Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa

An effective new penetration test approach to detect web attacks on web applications

Muhammed Onur Kaya [a], Huseyin Alperen Dagdogen [a], Mehmet Ozdem [b], Resul Das [a,*]

[a] Firat University, Faculty of Technology, Department of Software Engineering, 23119, Elazig, Türkiye
[b] Turk Telekom, Ankara, Turkiye

ARTICLE INFO

Keywords:
Web application security
Penetration test
Cyber security
Automated penetration testing tool

ABSTRACT

As web applications increasingly involve sensitive transactions such as e-commerce, online banking, and public services, they have become primary targets for cyberattacks. Therefore, web application penetration testing is vital for discovering and protecting against vulnerabilities in web-based systems. This study introduces an automated penetration testing tool that systematically applies comprehensive penetration testing methodologies to effectively identify and mitigate web application vulnerabilities. The proposed tool uses a hybrid approach that includes automated and manual testing phases for multiple attacks, including SQL Injection, Cross-Site Scripting, and Cross-Site Request Forgery. System diversity is increased, and the penetration testing process is enriched using Python scripts and APIs. The tool provides an effective mechanism for uncovering critical vulnerabilities by simulating real-world attacker behavior. Practical evaluations on various web applications demonstrate the tool's ability to identify vulnerabilities and increase system resilience. This research will help developers and security engineers apply this automated, specialized approach to security as our digital environment becomes more connected.

1. Introduction

Today, essential daily activities such as sending emails, conducting online banking, shopping, and accessing government services are predominantly carried out through web applications (Siddiquee, 2016). The intensive use of web applications in all areas of life has made them attractive targets for cyber attacks (Mallick & Nath, 2024). While users expect the web applications they use to be reliable and secure, they can quickly move away from these platforms in the event of a security breach or attack. The loss of user trust not only affects individual users; it can also cause serious damage to the reputation and revenues of businesses. Vulnerabilities in web applications can wreak havoc on a business model and result in customer loss in the long run (Li et al., 2024; Singh et al., 2020; Zhou et al., 2025). For this reason, security must be considered a priority from the development phase of web applications. A safe page will provide a smoother experience for the user and exceed the expectations of the standard functionality Hao et al. (2025). This is especially marked in environments where sensitive user data and money are involved. Security defects in web applications can become channels for various cyber attacks (Jang-Jaccard & Nepal, 2014; Perwej et al., 2021). Some of these most frequently seen threats on Web Applications include SQL Injection, Remote Code Execution (RCE), Cross-Site Scripting (XSS), Broken Authentication, and Cross-Site Request Forgery (CSRF) (Noman et al., 2020; Ravindran & Potukuchi, 2022; Sharif, 2022). SQL injection is a type of attack that exploits the database layer of web applications, leading to unauthorized access (Bhateja et al., 2021). XSS attacks are when harmful scripts are executed inside a user's browser, and this can have far-reaching consequences involving the compromise of the session information of that user (Rodríguez et al., 2020). CSRF attacks, on the other hand, force the user to make requests on their behalf, allowing systems to be misused. Broken authentication refers to security vulnerabilities that allow unauthorized users to log in Agrawal (2023). Such attacks not only lead to data loss but also increase the legal liabilities of businesses and undermine the reliability of protecting user data. The increase in cyber threats has made penetration tests a necessity to ensure security in web applications.

To support effective penetration testing and vulnerability management, standardized frameworks and classification systems have been developed to systematically define and track known vulnerabilities. Among these, Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) are the most widely recognized. While CVE is an accepted system to identify publicly known

* Corresponding author.
E-mail addresses: muhammedonurkya@gmail.com (M.O. Kaya), hadagdogen@firat.edu.tr (H.A. Dagdogen), mehmet.ozdem@turktelekom.com.tr (M. Ozdem), rdas@firat.edu.tr (R. Das).

https://doi.org/10.1016/j.eswa.2025.129623
Received 12 February 2025; Received in revised form 12 August 2025; Accepted 2 September 2025
Available online 27 September 2025