Required Security Steps, Analyze Security, Performance Metrics of the Web Service and Perform and Complete Security Requirements/Metrics, respectively.

CHAPTER 6

6. CONCLUSIONS

In this chapter, summary of the work done so far and the major contributions of the study will be discussed. Finally, the chapter ends with the recommendations for further research.

6.1. SUMMARY OF THE WORK DONE

In this study, the state-of-the-art information security framework for the web services was evaluated and classified into five categories after an overview of web services and security engineering. The role of the information security framework, as well as the benefits and the drawbacks of each step were presented. The validation of the framework was performed by considering the most dangerous software errors and the security vulnerabilities obtained in the test environment and considering the actions to be taken for the case studies stated in this study.

For the web services security, the required measurements are not considered as a whole in other studies. Since the security aspect essentially requires all the components in this manner, all the building blocks are combined into one platform which forms the proposed information security framework.

As part of the proposed information security, the penetration tests, vulnerability management and code review for the security gaps are initial measurements in order to identify what is going to be protected or what is supposed to be secure. For this manner, all the analysis of the web server assets are stated in order to determine the

security gaps existing. With respect to the security gaps discovered, the solution methodologies in order to mitigate are expressed.

Industry based security solutions are especially stated in this study. The main reason for this is that all the security requirements cannot be fulfilled by the actions taken by the web service assets themselves. The role of web services is mainly to give the exact service required from them. On the other hand, it is stated that all the security gaps cannot be mitigated by the web server assets themselves. It has appeared that the remarkable number of the security gaps can be mitigated by the industry based security solutions. In this manner, a different perspective should be expected for the security concept. As a result of this, the expectations from the industry based security solutions for the aim of web service security are stated clearly.

The continuity of the information security framework was also stated as the final part of the framework. The main aim here is that the framework should renew itself regularly. The continuity should be provided by the validation of the initial steps of the framework and renewing the steps within a periodic cycle since web services technology will not remain constant and will be developed regularly.

The effectiveness of the framework was tested under two different categories. Firstly, worldwide dangerous software errors was considered. How the information security framework would cover these was explicated. Thereafter, the information security framework was evaluated for the risk assessment results obtained in the test environment. In both situations, the results are clear and show the framework's efficiency so as to cover the security aspects. Secondly, case studies were stated and what could be done for these case studies with respect to the information security framework was discussed. Case studies stated in this study were the real experiences that the author has witnessed as a security field engineer. With the help of these experiences, another major profit of the information security framework was provided.

In this study, the methodologies for all the steps were presented. This study does not cover full technical details for all the steps. The study explicates an overall approach for the web services security. Nevertheless, this study is a significant guide for IT staff who are responsible for the continuity and security of the web services of an enterprise network. The major advantages brought by this framework are:

- The creation of the organizational intellect over the web services that will enhance web services security awareness,
- The increase in the security level of the web services,
- The security continuity of the web services.

This study also provides additional advantages such as:

- Identification of technical problems,
- Decrease in response time to the security incidents that may occur.

Having performed required prerequisites, this information security framework can easily be implemented in any enterprise network. The continuity is one of the main requirements. The procedures stated should be considered as implementation costs.

Proposing this information security framework to enterprise networks will be a powerful method and a first step guidance for the web service security in the enterprise networks, especially in governmental institutions and enterprise organizations.

6.2. FUTURE WORK

There are many concepts that can be added to the proposed framework as future work. First of all, we should not forget that the security aspect does not remain constant. Security aspect should be renewable, updated as the information technologies are developed as the necessities of the people increase day by day.

New security vulnerabilities are discovered each day. Hence, the security gaps on the assets never remain constant. In this manner, vulnerability exploitation methods also progress in the meanwhile. As a result of this, analyzing security metrics of the web services can be enhanced. New security terminology such as web application scanner, which is not yet common, is one of the examples for this situation.

The industry based security solutions presented in the framework are the common ones in today's technology. However, considering that there were no such security concepts ten years ago, this concept will regularly update itself. As a result, industry based security solutions may be altered. Because of this, performing and completing security requirements/metrics step can be extended.

As more progress have been performed in cloud computing, providing web services with the help of Representational State Transfer (REST) can be considered. In this manner, security concept in the cloud computing should be considered, as well.

On the other hand, an automated tool, software or software collection can be developed in order to cover the information security framework, which would automize the activities in this framework that would normally be carried out by the IT staff.

REFERENCES

Amazon Web Services, Inc. (2015). Websites & Website Hosting

Antunes, N., Vieira, M. (2014). Penetration Testing For Web Services, Computer Magazine 2 (47): 30-36, IEEE Computer Society.

Barna, C., Shtern, M., Smit, M., Tzerpos, V., Litou, M. (2014). Mitigating DoS Attacks Using Performance Model-Driven Adaptive Algorithms, ACM Transcations on Autonomous and Adaptive Systems 9 (1): Track 3

Berger, B., J., Sohr, K., Koschke R. (2013). Extracting and Analyzing the Implemented Security Architecture of Business Applications, European Conference on Software Maintenance and Reengineering: 37.

Booth, D., Haas, H., McCabe, F., Newcomer, E., Champion, M., Ferris, C., Orchard, D. (2004). Web Services Architecture, World Wide Web Consortium. http://www.w3.org/TR/ws-arch/#whatis

Charles, K. (2008). Information Security Overview from http://kellepcharles.blogspot.com.tr/2008/01/information-security-overview.html

eBay Inc. (2014). “eBay Inc. Ask eBay Users To Change Passwords” from http://announcements.ebay.com/2014/05/ebay-inc-to-ask-ebay-users-to-change-passwords/

eBay Inc. (2014). “Important – please change your eBay password” from http://announcements.ebay.com/2014/05/important-please-change-your-ebay-password/

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., Robinson, W. (2008). Performance Measurement Guide For Information Security, National Institute of Standards and Technology.

Dempsey, K., Chawla, N., S., Johnson, A., Johnston, R., Jones, A., C., Orebaugh., A., Scholl, M., Stine, K. (2011). Information Security Monitoring (ISCM) for Federal Information Systems and Organizations, National Institute of Standards and Technology.

Gülcanlı, Z., (2012). “Redhack bu kez Dışişleri'ni hack'ledi” from http://www.hurriyet.com.tr/planet/20904391.asp

Glenn, M. (2003). A Summary of DoS/DDoS Prevention, Monitoring, and Mitigation Techniques in Service Provider Environment, SANS Institute Reading Room Site.

Hong, Y., R., Kim, D. (2014). Content-based Control of HTTPs Mail for Implementation of IT-convergency Security Environment, J Intell Manuf 25: 231-239

Imperva Inc. (2012). Imperva's Hacker Intelligence Summar Report from http://www.imperva.com/docs/HII_The_Anatomy_of_an_Anonymous_Attack.pdf

Imperva Inc. (2014). Database Security – Audit and Protect Critical Databases from http://www.imperva.com/docs/DS_Database_Security.pdf

International Organization for Standardization. (2014). Information Security Management http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

Martin B., Brown, M., Paller, A., Kirby D. (2011). 2011 CWE/SANS Top 25 Most Dangerous Software Errors, Common Weakness Enumeration from http://cwe.mitre.org/top25/

Masood, A. (2013). Cyber Security for Service Oriented Architectures in a Web 2.0 World: An Overview of SOA Vulnerabilities in Financial Services, Technologies for Homeland Security (HST): 1-6, IEEE Computer Society.

