Jurnal Mantik, 8 (1) (2024), ISSN 2685-4236 (Online)

Published by:Institute of Computer Science (IOCS)

Jurnal Mantik

Journal homepage: www.iocscience.org/ejournal/index.php/mantik

Testing posketanmu website with google penetration testing and OWASP Top 10

Aida Fitriya Sebrina[1], Achmad Junaidi[2], Andreas Nugroho Sihananto[3]
[1,2,3]Department of Computer, Faculty of Computer Science, Informatic, National Development University "Veteran" East Java, Indonesia

A R T I C L E I N F O

Article history:

Received May 26, 2024
Revised May 29, 2024
Accepted May 30, 2024

Keywords:

Google Hacking;
OWASP Top 10 2021;
Penetration Testing;
Website Security.

ABSTRACT

Data integrity has become vital in the quickly evolving digital era, pushing cybersecurity to a critical concern. Securing cybersecurity is crucial for systems such as the Posketanmu website in Mojokerto Regency, as it is responsible for safeguarding sensitive personal information. The objective of this research is to detect, evaluate, and exploit on any security weaknesses present on the Posketanmu website. The methodology combines the Google Penetration Testing strategy with the latest OWASP Top 10 2021 criteria. The penetration testing procedure comprises five distinct steps: Initially, the process involves collecting data and comprehending the platform by utilizing several programs such as Nmap, Nslookup, Wappalizer, Whatweb, Whois, and Google Hacking. Furthermore, the process involves utilizing ZAP to do vulnerability scanning, resulting in the creation of thorough reports. Furthermore, doing a vulnerability assessment, which involves manual testing and classification according to OWASP standards. Furthermore, effectively capitalizing on all eleven identified vulnerabilities. Ultimately, the task involves adhering to the OWASP Top 10 2021 standards by documenting, reporting, and suggesting solutions for any identified issues. This investigation found and resolved four significant security vulnerabilities on the Posketanmu website: stored XSS, unset CSP header, unset Strict-Transport-Security header, and open redirect. The implementation of Google Penetration Testing and adherence to the OWASP Top 10 2021 criteria have greatly improved the security of the Posketanmu website, ensuring the protection of Mojokerto Regency citizens' data.

This is an open access article under the CC BY-NC license.

Corresponding Author:

Aida Fitriya Sebrina,
Department of Computer Science, Informatics,
National Development University "Veteran" East Java,
Jl. Rungkut Madya No.1 Gn Anyar, Gunung Anyar, Surabaya, East Java, Indonesia, 60294.
Email: achmadjunaidi.if@upnjatim.ac.id

1. INTRODUCTION

Cyberattacks in Indonesia have significantly increased, with 370.02 million attacks in 2022, a rise of 38.72% from the previous year(Umar et al., 2023)(Febriani, 2023). This places Indonesia third among the most targeted countries(Kominfo, 2018), causing harm

to organizations through data theft, operational disruptions, and financial losses(KOMINFO, 2016).

To address these threats, web security testing, such as web penetration testing, is essential. This technique identifies security vulnerabilities and provides improvement suggestions(Deng et al., 2023; Gary Mcgraw Brad Arkin, 2005). Dispendukcapil Kabupaten Mojokerto launched the POSKETANMU website in 2023 for online civil administration services(Thaoqid, 2023). With increasing use, ensuring the website's security is crucial.

OWASP Top 10 is a guideline for identifying common web security vulnerabilities, often used in penetration testing(*OWASP Top Ten*, n.d.; Priambodo et al., 2023). Previous research by Priambodo et al. (2023) used OWASP Top 10 and black box testing with tools like Vega and OWASP ZAP. However, this research did not combine other methods for more comprehensive results.

Google Hacking, also known as Google Dorking, is another important technique for finding sensitive information on the web(EITCA, 2023; Long, 2004). This study combines Google Penetration Testing and OWASP Top 10 2021 to provide more thorough results. Testing the POSKETANMU website revealed several significant security vulnerabilities. The results raised awareness about web security and prompted concrete improvement measures. Without this testing, the website would remain vulnerable to attacks that could lead to data theft and financial losses.

2. RESEARCH METHOD

The research aims to enhance comprehension through literature study, system functionality comprehension, information gathering, vulnerability scanning, assessment, testing, and documentation.

