Chapter 11
Reshaping Cybersecurity Practices by Optimizing Web Application Penetration Testing

Khalid Hussain
https://orcid.org/0000-0002-3714-8696
Albukhary International University, Malaysia

Md Amin Ullah Sheikh
Albukhary International University, Malaysia

Thiha Naing
Albukhary International University, Malaysia

Manzoor Hussain
Indus University, Pakistan

Noor Ul Amin
Taylor's University, Malaysia

ABSTRACT

Web application penetration testing is known as pretesting. It is a critical process for identifying and addressing security vulnerabilities in web applications. Statistics show that 88% of organizations worldwide experienced phishing attempts in 2019. The most significant security violation was predictable resource location attacks were 34%, SQL attacks at 20%, and code injection attacks at 10%, together generating 64% of total web application attack activity. Also, 75% of IT leaders lack confidence

DOI: 10.4018/979-8-3693-5415-5.ch011

in their web application security. The study of the literature review emphasizes the lack of security issues in web applications and some proposals about penetration testing procedures. The method sections talk about detailed procedures from scratch for doing web app pen tests. In the discussion section, the authors talk about some suggestions that organizations can follow to make their websites more secure and unauthorized access. In conclusion, conducting web application penetration testing in the proper way can play a crucial role in securing web applications.

1. INTRODUCTION

A web application is a dynamic and interactive website that is able to do specific functions through browser technologies (Gurunath & Samanta, 2021). Also, penetration testing which is known as "pen testing" in common, is a security testing of the applications that can evaluate the security of an IT infrastructure by safely identifying the weakness of the system called vulnerabilities (Shebli et al., 2018). Web application penetration testing follows some procedure or step sequence while doing pen testing. It includes planning and preparation, discovery, attacks, reports, etc. In planning and preparation, penetration testers identify the actual scope, their goal, duration, and all the basic information that is necessary at the first step. Then the discovery phase comes into play. It involves gathering information about the target, reconnaissance website structures, their technology use, and so on. The attacking phase is the most important part of penetration testing (Denis et al., 2016).

Pen testers apply their techniques to get the vulnerability manually and also use some automated tools. Finally, they report overall findings in proper documentation (Altulaihan et al., 2023). In this paper, we are going to show the actual process of conducting penetration testing from a hacker's mindset. Penetration testing in the proper way can identify vulnerabilities, prevent security breaches, improve security postures, guide security measures, assess the security state, and minimize security risk of the web application as well as the organizations (Aibekova & Selvarajah, 2022), (Khera et al., 2019), (Softić & Vejzović, 2023).

2. LITERATURE REVIEW

In web application security testing, companies perform penetration testing that can identify web application vulnerabilities and attackers' actions. (Goutam et. al., 2019) study vulnerability assessment and penetration testing to enhance the security of web applications. For testing vulnerabilities, a framework has been built. Today the leading methodology of web application security analysis is a combination of