e-ISSN: 2614-8404
p-ISSN: 2776-3234

Penetration Testing Tangerang City Web Application With Implementing OWASP Top 10 Web Security Risks Framework

Yoel Armando[1], Rosalina[2*]
[1,2]Study Program Informatics, Faculty of Computing, President University, Indonesia
[*]Email: rosalina@president.ac.id

Abstract – The speed of technological development has made it possible for all people to be connected to one another. The creation of web-based information systems that help in all areas, including government, health, and education, is one of the forces behind the development of technology. With these technological advancements, websites are susceptible to cybercrimes that could end in the theft of crucial data. Top 10 Web Application Security Risks is the most effective prevention process for decrease company information leaks. On the website tangerangkota.go.id, the researcher will conduct a test using the Top 10 Web Application Security Risks technique. Top 10 Web Application Security Risks consist of Broken Access Control, Cryptographic Failures, Injection, Insecure Design, Security Misconfiguration, Vulnerable and Outdated Components, Identification and Authentication Failures, Software and Data Integrity Failures, Security Logging and Monitoring Failures, Server-Side Request Forgery. The penetration testing results found on the Tangerang City website which are 4 injections, 2 broken access controls, 1 security misconfiguration.

Keywords – Penetration Testing, OWASP 10, Vulnerability Assessment, Exploitation.

I. INTRODUCTION

The advancement of information technology (IT), particularly the internet and information systems or applications that are web-based, has significantly altered human life. The security of users must be carried out in conjunction with this rapid technological advancement.

Internet users who browse the web need to be shielded. As a result, users should consider security as an important indicator. Due to the importance for protection, every field possesses distinct levels of security. Security in the public field (domain *.go.id) is distinct from those found in educational institutions (domain *.sch.id or.ac.id). There were 976.429.996 cyberattacks in 2022, with malware activities, web defacement, data breaches, human-operated ransomware, phishing, and advanced persistent threats continuing to cause the majority of traffic anomalies [1]. According to the report, the government agency sector was attacked by about 68% of respondents, followed by e-commerce by 17%, financial institutions by 11%, social media by 3%, and cryptocurrencies by 1%.

Tangerang in the province of Banten uses a web-based information system (with the domain * https://tangerangkota.go.id/) to disseminate information about official activities that is beneficial to residents in general and Tangerang residents in particular. Unfortunately, it cannot be denied that defacement attacks from outside sources led to user information being exposed within the Tangerang government website. One of the world's defacement archives, www.zone-h.org, allows users to view the attack's history. An archive website called Zone-H maintains a list of websites that have been affected.

Zone-h data indicates that cyberattacks caused by web defacement have occurred against the Tangerang website. Despite the fact that the attack took place in 2016, it may still occur due to a fresh revealing (vulnerability) that the manager of the Tangerang website has not yet discovered and may be exploited again.

The aims of this study is to analyze web security testing with the domain tangerangkota.go.id from attacks from irresponsible outsiders that can damage Tangerang City, analyze applications under development for web security testing, implement a system tool for testing security gaps in web applications.

Muhammad Subagja is testing the application security system using Zero Entry Hacking. The results are that each web he tests has 41 vulnerabilities, and the average CVSS is medium level [2]. Ahmad Fikri Zulfi found an XSS gap on two subdomains of Jember University that can be exploited to change the web's appearance or insert links to enter other websites. The vulnerability cannot be exploited further [3]. The definition of vulnerability is a weak point where a system is vulnerable to attack [4]. Vulnerability is a weakness that threatens an asset's integrity, confidentiality, and availability [5].

Afif Zirwan uses Acunetix WVS tools and information system security principles to test the Institute of Technology Padang website, and have six vulnerabilities with the CVSS are medium and high levels [6]. Common Vulnerability Scoring System (CVSS) is an open framework used to communicate the characteristics and impact of an application vulnerability. A decrease in the vulnerability score after improvement indicates that the security evaluation carried out has been able to reduce the risks that previously existed, and it can be said that the website has become relatively safe [7].

Harry and M. Akbar analysis of binadarma.ac.id vulnerability in the outdated version application using SQL Injection attacks and found several vulnerabilities due to the outdated application [8].

Mira and Michael do security analysis using vulnerability assessment principles and NMAP to check for denial of service attacks, find XSS vulnerabilities in PHP files, and find vulnerabilities to SQL Injection attacks [9]. Nmap or Network Mapper is an open-source

e-ISSN: 2614-8404
p-ISSN: 2776-3234

network security exploration and auditing tool [10]. Nmap is an application used to scan Mikrotik routers to identify existing vulnerabilities [11]. Nmap is a tool used to determine the computer's services through port scanning [12].

