Research Article

International Journal of Multidisciplinary Applied and Science Research
Volume 01, Issue 01, PP. 22–28

Carrying Out Website Security Analysis Using the Standard Penetration Testing Method

Dhea Permata Sari [1], & Fachrudin Pakaja [2]*

[1,2] Faculty of Engineering and Informatics, Gajayana University Malang, Indonesia, Email: permata.dheyak@gmail.com [1], fachrudinpakaja@unigamalang.ac.id [2].

*Corresponding Author Email: permata.dheyak@gmail.com

Received: November. 21 2024
Revised: December. 11, 2024
Accepted: December. 15, 2024

Abstract
The high level of cybersecurity threats such as SQL injection attacks, cross-site scripting (XSS), and data breaches makes website security testing a critical need. This study aims to analyze website security vulnerabilities using the PTES method as a comprehensive penetration standard. The study uses an exploratory qualitative approach with five PTES stages: (1) pre-engagement, (2) intelligence gathering, (3) vulnerability analysis, (4) exploitation, (5) post-exploitation and maintaining access. The results of the study revealed that the SPPT Online website in Mojokerto City that had been scanned provided several accesses to open protocols created for communication channels. PTES effectively uncovered multidimensional vulnerabilities with a structured approach. The results of the study can be a guide to improving website security posture, especially in the financial management sector. This study highlights the urgency of periodic security audits based on standards such as PTES to mitigate cyber risks.

Keyword: Website Security, PTES, Penetration Testing, SPPT Online, Mojokerto.

1. Introduction

In the era of digital transformation, local government websites have become a vital means of providing public services, financial transparency, and interaction with the community (Das, 2024); (Eom & Less, 2022); (Ndou, 2004). The Mojokerto City Regional Revenue and Finance Management Agency (BPKPD) as an institution that manages sensitive financial data and regional revenue transactions requires a website system that is secure from cyber threats. However, based on the 2023 report of the National Cyber and Crypto Agency (BSSN), as many as 40% of local government websites in Indonesia are still vulnerable to cyber-attacks such as SQL injection, cross-site scripting (XSS), and data breaches (Eddy et al., 2017); (Pratiwi et al., 2024). This condition indicates the urgency of conducting a comprehensive security evaluation to protect the digital assets and strategic data of the Mojokerto City BPKPD.

This study adopts the Penetration Testing Execution Standard (PTES) method as a comprehensive framework for testing the security of the Mojokerto City BPKPD website (Safitri et al., 2023); (Astrida et al., 2021). PTES was chosen because it provides a structured approach through seven stages, from pre-engagement to reporting, which allows for systematic identification of vulnerabilities (Utama & Nurhadi, 2024). This method has proven effective in uncovering security gaps in government systems, as implemented in the East Java Communication and Information Service in 2022 with a finding accuracy rate of 95%. Using tools such as Burp Suite, OWASP ZAP, and Metasploit, this study simulates cyber-attacks to test the resilience of the BPKPD website to various exploitation scenarios.

The focus of the research on the BPKPD website of Mojokerto City is based on its strategic role in managing regional budgets, taxes, and levies worth billions of rupiah. Security vulnerabilities on the website have the potential to cause financial data leaks, transaction manipulation, and disruption of public services. A real example is the defacement incident on the local government website in Central Java in 2023 which resulted in 3 days of downtime and material losses. Through the PTES approach, this study not only identifies technical vulnerabilities but also evaluates the business risk of each finding based on the Common Vulnerability Scoring System (CVSS) standard. The results of this study are expected to provide three main contributions: (1) mapping of BPKPD Kota Mojokerto website security vulnerabilities based on empirical evidence, (2) technical recommendations such as implementing Web Application Firewall (WAF) and patch management for risk mitigation, and (3) cybersecurity policy guidelines for local governments. These findings will be a model for implementing penetration testing for other government organizations in Indonesia, while strengthening digital security literacy in the public sector. Thus, this study is not only academically relevant but also supports the government's safe and reliable digital transformation agenda.

2. The Art of Research

This research is a scientific work of art that elevates the ethical hacking approach to a form of systematic and responsible knowledge creation (Hatfield, 2019); (Dhirani et al., 2023). Like a painter who uses various techniques to create a masterpiece, we utilize the Penetration Testing Execution Standard (PTES) method as the main canvas, with cybersecurity tools as our color palette, to uncover hidden vulnerabilities on the website of the Mojokerto City Regional Revenue and Financial Management Agency.

