Вісник Тернопільського національного технічного університету
https://doi.org/10.33108/visnyk_tntu
Scientific Journal of the Ternopil National Technical University
2024, № 4 (116) https://doi.org/10.33108/visnyk_tntu2024.04
ISSN 2522-4433. Web: ***visnyk.tntu.edu.ua***

UDC 004:056

ANALYSIS OF THE EFFICIENCY OF OPEN SOURCE AND COMMERCIAL VULNERABILITY SCANNERS FOR E-COMMERCE WEB APPLICATIONS

Bohdan Tryhubets; Myroslav Tryhubets; Nataliya Zagorodna

Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine

Abstract. *A comparative analysis of the efficiency of the latest versions of popular open source and commercial vulnerability scanners for e-commerce web applications is presented in this paper. A specially developed prototype of web application, OWASP Juice Shop, with embedded relevant vulnerabilities from OWASP Top 10, was chosen as the test object. The quantitative results of using different commercial scanners are described here. Acunetix is pampered to be the scanner that detected the largest number of vulnerabilities of various criticality levels. At the same time, the authors emphasize the need to use several scanners to increase the efficiency of vulnerability detection. The study highlights the importance of regular scanning and monitoring of web application security, especially for e-commerce organizations. However, the authors note that scanners are important but not the only tools for finding vulnerabilities in complex web applications.*

Key words: *vulnerability scanners, web applications, e-commerce, OWASP Top 10, OWASP Juice Shop, web application security.*

https://doi.org/10.33108/visnyk_tntu2024.04.023 *Received 05.09.2024*

1. INTRODUCTION

The coronavirus pandemic and the war in Ukraine have accelerated the already intensive pace of digitalization in all spheres of human life. In particular, this has led to an annual increase in the number of people who make purchases online and, consequently, store their personal and payment data on the servers of various online stores. The rapid growth of the e-commerce market makes it a target for attackers, creates new threats for users, and poses challenges for web application owners [13]. Personal data such as home address, date of birth, bank details, etc., are under special focus of attackers. Leakage of such sensitive data negatively affects the reputation of online stores, leads to financial losses for clients and entails significant fines under European and American jurisdictions.

To systematize information about vulnerabilities and methods of mitigating them, the OWASP community was created. It is an independent organization aimed at creating open standards and tools for assessing and improving the security of web applications. Another aspect of this organization's activity is the popularization of knowledge about web application security issues and research on methods for their protection.

OWASP provides a wide range of information, such as articles, blogs, books, various web tools, and methodologies that help developers, testers, and auditors identify and eliminate vulnerabilities. Additionally, OWASP supports an open environment that helps develop and improve existing tools. In 2003, the OWASP Top 10 standard was created, which proposed a methodology that identifies the 10 most common web application vulnerabilities that should obviously be considered when designing and testing software. Thanks to the regular work of the community and statistical research, the information in the standard is regularly updated to keep pace with the current challenges and reflect changes in technologies and new vectors of possible attacks. These updates usually include new methodologies and tools for assessing and

Corresponding author: Bohdan Tryhubets; e-mail: bogdantrigubets@gmail.com

improving the security of web applications. They help raise awareness among professionals in the field about security issues in this area and enable developers to create secure web applications by promptly taking into account new types of attacks by malicious actors. This research on web application security is based on the list of vulnerabilities formed in the latest update of the OWASP Top 10 standard in 2021.

The rapid growth in popularity and use of e-commerce applications among ordinary users has made them more attractive to cybercriminals as well. At the same time, along with malicious actors, the market for commercial cybersecurity services (penetration testing, security auditing, consulting on the implementation of cybersecurity measures, monitoring, and recovery after cyberattacks) is actively developing, as well as the market for specialized software for identifying potential vulnerabilities in web applications, which can be used by both cybersecurity experts and ordinary IT professionals in this field. Many companies cannot afford to pay for a highly qualified cybersecurity specialist, so in-house IT specialists are often involved in finding vulnerabilities by using specialized software.

