Matrik: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer
Vol. 22, No. 3, July 2023, pp. 481∼493
ISSN: 2476-9843, accredited by Kemenristekdikti, Decree No: 200/M/KPT/2020
DOI: 10.30812/matrik.v22i3.3018

OWASP Framework-Based Network Forensics to Analyze the SQLi Attacks on Web Servers

Imam Riadi, Abdul Fadlil, Muhammad Amirul Mu'min
Universitas Ahmad Dahlan, Yogyakarta, Indonesia

Article Info

Article history:

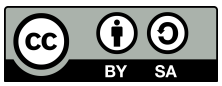
Received May 29, 2023
Revised Juny 23, 2023
Accepted July 08, 2023

Keywords:

Network forensic
Security
Vulnerability
Web servers

ABSTRACT

One of dangerous vulnerabilities that attack the web is SQLi. With this vulnerability, someone can obtain user data information, then change and delete that data. The solution to this attack problem is that the design website must improve security by paying attention to input validation and installing a firewall. This study's objective is to use network forensic tools to examine the designlink website's security against SQLi attacks, namely Whois, SSL Scan, Nmap, OWASP Zap, and SQL Map. OWASP is the framework that is employed; it is utilized for web security testing. According to the research findings, there are 14 vulnerabilities in the design website, with five medium level, seven low level, and two informational level. When using SQL commands with the SQL Map tool to get username and password information on its web server design. The OWASP framework may be used to verify the security of websites against SQLi attacks using network forensic tools, according to the study's findings. So that information about the vulnerabilities found on the website can be provided. The results of this study contribute to forensic network knowledge against SQLi attacks using the OWASP framework as well as for parties involved in website security.



Corresponding Author:

Muhammad Amirul Mu'min, +628989284518,
Master Program of Informatics,
Universitas Ahmad Dahlan, Yogyakarta, Indonesia,
Email: mumin2008048038@webmail.uad.ac.id

How to Cite:
Author, "OWASP Framework-Based Network Forensics to Analyze the SQLi Attacks on Web Serverse", *MATRIK: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer*, Vol. 22, No. 3, pp. 481-493, Jul, 2023.

1. INTRODUCTION

Web applications are gaining popularity with a wealth of more complex features [1]. This technology's complexity is the result of increasing customer demand for more attractive online services [2, 3]. Meanwhile, too-fast public release cycles make online security harder to scale [4, 5]. The year 2021 was arguably the worst record in cybersecurity history. The COVID-19 pandemic seems to have helped trigger a cyber pandemic with many data leaks, identity theft, and malware attacks. The following types of attacks often occur: Crypto mining, social engineering, data leakage, hacking, Cross-Site Scripting (XSS), SQL injection, Clickjacking, DoS, Credential Reusu, Man in the middle, Insider Threat, and Phishing [6]. SQL injection attacks are hacking operations a client application performs by modifying SQL commands in the client application's memory. It is a web application that compromises the database used to store data [7]. Injection method attacks have recently increased, resulting in losses to businesses, governments, communities, and individual targets [8]. Cyberattacks are a major problem for governments, businesses, and scientific institutions [9]. The NCSI (National Cyber Security Index) conducts assessments based on many indicators, including state cybersecurity laws and regulations, availability of government agencies in cybersecurity, government cooperation in cybersecurity, and public evidence such as official government websites or other related initiatives. Not only in Indonesia, government data leaks in developed countries also often occur. Indonesia's cyber security level indexreached 38.96 points. Malaysia finished first with 79.22 points. Singapore came in second with 71.43 points, followed by Thailand with 69.94 points [10]. A comparison of cybersecurity indices in Southeast Asia in 2022 is shown in Figure 1.