Meier, J., D., Farre, C., Bansode, P., Barber, S., Rea, D. (2007). Load-Testing Web Applications, Microsoft Patterns & Practices, Chapter 17.

Mell, P., Kent, K., Nusbaum, J. (2005). Guide to Malware Incident Prevention and Handling, National Institute of Standards and Technology.

Mell, P., Bergeron, T., Henning, D. (2005). Creating a Patch and Vulnerability Management Program, National Institute of Standards and Technology.

Munadi, R., Fajri, T., S., Meutia, E., D., Elizar. (2013). Analysis of SQL Injection Attack In Web Service (A Case Study of Website In Aceh Province), 3rd International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME): 431-435, IEEE Computer Society.

Newcomer, E. (2002). Understanding Web Services – XML, WSDL, SOAP, and UDDI, Addison-Wesley Professional

Open Web Application Security Project. (2013). Static Code Analysis from https://www.owasp.org/index.php/Static_Code_Analysis#Description

Open Web Application Security Project. (2014). Web Application Firewall from https://www.owasp.org/index.php/Web_Application_Firewall

Petukhov, A., Kozlov, D. (2008). Detecting Security Vulnerabilities in Web Applications Upensing Dynamic Analysis with Penetration Testing, Application Security Conference, OWASP.

Ross, R., Katzke, S., Johnson, A., Swanson, M., Stoneburner, G., Rogers, G., Lee, A. (2009). Recommended Security Controls for Federal Information Systems, National Institute of Standards and Technology.

Scarfone, K., Hoffman, P., Souppaya, M. (2009). Guide To Enterprise and Remote Access Security, National Institute of Standards and Technology.

Scarfone, K., Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems, National Institute of Standards and Technology.

Scarfone, K., Souppaya, M., Cody, A., Orebaugh, A. (2008). Technical Guide to Information Security Testing and Assessment, National Institute of Standards and Technology.

Social Engineer, Inc. (2014). The Social Engineering Framework from http://www.social-engineer.org/framework/general-discussion/social-engineering-defined/

Social Engineer, Inc. (2014). The Social Engineering Infographic from http://www.social-engineer.org/social-engineering/social-engineering-infographic/

Sommerville, I. (2007). Software Engineering, Addison-Wesley.

Uma, E., Kannan, A. (2014). Improved Cross Site Scripting Filter for Input Validation Against Attacks in Web Services, Kuwait J. Sci. 41 (2): 175-203

Tracy, M., Jansen, W., Scarfone, K., Winograd, T. (2007). Guidelines on Securing Public Web Servers, National Institute of Standards and Technology.

Vacca, J., R. (2013). Computer and Information Security Handbook, Second Eddition, Morgan Kaufmann.

Zhang, X., Hou, Y., Ma, J. (2013). Survey on the Web Services Security Specifications from http://www.scientific.net/AMR.655-657.1809