2. LITERATURE REVIEW

Web application security scanners are a cost-effective way to find vulnerabilities, allowing the assessment of web application security through the application of typical penetration testing methods [14]. They find potential weaknesses in web applications that can be exploited by attackers to carry out attacks on the site or its visitors. The advantages of automated penetration testing of web applications using vulnerability scanners are:

- reducing the time and resources required for testing,
- decreasing the dependence of test results on the knowledge of test engineers,
- the ability to conduct testing by ordinary IT specialists.

At the same time, web application security scanners have also certain disadvantages. In particular, the generated test results are not always accurate, and some vulnerabilities remain hidden since they cannot be identified by this software. It happens because scanners use only basic penetration testing tools, unlike qualified cybersecurity specialists who possess a broader set of knowledge and tools. However, the cost of software services and a security specialist can differ by tens or even hundreds of times, and not every business can afford a full range of services from qualified in cybersecurity companies. In the community of cybersecurity specialists, discussions are often held, and experiments are conducted to assess the quality of web application security scanners and identify the strengths and weaknesses of different scanners in relation to their cost [12].

Shay Chen, a well-known information security researcher and analyst, has repeatedly conducted comparative analyses of quantitative studies of various scanners, including both open-source and commercial scanners (in 2011, 2012, 2014, and 2016) [1]. However, this information is currently outdated because software of this format keeps up with the times and receives regular updates that supplement, expand, and add new functionality, changing the results of vulnerability detection and the scanner's performance. It is clear that the performance indicators of the same scanner in different versions can differ significantly. In addition, the attack vectors of malicious actors are also changing, and new vulnerabilities in old software are constantly emerging, which fraudsters promptly begin to exploit. Therefore, research of this format should be conducted regularly, taking into account the latest versions of scanners and an updated list of the most popular vulnerabilities.

Other researchers have conducted a comparative performance evaluation of only open-source web vulnerability scanners [2]. As a result of the study, it was found that there is a certain correlation between different characteristics of scanners (for example, scanning speed, coverage of vulnerability types) and the number of vulnerabilities detected by them.

As a result of the analysis of publications [1, 2], it was established that the object of scanning is specially formed web pages that use rather simple and slightly outdated technologies for displaying and processing information, which does not correspond to modern principles of constructing and functioning of e-commerce. The use of such research objects as a prototype of modern web applications does not reflect the real situation and, therefore, calls into question the possibility of applying the results of the conducted research in practice.

The well-known penetration tester and IT evangelist Kinnaird McQuade also conducted research analyzing the efficiency of free scanning tools [3]. The findings of his study indicated that all investigated scanners are effective in finding certain vulnerabilities; accordingly, the best option is to combine several scanners in the work. It should be noted that the results of studies [2] and [3], which were conducted in 2017 and 2014, respectively, can hardly be called relevant. Moreover, they completely left commercial vulnerability scanners out of consideration.

However, all the above-mentioned researchers note that there is a lack of thorough research in the literature with a systematic evaluation of the performance and comparison of web scanners that would take into account their regular updates, which is an urgent necessity for a dynamically developing market.

3. COMPARATIVE ANALYSIS OF SCANNERS

The purpose of this study is to conduct a comparative analysis of the latest versions of popular vulnerability scanners for web applications in the field of e-commerce

OWASP Juice Shop is an object that has been chosen for testing all scanners [4]. It is a specially developed prototype of an e-commerce web application that is unsecured and contains vulnerabilities from the entire OWASP Top Ten, along with many other security flaws that have been discovered on other websites. Such a site is an ideal object for research because, on the one hand, it is built using modern approaches to web development in e-commerce, and on the other hand, it contains embedded relevant vulnerabilities of varying complexity according to the OWASP standard.

In works [1]–[3], the efficiency of scanners was evaluated as a percentage ratio of found vulnerabilities to all embedded ones. However, as mentioned above, the object of the study was a web application built using fairly simple technologies and with a limited range of embedded vulnerabilities. That is why the relative accuracy of vulnerability detection was quite high. In the case of using OWASP Juice Shop [5] as a scanning object that is as close as possible to real conditions, reporting the results in a percentage format is impractical, since this prototype is complex and contains many relevant vulnerabilities that are beyond the capabilities of ordinary scanners.