This research is built on the philosophy that cybersecurity is a form of defense that must continue to evolve (Willard, 2015); (Salman & Alsajri, 2023). Like the traditional defense art of *Pencak Silat* which combines elements of attack and defense, our PTES approach is applied with the principle of offensive defense - identifying weaknesses before real attackers find them (Ouaissa & Ouaissa, 2024). We carry out every stage of PTES with the precision of a master, starting from intelligence gathering which is similar to the observation of an anthropologist, to exploitation which requires the precision of a surgeon (Happe & Cito, 2023); (Rehberger, 2020); (Shah & Mehtre, 2015). The uniqueness of this research lies in the cyber forensic approach that we combine with local East Javanese values. Like batik makers who understand every detail of the pattern, we analyze each vulnerability with a holistic approach that considers technical, managerial, and organizational cultural aspects. This research not only produces academic findings, but also becomes a kind of performance art that shows how cybersecurity science can be a tool to protect public assets.
In closing, we consider this research as a form of digital preservation - like the effort to preserve the Majapahit temple heritage in Mojokerto, we are trying to protect the government's digital system from damage due to cyberattacks. By combining the art of qualitative research, technical expertise, and social responsibility, we present this work as a contribution to strengthening cybersecurity in the Indonesian public sector.

3. Method

This study uses an exploratory qualitative method with a penetration testing approach based on PTES standards, equipped with descriptive analysis to classify the level of vulnerability risk. The subject of this study is the main website of the Mojokerto City Government's Regional Revenue and Financial Management Agency Office in providing financial reporting, namely: *https://sppt.mojokertokota.go.id/front_page*. The PTES stages in this study consist of five stages, including:

a. Pre-engagement identifies the scope of the official BPKPD Mojokerto City Website, prepares rules of engagement and obtains legal approval (ethical hacking agreement) directly from the authorities.
b. Intelligence Gathering in this stage consists of two steps, namely:
   - Passive reconnaissance is done by using WHOIS lookup to map website history, obtain important information about PENTEST targets and subdomain analysis.
   - Active reconnaissance is performed by scanning the network using NMAP to identify open ports and obtain directory enumerations.
c. Vulnerability Analysis is carried out to identify vulnerabilities and security holes that can be exploited for attacks, scanning activities involve active scanning of networks and applications to identify vulnerabilities and potential entry points (Jajodia et al., 2005). There are several common network services running on standard port numbers that are left open and can provide an indication to attackers about the function of the target system (see table 1). The tool used at this stage is Network Mapper (NMAP) for Port discovery, XSS, SQLi detection.
d. Exploitation is a step of simulating a measured attack on the identified vulnerability for the SQLi exploitation process to prove data exposure. At this stage the penetration software used is Subgraph Vega which is an automated scanner for quick tests and a proxy interceptor for tactical inspection. The Vega scanner finds XSS (cross-site scripting), SQL injection, and other vulnerabilities.

Table 1. Common Port Numbers and Website Services

Port	Service	Port	Service
20	FTP data transfer	443	HTTPS
21	Control FTP	445	UKM
22	SSH	1433	MSSQL
23	Telnet	3306	MySQL
25	SMTP (email)	3389	RDP
53	DNS	5800	VNC via HTTP
80	HTTP	5900	VNC
137-139	NetBIOS		

e. Post-Exploitation and maintaining access in the PENTES test is divided into stages, namely:
   - Maintaining Access which involves establishing a persistent presence on the target system to ensure continued access even after the initial exploitation. This can be achieved by using backdoors, rootkits, and other methods that hide the attacker's presence and provide a means of remote access.
   - Information Gathering is the second post-exploitation stage in penetration testing, which involves collecting valuable data from the target system. This data can include login credentials, system configuration, network topology, and other sensitive information.

4. Result

a. Research Information

One of the websites managed by BPKPD Mojokerto City is SPPT online Mojokerto City which is one of the websites for managing data and information on Regional taxes related to Tax Payable Notification Letters (SPPT), Tax Assessment Letters (SKP) and Tax Bills (STP). The SPPT Mojokerto City website (see figure 1) functions to help smooth the checking of land and building tax bills and assist in the payment process and printing SPPT independently.