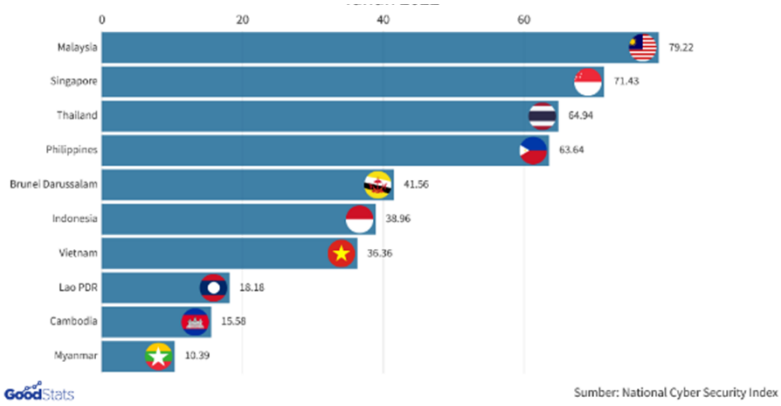


Figure 1. Cybersecurity Index of Countries in Southeast Asia

The cybersecurity index is closely related to the field of network forensics in the process of identifying web security systems. Network forensics is a science that focuses on computer networks and devices connected to a network to find the source of an attack on a server network [11]. A web server is an entity or network software that provides information from a website to clients. In summary, the main function of a web server is as a place for web applications on a network that functions to provide information from a website to clients [12–14]. Almost all applications today use databases to store transferred information, so some people deliberately take advantage of the loophole to steal information [15]. One database storage system that can be used is SQL (Structured Query Language). SQL systems can be attacked using SQL injection, a method of inserting commands on a web server. SQL injection (Structured Query Language) is used to insert SQL commands as input on a website to gain access rights to the database [16]. If the database can be accessed, a hacker can easily steal confidential data and manipulate or damage website data [17]. One method used to test websites for security vulnerabilities can be using the OWASP framework.

OWASP framework is a structured, multi-step framework for grouping information for domain security plans, assessments, and test reports that are verified and analyzed [18]. The OWASP Framework is an open-source framework published by the OWASP community that lists the top 10 vulnerabilities that can compromise website security. This list continues to grow and change as technology develops [19, 20]. Based on OWASP in 2004, there were ten types of attacks such as broken access control, security misconfiguration, insecure deserialization, injection, exposure of sensitive data, external XML entities, broken authentication, cross-site scripting, using components with known vulnerabilities, insufficient logging, and monitoring. Of the ten attacks, SQL injection was one of the easiest attacks to perform, accounting for about 44.11% after Local File Inclusion (LFI) compared to other attacks [21]. One of the tools used is SQL Map. These tools are open-source and can be installed on Kali Linux and Windows. This tool is used to detect and exploit injection vulnerabilities on the web. The application can take over database servers [22, 23]. The basic

step used in SQL injection is to enter standard commands in SQL, such as create, insert, update, drop, alter, union, and select, along with other commands [24].

Research [24] by title Vulnerability Analysis Website Renovaction Using a Suite of Security Tools Project Based on the Owasp Framework; the study aims to analyze website vulnerabilities to avoid cyber attacks, especially in the types of Cross Site Scripting &; SQL Injection attacks, by applying OWASP Top 10 2017 rules. References [25] by title research on Attack and Security Analysis on SQL Injection has the purpose of explaining how to deal with SQLi attacks and how these attacks exploit website vulnerabilities. Research by [26] titled SQL Injection Attack Analysis on Online Study Plan Card (KRS) Charging Server aims to simulate an injection attack on the Study Plan Card charging system to determine whether the system has an injection attack gap. Research [27] by title Security Analysis on Websites using the Information System Assessment Framework (ISSAF) and Open Web Application Security Version 4 (OWASPv4) using the Penetration Testing Method; the goal is to identify vulnerabilities in websites. The findings revealed several vulnerabilities, including lacking jquery updates on the ITTP website. A total of ten tests were conducted, with five using the ISSAF framework and five using OWASP version 4. Notably, during the ISSAF assessment, robots.txt files found on the S1 Informatics website, store important information and display exploitable sitemaps. Research [28] by title Website Vulnerability Testing and Analysis of Internet Management Information System Using OWASP approached gray box penetration testing for websites by utilizing the OWASP framework and OWASP ZAP tools to collect target information, perform automated scans with the help of OWASP ZAP, exploit scan results, generate reports, and offer recommendations. The results showed that the OWASP framework could be used to find high, medium, and low-level vulnerabilities in websites.

Previous studies have only mitigated injection attacks and have not tested injection attacks using SQL Map tools. In addition, the tools used have not covered all stages in the OWASP Framework. Therefore, this study used tools covering all stages of the OWASP Framework: Gathering Information using Whois tools, SSL Scan; Network Mapping using Nmap and OWASP Zap; Exploiting using SQL Map. This study aims to test the security of graphic designer websites from SQLi attacks using network forensic tools, namely Whois, SSL Scan, Nmap, OWASP Zap, and SQL Map based on the OWASP framework. The findings from this study are expected to be a valuable reference for institutions that utilize websites as information platforms in choosing the right web security tools.

This article is organized as follows: Section 1. Introduction, which includes distinctions from earlier research, part 2. Research Methods, which discusses the OWASP Framework to obtain the expected research results, part 3. Results and Analysis, which explains the research analysis results using the OWASP framework on a web server using the Whois, SSL Scan, Nmap, OWASP Zap, and SQL Map tools, section 4. The conclusion summarizes the study's findings and gives recommendations for future research.

2. RESEARCH METHOD

The OWASP Framework is used in this study to evaluate and test web server security in four stages: Data collection, Penetration Testing, Analysis, and Reporting. The OWASP framework is used to incorporate these four steps into testing. Figure 2 depicts the four processes that must be completed to achieve proper study results.