The list of web scanners does not include many free professional tools. For our study, we selected the most effective web scanners according to researchers and expert practitioners: OpenVAS and Nessus (free version for scanning 16 IP addresses/domains). The list was supplemented with commercial professional tools: Acunetix, Intruder, and Burp Suite Enterprise Edition. The main focus of the study is on finding vulnerabilities for e-commerce web applications.

The list of vulnerabilities to be searched for has been based on recommendations [7] and included SQL injections, cross-site scripting (XSS), authentication process violations, uncontrolled exposure of sensitive information, use of XML External Entities (XXE), access control violations, security configuration errors, insecure deserialization, use of components with known vulnerabilities, insufficient logging and monitoring, and others [8] [9][10][11][16].

The scanning results of the selected object by Acunetix and Burp Suite Enterprise Edition scanners are illustrated in Figures 1 and 2.

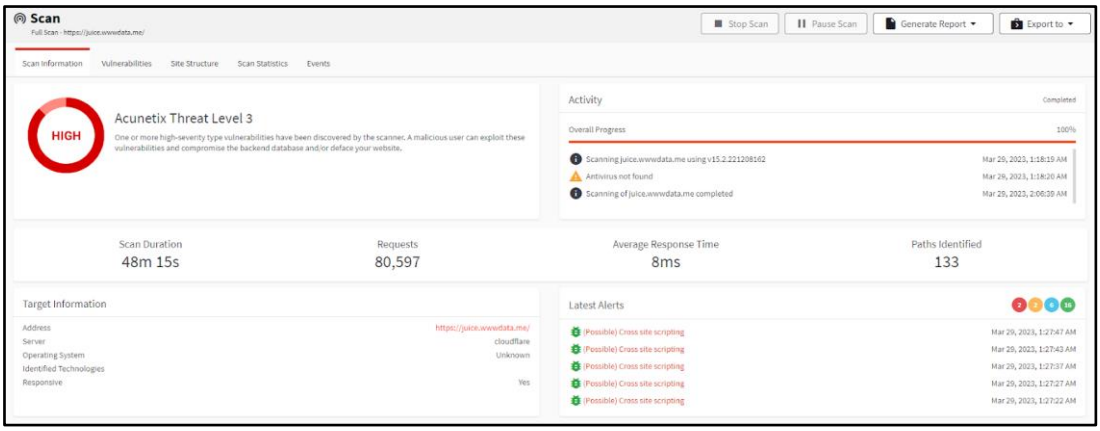

Figure 1. Acunetix scanning result.

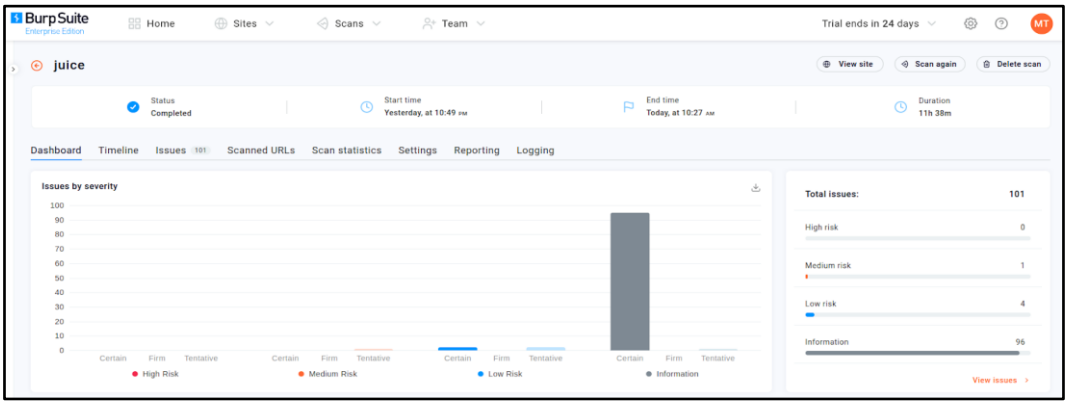

Figure 2. Burp Suite Enterprise Edition scanning result

As a result of the practical study, it was found that the research object contains a number of vulnerabilities. Table 1 includes vulnerabilities that were detected by each of the scanners, according to the OWASP Top Ten 2021 risk classification.