Feri, Harjono, and Agung analyzed security gaps using the open vulnerability assessment system and Acunetix web method to compare the result of the two tools and the results they found weaknesses in 9 data on OpenVAS with the scanning time of 60 minutes. In contrast, Acunetix WVS found weaknesses in 166 data with scanning times of 954 minutes [13].

Vulnerability Assessment (VA) is a process carried out on a website to define, identify and classify possible security gaps in computer networks or communication infrastructure [14]. Vulnerability Assessment is a step to detect, identify and study a computer system's or network infrastructure's weaknesses [15].

II. RESEARCH METHODOLOGY

The steps taken in testing the security system can be seen in Figure. 1.

Figure 1. Top 10 OWASP Framework

Based on the standards issued by the OWASP Framework, there are ten steps that can be taken to assess and test the security of a website:

1. Broken Access Control
   These vulnerabilities allow attackers to exploit these weaknesses to access unauthorized data or functions.
2. Cryptographic Failures
   This vulnerability arises due to the improper use of cryptographic technology in web applications, resulting in confidential data being accessible to attackers.
3. Injection This vulnerability is due to inadequate input methods in web applications, allowing attackers to insert malicious codes into systems that use inputs such as forms, URL parameters, or comment fields.
4. Insecure Design
   This vulnerability arises when the manager neglects the proper design of the security system in the web application, such as not creating a One Time Password (OTP) or authentication feature on the login page. This allows attackers to access sensitive data and even steal user information.
5. Security Misconfiguration
   This vulnerability occurs when unused features remain enabled or installed, the security system is not updated to the latest version, and default passwords are used. This allows attackers to perform DDOS attacks or brute force attacks and obtain sensitive data, such as user information.
6. Vulnerable and Outdated Components
   This vulnerability occurs in web applications that do not use the latest components or libraries and have vulnerabilities that can be exploited.
7. Identification and Authentication Failures
   This vulnerability occurs in web applications when attackers have a list of valid usernames and passwords, or when weak default passwords such as admin/admin are used.
8. Software and Data Integrity Failures
   This vulnerability occurs in web applications when attackers have a high probability of uploading updates to the system that they distribute, which can be downloaded or run by all installations.
9. Security Logging and Monitoring Failures
   This vulnerability occurs in web applications when managers ignore the results contained in logs, such as login failures, transaction failures, and unclear error warnings. This allows attackers to exploit this to perform various injections into the security system.
10. Server-Side Request Forgery
    This vulnerability occurs in web applications that allow attackers to manipulate HTTP requests made on the server side. This allows attackers to connect to the internal network or internet connection to the server to steal important data.

Black box testing is utilized during the process of penetration testing. The research process commences with planning and review, during which the object of research is selected and pertinent data is gathered. Subsequently, the scanning of the research object is carried out. Once exploitable information results are obtained from the scan results, the next step involves the use of tools or manual exploitation to exploit the gap information. For the purpose of penetration testing, researchers utilize a set of nine tools, which include NMAP, ZAP, SQLmap, BurpSuite, Wappalyzer, The Harvester, WHOIS, and CMD.

III. RESULTS AND DISCUSSION

Table 1. Project Summary

Type	*Description*	*URL*
Project/Object Scope	Web Dapodik Web sipdatapsm Web Sabakota Web silat	https://dapodik.tangerangkota.go.id/ https://sipdatapsm.tangerangkota.go.id/ https://sabakota.tangerangkota.go.id https://silat.tangerangkota.go.id/
Area	Production	
Methodology	Black-box Testing	
Date/Period	01 April 2023	Pentest #1

e-ISSN: 2614-8404
p-ISSN: 2776-3234

As showed in Table 1, the research object's scope is outlined, with the focus being on the production area that is currently utilized by the user. The methodology adopted by the researchers is black box testing. This approach signifies that the researchers undertake penetration testing without any prior knowledge of the research object.

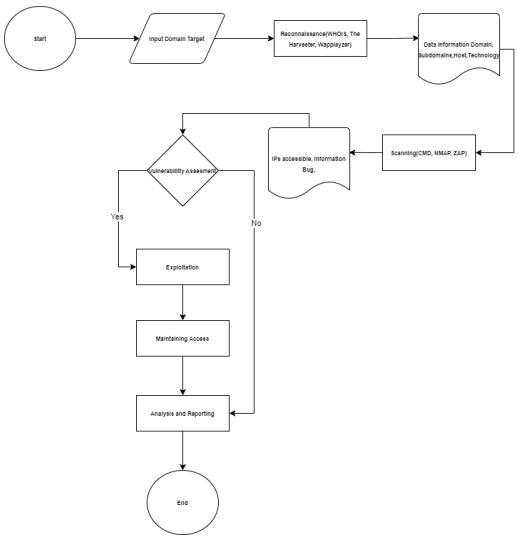

Figure 2. Step Penetration Testing

Figure 2 provides a detailed explanation of the steps executed by the researcher. There are several steps such as reconnaissance, scanning, exploitation, maintaining access, also analysis and reporting. In this context, reconnaissance serves to gather information about the domain, which will be highly beneficial for the scanning process. The results obtained from the reconnaissance process are as follows:

Table 2. Process of Reconnaissance

Tools Name	Data Obtained	Tools Function
Whois	Informasi Domain (Domain Created,Name hostmaster, Cellphone Number,Total Server)	Recconaissance
The Harvester	Emails and Total Host	Recconaissance
Wapplayzer	Built using PHP technology, nginx server, and javascript library	Recconaissance

As showed in Table 2, the subsequent step involves scanning, which serves to identify bug information associated with the domain. WHOIS is also an exceptional method to identify the domain owner. However, they also possess their own applications to search for information in the WHOIS database. This implies that any information an individual seeks will be presented in detail there [16]. The Harvester functions as a comprehensive information-gathering tool that is utilized by both ethical and non-ethical hackers to scrape emails, subdomains, hosts, employee names, open ports, and banners from various public sources, such as popular search engines [17]. The results obtained from the scanning process are as follows:

Table 3. Process of Scanning

Tools Name	Data Obtained	Tools Function
CMD	Accessible IP	Scanning
NMAP	Port, State, Service	Scanning
ZAP	Vulnerability Info, Risk Level	Scanning

As showed in Table 3, after obtaining information about the vulnerability contained in the domain, exploitation can be carried out based on the results of the scanning. Nmap is used to scan Mikrotik routers to identify existing vulnerabilities [18]. OWASP-ZAP is a vulnerability scanner application that is freely available (open source) and has been developed by the OWASP organization. It is extremely useful in assisting with the discovery of bug information [19]. The purpose of exploitation here is to verify whether the detected bug truly resides within the website and to identify any other potential bugs that have not yet been confirmed. The outcomes of the exploitation process are as follows:

Table 4. Process of Exploitation

Tools Name	Data Obtained	Tools Function
Burp Suite	Information Disclosure - Dapodik, Reflected XSS - Dapodik, Insecure Direct Object Reference (IDOR) – Tambah Dana LPJ Sabakota, Insecure Direct Object Reference (IDOR) – Cetak Profil Sabakota, Stored XSS - Sabakota	Exploitation
SQLmap	SQL Injection - Silat, SQL Injection - Sipdatapsm	Exploitation

As showed in Table 4, following the exploitation, it was found that there were several bugs in the Tangerang City subdomain. SQLMap is an open-source application or tool included in Kali Linux. This application is used to detect and exploit vulnerabilities in web applications. Researchers use this application during the exploitation phase [20]. The researchers then carried out maintaining access, which serves to re-exploit to reconfirm whether the bug has been fixed or remains unfixed. The results from the maintaining access process are as follows:

e-ISSN: 2614-8404
p-ISSN: 2776-3234

Table 5. Process of Maintaing Access

No.	Vulnerability Name	Category	Risk
1	*SQL Injection - Silat*	**Injection**	A3
2	*SQL Injection - Sipdatapsm*	**Injection**	A3
3	*Stored XSS - Sabakota*	**Injection**	A3
4	*Insecure Direct Object Reference (IDOR) – Cetak Profil Sabakota*	**Broken Access Control**	A1
5	*Insecure Direct Object Reference (IDOR) – Tambah Dana LPJ Sabakota*	**Broken Access Control**	A1
6	*Reflected XSS - Dapodik*	**Injection**	A3
7	*Information Disclosure - Dapodik*	**Security Misconfiguration**	A5

As showed Table 5, in the final stage, the researcher conducted an analysis related to the bug findings on the Tangerang City website. The researchers categorized the vulnerabilities found according to the OWASP Top 10 Web Security Risks Framework and conducted a security vulnerability assessment using the Common Vulnerability Scoring System (CVSS). The results are as follows:

Table 6. Process of Analysis and Reporting

No.	Vulnerability Name	Severity	Status
1	*SQL Injection - Sipdatapsm*	**Critical**	Validate
2	*SQL Injection - Silat*	**High**	Validate
3	*Stored XSS - Sabakota*	**High**	Validate
4	*Insecure Direct Object Reference (IDOR) – Cetak Profil Sabakota*	**High**	Validate
5	*Insecure Direct Object Reference (IDOR) – Tambah Dana LPJ Sabakota*	**High**	Validate
6	*Reflected XSS - Dapodik*	**Medium**	Validate
7	*Information Disclosure - Dapodik*	**Low**	Validate

As showed Table 6, the researchers discovered seven vulnerabilities within the Tangerang city website. The vulnerabilities found include one in the critical category, four in the high category, one in the medium category, and one in the low category.