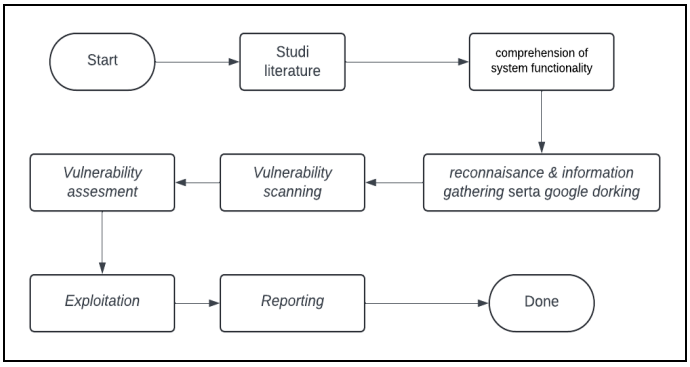

Figure 1. Research Method

2.1 Comprehession of System Functionality

Posketanmu is an internet-based platform by Mojokerto district's Civil Registration and Occupation Service, offering administrative services like issuance of ID cards, E-KTP, Act applications, and submissions.

2.2 Reconnaissance and Information Gathering

Reconnaissance can be active or passive, requiring knowledge of specific tools and techniques to protect websites(Odun-Ayo et al., 2022). The collected information includes system details and configurations, including operating systems, network configurations, active services, and applications, as shown in table 1.

Table 1. Tool for information gathering and usage plan

Tools	Usage Plan and Purpose
Mozilla Firefox	Ensures the website is accessible.
Whois	Offers details about domain ownership, administrative and technical duties, and host server information. It can be accessed using a command line interface on some operating systems(Charles J. Brooks, Christopher Grow, Philip Craig, 2018). 1) Visiting the website https://who.is/ 2) Scan the domain of the website with IP address 172.xx.xxx.x
Wappalyzer	Identifying more technologies, including databases, web servers, and analytical tools(Pram, 2023). 1) Accessing the website at the URL https://www.wappalyzer.com/ 2) Perform a scan on the domain Posketanmu.mojokertokab.go.id
Nslookup	Instructions for searching for and displaying DNS information associated with the domain, including the IP address of the target website(Charles J. Brooks, Christopher Grow, Philip Craig, 2018). 1) nslookup posketanmu.mojokertokab.go.id
Nmap	Perform a rapid port scan on the target and then modify it in greater depth and specificity(Charles J. Brooks, Christopher Grow, Philip Craig, 2018). 1) nmap stg-posketanmu.mojokertokab.go.id
Whatweb	Find the technology that was employed to scan the provided website, including the operating system, firewall, and cookies, among other details(Prasad, 2016). 1) Whatweb stg-posketanmu.mojokertokab.go.id
Google Dorking	Penetration testing method that uses specific search operators to find publicly available sensitive information(EITCA, 2023). This technique exploits Google's indexing capabilities to uncover data not typically found through standard searches(Long, 2004). 1) Site: posketanmu.mojokertokab.go.id filetype:sql 2) Site: posketanmu.mojokertokab.go.id filetype: .env 3) inurl:admin site: posketanmu.mojokertokab.go.id 4) intext:phpMyAdmin inurl:posketanmu.mojokertokab.go.id 5) intext:index.php inurl:posketanmu.mojokertokab.go.id

2.3 Vulnerability Scanning

Vulnerability scanning, vital for evaluating information system security, employs diverse tools to detect vulnerabilities and offer mitigation suggestions(AHSAN, 2022)(Zen Munawar et al., 2023)(Wang et al., 2021). This process is critical for identifying vulnerabilities in server applications and open ports to bolster network security and deter future attacks(Kendek Allo & Widiasari, 2024) Tools such as OWASP ZAP and Burp Suite facilitate thorough scanning and reporting.

2.4 Vulnerability Assesment

Pre-release vulnerability assessments and penetration tests are essential for detecting and rectifying flaws in systems, applications, and networks to avert attacks(Baballe et al., 2022). Post-scan assessments aid in categorizing and addressing vulnerabilities based on severity and standards, providing a comprehensive understanding to develop effective management strategies.