APPENDICES

A: Detailed Risk Analysis Report of the Test Environment

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
ID 1	[cpujul2012-392727,cpujuly 2013-1899826] Apache APR before 1.4.4 Remote DoS due to Infinite Recursion Condition in 'apr_fnmatch()'	SBV-31427	CVE-2011-0419	http	High	7.8	Apache software version should be upgraded.	Step 3 or Step 4
ID 2	Apache HTTP Server 2.2.17 Through 2.2.21 Remote DoS via a Specially Crafted Cookie	SBV-34339	CVE-2012-0021	http	High	7.8	Apache software version should be upgraded.	Step 3 or Step 4
ID 3	Allaire Jrun 2.3.x Sample Files Allows Files Disclosure and Code Execution	SBV-00808	CVE-2000-0539	http	High	7.5	All sample code, example applications, tutorials, and documentation should be removed	Step 3 or Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
							from the production servers.	
ID 4	Oracle 9iAS Allows Unauthenticated User Access To Sensitive Services	SBV-00867	CVE-2002-0563	http	Medium	5.0	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID 5	Apache HTTP Server 1.* and 2.* Remote Denial of Service via Partial HTTP Requests	SBV-37162	CVE-2007-6750	http	High	7.8	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 3 or Step 4
ID 6	GoAhead WebServer Remote DoS Vulnerability via Partial HTTP Requests	SBV-34796	CVE-2009-5111	http	High	7.8	The Vulnerability should be mitigated by	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
							the IPS or WAF signature .	
ID 7	Apache 2.2.11 and Prior mod_deflate Module Remote DoS Vulnerability	SBV-22817	CVE-2009-1891	http	High	7.8	Operating system-based patch should be applied.	Step 3
ID 8	PHP 5.2.11 and 5.3 Vulnerability Allows Remote Attackesr to Cause DoS via Multiple POST Requests	SBV-24273	CVE-2009-4017	http	Medium	5.0	PHP version should be upgraded .	Step 3
ID 9	PHP 5.3.x through 5.3.3 Remote Information Disclosure Vulnerability	SBV-28144	CVE-2010-4156	http	Medium	5.0	PHP version should be upgraded .	Step 3
ID 10	OpenSSL Remote DoS Vulnerability via a Malformed	SBV-25181	CVE-2010-0740	http	Medium	5.0	OpenSSL version should be upgraded .	Step 3 or Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	Record in a TLS Connection							
ID 11	OpenSSL 1.0.1g and Earlier Remote DoS in do_ssl3_write Function - CVE-2014-0198	SBV-44372	CVE-2014-0198	http	Medium	5.0	Operating system-based patch should be applied.	Step 3 or Step 4
ID 12	PHP 5.2.11 and 5.3 Vulnerability Allows Remote Code Execution via LD_LIBRARY_PATH Crafted Value	SBV-24274	CVE-2009-4018	http	High	7.5	PHP version should be upgraded.	Step 3
ID 13	PHP 5.3.7 and 5.3.8 'is_a()' Remote File-Include Vulnerability	SBV-33562	CVE-2011-3379	http	High	7.5	Operating system-based patch should be applied.	Step 3 or Step 4
ID 14	PHP 5.3.8 'zend_strndup' Function Flaw Allows Remote	SBV-34801	CVE-2011-4153	http	Medium	5.0	Operating system-based patch	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	DoS via Crafted Input						should be applied.	
ID 15	Apache Tomcat Before 5.5.35, 6.x Before 6.0.35, and 7.x Before 7.0.23 Hash Collision Remote DoS	SBV-34182	CVE-2011-4858	http	High	7.8	Apache software version should be upgraded.	Step 3 or Step 4
ID 16	Apache Tomcat 7.0.* Allows Remote DoS via Partial HTTP Requests	SBV-37746	CVE-2012-5568	http	High	7.8	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID 17	PHP Prior to 5.3.6 Intl Extension Remote DoS Vulnerability via an Invalid Argument	SBV-30731	CVE-2011-1467	http	Medium	5.0	PHP version should be upgraded.	Step 3
ID 18	PHP 5.3.3 and Earlier NumberFormatter::getSymbol	SBV-28709	CVE-2010-4409	http	Medium	5.0	Operating system-based patch	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	Integer Overflow Vulnerability						should be applied.	
ID 19	[cpujul2012-392727] PHP Before 5.3.9 Hash Collision Remote DoS Vulnerability	SBV-34176	CVE-2011-4885	http	High	7.8	PHP version should be upgraded.	Step 3
ID 20	FTP Server Accepts Anonymous Logins	SBV-00406	CVE-1999-0497	ftp	Medium	5.1	Anonymous authentiation method should be disabled on the FTP server.	Step 3
ID 21	Oracle Database XML DB Component Vulnerability	SBV-16569	CVE-2007-5513	ftp	Medium	5.0	Relevant Oracle patch should be applied.	Step 3
ID 22	[cpuapr2013-1899555, cpujuly2013-1899826] Apache HTTP	SBV-26196	CVE-2010-2068	http	Low	2.6	Apache software version should be	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	Server mod_proxy_http Remote Information Disclosure Vulnerability via HTTP Requests						upgraded.	
ID 23	Oracle sqldemos Allows Access to the Demo Index Page	SBV-05009		http	Medium	5.0	Access to the demo index page should be disabled.	Step 3
ID 24	Apache HTTP Server Foreign Language Files Information Disclosure Vulnerability	SBV-25568		http	Medium	5.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 25	Buffer Overflow in ApacheBench	SBV-01748	CVE-2002-0843	http	High	9.0	Apache software version	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	on Apache Web Server Enables Arbitrary Code Execution						should be upgraded.	
ID 26	Oracle Application Server SOAP Information Disclosure Vulnerability	SBV-32002		https	Medium	5.0	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID 27	[cpuapr2013-1899555] Apache Software Foundation 'mod_proxy' 2.2 through 2.2.11 Remote DoS Vulnerability	SBV-22752	CVE-2009-1890	http	High	7.8	Operating system-based patch should be applied.	Step 3
ID 28	PHP Prior to 5.2.10 JPEG Image Processing Remote DoS Vulnerability	SBV-23339	CVE-2009-2687	http	Medium	5.0	PHP version should be upgraded.	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
ID 29	HTTP handlers in ASP.NET Remote Information Disclosure Vulnerability	SBV-27593		http	Medium	5.0	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID 30	PHP 5 Multiple Remote vulnerabilities Allows Information Disclosure, Code Execution and DoS	SBV-26577	CVE-2010-2531	http	High	7.5	Operating system-based patch should be applied.	Step 3
ID 31	PHP 5.3-5.3.3 Remote Information Disclosure or Arbitrary Code Execution Vulnerability	SBV-27339	CVE-2010-2950	http	High	7.5	Operating system-based patch should be applied.	Step 3
ID 32	PHP 5.2 - 5.2.13 and 5.3 - 5.3.2 Stack Consumption Vulnerability	SBV-26951	CVE-2010-1917	http	Medium	5.0	Operating system-based patch should be applied.	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	Allows Remote DoS							
ID 33	PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3 Remote DoS Vulnerability via a Crafted ZIP Archive	SBV-28073	CVE-2010-3709	http	Medium	5.0	Operating system-based patch should be applied.	Step 3
ID 34	HP System Management Homepage before 6.3 Remote Privilege Escalation Vulnerability	SBV-31252	CVE-2011-1541	http	Critical	10.0	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID 35	PHP Remote Information Disclosure Vulnerability	SBV-30841		http	Medium	5.0	The Vulnerability should be mitigated by the IPS signature or firewall	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
							access rule.	
ID 36	OpenSSL 0.9.8 - 0.9.8y, 1.0.0 - 1.0.0l, 1.0.1 - 1.0.1g Remote Code Execution and DoS Vulnerability via Crafted DTLS ClientHello	SBV-44797	CVE-2014-0195	http	Medium	6.8	OpenSSL version should be upgraded.	Step 3 or Step 4
ID 37	OpenSSL Before 1.0.0f GOST ENGINE Remote DoS Vulnerability via Crafted Data from a TLS Client	SBV-34216	CVE-2012-0027	http	Medium	5.0	OpenSSL version should be upgraded.	Step 3
ID 38	OpenSSL Before 0.9.8s and 1.x Before 1.0.0f Remote DoS Vulnerability via a Crafted	SBV-34213	CVE-2011-4577	http	Low	2.6	OpenSSL version should be upgraded.	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	X.509 Certificate							
ID 39	OpenSSL 0.9.8 - 0.9.8y, 1.0.0 - 1.0.0l, 1.0.1 - 1.0.1g Remote DoS Vulnerability with Anonymous ECDH Cipher Suite	SBV-44796	CVE-2014-3470	http	Medium	4.3	OpenSSL version should be upgraded.	Step 3 or Step 4
ID 40	The substr_replace Function PHP 5.3.6 and earlier Remote Denial of Service Vulnerability	SBV-31534	CVE-2011-1148	http	High	7.5	Operating system-based patch should be applied.	Step 3 or Step 4
ID 41	Apache APR-util Before 1.3.10 Remote DoS Vulnerability via Unspecified Vectors	SBV-27540	CVE-2010-1623	http	Medium	5.0	Operating system-based patch should be applied.	Step 3
ID 42	HP System Management Homepage	SBV-27334	CVE-2010-3284	http	Medium	5.0	HP SMH software version	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	(SMH) Before 6.2 Remote Information Disclosure Vulnerability						should be upgraded.	
ID 43	Apache HTTP Server < 2.2.16 mod_cache and mod_dav Remote Denial of Service Vulnerabilities	SBV-26556	CVE-2010-1452	http	High	7.8	Apache software version should be upgraded.	Step 3
ID 44	[cpuapr2013-1899555] Apache HTTP Server 2.2.9 on Unix Remote Information Disclosure Vulnerability by Reading Responses	SBV-26857	CVE-2010-2791	http	Medium	5.0	Apache software version should be upgraded.	Step 3
ID 45	[cpujan2013-1515902] Apache Tomcat \ Oracle Fusion Middleware Inefficient	SBV-34537	CVE-2012-0022	http	Medium	5.0	Apache software version should be upgraded.	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	Parameter Handling Allows Remote DoS							
ID 46	Buffer Overflow in OpenSSL Handling of ASCII Integer Representation Allows Arbitrary Code Execution	SBV-01403	CVE-2002-0655	https	High	7.5	OpenSSL version should be upgraded.	Step 3
ID 47	PHP before 5.3.6 phar Extension Multiple Format String Vulnerabilities Allow Remote Code Execution	SBV-30596	CVE-2011-1153	http	High	7.5	PHP version should be upgraded.	Step 3 or Step 4
ID 48	OpenSSL 0.9.8 - 0.9.8y, 1.0.0 - 1.0.0l, 1.0.1 - 1.0.1g Remote DoS Vulnerability via Crafted DTLS Handshake	SBV-44794	CVE-2014-0221	http	Medium	4.3	OpenSSL version should be upgraded.	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
ID 49	Apache Tomcat 7.0.0 - 7.0.27, 6.0.0 - 6.0.35 'parseHeaders()' Error Allows Remote DoS	SBV-37205	CVE-2012-2733	http	High	7.8	Apache software version should be upgraded.	Step 3
ID 50	[cpujul2012-392727] HP System Management Homepage (SMH) Before 7.0 Multiple Vulnerabilities	SBV-38469	CVE-2011-1153	http	High	9.0	HP SMH software version should be upgraded.	Step 3 or Step 4
ID 51	OpenSSL Before 0.9.8s and 1.x Before 1.0.0f SGC Implementation Allows Remote DoS Vulnerability	SBV-34215	CVE-2011-4619	http	Medium	5.0	OpenSSL version should be upgraded.	Step 3
ID 52	[cpujul2009-091332] Jetty < 6.1.17 HTTP Server Remote Directory Traversal Vulnerability	SBV-22263	CVE-2009-1523	https	High	7.5	Jetty software version should be upgraded.	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
ID 53	OpenSSL 0.9.8h-0.9.8q and 1.0.0-1.0.0c OCSP DoS Vulnerability via a Crafted 'ClientHello' Message	SBV-29770	CVE-2011-0014	http	Medium	5.0	Operating system-based patch should be applied.	Step 3
