Security Vulnerability Analysis using Penetration Testing Execution Standard (PTES): Case Study of Government's Website

Muhammad Fakhrul Safitra*
Information System Department, School of Industrial and System Engineering, Telkom University, Indonesia
fakhrulsafitra@student.telkomuniversity.ac.id

Muharman Lubis
Information System Department, School of Industrial and System Engineering, Telkom University, Indonesia
muharmanlubis@student.telkomuniversity.ac.id

Adityas Widjajarto
Information System Department, School of Industrial and System Engineering, Telkom University, Indonesia
adtwjrt@telkomuniversity.ac.id

ABSTRACT

The rapid development of technology has impacted various aspects of life, including the way individuals, organizations, and governments deliver accurate, effective, and efficient information. XYZ local government, which is responsible for serving the community in the trade field, manages its information through the Communication and Information Agency (Diskominfo) of the XYZ region. Diskominfo employs technological advancements to provide the people of the XYZ region with direct access to accurate, precise, and reliable data through their website. However, the security of the website has become a crucial aspect to prevent attacks from malicious individuals that can cause damage to the system and harm the website owner. To analyze the website's security loopholes and vulnerabilities, the author performed a simulation of an attacker. The analysis aimed to evaluate the level of risk and confidence in the website. The results showed 42 alerts categorized into four risk levels: 9 vulnerabilities with a high-risk level, 13 vulnerabilities with a medium-risk level, 11 vulnerabilities with a low-risk level, and 9 vulnerabilities with an informational-risk level.

CCS CONCEPTS

• **Security and privacy**; • **Systems security**; • **Vulnerability management**; • **Penetration testing**;

KEYWORDS

Vulnerability Analysis, Website, Standard, Report, PTES

ACM Reference Format:
Muhammad Fakhrul Safitra, Muharman Lubis, and Adityas Widjajarto. 2023. Security Vulnerability Analysis using Penetration Testing Execution Standard (PTES): Case Study of Government's Website. In *2023 The 6th International Conference on Electronics, Communications and Control Engineering (ICECC 2023), March 24–26, 2023, Fukuoka, Japan.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3592307.3592329

*Muhammad Fakhrul Safitra is the corresponding author.

ICECC 2023, March 24–26, 2023, Fukuoka, Japan

ACM ISBN 979-8-4007-0000-2/23/03…$15.00
https://doi.org/10.1145/3592307.3592329

1 INTRODUCTION

Media information is no longer limited to print media, but there is another affordable alternative for information media which is utilizing the internet. The internet has the advantage of providing information and enabling services to interact with each other. One of the things done in using the internet is building a website that can effectively and efficiently disseminate information. Websites have become a very popular information media because they are easily accessible by internet users from various parts of the world and can be accessed anytime and anywhere. In addition, websites also have the advantage of being able to interact with users.[1].

Websites also have a role in being a recognition of an institution's credibility by presenting information, publications, promotions, communication facilities, and data presentation for various parties. Quality data processing and collection are important in decision making and determining the future direction of an institution. Data is important because it can be traded for extortion, fraud, and even phishing schemes that can occur to individuals and institutions. In contrast, cyber attacks that target individuals or individuals as victims with the spread of fake news or hoaxes can create a doctrine that the disseminated news is the truth spread through social media. Therefore, the scope of the cyber and information arena has become the most current ongoing battle.

Between the period of January 1st to April 12th, 2020, a total of 88,414,296 cyber attacks were recorded by the State Cipher and Cyber Agency's (BSSN) National Cyber Security Operations Center (Pusopskamsinas). In addition to the calculation of attacks from January 1 to April 12, 2020, BSSN has also released a classification of attacks from January to April 12, 2020. The attacks that occurred can be seen from the existence of 3 popular attacks; the first is Trojan Activity attacks, accounting for 56% of the total attacks, followed by Information Gathering attacks, which account for 43% of the total attacks, relatively less than Trojan Activity attacks. Web Application Attacks ranked third with 1% of the total attacks.