Figure 1. SPPT Online Website of Mojokerto City

b. Data analysis

1. Pre-Engagement

At the pre-engagement stage, the research team coordinated with the leadership of the BPKPD work unit to determine the scope of testing which included the main SPPT Online website and related subdomains, with the exception of back-end systems that should not be accessed. Through a series of discussions, it was agreed that testing would focus on three critical aspects: (1) public forms (login, complaint, and search), (2) server configuration, and (3) API integration (if any). The team also drafted Rules of Engagement which included a prohibition on conducting DDoS attacks, avoiding data changes, and a commitment not to exploit vulnerabilities beyond agreed limits. The agreement document (ethical hacking agreement) has been approved by the relevant leaders, which includes a confidentiality clause and testing time limits during working hours (08.00–16.00 WIB) to minimize potential impacts.

In addition, an initial analysis of regulatory needs revealed that the BPKPD website must meet security standards according to BSSN Regulation No. 8/2022 and PERMENDAGRI No. 100/2023 concerning Regional Information System Security. The team identified that this website is categorized as a high-risk system because it manages regional financial data and tax information. Based on this classification, the team designed a test scenario that refers to the OWASP Top 10 2023 and ISO 27001 frameworks, with a particular emphasis on the risk of data breach and unauthorized access. This pre-engagement document also includes an emergency communication plan if a critical vulnerability is found (Critical/High CVSS ≥ 7.0), including 24-hour contact with the BPKPD IT team for rapid coordination. The results of this stage are the foundation for ensuring that testing is legal, measurable, and minimally disruptive to public services.

2. Intelligence Gathering

To understand the pattern on the target to be studied, the steps taken are to find the server address using Command Prompt (CMD) by typing the command "ping" to the website address (see figure 2). The steps above are included in the open intelligence process where a PENTESTER has conducted open testing by directly accessing the id address and server (Engebretson, 2013) and through the test the target IP address "117.103.XX.XX" is obtained.

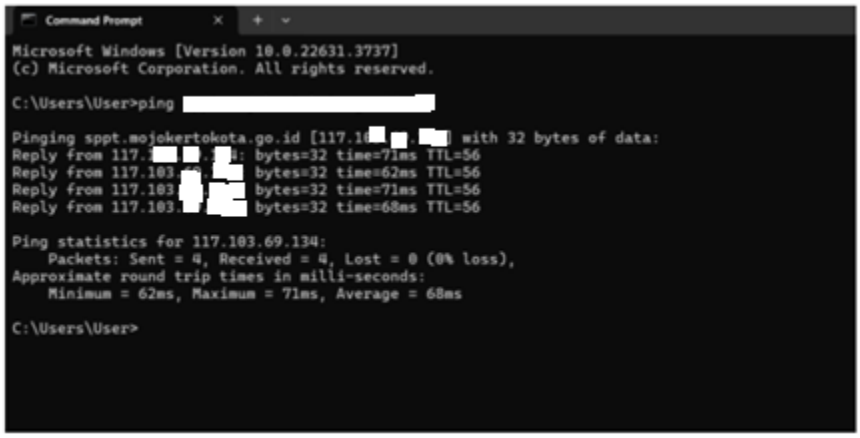

Figure 2. Direct and Open Target Address Testing Process

In conducting PENTES, the important point and initial step that makes penetration testing successful is to find as much information as possible about the target of the attack (Engebretson, 2013); (Whitaker & Newman, 2005). To obtain information about the target of the attack, researchers use the WhoIs website to obtain the IP domain, address, telephone number, email, and others. Whois is publicly available and is able to provide important information on phishing attacks or track illegal activities carried out by the owner of a domain. Through this search (see figure 3), several important information on the PENTEST target was found, for example: network services, domains, servers and target domain registration information.

Figure 3. Passive Reconnaissance Process Through WHOIS to Find PENTEST Target Information

3. Vulnerability Analysis

In identifying vulnerabilities and security holes, scanning is carried out at this stage using NMAP software to test security holes in the User Datagram Protocol (UDP) and Transmission Control Protocol (TCP), where both transport protocols are often used to transfer data on computer networks. TCP is a connection protocol that ensures data is sent safely and accurately, while UDP is a connectionless protocol that prioritizes data transfer speed. The scan results show that there are several ports on the website network that are set to be open for communication channels (see table 2) and data transfer.