ID 54	cURL libcurl Remote DoS Vulnerability via Crafted Compressed Data	SBV-25177	CVE-2010-0734	http	Medium	5.1	cURL software version should be upgraded.	Step 3
ID 55	PHP < 5.2.12 session.save_path Remote Arbitrary Code Execution Vulnerability	SBV-24411	CVE-2009-4143	http	High	7.5	Operating system-based patch should be applied.	Step 3
ID 56	OpenSSL Remote DoS and Database Write Vulnerability due to Use-After-Free in	SBV-44019	CVE-2010-5298	http	Medium	4.0	OpenSSL version should be upgraded.	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	ssl3_release_read_buffer() - CVE-2010-5298							
ID 57	[cisco-sa-20030930-ssl] OpenSSL 0.9.6 and 0.9.7 ASN.1 inputs DoS	SBV-02684	CVE-2003-0544	https	High	7.8	OpenSSL version should be upgraded.	Step 3 or Step 4
ID 58	OpenSSL 0.9.7 ASN.1 Encoding Allows DoS and Code execution	SBV-02685	CVE-2003-0545	https	Critical	10.0	OpenSSL version should be upgraded.	Step 3 or Step 4
ID 59	[cisco-sa-20030930-ssl] Integer Overflow in OpenSSL 0.9.6 and 0.9.7 ASN.1 Tag Values	SBV-02683	CVE-2003-0543	https	High	7.8	OpenSSL version should be upgraded.	Step 3 or Step 4
ID 60	DoS in Apache <=1.3.27 rotatelogs	SBV-01960	CVE-2003-0460	https	High	7.8	Apache software version should be upgraded.	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
ID 61	Oracle XSQL Servlet Sample Application Allows to Query the Database	SBV-01933	CVE-2002-0569	https	Medium	5.0	Sample applications should be removed from the production servers.	Step 3 or Step 4
ID 62	BIND - Malicious modification of DNS records	SBV-00669	CVE-1999-0184	domain_u	Medium	6.4	The name server should be recompiled without -DALLOW_UPDATES option.	Step 3
ID 63	Microsoft IIS Printers Virtual Directory Has Been Detected on the Host	SBV-30415		https	Info	0.0	The Vulnerability should be mitigated by the IPS signature.	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
ID 64	Microsoft Internet Information Services Scripts Virtual Directory Has Been Detected on the Host	SBV-30416		https	Info	0.0	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID 65	[cpujul2009-091332] Oracle Application Server and BEA Product Suite W3C XML Signature Syntax Remote Vulnerability	SBV-22886	CVE-2009-0217	http	Medium	5.0	Relevant Oracle patch should be applied.	Step 3 or Step 4
ID 66	SSL/TLS X.509 Self-Signed Certificate Obtained	SBV-18251		http	Medium	5.0	The Vulnerability should be mitigated by the IPS signature.	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
ID 67	[cpujul2009-091332] Oracle Database 10 - 10.1.8.3 Secure Enterprise Search Component Unspecified Vulnerability	SBV-22881	CVE-2009-1968	http	Medium	4.3	Relevant Oracle patch should be applied.	Step 3 or Step 4
ID 68	Oracle 9i Application Server Path Revealing Vulnerability	SBV-00829	CVE-2001-1372	http	Medium	5.0	The product should be upgraded.	Step 3
ID 69	Oracle 9i Application Server Allows Information Disclosure	SBV-02029	CVE-2002-0568	http	Medium	5.0	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID 70	OpenSSL <=1.0.0l ECDSA Remote Information	SBV-43707	CVE-2014-0076	http	Medium	4.3	Operating system-based patch	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	Disclosure Vulnerability via FLUSH+RELOAD Cache						should be applied.	
ID 71	[cpujul2012-392727] Apache HTTP Server 'mod_proxy' Remote Security Bypass Vulnerability	SBV-33915	CVE-2011-4317	http	Medium	5.0	Operating system-based patch should be applied.	Step 3
ID 72	SSL Certificate has Expired	SBV-04923		https	Info	0.0	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID 73	TLS/SSL Server X.509 Certificate MD5 Signature Detected	SBV-03326		https	Info	0.0	The Vulnerability should be mitigated by the IPS	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
							signature .	
ID 74	Microsoft Internet Information Services was Detected on the Host	SBV-29632		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature .	Step 4
ID 75	[cpujul2009-091332] Oracle Application Server 10 - 10.1.2.3 HTTP Server Component Unspecified Vulnerability	SBV-22887	CVE-2009-1976	http	Medium	4.3	Relevant Oracle patch should be applied.	Step 3
ID 76	SSL/TLS Server Preferred CipherSuite Detection	SBV-03326		https	Info	0.0	The Vulnerability should be mitigated by the IPS signature .	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
ID 77	Oracle Application Server Oracle HTTP Server Component Unspecified Remote Vulnerability	SBV-16577	CVE-2007-5518	http	Medium	5.0	Relevant Oracle patch should be applied.	Step 3
ID 78	HTTP Version Obtained via Web Server	SBV-32054		http	Info	0.0	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID 79	Web Server HTTP TRACE Method Enabled	SBV-03326		https	Info	0.0	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
ID 80	FTP Server Detected on the Host	SBV-24514		ftp	Info	0.0	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID 81	McAfee ePolicy Orchestrator is Running	SBV-04171		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID 82	Oracle Application Server Oracle Portal Component Unspecified Remote Vulnerability	SBV-16571	CVE-2007-5522	http	Medium	4.3	Relevant Oracle patch should be applied.	Step 3
ID 83	TLS-SSL Server Untrusted X.509	SBV-03326		https	Info	0.0	The Vulnerability should be	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	Certificate Detection						mitigated by the IPS signature.	
ID 84	Oracle Enterprise Manager Web Console Has Been Detected on the Host	SBV-30475		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID 85	Microsoft Internet Information Services NTLM Authentication is Disabled on the Host	SBV-30551		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID 86	Siebel SimBuilder Component in Oracle Siebel Enterprise Multiple Vulnerabilities	SBV-18200	CVE-2008-1831	http	Medium	6.4	The Vulnerability should be mitigated by the IPS	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
							signature .	
ID 87	Oracle Secure Enterprise Search or Ultrasearch Component Remote Unspecified Vulnerability DB04	SBV-18183	CVE-2008-1814	Local Service	Medium	5.5	The Vulnerability should be mitigated by the IPS signature .	Step 4
ID 88	[cpujan2008-086860] Oracle PeopleTools Critical Patch Jan. 2008: Unspecified Vulnerabilities [PSE01, PSE03, PSE04]	SBV-17381	CVE-2008-0348	http	High	7.5	The Vulnerability should be mitigated by the IPS or WAF signature .	Step 4
ID 89	WWW Server Hidden Name Has Been Detected on the Host	SBV-31231		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature .	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
ID 90	Oracle Database 9.0.1.5 FIPS+, 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.3 Multiple Vulnerabilities	SBV-18182	CVE-2008-1813	Local Service	Medium	5.5	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID 91	Microsoft Internet Information Services Anonymous Access is Enabled	SBV-30553		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID 92	Oracle Application Express in Oracle Application Express 3.0.1 Unspecified Vulnerability APEX02	SBV-18191	CVE-2008-1822	Local Service	Medium	4.0	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
ID 93	Oracle Application Server and Collaboration Suite Vulnerability in the Oracle Containers for J2EE	SBV-16583	CVE-2007-5521	http	Medium	4.3	Relevant Oracle patch should be applied.	Step 3
ID 94	SSL Certificates with a Short Public Key Are Used by the Web Server	SBV-27592		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 95	Disabled Microsoft IIS Basic Authentication Scheme was Detected on the Host	SBV-30554		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature or	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
							firewall access rule.	
ID 96	[cpujul2010-155308] Oracle Database Server Application Express Component Remote Vulnerability via Unknown Vectors	SBV-26413	CVE-2010-0892	http	Medium	5.8	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 97	Oracle Database Vault Component Unspecified Remote Vulnerability	SBV-16579	CVE-2007-5512	Local Service	Medium	5.0	Relevant Oracle patch should be applied.	Step 3
ID 98	TLS/SSL Enumeration of X.509 Certificate Fields	SBV-16689		https	Info	0.0	The Vulnerability should be mitigated by the IPS signature or	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
							firewall access rule.	
ID 99	Oracle Portal Component in Oracle Application Server Unspecified Vulnerability	SBV-19830	CVE-2008-3977	http	Medium	5.0	Operating system-based patch should be applied.	Step 3 or Step 4
ID 100	SSL/TLS X.509 Certificate Server Name and Common Name Mismatch	SBV-18246		https	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 101	Microsoft IIS "Use Host Header Name" Setting is Disabled on the Host	SBV-30567		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
							or firewall access rule.	
ID 102	Oracle Database and Enterprise Manager Database Control component Unspecified Vulnerability	SBV-16564	CVE-2007-5530	http	Medium	5.0	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID 103	Web Server with Broken Links Has Been Detected	SBV-32059		http	Info	0.0	The Vulnerability should be mitigated by the WAF solution.	Step 4
ID 104	Oracle E-Business Suite 11.5.10.2 , 12.0.4 Multiple Unspecified Vulnerabilities	SBV-18196	CVE-2008-1827	Local Service	High	7.5	The Vulnerability should be mitigated by the IPS signature.	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
ID 105	SSL Server Information was Detected in the Host	SBV-28846		https	Info	0.0	The Vulnerability should be mitigated by the WAF solution.	Step 4
ID 106	Microsoft NetBIOS Names Information Has Been Detected on the Host	SBV-30424		netbios-ssn	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 107	Oracle E-Business Suite 11.5.10.2 Multiple Unspecified Vulnerabilities APP01, APP10, APP05	SBV-18195	CVE-2008-1826	http	Medium	5.0	The Vulnerability should be mitigated by the IPS signature.	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
ID 108	NetBIOS Null Session Enabled	SBV-03326		netbios-ssn	Info	0.0	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID 109	SSL Supported Cipher Suite Has Been Detected on the host	SBV-30883		https	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 110	Oracle Dynamic Monitoring Service in Oracle Application Server Unspecified	SBV-18193	CVE-2008-1824	Local Service	Medium	4.3	The Vulnerability should be mitigated by the IPS or WAF	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	Vulnerability AS02						signature.	
ID 111	Web Server Redirection Status was Detected on the Host	SBV-30864		http	Info	0.0	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID 112	Oracle Application Server and Collaboration Suite Oracle Portal Component Remote Vulnerability	SBV-16576	CVE-2007-5517	Local Service	Medium	5.8	Relevant Oracle patch should be applied.	Step 3