Cyber attacks have become a weapon of war and are supported by existing technology [2], Limited or massive cyber attacks have occurred several times carried out by external parties in Indonesia, and this can lead us to conclude that war will soon be waged using cyber attacks. When we talk about defense, we must first determine the threat. According to Law No. 3 of 2002 on National Defense, there are two types of threats to the state's defense: military threats and non-military threats. Non-military threats encompass cyber threats, as stated in the legislation [3].

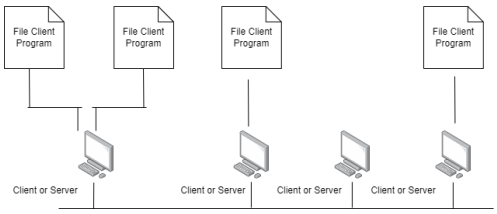

Figure 1: Peer to Peer

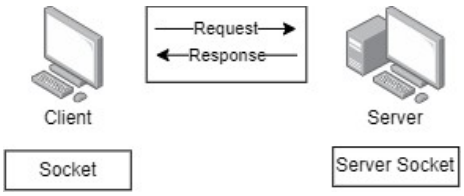

Figure 2: Illustration of client-server

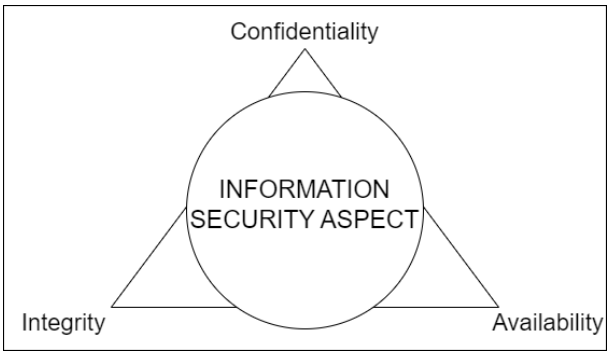

Figure 3: Information Security Aspects

Indonesia has a critical record that needs to be considered and addressed regarding the increasing number of cybercrime cases. This record highlights that cybercrime is a matter that needs to be seriously considered for the security of websites. This record reinforces the need for security vulnerability analysis [4].

Analysis is conducted to prepare for worst-case scenarios by anticipating appropriate strategies to respond to such attacks [5]. The security vulnerability analysis in this research depicts a simulation of unauthorized attackers entering the security controls, and from this simulation, we can prepare recommendations to deal with it.

This research observes the input and output results without knowing the internal structure, detailed implementation, and internal paths of a website program in conducting vulnerability analysis. The research on the XYZ Local Government website is conducted using the Penetration Testing Execution Standard (PTES) framework.

2 LITERATURE REVIEW

2.1 Information System

A system can be defined as a collection of interrelated and organized elements that collaborate to perform a specific function and achieve a common objective. The properties of a system are composed of distinct elements, including system boundaries, system components, external environment, system interfaces, system inputs, system outputs, system processing, and system objectives [6]. Information is a set of processed data that is relevant and meaningful to the receiver in reducing uncertainties when making decisions. An information system is composed of hardware, software, communication networks, data sources, and people who gather, transform, and distribute information within an organization [7].

2.2 Computer Network

A computer network is a collection of interconnected computers that exchange data/information and share resources. In computer networks, there are known connection systems, namely:

- Peer-to-Peer, which is a network consisting of several interconnected computers. Peer-to-peer is a model in which each computer can use resources on other computers or provide resources to other computers [8]. In other words, it can function as both a client and a server at the same time. Figure 1 presents an illustration of the peer-to-peer concept.
- Client-Server, which is a computer network that distinguishes between clients and servers. In a system that uses client-server, applications can operate independently even if they are not located in the same place [8]. The way it works can be seen in Figure 2.