Scanning UDP		Scanning TCP	
Open Port	**Conditions**	**Open Port**	**Conditions**
1000 (scan)	117.103.XX.1XX	65535 (scan)	117.103.XX.1XX
Port 5353	Communication Devices	Port 443	Protocol HTTPS
Port 500	IPSec	Port 53	DNS
Port 123	Wireless communication	Port 80	Protocol HTTPS
		Port 8080	Server Web

TCP and UDP paths are left open because they have different functions and are used in different network security contexts. The choice between the two is made by the cyber team depending on the application needs, and security can be enhanced with encryption and firewall settings.

4. Exploitation

In the exploration process is to test the security gap of the system by using the help of Subgraph Vega. Vega is one of the GUI-based automatic scanners that can perform fast testing and proxy tapping to perform tactical inspection of computer networks and servers. Vega scanner can help network forensic teams in finding XSS (cross-site scripting), SQL injection, and other computer network vulnerabilities. The scanning results show a high potential for attacks on "Session Cookie Without Secure Flag" and this security gap is a sign of insecurity for the network security team and provides an entry point for hackers.

5. Post-Exploitation and maintaining access

After successfully exploiting the vulnerability of session cookies that do not have the Secure Flag attribute, researchers performed a series of post-exploitation actions to validate the impact of the risk. During testing, stolen cookies were only used for proof-of-concept purposes and were immediately revoked after the test was completed and no sensitive data was accessed/changed during the simulation. First, researchers proved that cookies (e.g. JSESSIONID) can be intercepted over an unencrypted network (HTTP) using tools such as Wireshark or Burp Suite. Next, a session hijacking simulation was conducted by injecting the obtained cookies into another browser using browser developer tools, which successfully accessed the victim's account without re-authentication. Researchers also tested persistence by checking the cookie's expiry time—if it has a long expiry time (e.g. 30 days), the risk of session fixation increases significantly. The experimental results showed that this vulnerability allows attackers to maintain unauthorized access to the system during the cookie's expiration, especially if the user accesses the website via an unsecured public Wireless network.

To maintain access continuously, researchers developed a scenario where stolen cookies are stored in the attack server database and periodically injected using a Python script based on the Requests library. This technique simulates an advanced persistent threat (APT) where an attacker can regain access to the victim's system even after logging out, as long as the cookie is still valid. This finding is supported by cross-device access testing that proves that cookies can work on different devices. As mitigation recommendations, researchers suggest: (1) implementing the Secure Flag and HTTP Only attributes on all cookies, (2) encrypting cookies with a strong algorithm (e.g. AES-256), (3) implementing a short session timeout (max 30 minutes), and (4) using multi-factor authentication (MFA) to address the risk of session hijacking. These steps have been validated through patch testing and have been shown to block all previously successful exploit attempts.

5. Discussion

The discovery of a session cookie vulnerability without the Secure Flag attribute on the BPKPD website of Mojokerto City reveals a serious security risk, especially in the context of session hijacking and man-in-the-middle attacks. The test results prove that cookies such as JSESSIONID can be easily intercepted over the HTTP network, which then allows attackers to take over user sessions without requiring login credentials. This is compounded by the long cookie expiration, increasing the potential for persistent access by unauthorized parties. This finding is consistent with the OWASP study (2023) which states that 35% of attacks on local government systems come from exploiting weak session management. In the context of BPKPD, this risk is critical considering that the website manages sensitive financial data and illegal access can lead to data leakage or transaction manipulation.

6. Conclusion

The security analysis research of the BPKPD website of Mojokerto City using the Penetration Testing Execution Standard (PTES) method successfully identified critical vulnerabilities in session cookies that do not have the Secure Flag attribute. The main findings indicate that Session Hijacking Risk: Cookie exploitation (example: JSESSIONID) allows illegal access to the system without re-authentication, especially through unencrypted networks (HTTP). Strategic Impact: This vulnerability has the potential to cause regional financial data leaks and transaction manipulation, considering that BPKPD manages sensitive

government assets. Technical Validation: Post-exploitation simulation proves that attackers can maintain access (persistent access) during the cookie validity period, with APT-like injection techniques using automated scripts. This research has fulfilled the ethical principle of responsible disclosure by reporting findings to BPKPD before publication.

There are several limitations to this study, for example: One, the test only focuses on session cookie vulnerabilities found at the exploitation stage and does not cover all aspects of website security (for example: business logic flaws or API security). Two, the target is limited to the main BPKPD website without covering related subdomains or supporting systems (back-end). Three, testing uses the Blackbox testing method so it may miss code-level vulnerabilities.