Table 1

Results of vulnerability detection by the studied scanners based on the testing of the OWASP Juice Shop application

OWASP/Scanners	Acunetix	Intruder	Burp Suite Enterprise Edition	Nessus Professional	OpenVAS
1	2	3	4	5	6
A01:2021-Broken Access Control	Unrestricted access to Prometheus Metrics	-		-	-
A02:2021-Cryptographic Failures	Cookies without HttpOnly flag set, Cookies without Secure flag set	-	Private IP addresses disclosed	-	-
A03:2021-Injection	SQL injection, (Possible) Cross-site scripting	-	Cross-site scripting (reflected)	-	-
A04:2021-Insecure Design	-	-		-	-

End of table 1

1	2	3	4	5	6
A05:2021-Security Misconfiguration	Clickjacking: X-Frame-Options header, HTTP Strict Transport Security (HSTS) not implemented, Content Security Policy (CSP) not implemented, Permissions-Policy header not implemented	Strict Transport Security HTTP Header Not Set	Strict transport security not enforced	HSTS Missing From HTTPS Server	-
A06:2021-Vulnerable and Outdated Components	Vulnerable JavaScript libraries		Vulnerable JavaScript libraries	-	-
A07:2021-Identification and Authentication Failures	-	-	-	-	-
A08:2021-Software and Data Integrity Failures	-	-	-	-	-
A09:2021-Security Logging and Monitoring Failures	-	-	-	-	-
A10:2021-Server-Side Request Forgery	-	-	-	-	-

All vulnerabilities were divided into 4 categories, according to their type and potential threat, according to the CVSS classification [6]:

1. High – high-level vulnerabilities. (Injections, authentication errors, and vulnerabilities related to privileges).
2. Medium – medium-level vulnerabilities. (Software failure, vulnerabilities from external entities, vulnerabilities related to data confidentiality).
3. Low – low-level vulnerabilities. (Low severity vulnerabilities such as vulnerabilities from local entities, vulnerabilities related to trust, and vulnerabilities related to incorrect input processing).
4. Informational – vulnerabilities that were detected but do not have a specific severity level and provide information that may be useful for further analysis. (Vulnerabilities that provide information but do not have a specific severity level and do not have a direct impact on system security, such as lack of input validation and information leakage.)

Let's describe in more detail the vulnerabilities found by each of the scanners [15]. The Acunetix scanner found the largest number of serious web vulnerabilities in the OWASP Juice Shop web application. In particular, the following high vulnerabilities were detected: SQL injections (2); medium vulnerabilities: application error messages (1), low vulnerabilities: issues with JavaScript libraries (1), lack of security settings for cookies (3), issues with HTTP Strict Transport Security (HSTS) (1), and informational vulnerabilities: potential Cross-site scripting (XSS) attacks (9), detection of internal IP addresses, and other issues (4). In total, 22 vulnerabilities were detected. The effectiveness of this tool makes it an important element in testing the security of e-commerce web applications.

The Nessus scanner, a commercial product, detected only a few informational vulnerabilities. The detected vulnerabilities include the absence of HSTS on the HTTPS server (1), allowed HTTP methods for each directory (1), HTTP server type and version (1), information about the Hypertext Transfer Protocol (HTTP) (1), and information about HTTP redirection (1). In total, the Nessus scanner detected 5 informational vulnerabilities.

Intruder, which is also a commercial product, detected several low vulnerabilities. Specifically, it found information leakage through an error page (1) and the absence of the Strict Transport Security header in HTTP (1). In total, the Intruder scanner detected only two low vulnerabilities.