2.3 Information System Security

One of the valuable assets that needs to be carefully guarded is information system security, to prevent and detect threats to the system and prepare for them. Information security has several aspects that need to be understood and protected, and there are three common aspects known as the CIA triangle model: Confidentiality, Integrity, and Availability (figure 3). This information should be protected from threats and dangers [9].

2.4 Cybersecurity

Cybersecurity refers to a range of measures, policies, tools, and techniques employed to safeguard sensitive organizational and personal data from unauthorized access, use, or theft. This encompasses a wide range of assets, including hardware, software, telecommunications infrastructure, services, personnel, and applications. The purpose of cybersecurity is to mitigate risks to the confidentiality, integrity, and availability of information (often referred to as "CIA") and to protect against various threats to these values [10].

2.5 Website Security

As the use of websites continues to grow from year to year, awareness of information security aspects should also be developed. Information security of a website can be defined as a necessity to obtain protection against information as an asset that exists on the website, such as regulating information access, managing user identities, and so on [11]. In a website, there are sensitive and important data that can be detrimental, and the lack of attention to this matter can result in security vulnerabilities that can be exploited by

an attacker. Security vulnerabilities on a website can be identified through security vulnerability analysis [8].

2.6 Threat to Information System Security

There are two categories of threats to information security, namely active and passive threats. Active threats refer to malicious activities such as data theft, unauthorized system usage, illegal destruction, and unauthorized modification. On the other hand, passive threats include non-malicious events such as system failures, human errors, and natural disasters [12].

With these threats, efforts must be made to secure both from active and passive attacks through the implementation of appropriate controls. The controls include the implementation of various policies, procedures, structures, practices, and specific functions. All these controls must be applied to maintain information security [9].

2.7 Security Testing of Information Systems

Information Security is constantly evolving and increasing. In this regard, it can trigger an increase in criminal activities. Security system testing is needed to find security vulnerabilities in anticipation of criminal activity against information security [13].

1. Vulnerability, weaknesses that exist in the design, implementation, or operation, and management found in the network system that can threaten.
2. Vulnerability Assessment, an activity that assesses security controls internally and externally by identifying vulnerabilities in systems, computer networks, applications, or other parts that create opportunities for attacks on target assets.
3. Penetration Testing is a type of security testing where an assessor emulates real-world attacks to discover ways to bypass security features of an application, system, or network.

2.8 Information Security System Testing Standarization

Penetration Testing Execution Standard (PTES) is a standard used to try to identify security vulnerabilities on a website to be used as a precaution in the future [14].

1. Pre-Engagement Interactions aims to explain various tools and techniques used to assist before conducting penetration testing.
2. In the Intelligence Gathering stage, information is gathered about the target for the penetration testing. The purpose of this is to obtain relevant information that will enable the design of appropriate actions in accordance with the agreed objectives of the test.
3. In the stage of Threat Modeling, the required approach for conducting penetration testing is identified and examined. This phase is essential for both the tester and the target object, as modeling can provide a clear understanding of the risks involved and help establish priorities.
4. Vulnerability Analysis is a process of identifying weaknesses in systems and applications that can potentially be exploited by attackers.
5. In the exploitation phase of a Penetration test, the main objective is to gain unauthorized access to the system by circumventing any security measures that have been implemented.
6. The post-exploitation phase aims to assess the extent of the system's vulnerability after the initial breach and determine how to maintain control for subsequent attacks.
7. Reporting, at this stage, documents determine the basic criteria for reporting the penetration testing report. The level of value is established based on the level of sensitivity of the stored data and its usefulness.

3 RESEARCH METHOD

This research utilizes the conceptual model reference from Hevner's research [15]. The conceptual model used in this research is as follows.