2.5 Exploit

The exploitation phase involves testing identified vulnerabilities to confirm their exploitability and understand their impact(Fachri, 2023). This phase helps organizations identify and manage security weaknesses. ZAP scanning identified 19 vulnerabilities in Posketanmu, with 11 pending exploitation. During the exploitation stage for the

Posketanmu website, various tools are utilized, including the ones listed in table 2. below:

Table 2. Tool and usage plan for exploitation

Tools	Usage Plan and Purpose
Mozilla Firefox	Using tools such as Whois, Wappalyzer, and cookie editor to manually test websites, identify vulnerabilities including XSS and open redirect, and navigate accordingly.
Kali Linux	Wireshark and BetterCap aid in monitoring and analyzing network traffic, facilitating website testing and targeted attacks. Kali Linux offers tools for gathering information about targets(Mundalik, 2015).
Burpsuite	Performing manual vulnerability testing entails examining website traffic for patterns and potential vulnerabilities, manipulating them to assess weaknesses, and offering a thorough overview for simulated attacks.
Wireshark	Captures cookie caught by Wireshark for detailed analysis and detecting potential network and security issues(M. Ferdy Adriant, 2015).
Bettercap	Monitor network activity and analyze data traffic(Mada, 2021).

2.6 Reporting

In the reporting stage, the tester prepares a final report detailing the system and the results of vulnerability tests before and after exploitation(Fachri, 2023). This report is analyzed to identify necessary adjustments to protect the system, aiding in understanding and addressing vulnerabilities(Dayan et al., 2023). Here is a table 3. listing the vulnerabilities found on the posketanmu website and the potential impacts they may have:

Table 3. Vulnerability and their impact

No	Vulnerability	Impact
1	Open Redirect	Allows attackers to covertly redirect users to malicious websites.
2	Cross site Scripting Stored (XSS stored)	Enables injection of malicious code, leading to data theft or control over user browsers.
3	Content Security Policy (CSP) Header Not Set	Exposes the website to XSS and clickjacking attacks due to lack of CSP implementation.
4	Cross Domain Misconfiguration	Enables cross-site attacks such as XSS and CSRF.
5	Big Redirect Detected	Redirects to undesired webpages without validation, risking sensitive information theft or phishing.
6	Cookie No HttpOnly Flag	Allows attackers to steal cookies using JavaScript due to the absence of HttpOnly flag.
7	Cookie Without Secure Flag	Enables cookie theft via unsecured HTTP connections due to lack of Secure flag.
8	Cross-Domain JavaScript Source File Inclusion	Allows execution of harmful JavaScript from external websites.
9	Secure Pages Include Mixed Content	Makes safe pages vulnerable to attacks by including insecure content.
10	Strict-Transport-Security Header Not Set	Exposes the website to interception and SSL Striping/HSTS Hijacking due to lack of HSTS headers.
11	Timestamp Disclosure - Unix	Allows monitoring of user activities by disclosing Unix timestamps.

3. RESULTS AND DISCUSSIONS

The chapter discusses the results and analysis of a penetration test study that used Google Penetration Testing and followed the OWASP Top 10 2021 Method. The focus is on the detailed findings obtained from the performed penetration tests.

3.1 RECONNAISSANCE AND INFORMATION GATHERING

The reconnaissance and information gathering method on the Posketanmu website has effectively gathered a diverse range of essential information, which is subsequently recorded in the form of table 5 below.

Table 2. information gathering result

No	Tool	Result
1	*Nslookup*	The IPs are 1xx.xx.xxx.x and 1xx.xx.xxx.x (in IPv4 format).
2	*Nmap*	Port service : port 80 with service Http, port 443 withservice Https, port 8080 with service Http-proxy, port 8443 withservice Http-alt
3	*Whois*	IP address 1xx.xx.xxx.x located at 201 Townsend Street, United States, registered on February 25, 2015, and updated on May 20, 2021.
4	*Wappalizer*	The website utilizes the Bootstrap and Laravel UI frameworks, in addition to the Toastr JavaScript framework. HSTS enhances security. The Content Delivery Network services utilized are Unpkg, Cloudflare, Cdnjs, and jsDelivr.
5	*Whatweb*	The website utilizes the Cloudflare web server and is built on the Laravel framework. The implemented security measures consist of XSRF-TOKEN cookies, Laravel sessions, and other features.
6	*Google Dorking*	There are no links that contain any sensitive information.