The Burp Suite Enterprise Edition software product detected various vulnerabilities during the analysis, including medium vulnerabilities: cross-site request forgery (1), low vulnerabilities: lack of enforced strict transport security (1), open redirection (2), JavaScript dependency vulnerability (1). Regarding informational vulnerabilities, issues with the TLS certificate (1), potential Cross-site scripting (XSS) attacks (1), issues with trusted sources in Cross-origin resource sharing (70), leakage of private IP addresses (1), and others were detected. In total, Burp Suite Enterprise Edition detected 1 medium, 5 low, and 87 informational vulnerabilities.

The OpenVAS scanner, although less effective than the other mentioned tools, still detected a vulnerability in the system. It found one vulnerability in the SSL/TLS ciphers for HTTPS, which belongs to the category of high-level vulnerabilities.

Acunetix, a commercial solution, showed the highest effectiveness in this study, detecting a wide range of vulnerabilities and providing detailed information about their potential impact and mitigation options. However, taking into account the results of all scanners, we agree with the author of the article [3] that the best solution is to combine several scanners.

The results of the vulnerability scanner research may differ significantly from the results in other articles due to large differences in the complexity of the implementation of scanned objects and the total number of embedded vulnerabilities. To avoid creating the illusion that modern versions of scanners perform worse than those analyzed by the authors [1]-[3], during this study, it was decided to evaluate the performance of scanners based on the absolute indicators of the number of vulnerabilities found, rather than relative ones. We consider it impractical to compare the absolute indicators of test results with the known relative ones given in the mentioned publications, because the percentage of detected vulnerabilities depends, among other things, on the total number of embedded vulnerabilities, which was relatively small in the studies of other authors.

4. CONCLUSIONS

As a result of this study, the OWASP Juice Shop e-commerce web application has been chosen for web scanners testing. This prototype contains embedded relevant vulnerabilities that reflect real-life attack scenarios that can be encountered in everyday life in a real web environment using the latest versions of popular open source and commercial web vulnerability scanners (Acunetix, Nessus, Intruder, Burp Suite Enterprise Edition, and OpenVAS). The comparative study of efficiency of given scanners has been conducted here.

The use of the above-mentioned environment and scanners allowed us to identify and analyze in detail potential vulnerabilities that may occur in the context of e-commerce. It was found that the list of detected vulnerabilities for e-commerce web applications does not have significant differences compared to web applications of other types. However, the only presence of such vulnerabilities in web applications that handle confidential user data, including payment and personal information, carries particularly high risks for both businesses and end users.

This research emphasizes the importance of regular scanning and monitoring of web application security. This is especially important for organizations operating in the field of e-commerce, where even minor vulnerabilities can lead to significant reputational and financial

losses. The obtained results can serve as a basis for further research in this area and provide guidance for improving web application security practices.

However, it should be noted that web application scanners are important but not the only tools in the work of cybersecurity professionals who are engaged in vulnerability detection[17]. In the case of working with web applications that use a combination of complex technologies for displaying content to web browsers, web scanners are not capable of finding all vulnerabilities and fully simulating user behavior.