In this study, the conceptual model utilized is comprised of three distinct components: environment, research, and scientific foundations, as depicted in Figure 4. The environment describes the problem space. Entities within the environment include people who are still unaware of website security issues and require technologies to search for vulnerabilities, such as using a virtual machine that contains Kali Linux and using tools within Kali Linux such as OWASP ZAP, Acunetix, Nmap, Paros, and others. The research section includes the objectives, problems, and tasks. The research contains entities for building and evaluating. The build entity contains artifacts used to identify security gaps on the target website and analyze these gaps. The evaluation of this research will be conducted subsequently. Several theories are used as the scientific foundations for this research, including Penetration Testing Execution Standard (PTES) and black box testing.

4 RESULT DISCUSSION

The aim of **Pre-Engagement** Interaction is to provide an explanation and presentation of the tools and techniques that can be used and are available during the **pre-engagement** interaction stage. The information obtained can come from the experiences of experts collected to help gather information in the **pre-engagement** interaction stage, or it can also be assisted by various tools.

Table 1 describes the hardware specifications of the target device.

The **Intelligence Gathering** phase involves gathering information about the target through reconnaissance. This information is useful in the vulnerability assessment and exploitation phase of the penetration testing. The greater the amount of information collected at this stage; the more attack vectors can be utilized on the target system.

The DNS lookup testing on http://disperindag.xxxprov.go.id/ A Record of the domain shown in Figure 5 provides information about the server and address information of the XYZ regional government website.

Intelligence Gathering Nmap Scanning is the activity of checking the TCP and UDP port status on a machine, as shown in figure 6, to gather information on the target system.

Intelligence Gathering utilizes the DIG (Domain Information Groper) tool, a powerful command-line tool used to request information about DNS name servers. For system administrators, the

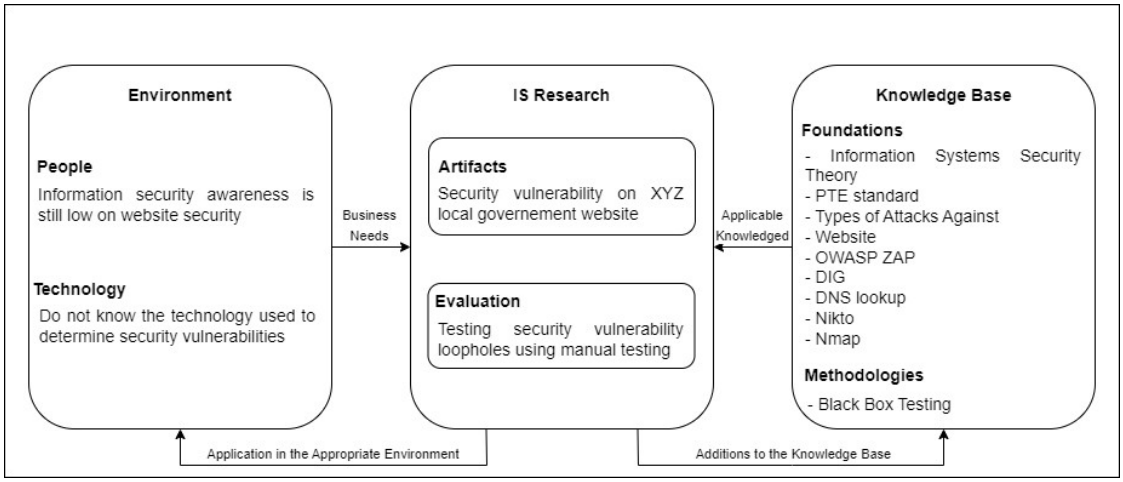

Figure 4: Information System Research Framework

Table 1: Target Hardware Specifications

Component Name		Information
Hardware Specifications (Main OS)	Processor	Intel ®Xeon ®CPU E5-2620 V3 @2.40 GHz 12- core
	Memory	32GB
	Hard Disk	1 TB
	Systems Type	64-bit Operating System
	Operating System	Ubuntu

Figure 5: Test DNS lookups

dig command is the most used tool to troubleshoot DNS problems because of its flexibility and ease of use. This is shown in figure 7.