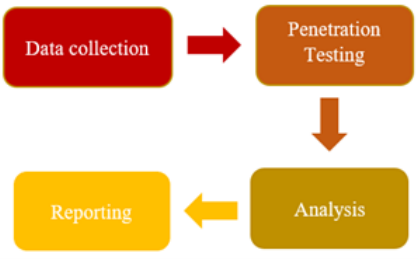


Figure 2. Stages of Research Methods Using the OWASP Framework

During the data collection phase, information related to the selected topic is gathered, and a survey is conducted. Subsequently, penetration testing is performed on the website to evaluate its security. This testing involves a pentester simulating a real attack to identify vulnerabilities that could potentially compromise the application, system, or network's security features. An extensive analysis of the web server is conducted during this stage to pinpoint any weaknesses. Finally, a detailed report is prepared, describing the analysis results and findings obtained from the testing process. There are three stages in conducting testing using the OWASP framework, which can be seen in Figure 3.

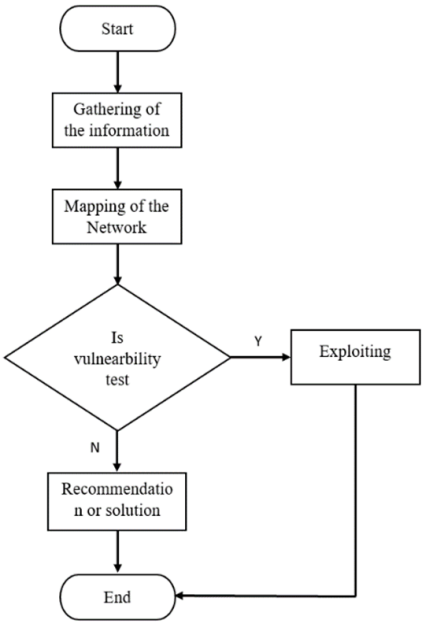


Figure 3. Flowchart Testing Stages Using the OWASP Framework

Figure 3 is the testing stage in this study using OWASP Framework. Namely, in the first stage, information is gathered using Whois and SSL Scan; the second stage of mapping the network is to scan for vulnerabilities using Nmap and OWASP ZAP tools. After performing a complete vulnerability scan, proceed to the third stage, which is exploiting using SQL map tools.

A schematic diagram of the SQL injection test scenario on the web server using the SQL map tool is shown in Figure 4.

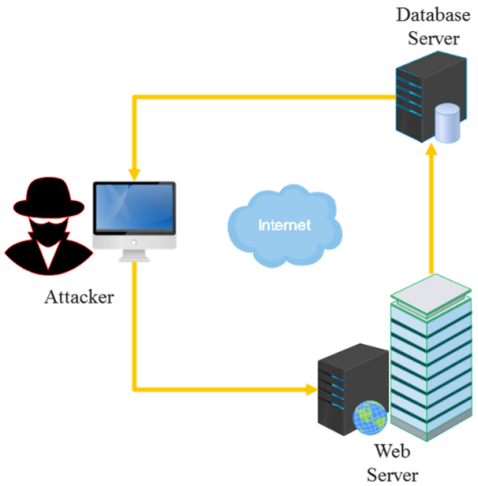


Figure 4. A Schematic Diagram of the SQL Injection Test Scenario on the Web Server by Using the SQL Map Tool

In Figure 4, it can be explained that the schematic diagram is the attack scenario in this study. Attackers connected to an internet network attack the web server using SQL Map tools. SQL Map sends database requests from a web server with SQL commands. A web server not protected by a firewall will send requests to the attacker.

The OWASP framework testing process aims to evaluate the vulnerabilities on the web server after the completion and implementation stages are carried out. The tools used in the analysis using the OWASP framework are shown in Table 1.

Table 1. The Tools Used in the Analysis Using the OWASP Framework

Stages	Tools	Information
Gathering of the information	Whois dan SSL Scan	Looking for website information
Mapping of the Network	Nmap	Scan ports
	OWASP Zap	Vulnerability Scan
Exploiting	SQL Map	Vulnerability Exploitation

3. RESULT AND ANALYSIS

Based on the OWASP framework, several stages exist to determine and combine the vulnerability risk level on a web server. The stages include Data Collection, Penetration Testing, Analysis, and Reporting [29].

3.1. Data Collection

At this stage, the data collected to support the experiment in this study is data on the designlink.com.hk website. The OWASP framework is used to find vulnerabilities that exist on the web.