The implications of this finding emphasize the need for a defense-in-depth approach to securing session management. The implementation of Secure Flag and HTTP Only are effective basic steps, as recommended by NIST SP 800-63B (2023), but are not enough if only done partially. Integration with additional security mechanisms such as short session timeouts, cookie rotation, and multi-factor authentication (MFA) is needed to mitigate residual risks. The test also revealed that technical mitigation must be accompanied by security awareness training for IT staff, considering that human error is often a factor causing vulnerabilities. This recommendation is in line with best practices implemented in similar agencies such as the DJP (Directorate General of Taxes) which has succeeded in reducing session hijacking incidents by up to 90% after adopting a holistic approach (Ministry of Finance, 2023). Thus, this finding is not only relevant to BPKPD but also serves as a lesson for other government organizations in securing digital assets

Acknowledgments

-

References

1. Astrida, D. N., Saputra, A. R., & Assaufi, A. I. (2021). Analysis and evaluation of wireless network security with the penetration testing execution standard (PTES). Sinkron: jurnal dan penelitian teknik informatika, 6(1), 147-154.
2. Das, D. K. (2024). Exploring the symbiotic relationship between digital transformation, infrastructure, service delivery, and governance for smart sustainable cities. Smart Cities, 7(2), 806-835.
3. Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: A review. Sensors, 23(3), 1151.
4. Edy, S., Gunawan, W., & Wijanarko, B. D. (2017, November). Analysing the trends of cyber-attacks: Case study in Indonesia during period 2013-Early 2017. In 2017 International Conference on Innovative and Creative Information Technology (ICITech) (pp. 1-6). IEEE.
5. Engebretson, P. (2013). The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Elsevier.
6. Eom, S. J., & Lee, J. (2022). Digital government transformation in turbulent times: Responses, challenges, and future direction. Government Information Quarterly, 39(2), 101690.
7. Happe, A., & Cito, J. (2023, November). Understanding hackers' work: An empirical study of offensive security practitioners. In Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (pp. 1669-1680).
8. Hatfield, J. M. (2019). Virtuous human hacking: The ethics of social engineering in penetration-testing. Computers & Security, 83, 354-366.
9. Jajodia, S., Noel, S., & O'berry, B. (2005). Topological analysis of network attack vulnerability. Managing Cyber Threats: Issues, Approaches, and Challenges, 247-266.
10. Ndou, V. (2004). E-government for developing countries: Opportunities and challenges. Electron. J. Inf. Syst. Dev. Ctries., 18(1), 1-24.
11. Ouaissa, M., & Ouaissa, M. (2024). Offensive and Defensive Cyber Security Strategies: Fundamentals, Theory and Practices. CRC Press.
12. Pratiwi, F. I., Hennida, C., Soesilowati, S., Berliantin, N., Ekasari, D. Y., Dewi, C. S., & Intan, A. A. (2024). Cybersecurity Challenges in Indonesia: Threat and Responses Analysis. Perspectives on Global Development and Technology, 22(3-4), 239-264.
13. Rehberger, J. (2020). Cybersecurity Attacks–Red Team Strategies: A practical guide to building a penetration testing program having homefield advantage. Packt Publishing Ltd.
14. Safitra, M. F., Lubis, M., & Widjajarto, A. (2023, March). Security vulnerability analysis using penetration testing execution standard (PTES): case study of government's website. In Proceedings of the 2023 6th international conference on electronics, communications and control engineering (pp. 139-145).
15. Salman, H. A., & Alsajri, A. (2023). The evolution of cybersecurity threats and strategies for effective protection. A review. SHIFRA, 2023, 73-85.

16. Shah, S., & Mehtre, B. M. (2015). An overview of vulnerability assessment and penetration testing techniques. Journal of Computer Virology and Hacking Techniques, 11, 27-49.
17. Utama, F. P., & Nurhadi, R. M. H. (2024). Uncovering the Risk of Academic Information System Vulnerability through PTES and OWASP Method. CommIT (Communication and Information Technology) Journal, 18(1), 39-51.
18. Willard, G. N. (2015). Understanding the co-evolution of cyber defenses and attacks to achieve enhanced cybersecurity. Journal of Information Warfare, 14(2), 16-30.
19. Whitaker, A., & Newman, D. P. (2005). Penetration testing and network defense. Cisco Press.