The process of **threat modeling** is utilized to enhance the security of a network by recognizing weaknesses, determining goals, and devising countermeasures to mitigate or minimize the impact of cyber attacks on the system. **Threat modelling** in this phase is used as a modelling approach for the testing that will be conducted. Modelling is used to facilitate the tester and the target company to understand the security vulnerabilities that will be found to conduct the testing in this research. Figure 8 illustrates the threat modelling of Distributed Denial of Service (DDoS) attack.

Vulnerability Analysis is the process of identifying weaknesses in a system or application that can be exploited by the tester. The vulnerabilities that could be identified on the target website may vary from misconfigured hosts and services to insecure application design. In this case, the tester utilized OWASP ZAP to identify vulnerabilities on the target website.

Figure 6: Port Scanning on the XYZ Local Government Website

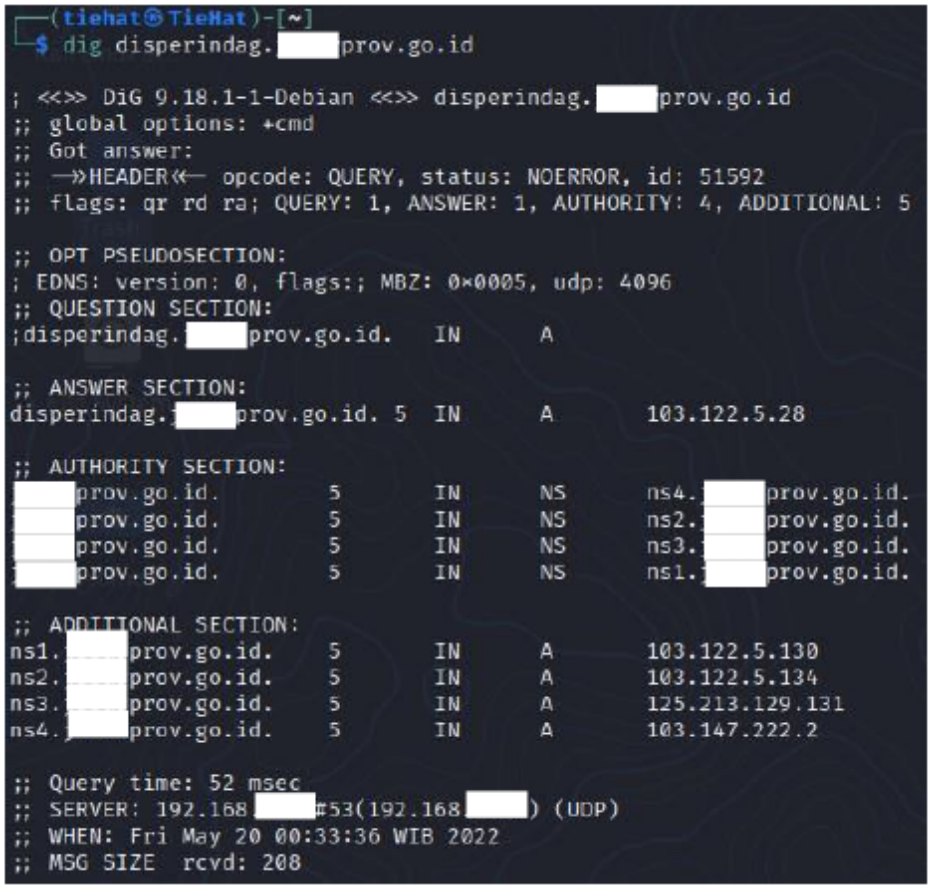

Figure 7: Intelligence gathering using DIG tools

Here are 42 security vulnerability alerts detected using OWASP ZAP tool. (figure 9)

The recommendation that can be made is to also use a Web Application Firewall (WAF). Implementing Modsecurity as a Web Application Firewall (WAF) solution can secure a web application.