3.2. Penetration Testing

Penetration testing is a stage of testing on the web to find vulnerabilities, identify poor system configurations, hardware and software defects, and identify technical weaknesses in the information system being tested [30]. Penetration testing is useful for finding and addressing vulnerabilities in network infrastructure, showing how vulnerable it is to malicious attacks on the network. There are three stages carried out in penetration testing: gathering the information, mapping the network, and exploiting it. Gathering the information is the first step in identifying vulnerabilities. This includes searching for more in-depth information about the web server. At this stage, the desired information on the web server will be obtained using the whois and SSL Scan tools. The results using the whois tool are shown in Figure 5.

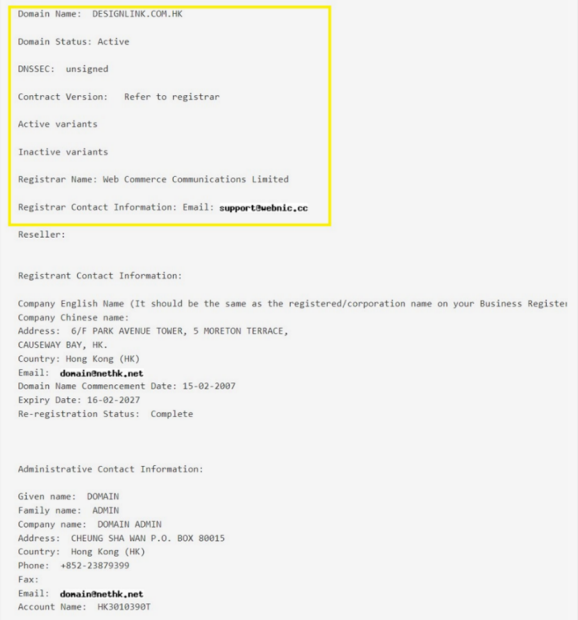


Figure 5. The Results Using the Whois Tool

From Figure 5, it can be explained that the Whois tool gets information about web servers such as domain name, domain registry, registration contact, registration email, and registration expiration. Figure 6 is the result of searching for information using the SSL Scan (Secure Socket Layer) tool.

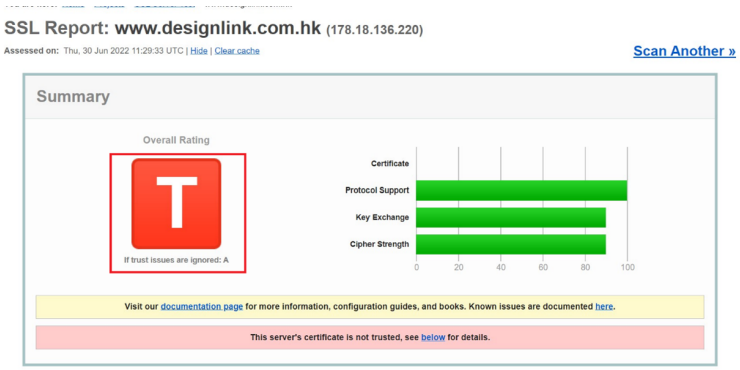


Figure 6. The results of the SSL Scan tool Scanning

Figure 6 shows that SSL scanning tools found that the Web server does not use SSL security when hosting, so hackers can easily hack the Web server. Therefore, more attention should be paid to the support protocol by using the latest version. Mapping the network on a web server using the OWASP Framework with Nmap and OWASP Zap tools is scanning ports/hosts and looking for vulnerabilities on the web server. The results of the port scanning can be seen in Figure 7.

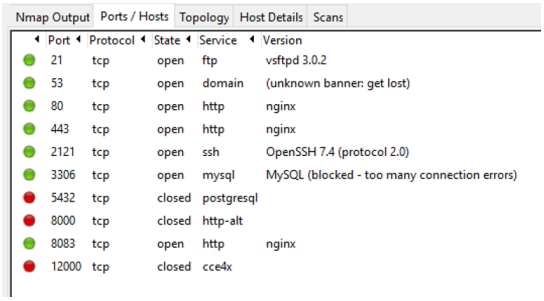


Figure 7. Port Scan Results Using the Nmap Tool

In Figure 7, the results of testing using Nmap tools showed there are seven ports with open status, namely ports 21, 53, 80, 443, 2121, 3306, and 8083 with the TCP (Transmission Control Protocol) protocol, and three ports with closed status, namely 5432, 8000, and 1200. Figure 8 is the result of a scan using the OWASP Zap tool.

