IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 1, March 2024

Survey on Web Security Scanner: The State of Features and Vulnerability Checks

Rumana Anjum[1], Affan Baig[2], Afreen Suraiya[3], Misbah Sultana[4], Sara Farheen[5]

Faculty, Department of Computer Science and Engineering[1]

Student, Department of Computer Science and Engineering[2,3,4,5]

Vidya Vikas Institute of Engineering and Technology, Mysuru, Karnataka, India

Abstract*: The development has been lacked in categorization of web security scanning. The testers use binge-tool-scanning (running security scanning one after the other) where issue of availability and accessibility of proper tools arises. In this study, the issue of automation by running multiple scans to evaluate vulnerabilities, effectively judging, saving the precious time and addressing the accurate results. There been many overlaps between the scanning tools which makes this problem more challenging. This executes multitude of web security scanning tools, does other custom added checks and prints the result spontaneously. In an era dominated by digital connectivity and online interactions, the security of web applications stands at stage of critical concern.*

Keywords: Vulnerability, Web Application, Firewalls, Scanning

I. INTRODUCTION

Web application plays a pivotal role in today's digital landscape, serving as critical components for businesses, organizations and individuals. However, their widespread adoption also exposes them to security risks. Malicious actors exploit vulnerabilities in web applications to compromise sensitive data, disrupt services and gain unauthorized access. To mitigate these risks, security professionals rely on web vulnerability scanners.

In this survey paper, we delve into the world of web vulnerability scanner, exploring their capabilities, limitations and impact on application security. We examine various aspects including vulnerability detection techniques, false positives, coverage. By understanding the strength and weakness and different tools, we aim to provide insights that can enhance security posture of web applications.in just one-step installation, saves lot of time and checks for same vulnerability with multiple tools to help in zero-in on false positives effectively. This tool serves as a proactive defence mechanism, systematically scanning web application for potential weakness, loopholes that could be exploited.

II. RELATED WORK

2.1 Understanding Web Scanning process

This is specialized tool designed to assess the security posture of web application. The systematically probe for vulnerabilities, aiming to identify weakness that could be exploited by attackers. These scanners operate from an eternal perspective, simulating how an adversary might interact with the application. By doing so, they stress-test the application's defences. The scanner begins by exploiting the application's structure. It follows links, collects information about pages, forms and endpoints. This step is crucial for understanding the application's attack surface. Detects if the application is vulnerable to malicious scripts injected into web pages. Identifies vulnerabilities that a allow attackers to manipulate database queries. Flags potential unauthorized actions triggered by forged requests. Checks for non-intrusive checks which examine items without actively interacting with the application. This provides valuable insights without affecting the applications behaviour.

2.2 Limitations and Challenges

Scanners may report vulnerabilities that don't actually exist. Balancing sensitivity and specificity is crucial. Some scanners may miss certain vulnerabilities or fail to explore all parts of the application. Scanners lack contextual understanding, which can lead to oversights. While dynamic scanners focus on runtime behaviour, static analysis tools

DOI: 10.48175/IJARSCT-15627

examine source code. Combining both approaches enhances accuracy. Open-source scanners provide flexibility and community support. Ability to customize scans based on your application's unique characteristics. The format of the structure of code must be so understandable to everyone and deliver the required prospect of need to testers out there who are facing so difficulties in their day-to-day work.

2.3 Conditional text generation

Web vulnerability scanners play a critical role in identifying flaws within the web applications. However, their effectiveness relies on accurate detection and precise reporting. This introduces a dynamic dimension to vulnerability scanning by mitigating the generated output based on specific conditions. If a SQL injection vulnerability is detected, the report can emphasize the potential impact on user credential. If XSS flaw affects a public facing page, the report can highlight the risk to end users. Not all vulnerabilities are equal. Some demand immediate attention, while others may pose minimum risk. High severity vulnerabilities trigger urgent alerts, emphasizing the need for immediate remediation. Instead of merely listing vulnerabilities, conditional text generation can describe potential attack information.

III. PRE-REQUISITES

A clear research question or objective that guides the selection and evaluation of the web vulnerability scanners.

A set of criteria or metrics to measure the performance and effectiveness of the web vulnerability scanners, such as coverage, accuracy, false positives, scalability, usability, etc.

A collection of web applications or services that represent the target domain or scope of the survey, and that contain different types of web vulnerabilities, such as SQL injection, cross-site scripting, command injection, etc.

A methodology or procedure to apply the web vulnerability scanners to the web applications or services, and to collect and analyze the results.

A comparison and discussion of the strengths and weaknesses of the web vulnerability scanners, and the implications and limitations of the survey.

IV. EXPECTED OUTCOME

A description of the methodology and criteria used to compare and assess the scanners, such as the type of scan, the target web applications, the vulnerability types, and the metrics of coverage, accuracy, and false positives. A presentation and analysis of the results, highlighting the performance and trade-offs of each scanner for different vulnerability types, and identifying the best practices and challenges for using web vulnerability scanners.

V. CONCLUSION

Web vulnerability scanners are useful tools for detecting security flaws in web application and network perimeters. However, they have limitation in terms of coverage, accuracy and false positives. Therefore, web vulnerability must be complementary technique to other approaches as well, such as Static Analysis, code review and manual testing. By combining different methods, web developers and security professional can achieve a higher level of assurance and protection for their web application and services.

REFERENCES

[1]. R. Utaya Surian, Nor Azlina Abd Rahman, Yogeswaran Nathan, Nscanner: Vulnerabilities Detection Tool for Web Application,2020

[2]. Rajab Mohammed imam, Ife Olalekan Ebo, Abdullahi isa Ahmed, VulScan: A Web-Based Vulnerability Multi-Scanner for Web. Retrieved from,2023.

[3]. Rathod, S. K., Jagtap, J. R., Satpute, A. P., Shikhare, K. A., Pujari,A. S., & Pandit. An Automatic Vulnerability Scanner for Web Applications with Firewall Techniques.2022

[4]. Prasanth Satya Sai Kiran Gandikota, Sushani S, Deekshitha Valluri, Gopi Krishna Yanala, Web Application through Comprehensive Vulnerability Assessment,2023.

[5]. Sheetal Bairwa, Bhawna Mewara and Jyoti Gajrani, Vulnerability Scanners: A Proactive Approach To Assess Web Application Security,2014.

[6]. Sandeep Kumar, Renuka Mahajan, Naresh Kumar, Sunil Kumar Khatri., A Study on Web Application Security and Detecting Security,2017.

[7]. Thinzar Aung, Zin Thu Thu Myint, Effective Web Application Vulnerability Testing System Using Proposed XSS_SQL_Scanning_Algorithm,2020

[8]. Sanjukta Mohanty, Arup Abhinna Acharya, Detection of XSS Vulnerabilities Using Security Testing Approaches,2021.

[9]. Divyani Yadav, Deeksha Gupta, Dhananjay Singh, Devendra Kumar, Upasana Sharma, Vulnerabilities and Security of Web Applications,2018.

[10]. Omar Cheikhrouhou, Moez Krichen, Habib Hamam & Abdelouahid Derhab, OWASP Ten Driven Survey on Web Application Protection Methods,2021

DOI: 10.48175/IJARSCT-15627