Web Application Firewall (WAF) is a firewall used to protect web applications. WAF is designed to prevent threats from attackers. Modsecurity is used to filter incoming and outgoing data, monitor traffic, and block traffic deemed as a threat to the web application.

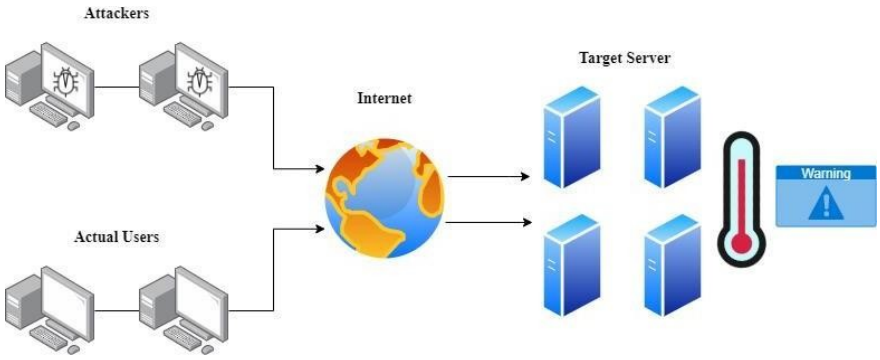

Figure 8: Threat modelling DDoS

Figure 9: Shows 42 security vulnerability warnings using OWASP ZAP tools

Modsecurity is used by setting established rules and does not provide much workload on the web server, resulting in good testing results.

In Figure 10, it shows the mechanism of a web server without WAF. When an attacker makes a potentially harmful request, the web server receives it and passes it directly to the database server, allowing access to the data in the database server or modifying it. For non-malicious requests, it can also have direct access to the database server.

Figure 11 shows the mechanism of a web server with WAF installed. When an attacker makes a potentially harmful request, the web server that has been equipped with WAF can immediately block the attack request before it reaches the database server. For requests that are not potentially harmful, they can directly access

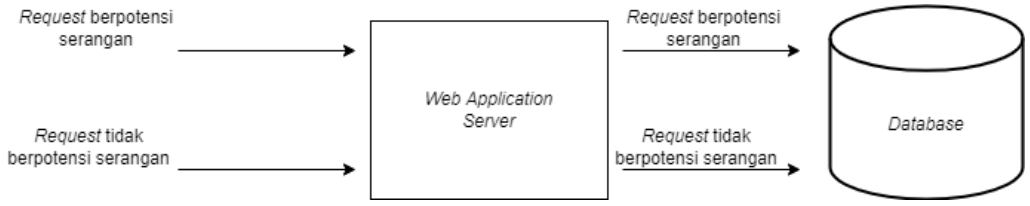

Figure 10: Web Server Diagram without WAF

Figure 11: Web Server Diagram using WAF

the database server without being prevented by WAF. By implementing WAF, the website belonging to local government XYZ can be safeguarded against harmful attacks, including but not limited to SQL Injection and Cross-Site Scripting.

5 CONCLUSION

Based on the vulnerability analysis of the XYZ local government website, it can be concluded that:

- In this study, several tools were used to perform vulnerability assessment and penetration testing. The target website was subjected to information gathering techniques such as the use of Nmap and DIG commands, which disclosed that certain ports including 21/TCP, 22/TCP, 80/TCP, 110/TCP, 443/TCP, 1723/TCP, and 4443/TCP were open, and the IP address 103.122.x.xx was also obtained to facilitate vulnerability scanning. The utilization of OWASP ZAP for vulnerability scanning resulted in the detection of 42 alerts, which were categorized into four levels of risk. There were 9 vulnerabilities with high risk, 13 vulnerabilities with medium risk, 11 vulnerabilities with low risk, and 9 vulnerabilities with informational risk.
- The target website still has high-risk security vulnerabilities, so it needs to take several preventive measures, such as using parameterized SQL queries, validating input data using regular expressions, adding escape characters, checking debug modes, checking the security of the database used, conducting regular security testing of the website application, and using web application firewall security tools. These preventive measures are taken to prevent unwanted incidents from happening to important data.