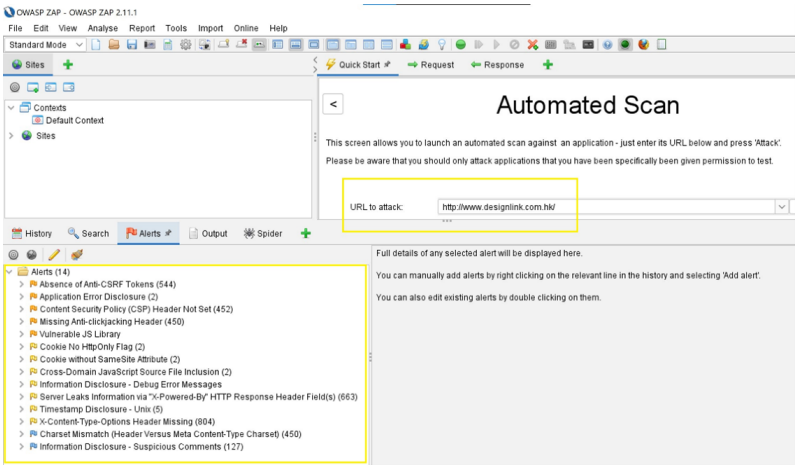


Figure 8. Scan Results Using the OWASP Zap tool

Figure 8 illustrates the scanning so that incoming data and information can be known how vulnerable or secure the web server is and all the associated risks and also to find vulnerabilities or threats embedded in the web server. The results can be seen in Figure 9.

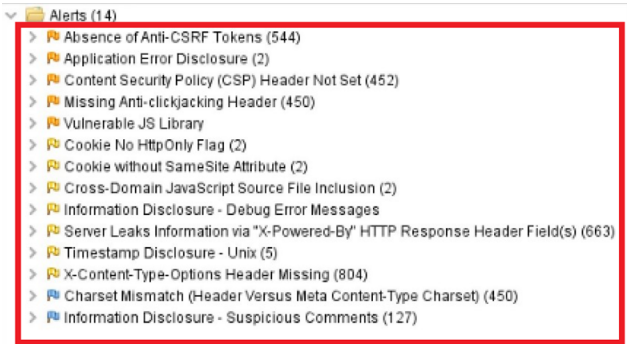


Figure 9. Vulnerability Results Using OWASP Zap Tools

Figure 9 depicts the results of vulnerabilities on a web server with 14 vulnerabilities, five with a medium level, seven with a low level, and two with an informational level. This scanning has no high-level vulnerabilities, but many medium-level vulnerabilities must be fixed.

Exploiting testing of security vulnerabilities from data obtained previously can be used as material for further vulnerability testing using SQL Map tools. The results can be seen in Figure 10.

Figure 10. URL Input

Figure 10 shows SQL commands performed on a web server not protected against SQL injection vulnerabilities to obtain database information using the dbs command. The result of a database query can be seen in Figure 11.

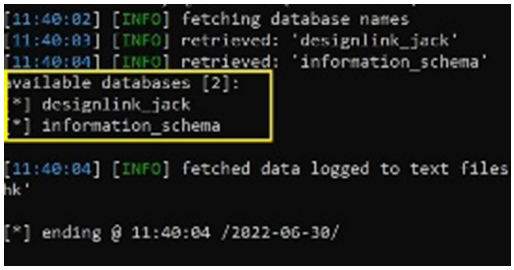


Figure 11. Result of -dbs Request

Figure 11 shows the results of the dbs command finding two database names: accurate and information_schema. The web does not have any security that causes attackers to get that information easily. Figure 12 is a command to display a list of tables.

Figure 12. Result of -dbs Request

Figure 12 shows the usage of SQL Map tools to bring up a list of tables to find table data on the web server, as seen in Table 2. The obtained results correspond to the requests made for the table data.

Table 2. Tables Query Results

No	Nama tables
1	Dnd_adminlogin
2	Dnd_blog
3	Dnd_blog_categories
4	Dnd_brands
5	Dnd_contactus

Table 2 displays the query results by running the -tables command and finding eight tables in the designlink_jack database. Figure 13, on the other hand, shows the dnd_adminlogin table command.

Figure 13. Command Table dnd_adminlogin

In Figure 13, the command -T dnd_adminlogin -dump is performed to display the contents of the columns in the dnd_adminlogin table. The results can be seen in Table 3.

Table 3. Results of the Table dnd_adminlogin

id	username	password
1	dndlink	SSGBj6Tuy

Table 3 illustrates the successful extraction of data and information from the web server utilizing the SQL Map tool's SQL command.

3.3. Analysis

The vulnerability results from testing the web server in the previous stage will be analyzed. The analysis will be carried out on the web server that is the target of this research. The analysis results using the OWASP Framework can be seen in Table 4.