3.2 VULNERABILITY SCANNING

To identify website weaknesses utilize OWASP ZAP along with automated and manual procedures, as well as conventional spider and active scan techniques.

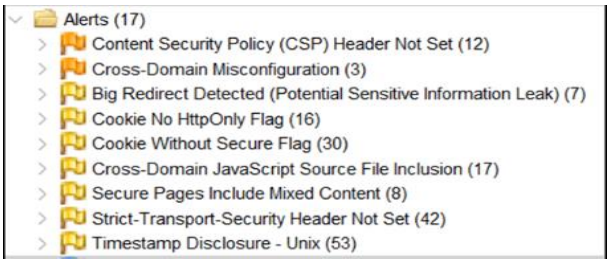

Figure 2. The results of vulnerability scanning that will be exploited.

Figure 2. represents the results of a scan conducted by OWASP ZAP on the target website stg-posketanmu.mojokertokab.go.id, revealing the presence of several vulnerabilities. The scan results indicated the presence of 2 moderate risk, 7 low risk, and 8 instances of identifiable informational.

3.3 VULNERABILITY ASSESMENT

A vulnerability assessment identifies and documents website weaknesses, with data on vulnerabilities and risk levels presented in Table 6.

Table 3. Vulnerabilities assessment by category OWASP Top 10

No	Vulnerabilities	Severity level	Kategory OWASP Top 10
1	Open redirect	High	A03:2021- Injection
2	Cross-Site Scripting	Medium	A03:2021- Injection
3	Content Security Policy (CSP) Header Not Set	Medium	A01:2021 - Broken Access Control
4	Cross domain Misconfiguration	Medium	A01:2021 – Broken Access Control
5	Big Redirect Detected	Low	A01:2021 – Broken Access Control
6	Cookie No HttpOnly Flag	Low	A05:2021 – Security Misconfiguration
7	Cookie Without Secure Flag	Low	A05:2021 – Security Misconfiguration
8	Cross-Domain JavaScript Source File	Low	A08:2021 – Software and Data Integrity

No	Vulnerabilities	Severity level	Kategory OWASP Top 10
	Inclusion		Failures
9	Secure Pages Include Mixed Content	Low	A05:2021 – Security Misconfiguration
10	Strict-Transport-Security Header Not Set	Low	A02:2021 – Cryptographic Failures
11	Timestamp Disclosure - Unix	Low	A01:2021 – Broken Access Control

3.4 EXPLOITATION

3.4.1 CSP-001 CONTENT SECURITY POLICY (CSP) HEADER NOT SET

The CSP-001 vulnerability reveals a critical flaw in the website's security by not implementing the Content Security Policy (CSP) header. This oversight opens the door to potential XSS attacks, endangering user data and system integrity. During manual inspection of network and browser console, a script injection test `setTimeout"console.log('hello world page help')", 500)` uncovered the absence of CSP implementation, allowing malicious scripts to execute unchecked.

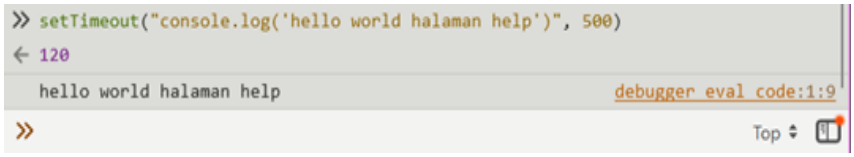

Figure 3. Output console browser page /help

3.4.2 CDM-001 CROSS DOMAIN MISCONFIGURATION

Cross-Domain Misconfiguration (CDM-001) poses a significant risk by permitting access to resources from any domain, potentially exposing sensitive data to unauthorized parties. Despite efforts to mirror the 'Origin' header in the server's response, the vulnerability went undetected, leaving the website vulnerable to exploitation.

3.4.3 BDR-001 BIG REDIRECT DETECTED (SENSITIF INFORMATION LEAK)

The Big Redirect Detected (BDR-001) vulnerability, while potentially severe, was not present in the Posketanmu website. Attempts to redirect users to unauthorized websites like http://attacker.com failed, and manual inspection revealed no instances of sensitive information leakage, suggesting the site's resilience to such attacks.

3.4.4 OPR-001 OPEN REDIRECT

In the case of Open Redirect (OPR-001), the website displayed vulnerability to this threat, as evidenced by successful redirection to unexpected URLs like in figure 4. By manipulating the 'Referer' option, attackers could potentially lead users to malicious websites, compromising their security and data privacy.