REFERENCES

[1] Y. Trimarsiah and M. Arafat, "Analisis dan Perancangan Website Sebagai Sarana Informasi Pada Lembaga Bahasa Kewirausahaan dan Komputer Akmi Baturaja," Jurnal Ilmiah Matrik, vol. 19, no. 1, pp. 1–10, 2017.
[2] Y. Hollander, "Prevent Web Site Defacement," 2000. [Online]. Available: http://www.entercept.com.
[3] B. A. Soewardi, "Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi indonesia," Media Informasi Ditjen Pothan Menhan. Media Informasi Ditjen Pothan Kemhan, Mar. 2013.
[4] A. Almaarif and M. Lubis, "Vulnerability Assessment and Penetration Testing (VAPT) Framework: Case Study of Government's Website," Int J Adv Sci Eng Inf Technol, vol. 10, no. 5, pp. 1874–1880, 2020, doi: 10.18517/ijaseit.10.5.8862.
[5] A. Widjajarto, M. Lubis, and V. Ayuningtyas, "Vulnerability and risk assessment for operating system (OS) with framework STRIDE: Comparison between VulnOS and Vulnix," Indonesian Journal of Electrical Engineering and Computer Science, vol. 23, no. 3, pp. 1643–1653, Sep. 2021, doi: 10.11591/ijeecs. v23.i3. pp1643-1653.
[6] S. Liu, Z. Li, and X. Cheng, "Introduction to the special section on Quality, Reliability and Resilience in Hybrid Information Systems," Computers and Electrical Engineering, vol. 70, pp. 1105–1107, Aug. 2018, doi: 10.1016/j.compeleceng.2018.07.039.
[7] S. Ferré and O. Ridoux, "Introduction to logical information systems," Inf Process Manag, vol. 40, no. 3, pp. 383–419, May 2004, doi: 10.1016/S0306-4573(03)00018-9.
[8] H. Setiawan, L. E. Erlangga, and I. Baskoro, "Vulnerability Analysis Using the Interactive Application Security Testing (IAST) Approach for Government X Website Applications," in 2020 3rd International Conference on Information and Communications Technology, ICOIACT 2020, Nov. 2020, pp. 471–475. doi: 10.1109/ICOIACT50329.2020.9332116.
[9] M. P. Mokodompit and N. Nurlaela, "Evaluasi Keamanan Sistem Informasi Akademik Menggunakan ISO 17799:2000," JURNAL SISTEM INFORMASI BISNIS, vol. 6, no. 2, pp. 97–104, Jan. 2016, doi: 10.21456/vol6iss2pp97-104.
[10] H. Ardiyanti, "Cyber-Security dan Tantangan Pengembangannya di Indonesia," Politica, vol. 5, no. 1, 2014, [Online]. Available: http://kominfo.go.id/index.php/content/detail/3980/
[11] J. Grossman, "The State of Website Security," Institute of Electrical and Electronics Engineers (IEEE), Aug. 2012. doi: 10.1109/msp.2012.111.
[12] Paryati, "Keamanan Sistem Informasi," Seminar Nasional Informatika, pp. 379–386, 2008, [Online]. Available: www.upnyk.ac.id
[13] A. W. Kuncoro and F. Rahma, "Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review," AUTOMATA, vol. 3, no. 1, 2022, [Online]. Available: https://www.sciencedirect.com
[14] The PTES Team, The Penetration Testing Execution Standard Documentation. 2022.
[15] A. R. Hevner, S. T. March, J. Park, and S. Ram, "DESIGN SCIENCE IN INFORMATION SYSTEMS RESEARCH 1," Design Science in Information Systems Research, vol. 28, no. 1, pp. 75–105, 2004.