Table 4. Recapitulation of Found Vulnerabilities

Risk Level	Number of Alerts
High	0
Medium	5
Low	7
Informational	2

Table 4 shows a high level of vulnerability that has a score of 0% or no vulnerability; a medium level has a value of 33.3% (5) vulnerability, that is, Absence of Anti-CSRF Tokens, Application Error Disclosure, Content Security Polyce (CSP) Header Not Set, Missing Anti-clickjacking Header, Vulnerable JS Library; a low level has a value of 50% (7) vulnerability that is Cookie No HttpOnly flag, Cookie without SameSite Attribute, Cross-Domain JavaScript Source File Inclusion, Information Disclosure-Debug Error Messages, Server Leaks Information via X-Powered-By HTTP Response Header Fields, Timestamp Disclosure-Unix, X-Content-Type-Options Header Missing; and an information level has a value of 16.7% (2) vulnerability that is Charset Mismatch (Header Versus Meta Content-Type Charset), Information Disclosure-Suspicious. The website can still be regarded as safe based on the vulnerabilities discovered. The results of the security testing analysis based on the Top 10 OWASP of 2021 are shown in Table 5.

Table 5. Vulnerability Based on the Top 10 OWASP in 2021

Vulnerability	Solution
Broken Access Control	Implementing an access control system is reused in all applications to minimize CORS (Cross-Origin Resource Sharing) users so that users cannot create, read, update, or delete records freely. The access control model should limit this by using ownership for each record and disabling the web server listing directory.
Cryptographic Failures	Not Found
Injection	Not Found
Insecure Design	Not Found
Security Misconfiguration	System maintainers can review and update the appropriate configuration for all security notes, updates, and patches as part of the patch management process.
Vulnerable and Outdated Components	Removes unused dependencies, unnecessary features, components, files, and documentation.
Identification and Authentication Failures	Not Found
Software and Data Integrity Failures	Use digital signatures or similar mechanisms to verify that software or data is not manipulated from an expected source.
Security Logging and Monitoring Failures	Not Found
Server-Side Request Forgery	Not Found

3.4. Reporting

At this stage, the step performed is summarizing the results of the analysis that has been carried out and creating a report on the results found on the web server. Table 6 presents a report on the research data acquired through implementing the OWASP Framework.

Table 6. Report on Research Results Using OWASP Framework

Stage	Parameter	Tools	Result
Gathering of the information	Domain name, domain status, email, expiry date.	Whois	success
	Overall rating	SSL Scan	success
Network Mapping	Port	Nmap	success
	Vulnerability	OWASP Zap	success
Exploiting	Username and password	SQL Map	success

Table 5 provides information on how the OWASP Framework can be used to discover ownership data of a website domain and identify vulnerabilities associated with the website. A comparison of research results obtained in other studies using the OWASP framework can be seen in Table 7.

Table 7. Comparison with Previous Research

No	Title	Object	Parameter	Tools	Result
1	Web Server Security Analysis using the OWASP Mantra Method	Web	DDoS	Acunetix	The OWASP test results reveal that authentication, authorization, and session management have been incorrectly implemented.
2	Security analysis to determine vulnerabilities in DVWA Lab Esting Using Penetration Testing Standart OWASP	Website DVWA Lab	SQL injection	DVWA	In the test results, there are MySQL functions and queries that are not filtered, so in this case, it is not feasible to use in terms of websites because attackers can take over servers and databases.
3	Quality Analysis of Website-Based E-Office Information System Security on Rosma Stmik Using OWASP Top 10	E-office information system	Injection, Broken Authentication, Sensitive data Exposure, XXE, Broken access control, Security Misconfiguration, XSS, Insecure deserialization, using components with known Vulnerabilities	OWASP Zap and SQL Map	In the test results, the e-office information system has 13 vulnerabilities, and based on OWASP TOP 10, the e-office information system STMIK ROSMA was detected to have four vulnerabilities.
4	This study	Web server	SQL Injection	Whois, SSL Scan, Nmap, OWASP Zap, and SQL Map	The results found the web server is at a moderate level, and using SQL Map, the web username and password were obtained.

Based on Table 8. it can be seen that the results of the researchers' research were compared with the research on Web Server Security Analysis with the OWASP Mantra Method [30],using Acunetix tools to get results reaching around 90%, authentication management, authorization, and session management were not implemented properly. Security analysis research to find out vulnerabilities in DVWA Lab Esting Using the OWASP Penetration Testing Standard [31], using DVWA tools, the test results show that there are unfiltered MySQL functions and queries, so in this case they are not suitable for use on websites because attackers can take switch servers and databases. Research on Analysis of Security Quality of Website-Based E-Office Information Systems on Rosma STMIK using OWASP Top 10 [18]. using the OWASP Zap tool was detected to have four vulnerabilities: sensitive data exposure, security configuration errors, cross-site scripting, and Insecure Drops. When compared with previous research, this research uses the same OWASP framework. The tools used in this research are Whois, SSL Scan, Nmap, OWASP Zap, and SQL Map. Results found using Whois retrieved the web identity, SSL Scan found the web in an Overall Rating state, Nmap found three ports with a closed status and seven ports with an open status, OWASP Zap found moderate web design vulnerabilities, with a total of 14 vulnerabilities, and SQL Map successfully retrieved web design username and password data. Whereas in previous studies only used one tool to test web servers without searching for information about the web and scanning network ports as was done in this study. The results of this study contribute to forensic network knowledge against SQLi attacks using the OWASP framework as well as for parties involved in website security.

