Chapter 6
Design, Development, and Testing of Web Applications: Security Aspects

Ufuk Uçak
Ahmet Yesevi University, Turkey

Gurkan Tuna
Trakya University, Turkey

ABSTRACT

Today, with the changes and developments in software technologies, web applications have gained an important place by being actively used in many sectors. Due to the fact that web applications do not require installation costs and are easily accessible and operable, the increased usage rate in recent years makes these systems the target of cyber hackers. As a result of cyber attacks, services are blocked, and material and moral damages and data privacy violations are experienced. Within the scope of this study, web applications are explained, vulnerabilities that threaten software security and the measures that can be taken against these vulnerabilities are included. Particularly, security threats to web applications, security principles, secure software development lifecycles, test tools, and hardware and software products used for security are examined. In addition, SAMM and BSIMM models, which are maturity models used in secure software development, are discussed.

INTRODUCTION

Today, with the advancements in technology, traditional approaches are no longer used or effective in software development and software security. Security threats posed by software applications are increasing day by day. Security threats endanger the data security of corporations and organizations, as well as cause material and moral damages. Therefore, in recent years, software security has emerged to protect against cyber attacks on applications. Within the scope of software security, there are responsibilities

DOI: 10.4018/978-1-6684-6914-9.ch006

for both software developers and database managers. Accordingly, corporations and organizations need to change their software development methodologies.

Web applications are defined as computer programs that can perform some functions using web browsers as clients. Web applications have started to be used more and more each day as they replace existing traditional applications, and they have become very critical systems. Because businesses rely on web applications more and carry out their transactions using them. However, this trend has become a major concern (Shahid et al., 2022). Due to their various security vulnerabilities, cyber attackers can cause significant damage to business processes which typically lead to the loss of credibility and reputation, and cause data loss (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2021). Unauthorized access of cyber attackers may result in data breaches, and as a result of such access the cyber attackers may be able to view, copy, or share data. Therefore, it is necessary to identify the security vulnerabilities of web applications in use and then determine the precautions to be taken for these vulnerabilities (Handa, Negi, & Shukla, 2021). In addition to protecting computer networks using firewalls, intrusion prevention systems and anti-virus applications, these precautions involve keeping web applications up-to-date, updating software development methodologies, and using secure communication protocols.

In this chapter, based on an extensive literature review and using examples from our own application development experience, we first present the features of web applications, review how web applications are developed and deployed, identify the common security-related vulnerabilities of web applications. Then, we focus on the design principles of secure application development cycles by taking into consideration selected maturity models. Moreover, we try to explain how the measures to be taken in software development life cycles can address the well-known vulnerabilities of web applications against cyber attacks.

WEB APPLICATIONS

As the literature and news prove that web applications are inherently exposed to cyber threats. Therefore, the security vulnerabilities of web applications must be identified and then existing web applications must be secured with measures to be taken. As well as the existing web applications, future ones must be secured using secure application development practices.

A web client is a program that allows users to access web services, and with this access, they are processed and displayed in HyperText Markup Language (HTML) standards. Web clients are widely known examples of web browsers such as Google Chrome, Internet Explorer, and Mozilla Firefox. On the other hand, the web server processes Hypertext Transfer Protocol (HTTP) requests sent by web clients and sends their response back to the client. The web server responds to the request sent by the clients with HTTP in the same way. HTTP is used to transport information on the web and is used by clients to access web applications. Thanks to this protocol, all information can be accessed through the web server. The web client sends its requests using HTTP and the web server responds to the client using it, too. The way how content is sent to the clients by web servers is divided into two types as static and dynamic. Static content shows the page on the web server to the user as it is. It does not change according to the user's request. The HTML page prepared by the application is directly in front of the user.

It is necessary to point out the difference between web applications and websites here. Websites have a static structure. However, web applications have a dynamic structure and are basically software with user experience. Web applications are a bridge that connects to web servers running in the background through any browser. The clients are user computers that can receive service from a server. Web tech-