ID 113	Enumerated Microsoft IIS Server Extensions were Detected on the Host	SBV-30569		http	Info	0.0	The Vulnerability should be mitigated by the IPS or WAF	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
							signature .	
ID 114	Microsoft SQL Server Authentication Mode Is Reported	SBV-27590		ms-sql-s	Info	0.0	The Vulnerability should be mitigated by the IPS or WAF signature .	Step 4
ID 115	Microsoft IIS Script Mapping Configuration Has Been Detected on the Host	SBV-30419		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 116	A database service is running, e.g. a SQL server, Oracle, or MySQL.	SBV-00433		ms-sql-s	Info	0.0	The Vulnerability should be mitigated by the	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
							WAF solution.	
ID 117	Oracle Portal Component in Oracle Application Server 9.0.4.3 Unspecified vulnerability AS03	SBV-18194	CVE-2008-1825	Local Service	Medium	4.3	The Vulnerability should be mitigated by the WAF solution.	Step 4
ID 118	Enumerated Microsoft SQL Server Instances Detection	SBV-30550		ms-sql-m	Info	0.0	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID 119	Oracle Application Server and Collaboration Suite Oracle Portal Component Unspecified Vulnerability	SBV-16565	CVE-2007-5526	http	Low	2.6	Relevant Oracle patch should be applied.	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
ID 120	Anonymous Authentication is Enabled on the SSL Server	SBV-27599		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 121	Testing, Temporary, or Default Web Server Welcome Page were Found on the Server	SBV-05001		http	Info	0.0	The default welcome and test pages should be removed.	Step 3
ID 122	Oracle Application Server, Database and Enterprise Manager Vulnerability in Oracle Help for Web	SBV-16582	CVE-2007-5531	Local Service	Medium	4.3	Relevant Oracle patch should be applied.	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
ID 123	Clear-Text SSL Communication Support Has Been Detected on the Host	SBV-27608		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 124	[MS03-034] NetBT Name Service in Windows NT 4.0, 2000, XP, and Server 2003 Allows Information Disclo	SBV-02250	CVE-2003-0661	Local Service	Medium	5.0	Appropriate Microsoft patch should be applied.	Step 3
ID 125	NetBIOS Bindings Information Has Been Detected on the Host	SBV-30423		Local Service	Info	0.0	The Vulnerability should be mitigated by the IPS signature	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
							or firewall access rule.	
ID 126	Oracle Application Server and Collaboration Suite Portal Component Unspecified Vulnerability	SBV-16568	CVE-2007-5519	http	Medium	5.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 127	SSH Protocol Supported Version Has Been Detected on the Host	SBV-30868		ssh	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
ID 128	Apache htpasswd Buffer Overflow Vulnerability	SBV-10437		http	Medium	4.6	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 129	WebDAV Extensions are Installed on Server	SBV-01328		http	Info	0.0	If the use of Webdav is not required, it should be disabled.	Step 3
ID 130	Oracle 9i Application Server Multiple Sample Pages Remote Information Disclosure Vulnerability	SBV-24870	CVE-2002-1632	http	Medium	5.0	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
ID 131	Microsoft Windows IIS ASP.NET Product Version was Detected	SBV-25235		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 132	SSL Web Server Version Information has been Obtained	SBV-30532		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 133	PHP < 5.2.11 Unspecified Vulnerability Related to "Missing Sanity Checks around	SBV-23574	CVE-2009-3292	http	High	7.5	PHP version should be upgraded.	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	Exif Processing"							
ID 134	PHP enable_dl Option is Activated on the Remote Host	SBV-27613		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 135	OpenSSL 0.9.8h-0.9.8j CMS_verify Function Security Bypass Vulnerability	SBV-21472	CVE-2009-0591	http	Medium	5.0	OpenSSL version should be upgraded.	Step 3
ID 136	The Session Extension feature of PHP Remote Security Bypass Vulnerability	SBV-27596		http	Medium	4.3	PHP version should be upgraded.	Step 3
ID 137	Apache HTTP Server OS Information	SBV-25569		http	Medium	5.0	The Vulnerability should be	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	Disclosure Vulnerability						mitigated by the IPS or WAF signature.	
ID 138	PHP Display_Errors Directive Setting is "ON" on the Host	SBV-30528		http	Info	0.0	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID 139	PHP File_Uploads Option is Enabled on the Host.	SBV-30539		http	Info	0.0	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID 140	PHP Safe_Mode Option	SBV-30540		http	Info	0.0	The Vulnerability should be	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	is Disabled on the Host						mitigated by the IPS or WAF signature.	
ID 141	PHP file phpinfo.php Has Been Detected on the Host	SBV-30463		http	Info	0.0	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID 142	PHP < 5.2.11 Unspecified Vulnerability in the Imagecolortransparent Function	SBV-23575	CVE-2009-3293	http	High	7.5	PHP version should be upgraded.	Step 3
ID 143	SMTP Server Connection are Allowed on the Host	SBV-30558		smtp	Info	0.0	PHP version should be upgraded.	Step 4
ID 144	PHP before 5.2.11 php_openssl_ap	SBV-23548	CVE-2009-3291	http	High	7.5	PHP version should be	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	ply_verification_policy Function Unspecified Vulnerability						upgraded.	
ID 145	HP System Management Homepage (SMH) Before 7.3 Remote Information Disclosure Vulnerability	SBV-43818	CVE-2013-4846	http	Medium	5.0	HP SMH software version should be upgraded.	Step 3
ID 146	OpenSSL 0.9.8 - 0.9.8y, 1.0.0 - 1.0.0l, 1.0.1 - 1.0.1g Remote Man-in-the-middle Attack (CCS Injection Vulnerability)	SBV-44793	CVE-2014-0224	http	Medium	6.8	Operating system-based patch should be applied.	Step 3 or Step 4
ID 147	Apache JServ Protocol Connector was Detected on the Host	SBV-30885		ajp13	Info	0.0	The Vulnerability should be mitigated by the IPS	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
							or WAF signature .	
ID 148	SSL Server Supporting Weak Encryption Has Been Detected on the Host	SBV-28908		https	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 149	Microsoft SQL Server UDP 1434 Database Instance TCP Information Disclosure	SBV-03326		ms-sql-m	Info	0.0	The Vulnerability should be mitigated by the IPS signature .	Step 4
ID 150	Fopen_wrappers.c in PHP 5.3.0-5.3.3 Remote Open_basedir Restrictions	SBV-28072	CVE-2010-3436	http	Medium	5.0	Operating system-based patch should be applied.	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	Bypass Vulnerability							
ID 151	The default Error Page Version for Apache Tomcat Has Been Detected on the Host	SBV-32836		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 152	SSL/TLS Supports DEFLATE Compression	SBV-03326		https	Info	0.0	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID 153	Apache Tomcat Remote Security Bypass due to HTTP Digest Caching	SBV-37445	CVE-2012-5886	http	Medium	5.0	Operating system-based patch should be applied.	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	Information about Users							
ID 154	Apache Tomcat Remote Security Bypass due to HTTP Digest Tracking cnonce Instead of nonce and nc	SBV-37444	CVE-2012-5885	http	Medium	5.0	Operating system-based patch should be applied.	Step 3
ID 155	Apache Tomcat Remote Security Bypass due to HTTP Digest Improperly Checking for Stale Nonce Values	SBV-37446	CVE-2012-5887	http	Medium	5.0	Operating system-based patch should be applied.	Step 3
ID 156	SMTP Service Detection	SBV-29633		smtp	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
							access rule.	
ID 157	HTTP Server that Handles Session using Set-Cookie Has Been Detected on the Host	SBV-30880		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 158	Default Installation Page Has Been Detected on the Host	SBV-30858		http	Info	0.0	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID 159	Microsoft Terminal Service Has Not Been Configured	SBV-03326		Local Service	Info	0.0	The Vulnerability should be mitigated by the	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	Network Level Authentication						IPS signature.	
ID 160	SSL Certificate Key Length Less Than 1024 Bits	SBV-03326		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID 161	WebDAV Has Been Detected on the Host	SBV-30861		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 162	Service Location Protocol Service Has Been	SBV-28845		slp	Info	0.0	The Vulnerability should be mitigated by	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	Detected on the Host						the IPS signature or firewall access rule.	
ID 163	Microsoft SharePoint Server Has Been Detected	SBV-28820		http	Info	0.0	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID 164	Microsoft ASP.NET State Service Has Been Detected	SBV-27603		http	Info	0.0	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID 165	Microsoft IIS Tilde Character Short File Name	SBV-03326		http	Info	0.0	The Vulnerability should be	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
	Disclosure (142982)						mitigated by the IPS signature.	
ID 166	DNS Cache Snooping Vulnerability	SBV-03326		domain_u	Info	0.0	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID 167	DNS Server Cache Allows Snooping on the Host	SBV-30565		domain_u	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 168	DNS Server Has Been Detected on the Host	SBV-31351		domain_u	Info	0.0	The Vulnerability should be	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
							mitigated by the IPS signature or firewall access rule.	
ID 169	DNS Spoofed Request Amplification Has Been Detected	SBV-31566		domain_u	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 170	DNS Server With DNSSEC Aware Resolver Has Been Detected on the Host	SBV-30476		domain_u	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
							access rule.	
ID 171	Microsoft Windows NETBIOS Anonymous Accessible Shares Detected	SBV-03326		microsoft-ds	Info	0.0	The Vulnerability should be mitigated by the IPS signature.	Step 4
ID 172	Microsoft Internet Information Services IISADMPWD Virtual Directory Has Been Detected on the Host	SBV-30413		https	Info	0.0	The Vulnerability should be mitigated by the IPS or WAF signature.	Step 4
ID 173	Microsoft IIS MSADC Virtual Directory Has Been Detected on the Host	SBV-30414		https	Info	0.0	The Vulnerability should be mitigated by the IPS or WAF	Step 4