4. CONCLUSION

Based on the results of the analysis on the website design using the OWASP framework in testing against SQLi attacks. The results of the Whois tool get a web identity, SSL Scan gets an Overall Rating value, Nmap finds three ports with closed status and seven ports with open status, OWASP Zap finds 14 vulnerabilities including; five at Intermediate level, seven at low level, and two at Information level, and the SQL Map tool successfully retrieved usernames and passwords on the web. This illustrates that the web server design does not have adequate security and validation against the vulnerabilities of various attacks, especially injection. attacks. From the results of using SQL Map tools for injection attacks to get results that are right on target, it shows that SQL Map can detect databases and important data on web servers only when the website is not protected, whereas when the website is protected, SQL Map will fail to exploit the website. This research is in accordance with the objectives of the researcher, so that the researcher can obtain the results as expected. Future research, the researcher suggests studying many SQLi techniques using various frameworks and tools to run web server penetration testing. Future research should reveal more SQL injection techniques using various frameworks and tools to execute web server penetration testing.

5. DECLARATIONS

AUTHOR CONTIBUTION

This study was compiled by three authors divided into their respective tasks. Muhammad Amirul Mu'min compiles and designs work, collects, analyzes, and interprets data. Imam Riadi and Abdul Fadlil as supervisors for articles to be published.

FUNDING STATEMENT

This study received no specific financing from any funding agency in the public, commercial, or non-profit sectors.

COMPETING INTEREST

I am unrepresented by conflicting financial, public, or institutional interests.

REFERENCES

[1] I. N. T. A. Putra, "Pengembangan Sistem Inventaris Berbasis Qr Code Menggunakan Web Service Pada Bidang Sarana Dan Prasarana Stmik Stikom Indonesia," *Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI)*, vol. 7, no. 3, pp. 315–323, 2019.

[2] I. Riadi, D. Aprilliansyah, and S. Sunardi, "Mobile Device Security Evaluation using Reverse TCP Method," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, vol. 4, no. 3, pp. 289–298, 2022.

[3] B. Wiguna, W. A. Prabowo, and R. Ananda, "Implementasi Web Application Firewall dalam Mencegah Serangan SQL Injection pada Website," *Digital Zone: Jurnal Teknologi Informasi dan Komunikasi*, vol. 11, no. 2, pp. 245–256, 2020.

[4] A. Purwanto and A. W. R. Emanuel, "The State of Website Security Response Headers in Indonesia Banking," *AIP Conference Proceedings*, vol. 2296, no. November, pp. 1–8, 2020.

[5] D. Kellezi, C. Boegelund, and W. Meng, "Securing Open Banking with Model-View-Controller Architecture and OWASP," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–13, 2021.

[6] A. Adianto, "Mengenal 14 Jenis Serangan Siber dan Cara Mencegahnya," 2023.

[7] K. Goel and A. H. Hofstede, "Privacy-Breaching Patterns in NoSQL Databases," *IEEE Access*, vol. 9, no. 5, pp. 35 229–35 239, 2021.

[8] M. Fierza and E. Erlangga, "Analisa Celah Keamanan Dalam Pengembangan Website E- Commerce (Studi Kasus : Mataharimu.Com)," *Jurnal Ilmiah Computing Insight*, vol. 3, no. 2, pp. 20–27, 2021.

[9] Pramono, A. Sunyoto, and E. Pramono, "Deteksi Serangan SQL Injection Menggunakan Hidden Markov Model," *Jurnal Tecnoscienza*, vol. 5, no. 2, pp. 243–256, 2021.

[10] N. N. Alifah, "Keamanan Siber Negara Asia Tenggara 2022, Indonesia Peringkat Berapa?" 2022.

[11] S. Suharti, A. Yudhana, and I. Riadi, "Forensik Jaringan DDoS menggunakan Metode ADDIE dan HIDS pada Sistem Operasi Proprietary," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 21, no. 3, pp. 567–582, 2022.

[12] A. Anggrawan, R. Azhar, B. K. Triwijoyo, and M. Mayadi, "Developing Application in Anticipating DDoS Attacks on Server Computer Machines," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 20, no. 2, pp. 427–434, 2021.

[13] M. G. Valls and L. Song, "Mejora de la seguridad de los servidores web en sistemas críticos de IoT a través del autocontrol de vulnerabilidades," *Sensors*, vol. 22, no. 13, pp. 1–17, 2022.