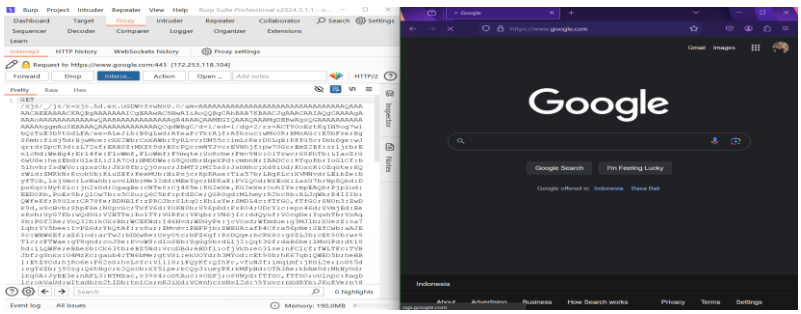

Figure 4. Open redirect succesfull in login page

3.4.5 CNH-001 COOKIE NO HTTPONLY FLAG

Cookie No HttpOnly Flag (CNH-001) was not found to be a vulnerability on the website. Despite initial concerns about cookie security, attempts to log back into the site using captured cookie data prompted re-authorization requests, indicating robust security measures in place to prevent unauthorized access to user sessions

3.4.6 CWS-001 COOKIE WITHOUT SECURE FLAG

The "cookie without secure flag" vulnerability was assessed using Wireshark to monitor network activity. Despite cookies being transmitted with GET requests, attempts to modify and reuse cookies for re-login were unsuccessful, indicating the website's immunity to this vulnerability.

3.4.7 XJS-001 JAVASCRIPT DOMAIN FILE INCLUSION

On the registration page, an experiment was conducted to test the susceptibility of a JavaScript file to XSS attacks. Despite altering a vulnerable JavaScript file, the website remained impervious to "JavaScript Domain File Inclusion" due to secure CDN usage and no observable impact on the main interface.

3.4.8 SMC-001 SECURE PAGE INCLUDE MIX CONTENT

By ensuring all content uses HTTPS, including previously vulnerable links, the website is protected against "secure page include mix content" vulnerabilities. The removal of mixed content eliminates any security risks associated with HTTP loading on an HTTPS-enabled site.

3.4.9 STS-001 STRICT TRANSPORT SECURITY HEADER NOT SET

The absence of the HSTS header in the HTTP server response indicates a vulnerability to HSTS hijacking. However, tests using Bettercap and Wireshark did not find any personal data leaks during login. Despite the missing HSTS configuration, additional security measures like XSRF tokens and captchas are in place to enhance protection.

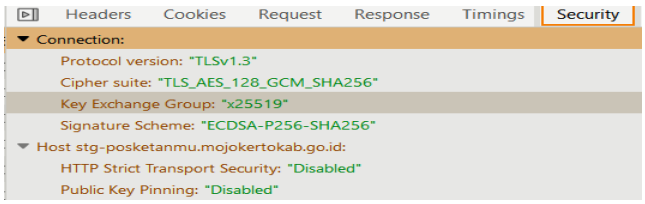

Figure 5. Security console shows the website has not implemented the hsts header.

3.4.10 TDS-001 TIMESTAMP DISCLOSURE

Despite multiple XSS tests conducted, the website was found vulnerable to stored XSS attacks. Manipulating POST requests with XSS payloads resulted in successful injections and the display of warning messages on vulnerable pages, indicating susceptibility to this type of attack.

3.4.11 XSS-001 CROSS-SITE SCRIPTING (STORED)

Despite multiple XSS tests conducted, the website was found vulnerable to stored XSS attacks. Manipulating POST requests with XSS payloads resulted in successful injections and the display of warning messages on vulnerable pages, indicating susceptibility to this type of attack.