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
							signature .	
ID 174	NTP <4.2.7p26 Remote DoS Vulnerability via Forged REQ_MON_GETLIST Request	SBV-43060	CVE-2013-5211	Local Service	Medium	5.0	NTP software version should be upgraded .	Step 3 or Step 4
ID 175	Remote FTP Server with Clear Text Authentication Has Been Detected on the Host	SBV-30397		ftp	High	7.5	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 176	Weak SSL Ciphers Detected	SBV-01394		https	Low	2.6	Support for the low encryption ciphers should be disabled.	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
ID 177	SSH2 Server Weak Key Exchange Algorithm or Symmetric Cipher	SBV-05892		ssh	Low	2.6	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 178	OpenSSL Before 0.9.8s and 1.x Before 1.0.0f DTLS Implementation Allows Remote Information Disclosure	SBV-34217	CVE-2011-4108	http	Medium	5.0	Operating system-based patch should be applied.	Step 3
ID 179	OpenSSL Before 0.9.8s and 1.x Before 1.0.0f SSL v3 Weak Encryption	SBV-34214	CVE-2011-4576	http	Medium	5.0	OpenSSL version should be upgraded.	Step 3

ID	Risk Definition	SBV ID	CVE ID	Service	Severity	CVSS Score	Solution	Steps
ID 180	Check Point FireWall-1 with ICA Service Has Been Detected on the Host	SBV-32228		http	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4
ID 181	A NTP Server Has Been Detected on the Host	SBV-31356		Local Service	Info	0.0	The Vulnerability should be mitigated by the IPS signature or firewall access rule.	Step 4