REFERENCES

[1] M. Ayu, "BSSN Paparkan Serangan Keamanan Siber di Tahun 2022 Alami Penurunan Dibanding Tahun 2021," *cloudcomputing.id*, Jan. 24, 2023. [Online]. Available: https://www.cloudcomputing.id/berita/bssn-paparkan-serangan-siber-alami-penurunan.

[2] M. Subagja, "*Penetration Testing Terhadap Website Asosiasi Pekerja Professional Informasi Sekolah Indonesia (APISI)*," 2019.

[3] Ahmad Fikri Zulfi, "*Evaluation of Student Information System Application Security Using Vapt Framework (Case Study: Sister Universitas Jember)*," 2017.

[4] A. Susanto and W. K. Raharja, "*Simulation and Analysis of Network Security Performance Using Attack Vector Method for Public Wifi Communication*," IJICS (International J. Informatics Comput. Sci., vol. 5, no. 1, 2021, pp. 7–15.

[5] D. C. Angir, Agustinus, Justinus, "*Vulnerability Mapping Pada Jaringan Komputer Di Universitas X*", Jurnal infra vol. 3, no. 2, 2015.

[6] Afif Zirwan, "*Pengujian Dan Analisis Keamanan Website Institut Teknologi Padang Menggunakan Acunetix Vulnerability Scanner*," 2022.

[7] A. Marta, D. Setiyadi, and Fata, "*Keamanan Website Menggunakan Vulnerability Assessment*," Information for Educators and Professionals, vol. 2, no. 2, Juni 2018, pp. 171-180.

[8] Harry, M. Akbar, Andri, "*Vulnerability Assessment Pada Web Server*," 2018.

[9] Mira and Michael, "*Vulnerability Assesment Untuk Meningkatkan Kualitas Kemanan Web*," 2021.

[10] Brown and Nicholas, *Nmap 7: From Beginner to Pro*. USA: Independently Published, 2019.

[11] I. Kamilah and A. Hendri Hendrawan, "*Analisis Keamanan Vulnerability pada Server Absensi Kehadiran Laboratorium di Program Studi Teknik Informatika*," Pros. Semnastek, vol. 16, no. 0, 2019, pp. 1–9.

e-ISSN: 2614-8404
p-ISSN: 2776-3234

[12] M. Anis and Emah, "*Network Security Monitoring with Intrusion Detection System*," JUTIF, vol. 3, no. 2, April 2022, pp. 249-253.

[13] Feri, Harjono, and Agung, "*Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix WVS*," 2019.

[14] Mona, "*Analisis Celah Keamanan Website Sitasi Menggunakan Vulnerability Assessment*," Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi, vol. 1, no. 9, 2023, pp. 1-7.

[15] Fadli and Sofyan, "*Implementasi Metode Vulnerability Dan Hardening Pada Sistem Keamanan Jaringan*," Jurnal Teknologi Elektro, vol. 9, no. 1, 2018.

[16] Timoteus and Jimmy, "Analisis Yuridis Pelaksanaan Tugas Pokok Pengelola Domain Internet Indonesia," NJLO, vol. 1, no. 1, Juli 2020, pp. 53-63.

[17] Thecybersecurityman, "PenTest Edition: Using "theHarvester" to Gather Email accounts, Subdomains, Hosts, LinkedIn Users, Banner Information, and More!" thecybersecurityman.com, Aug. 1, 2018. [Online]. Available: https://thecybersecurityman.com/2018/08/01/pentepe-edition-using-theharvester-to-gather-e-mail-accounts-subdomains-hosts-linkedin-users-banner-information-and-more/

[18] I. Kamilah and A. Hendri Hendrawan, "Analisis Keamanan Vulnerability pada Server Absensi Kehadiran Laboratorium di Program Studi Teknik Informatika," Pros. Semnastek, vol. 16, no. 0, 2019, pp. 1–9.

[19] Dennis, Muhardi, and Warih, "Analisis Resiko Keamanan Terhadap Website Dinas Penanaman Modal Dan Pelayanan Terpadu Satu Pintu Pemerintahan Xyz Menggunakan Standar Penetration Testing Execution Standard (Ptes)," e-Proceeding of Engineering, vol. 7, no. 1, April 2020, pp. 2090.

[20] Sudiharyanto, Roy, and Ihsan, "Analisa Serangan Sql Injeksi Menggunakan Sqlmap," Jurnal Sistem dan Teknologi Informasi, vol. 4, no. 2, 2018, pp. 88-94.