Figure 6. XSS stored exploitation

3.5 REPORTING

3.5.1 PENETRATION TEST RESULT REPORT

Below is a test report regarding the website. The following table provides a compilation of recognized vulnerabilities, the potential consequences that may occur due to these flaws, and the current vulnerability status of the site:

Table 4. Penetration test result report

No	Test Code	Vulnerability	Status
1	CSP-001	Content Security Policy (CSP) header not set	Found
2	CDM-001	Cross Domain Misconfiguration	Not Found
3	BRD-001	Big redirect detected	Not Found
4	OPR-001	Open redirect	Found
5	CNH-001	Cookie No HttpOnly Flag	Not Found
6	CWS-001	Cookie without secure flag	Not Found
7	XJS-001	Cross-domain Javascript source file inclusion	Not Found
8	SMC-001	Secure page include mix content	Not Found
9	STS-001	Strict-Transport-Security Header Not set	Found
10	TSD-001	Timestamp disclosure	Not Found
11	XSS-001	XSS On email parameter “Pengajuan-Akta”	Found

The table 7. presents a summary of the vulnerabilities discovered during the testing and the current vulnerability status of the Posketanmu website. Posketanmu.mojokertokab.go.id exposes four vulnerabilities or vulnerabilities insecurity, including missing of a CSP header, an Open Redirect vulnerability, the lack of Strict-Transport security Headers, and vulnerability to XSS Stored attacks.

3.5.2 RECOMMENDATIONS FOR IMPROVEMENT

Based on the OWASP Top 10 security standards for 2021, the tests find weaknesses that need to be fixed right away and suggest ways to make things better.

1) CSP header not set vulnerabilities with codes CSP-001 to CSP-010 will be fixes if Content-Security-Policy (CSP) header should be used properly by the web server, the application, the load manager, and any other parts. The browser is a CSP, can control what kind of data sent. To enable CSP, the web server can include an HTTP `Content-Security-Policy` response header. For site only content restriction, This rules means is that if authorized content from trusted domains and subdomains,

then only are allowed. `Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' mojokertokab.. go. id *. mojokertokab. go. id cdn. cloudflare. com *. cdn. cloudflare. com.`

2) To XSS prevention for XSS-11 to XSS-37, make sure to encode any non alphanumeric characters based on where they will be used (such, as in HTML, attributes, URIs, JavaScript or CSS). Encode the output according to the components to protect against XSS vulnerabilities. It's important to validate inputs, from both clients and servers to prevent stored XSS attacks.
3) Correction suggested Open Redirecting for OPR-001 until OPR-007 should be avoided if at all possible when open redirection vulnerabilities are found. Make sure to prevent redirection vulnerabilities by not letting user input control the destination URL. Validate user input thoroughly to clean it up and create a list of trusted URLs. Prior, to redirection have a page that requests confirmation from the user.
4) Code of Test: STS-001 and the vulnerability is Header for Strict Transport Security Not Set. To add domain to the HSTS preload list overseen by Chrome, Firefox and Safari insert the following header; `Strict Transport Security; max age=31536000; includeSubDomains; preload`.

4. CONSLUSION

The security testing of posketanmu.mojokertokab.go.id using Google Penetration Testing and OWASP Top 10 2021 identified 19 vulnerabilities, with 11 tested and 4 found: CSP header not set, open redirect, stored XSS, and Strict-Transport-Security header not set. Recommended actions include setting CSP headers, validating and sanitizing URLs, validating client and server-side input, and using HSTS headers. This research contributes to the field by providing a detailed methodology for identifying and addressing web vulnerabilities, enhancing web security practices.

However, it has limitations, as the recommendations focus only on identified vulnerabilities. Future research should explore the implementation of these actions and develop advanced attack scenarios, such as layered XSS attacks.

Immediate fixes for the vulnerabilities are necessary, followed by re-testing to ensure effectiveness. Advanced testing methods beyond Google Penetration Testing and OWASP Top 10 2021 are also recommended. Implementing these steps will enhance website security, reduce attack risks, and better protect user data.

REFERENCES

AHSAN, M. U. H. (2022). *Analisa Kerentanan Sistem Dengan Menerapkan Open Vulnerability Assessment System Menggunakan Greenbone Vulnerability Management (GVM)*. Universitas Mercu Buana.

Baballe, M. A., Polytechnic, K. S., & Polytechnic, K. S. (2022). *Review of Computer Engineering Research*. *9*(May), 1–22.