B: Organizational Web Services Security Perception Survey

İşletme Ağlarında Web Servis Güvenliği Üzerine Bir Araştırma

Orta Doğu Teknik Üniversitesi

Enformatik Enstitüsü

Bilişim Sistemleri

Bu araştırma "İşletme Ağlarında Web Servis Güvenliği için Bir Bilgi Güvenliği Çerçevesi" başlıklı akademik çalışma için gerçekleştirilmektedir.

Bölüm 1:

1. Göreviniz/mevkiiniz nedir?
   ( ) görevinde/mevkiinde hizmet vermekteyim.

2. Kaç yıldır bilgisayar/internet kullanıyorsunuz?
   ( ) yıldır bilgisayar/internet kullanıyorum.

3. Kaç yıldır bilgi işlem departmanında çalışıyorsunuz?
   ( ) yıldır bilgi işlem departmanında çalışıyorum.

4. DMZ (Demilitarized Zone/Silahsızlaştırılmış bölge) hakkında bilginiz hangi seviyedir?
   Kapsamlı bilgim bulunmaktadır. ( )
   Genel bilgim bulunmaktadır. ( )
   Kısmi bilgim bulunmaktadır. ( )
   Herhangi bir bilgim bulunmamaktadır. ( )

5. Kurum topolojisine ne kadar hakimsiniz?
   Kapsamlı bilgim bulunmaktadır. ( )
   Detaylı bilgim bulunmaktadır. ( )
   Sorumlu olduğum varlıkların topolojisini biliyorum. ( )
   Herhangi bir bilgim bulunmamaktadır. ( )
6. IT alt yapınızdaki web servisleri hakkındaki bilginiz hangi seviyededir?
   Kapsamlı bilgim bulunmaktadır. ( )
   Genel bilgim bulunmaktadır. ( )
   Kısmi bilgim bulunmaktadır. ( )
   Herhangi bir bilgim bulunmamaktadır. ( )

7. Web servisleriniz üzerinden verilen hizmetlerin sürekliliği hangi şekildedir?
   Kesintisiz 7/24 hizmet vermelidir. ( )
   Periyodik vakitlerde hizmet vermelidir. ( )
   Talep edilen vakitlerde hizmet vermelidir. ( )

8. Web servisleri üzerinden verilen hizmetlerde olası herhangi bir kesinti/servis dışı duruma tahammül ne kadardır?
   Hizmet kesintisine hiç bir şekilde tahammül yoktur. ( )
   Çok kısa süreli kesintilere tahammül vardır. ( )
   Gerektiğinde uzun süreli kesintiye tahammül vardır. ( )

Bölüm 2:

9. Var olan web servislerinizin konumlandırılması ne şekildedir?
   (Birden fazla seçeneği işaretleyebilirsiniz.)
   DMZ ağındadır. ( )
   Yerel ağ/Sistem ağındadır. ( )
   Veritabanı ağındadır. ( )
   Diğer ağdadır. ( )

10. Var olan web servislerinizin diğer uygulamalarla olan entegrasyonu ne şekildedir?
    (Birden fazla seçeneği işaretleyebilirsiniz.)
    Etki alanına dahildir. ( )
    Web servisine özel veritabanı ile entegre çalışmaktadır. ( )
    Başka web servisleri ile entegre çalışmaktadır. ( )
    Diğer. ( )

11. Web servislerininin bulunduğu sunucular hakkında aşağıdakilerden hangisi geçerlidir?
    (Birden fazla seçeneği işaretleyebilirsiniz.)
    Fiziksel platformdur. ( )
    Sanallaştırma platformu üzerindedir. ( )
    Yedekli yapıda çalışmaktadır. ( )

12. Periyodik olarak işletim sistemi, yazılım güncellemesi gerçekleştirilmekte midir?
    (Birden fazla seçeneği işaretleyebilirsiniz.)
    Güncel versiyonun stabilitesine göre gerçekleştirilmektedir. ( )
    Test işlemleri yapılmadan herhangi bir güncelleme yapılmamaktadır.( )
    Gerekmediği sürece herhangi bir güncelleme yapılmamaktadır. ( )
    Hayır, gerçekleştirilmemektedir. ( )

13. Web servislerin yapılandırma, yazılım yedeği otomatik olarak alınmakta mıdır?
    (Birden fazla seçeneği işaretleyebilirsiniz.)
    Evet, periyodik olarak otomatik olarak alınmaktadır. ( )
    Evet, periyodik olarak manuel olarak alınmaktadır. ( )
    Herhangi bir çalışma gerçekleştirilmeden önce alınmaktadır. ( )

Hayır, alınmamaktadır. ( )

14. Gerçekleştirilen yedeklemenin kullanılabilirliği test edilmekte midir?
(Birden fazla seçeneği işaretleyebilirsiniz.)
Evet, periyodik olarak test edilmektedir. ( )
Herhangi bir çalışma öncesi test edilmektedir. ( )
Hayır, edilmemektedir. ( )