[14] B. Mburano and W. Si, "Evaluation of Web Vulnerability Scanners Based on OWASP Benchmark," *26th International Conference on Systems Engineering, ICSEng 2018 - Proceedings*, vol. 12, pp. 11 068–11 076, 2019.

[15] T. Hardiani, D. Wijayanto, N. Latifah, P. Studi, and T. Informasi, "Data Security Analysis with OWASP framework on website XYZ," *CYBERNETICS*, vol. 6, no. 01, pp. 10–20, 2022.

[16] M. N. Hafizh, I. Riadi, and A. Fadlil, "Forensik Jaringan Terhadap Serangan ARP Spoofing menggunakan Metode Live Forensic," *Jurnal Telekomunikasi dan Komputer*, vol. 10, no. 2, pp. 111–120, 2020.

[17] F. M. M. Mokbal, W. Dan, A. Imran, L. Jiuchuan, F. Akhtar, and W. Xiaoxi, "MLPXSS: An Integrated XSS-Based Attack Detection Scheme in Web Applications Using Multilayer Perceptron Technique," *IEEE Access*, vol. 7, pp. 100 567–100 580, 2019.

[18] Y. Yudiana, A. Elanda, and R. L. Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP Top 10," *CESS (Journal of Computer Engineering, System and Science)*, vol. 6, no. 2, pp. 185–191, 2021.

[19] I. Riadi, R. Umar, and T. Lestari, "Analisis Kerentanan Serangan Cross Site Scripting (XSS) pada Aplikasi Smart Payment Menggunakan Framework OWASP," *JISKA (Jurnal Informatika Sunan Kalijaga)*, vol. 5, no. 3, pp. 146–152, 2020.

[20] A. Alanda, D. Satria, H. A. Mooduto, and B. Kurniawan, "Mobile Application Security Penetration Testing Based on OWASP," *IOP Conference Series: Materials Science and Engineering*, vol. 846, no. 1, pp. 1–13, 2020.

[21] R. Hermawan, "Teknik Uji Penetrasi Web Server Menggunakan SQL Injection dengan SQLmap di Kalilinux," *STRING (Satuan Tulisan Riset dan Inovasi Teknologi)*, vol. 6, no. 2, pp. 210–216, 2021.

[22] T. D. P. Irwansyah, "Evaluasi Keamanan Sistem Informasi Pada Lembaga Pemerintahan Provinsi Sumatera Selatan," no. November, pp. 1–14, 2022.

[23] A. Evwiekpaefe, A. E. Evwiekpaefe, and I. Habila, "Implementing SQL Injection Vulnerability Assessment of an E-commerce Web Application using Vega and Nikto Tools," © *Afr. J. Comp. & ICT*, vol. 14, no. 1, pp. 1–8, 2021.

[24] E. Darwis, Junaedy, and I. A. Musdar, "Analisis Kerentanan Website Renovaction Menggunakan Rangkaian Security Tools Project Berdasarkan Framework Owasp," *KHARISMA Tech*, vol. 17, no. 1, pp. 1–15, 2022.

[25] A. D. Djayali, "Analisa Serangan SQL Injection pada Server pengisian Kartu Rencana Studi (KRS) Online," *Jurnal Manajemen Informatika dan Komputer*, vol. 1, no. 1, pp. 16–24, 2020.

[26] D. P. Anggraeni, B. P. Zen, and M. Pranata, "Security Analysis on Websites Using the Information System Assessment Framework (ISSAF) and Open Web Application Security Version 4 (OWASPV4) Using the Penetration Testing Method," *Jurnal Pertahanan*, vol. 8, no. 3, pp. 497–506, 2022.

[27] D. Priyawati, S. Rokhmah, and I. C. Utomo, "Website Vulnerability Testing and Analysis of Internet Management Information System Using OWASP," *International Journal of Computer and Information System (IJCIS) Peer Reviewed-International Journal*, vol. 03, no. 03, pp. 2745–9659, 2022.

[28] B. Ghozali, K. Kusrini, and S. Sudarmawan, "Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating," *Creative Information Technology Journal*, vol. 4, no. 4, pp. 264–275, 2019.

[29] I. G. A. S. Sanjaya, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," *Jurnal Ilmiah Merpati*, vol. 8, no. 2, pp. 113–124, 2020.

[30] B. Subana, A. Fadlil, and Sunardi, "Web Server Security Analysis Using The OWASP Mantra Method," *Mobile-Based National University Online Library Application Design*, vol. 4, no. 3, pp. 1–7, 2020.

[31] A. P. Armadhani, D. Nofriansyah, and K. Ibnutama, "Analisis Keamanan untuk Mengetahui Vulnerability pada DVWA Lab esting Menggunakan Penetration Testing Standart OWASP," *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)*, vol. 21, no. 2, pp. 80–88, 2022.