Charles J. Brooks, Christopher Grow, Philip Craig, D. S. (2018). *Cybersecurity Essentials*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781119369141

Dayan, R., Muhyidin, Y., & Singasatia, D. (2023). Analisis Keamanan Jaringan Pada Wireless Local Area Network Terhadap Serangan Brute Force Menggunakan Metode Penetration Testing. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *7*(3), 2051–2056. https://doi.org/10.36040/jati.v7i3.7097

Deng, G., Liu, Y., Mayoral-Vilches, V., Liu, P., Li, Y., Xu, Y., Zhang, T., Liu, Y., Pinzger, M., & Rass, S. (2023). *PentestGPT: An LLM-empowered Automatic Penetration Testing Tool*. 1–17.

EITCA. (2023). *What is Google hacking and how is it used in penetration testing for web applications?* Eitca.Org.

Fachri, F. (2023). Optimasi Keamanan Web Server Terhadap Serangan Brute-Force Menggunakan Penetration Testing. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *10*(1), 51–58. https://doi.org/10.25126/jtiik.20231015872

Febriani, P. (2023). *BSSN Catat 370,02 Juta Serangan Siber ke Indonesia pada 2022*. DataIndonesia.Id.

Gary Mcgraw Brad Arkin, S. S. (2005). Building Security In - Software penetration testing. *Software Penetration Testing*.

Kendek Allo, A., & Widiasari, I. R. (2024). Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning. *Jurnal JTIK (Jurnal Teknologi Informasi Dan Komunikasi)*, *8*(2), 316–323. https://doi.org/10.35870/jtik.v8i2.1723

Kominfo. (2018). *Indonesia Negara Ketiga Paling Sering Terkena Serangan Siber*. Kominfo.Go.Id.

KOMINFO. (2016). *Kebijakan Keamanan dan Pertahanan Siber*. Aptika.Kominfo.Go.Id.

Long, J. (2004). *Google Hacking for Penetration Testers* (D. Bordwell (Ed.)). Andrew Wiliam.

M. Ferdy Adriant, I. M. (2015). 172890-ID-none. *Implementasi Wireshark Untuk Penyadapan (Sniffing) Paket Data Jaringan*, 224–228.

Mada, M. (2021). *Install Bettercap di Kali Linux 2020.x*. Medium.Com.

Mundalik, S. S. (2015). Penetration Testing: An Art of Securing the System (Using Kali Linux). *International Journal of Advanced Research in Computer Science and Software Engineering*, *5*(10), 235–242.

Odun-Ayo, I., Owoka, E., Okuoyo, O., Ogunsola, O., Ikoh, O., Adeosun, O., Etukudo, D., Robert, V., & Oyeyemi, G. (2022). Evaluating Common Reconnaissance Tools and Techniques for Information Gathering. *Journal of Computer Science*, *18*(2), 103–115. https://doi.org/10.3844/jcssp.2022.103.115

OWASP Top Ten. (n.d.). OWASP.

Pram, E. (2023). *Apa itu Wappalyzer? dan Cara Menggunakannya*. Prameko.Com.

Prasad, P. (2016). *Mastering Modern Web Penetration Testing*. Packt Publishing.

Priambodo, D. F., Rifansyah, A. D., & Hasbi, M. (2023). Penetration Testing Web XYZ Berdasarkan OWASP Risk Rating. *Teknika*, *12*(1), 33–46. https://doi.org/10.34148/teknika.v12i1.571

Thaoqid, H. (2023). *Pelayanan Administrasi Kependudukan di Kabupaten Mojokerto Dikeluhkan Warga*. Jatim.Times.Co.Id.

Umar, R., Riadi, I., & Elfatiha, M. I. A. (2023). Analisis Keamanan Sistem Informasi Akademik Berbasis Web Menggunakan Framework ISSAF. *Jutisi: Jurnal Ilmiah Teknik Informatika Dan Sistem Informasi*, *12*(1).

Wang, L., Abbas, R., Almansour, F. M., Gaba, G. S., Alroobaea, R., & Masud, M. (2021). An empirical study on vulnerability assessment and penetration detection for highly sensitive networks. *Journal of Intelligent Systems*, *30*(1), 592–603. https://doi.org/10.1515/jisys-2020-0145

Zen Munawar, S. T., Kom, S., Kom, M., Putri, N. I., Kharisma, I. L., Kom, M., Insany, G. P., ST, S., Kom, M., & Nurhadi, S. (2023). *Keamanan Sistem Informasi: Prinsip Dasar, Teori, dan Rekayasa Penerapan Konsep*. Kaizen Media Publishing.