15. Web servisleri üzerinde log yönetimi nasıl gerçekleştirilmektedir.?
(Birden fazla seçeneği işaretleyebilirsiniz.)
Web servis logları tutulmamaktadır. ( )
Web servis logları sadece sunucu üzerinde tutulmaktadır. ( )
Web servis logları 3. parti başka bir log ürününe aktarılmaktadır. ( )

16. Web servis log yönetimi gerçekleştiriliyorsa ne kadar sürelik log tutulmaktadır?
(Birden fazla seçeneği işaretleyebilirsiniz.)
0-6 aylık log tutulmaktadır. ( )
0-1 yıllık log tutulmaktadır. ( )
0-2 yıllık log tutulmaktadır. ( )
Daha fazla sürede log tutulmaktadır. ( )

Bölüm 3:

17. Kurum web servisleri daha önceden herhangi bir siber saldırıya maruz kalmış mıdır?
Evet, kalmıştır. ( )
Hayır, kalmamıştır. ( )

18. Web servislerinin saldırılardan korunması için herhangi bir güvenlik önlemi mevcut mudur?
Evet, kapsamlı olarak bulunmaktadır. ( )
Evet, kısmi olarak bulunmaktadır. ( )
Hayır, bulunmamaktadır. ( )

19. Herhangi bir güvenlik önlemi mevcut ise, bunlar nelerdir?
(Birden fazla seçeneği işaretleyebilirsiniz.)
Güvenlik Duvarı ( )
Saldırı Tespit ve Önleme Sistemi ( )
Web Uygulama Güvenlik Duvarı ( )
DDoS Tespit ve Önleme Sistemi ( )
DNS Güvenlik Duvarı ( )
Diğer ( )

20. İlgili web servislerine erişim portları nasıl yapılandırılmıştır?
(Birden fazla seçeneği işaretleyebilirsiniz.)
HTTP 80/HTTPS 443/Diğer bütün her yöne açılmıştır. ( )
Yönetimsel erişim portları web servis yöneticilerine açıktır. ( )
Geri kalan TCP ve UDP portları erişime kapalıdır. ( )

21. Kritik bilgi transferi içeren web servislerinde herhangi bir şifreleme gerçekleştirilmekte midir?
Evet, gerçekleştirilmektedir. ( )
Hayır, gerçekleştirilmemektedir. ( )

22. Varsa mevcut şifreli web servis trafiğini güvenlik bileşenleri analiz edebilmekte midir?
Evet, analiz edebilmektedir. ( )
Hayır, analiz edememektedir. ( )

23. Güvenlik bileşenlerinde periyodik olarak imza/saldırı veritabanı güncellemesi yapılmakta mıdır?
Evet, yapılmaktadır. ( )
Hayır, yapılmamaktadır. ( )

24. Güvenlik bileşenlerinde var olan web servisleri için spesifik güvenlik politikaları oluşturulmuş mudur?
Evet, oluşturulmuştur. ( )
Hayır, oluşturulmamıştır. ( )

25. İlgili güvenlik politikaları ilgili web servisler için atanmış mıdır?
Evet, atanmıştır. ( )
Hayır, atanmamıştır. ( )

26. Oluşturulan politikalara istinaden yanlış pozitif alarmlar takip edilip düzeltilmekte midir?
Evet, düzeltilmektedir. ( )
Hayır, düzeltilmemektedir. ( )

Bölüm 4:

27. Güvenlik ürünlerinin etkin bir şekilde çalıştığını teyit etmek için ne gibi önlem/önlemler alınmaktadır?
(Birden fazla seçeneği işaretleyebilirsiniz.)
Periyodik saldırı tatbikatları gerçekleştirilmektedir. ( )
Periyodik yapılandırma/analiz kontrolleri gerçekleştirilmektedir. ( )

28. Var olan güvenlik bileşenlerinin kontrol edilmesi için tatbikat yapılmakta mıdır?

Hayır, yapılmamaktadır. ( )
Evet, yapılmaktadır. ( )

29. Tatbikat hangi aralıklarla yapılmaktadır?
Yılda bir kez. ( )
Yılda iki kez. ( )
Yılda üç kez. ( )
Daha fazla. ( )

30. Belirli aralıklarla penetrasyon testleri gerçekleştirilmekte midir?
Evet, gerçekleştirilmektedir. ( )
Hayır, gerçekleştirilmemektedir. ( )

31. Penetrasyon testlerinde elde edilen bulgulara göre alınan aksiyonlar nelerdir? (Birden fazla seçeneği işaretleyebilirsiniz.)
Kritik ve yüksek seviyeli açıklıklar ivedi olarak kapatılmaktadır. ( )
Orta ve düşük seviyeli açıklıklar önceliklendirmeye göre kapatılmaktadır. ( )
Düşük seviyeli açıklıklar için aksiyon alınmamaktadır. ( )

C: CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name:	Sarıkoz, Bahadır Gökhan
Nationality:	Turkish (TC)
Data and Places of Birth:	31 December 1986, Ankara
Marital Status:	Married
Phone:	+90 532 267 07 24
Email:	bahadir.sarikoz@metu.edu.tr

EDUCATION

Degree	Institution	Year
M.Sc	METU, Information System	2015, January
B.Sc	METU, Electrical-Electornics Engineering	2010, June
High School	Nermin Mehmet Çekiç Anatolian High School	2004, June

WORK EXPERIENCE

Year	Place	Enrollment
2013 – Present	Barikat Information Security	Security Account Manager
2011 - 2013	Barikat Information Security	Technical Support Engineer
2008 August	Türk Telekomunikasyon A.Ş.	Intern Engineering Student
2009 September	Türk Telekomunikasyon A.Ş.	Intern Engineering Student

FOREIGN LANGUAGES

Advanced English, Beginner-level German, Beginner-level French

D: VITA

Bahadır Gökhan Sarıkoz was born in Altındağ, Ankara on December 31, 1986. He received his B.Sc degree in Electrical-Electronics Engineering from Middle East Technical University in June 2010. He worked in Barikat Information Security as a technical support engineer from 2011 to 2013. Since then he has been a security account manager in Barikat Information Security. His main areas of interest are information security, network security, security modelling and information security technologies.

TEZ FOTOKOPİSİ İZİN FORMU

ENSTİTÜ

Fen Bilimleri Enstitüsü ☐

Sosyal Bilimler Enstitüsü ☐

Uygulamalı Matematik Enstitüsü ☐

Enformatik Enstitüsü [x]

Deniz Bilimleri Enstitüsü ☐

YAZARIN

Soyadı : SARIKOZ
Adı : BAHADIR GÖKHAN
Bölümü : BİLİŞİM SİSTEMLERİ

TEZİN ADI :
AN INFORMATION SECURITY FRAMEWORK FOR THE WEB SERVICES IN ENTERPRISE NETWORKS

TEZİN TÜRÜ : Yüksek Lisans [x] Doktora ☐

1. Tezimin tamamından kaynak gösterilmek şartıyla fotokopi alınabilir. [x]
2. Tezimin içindekiler sayfası, özet, indeks sayfalarından ve/veya bir bölümünden kaynak gösterilmek şartıyla fotokopi alınabilir. [x]
3. Tezimden bir (1) yıl süreyle fotokopi alınamaz. [x]

TEZİN KÜTÜPHANEYE TESLİM TARİHİ :