References

1. Shay Chen (2023). Web Application Scanners. SecTools.Org: Top 125 Network Security Tools. Available at: https://sectools.org/tag/web-scanners/.
2. Hindawi. Performance-Based Comparative Assessment of Open Source Web Vulnerability Scanners. Available at: https://www.hindawi.com/journals/scn/2017/6158107/. https://doi.org/10.1155/2017/6158107
3. Kinnaird McQuade. Open Source Web Vulnerability Scanners: The Cost Effective Choice? - ISSN: 2167-1508. Available at: https://www.researchgate.net/profile/Kinnaird-Mcquade/publication/267026342_Open_Source_Web_Vulnerability_Scanners_The_Cost_Effective_Choice/links/546150000cf2c1a63bff83dc/Open-Source-Web-Vulnerability-Scanners-The-Cost-Effective-Choice.pdf.
4. OWASP Juice Shop. Available at: https://owasp.org/www-project-juice-shop/.
5. OWASP Foundation, the Open Source Foundation for Application Security. Available at: https://owasp.org/.
6. Common Vulnerability Scoring System Calculator. Available at: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator.
7. CWE Version 4.10. Available at: https://cwe.mitre.org/data/published/cwe_v4.10.pdf.
8. The Basics of Web Hacking: Tools and Techniques to Attack the Web by Josh Pauli. ISBN: 978-0124166004.
9. Hacking Exposed Web Applications, 3rd Edition by Joel Scambray. ISBN: 978-0071740647.
10. OWASP Web Security Testing Guide (WSTG). Available at: https://owasp.org/www-project-web-security-testing-guide/.
11. SANS Institute – Web Application Penetration Testing. Available at: https://www.sans.org/white-papers/web-application-penetration-testing.
12. Comparative Study of Automated Web Vulnerability Scanners. Available at: https://ieeexplore.ieee.org/document/8691130 .
13. Stuttard D., & Pinto M. (2018). The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (2nd ed.). Wiley.
14. Messier R. (2019). Network Vulnerability Assessment: From Auditing to Continuous Monitoring. O'Reilly Media.
15. Hope P., & Walther B. (2021). Web Security for Developers: Real Threats, Practical Defense. No Starch Press.
16. NIST. (2023). National Vulnerability Database. Available at: https://nvd.nist.gov/.
17. OWASP ZAP Development Team. (2023). OWASP Zed Attack Proxy (ZAP). Available at: https://www.zaproxy.org/.

УДК 004:056

АНАЛІЗ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ БЕЗКОШТОВНИХ ТА КОМЕРЦІЙНИХ СКАНЕРІВ ВРАЗЛИВОСТЕЙ ДЛЯ ВЕБ-ЗАСТОСУНКІВ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Богдан Тригубець; Мирослав Тригубець; Наталія Загородна

Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, Україна

Резюме. *Проведено порівняльний аналіз ефективності використання популярних безкоштовних та комерційних сканерів вразливостей останніх версій для веб-застосунків електронної комерції.*

Актуальність зумовлена стрімким зростанням ринку електронної комерції, що робить його привабливою мішенню для зловмисників та створює нові загрози для користувачів і виклики для власників веб-застосунків. Сканери вразливостей є бюджетним способом пошуку слабких місць у веб-застосунках, проте їх ефективність потребує регулярного переоцінювання в зв'язку з появою нових векторів атак та оновленням сканерів. Метою дослідження було проведення порівняльного аналізу сканерів вразливостей останніх версій для веб-застосунків у сфері електронної комерції. Об'єктом тестування обрано спеціально розроблений прототип веб-застосунку OWASP Juice Shop, який містить актуальні вразливості з OWASP Top 10 та відображає реальні сценарії атак. Для аналізу обрано безкоштовні сканери OpenVAS та Nessus (безкоштовна версія) та комерційні інструменти Acunetix, Intruder, Burp Suite Enterprise Edition. Кількісні результати сканування показали, що комерційний сканер Acunetix виявив найбільшу кількість вразливостей різних рівнів критичності – загалом 22, зокрема 2 високих, 1 середню, 6 низьких та 13 інформаційних. Burp Suite Enterprise Edition знайшов 1 середню, 5 низьких та 87 інформаційних вразливостей. Nessus виявив лише 5 інформаційних вразливостей, Intruder – 2 низькі, а OpenVAS – 1 високу. Водночас, автори наголошують, що найкращим рішенням є одночасне використання кількох сканерів для підвищення ефективності пошуку вразливостей. Разом з тим, сканери не здатні знайти усі вразливості та повноцінно змоделювати роботу користувача у випадку складних за структурою веб-застосунків, які використовують поєднання різних веб-технологій. Отримані результати можуть стати основою для подальших досліджень у цій області та орієнтиром для покращення практик щодо безпеки веб-застосунків.

Ключові слова: *сканери вразливостей, веб-додатки, електронна комерція, OWASP Top 10, OWASP Juice Shop, безпека веб-додатків.*

https://doi.org/10.33108/visnyk_tntu2024.04.023 *Отримано 05.09.2024*