Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 1, January 2023
https://doi.org/10.47709/cnahpc.v5i1.1991

Submitted : January 12, 2023
Accepted : January 19, 2023
Published : January 19, 2023

Vulnerability Assessment with Network-Based Scanner Method for Improving Website Security

Dewi Laksmiati
Universitas Bina Sarana Informatika, Indonesia
dewi.dlk@bsi.ac.id

ABSTRACT

The digital world has seen a significant increase in security threats in recent years, with hacker attacks on websites being a major concern in cybersecurity. One platform that is particularly vulnerable is WordPress, which is widely used and therefore a popular target for hackers. About 95.62% hacked website in 2021 is WordPress based site. Therefore, to improve website security we conducted a vulnerability assessment on a WordPress based website, in order to identify vulnerabilities that may be exploited by hackers. To do the vulnerability assessment, we used the network-based scanner based to detect vulnerabilities on the WordPress website. Our results showed that the website had several vulnerabilities that needed to be addressed and fixed immediately. The conclusion of our research highlights the importance of conducting regular vulnerability assessments on WordPress-based websites to reduce the risk of vulnerabilities being exploited. By taking proactive measures to identify and fix vulnerabilities, website owners can better protect their sites from potential hacker attacks. It is crucial for website owners to be aware of the risks posed by security threats in the digital world and to take steps to mitigate these risks to protect their businesses and their customers.

Keywords: Vulnerability assessment, hacker attacks, WordPress, cybersecurity, website vulnerabilities

1. INTRODUCTION

The digital world has seen a significant increase in security threats in recent years. Security threats commonly not differs the target, but they will have a greater impact if they attack companies. hacker attacks on websites being a major concern. Therefore, cybersecurity is extremely important for companies, especially in the digital age. Cybersecurity helps protect companies from hacking attacks that can damage systems, steal data, or disrupt business activities. The history of cybersecurity dates to the 1943 when first digital computer, ENIAC was invented by J. Presper Eckert and John Mauchly at the University of Pennsylvania.(ComputerHope, 2022)

However, since the 1980s, hacking attacks have become more common, making companies more aware of cybersecurity, and now in the internet era. The cybersecurity has more important role, and it is estimated that the number of new threats is doubling every year, and the global cost of data breaches is measured in trillions of dollars per year.(Borky & Bradley, 2019). Security evaluation has important role in cybersecurity, it is conducted to find vulnerabilities on the website and provide solutions to the vulnerabilities found. This security evaluation prevents the risk of losing important data and additional budget expenditures if the website experiences malfunction or crash(Tania, Setiyadi, & Khasanah, 2018). The current forms of cyber threats include Advanced Persistent Threats (APT) attacks, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, Defacement attacks, Phishing attacks, Malware attacks, Trojan Horse attacks, Password Cracking, and Spa (Zen, Gultom, & Reksoprodjo, 2020) m. Unfortunately, the cybersecurity role in company is not easily filled, over 60 percent of respondent organizations experience at least three months of unfilled cybersecurity positions when hiring new staff(ISACA, 2019).

In cybersecurity nowadays, web application has become common target, Web applications can perform a wide range of functions, such as allowing users to enter data, process transactions, or access information. These applications are often used in business, education, and government settings to streamline processes and improve efficiency. One of the main advantages of web applications is that they can be accessed from any device with an internet connection, providing greater flexibility and mobility. Additionally, web applications can be updated and maintained remotely, making them easy to scale and adapt to changing needs. In conclusion, web applications are a valuable tool for

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 1, January 2023
https://doi.org/ 10.47709/cnahpc.v5i1.1991

Submitted : January 12, 2023
Accepted : January 19, 2023
Published : January 19, 2023

organizations seeking to leverage the power of the internet to enhance their operations and better serve their customers.

WordPress is one of the most widely used web applications in the world. It is a content management system (CMS) web application which allows users to easily create, manage, and publish content on the internet. CMS is a software application that is used to create, manage, and publish digital content, such as websites and blogs. A CMS typically includes a user-friendly interface that allows users to easily add and edit content, as well as control the appearance and functionality of their website. Some popular CMS platforms include WordPress, Joomla, and Drupal. WordPress leads as the most widely used CMS currently, about 43.1% of all websites on the internet are using WordPress(W3Techs, 2023). As the most widely used platform in the internet WordPress is being popular target for hackers. About 95.62%% hacked website in 2021 is WordPress based.(Moran, 2022). Therefore, it is important for users to conduct vulnerability assessment to anticipate vulnerabilities that might be exploited by hackers.

Vulnerability assessment is one way to improve cybersecurity for a company. Vulnerability assessment is the process of identifying computer system vulnerabilities that can be exploited by hackers. By conducting vulnerability assessment, companies can find out what vulnerabilities exist in their system and take action to fix them.

In this study, we used vulnerability assessment methods to identify vulnerabilities on the WordPress-based website www.mobilemuslim.id. We used tools such as Nmap and WPScan to detect vulnerabilities on the website. The results of the study are expected to provide important information for the company about vulnerabilities on its website and take the appropriate action to fix them.

2. LITERATURE REVIEW

Web Application

A web application is a software application that is accessed via the web browser and is usually connected to the internet. Web applications are often used to provide online services or features such as email, to-do lists, or e-commerce platforms. Most of the Web applications used today have a need to store data between browser requests. For example, an e-store application needs to remember which items a client has added to the shopping cart while processing the steps of making an order(Malinova, Rahneva, & Golev, 2014). One of the main advantages of web applications is their accessibility from a variety of devices with installed web browsers, such as computers, smartphones, or tablets. This allows users to access the application from anywhere and at any time if they are connected to the internet.

A web application is an application that operates on the Internet or an intranet using a web browser. An application written in a web-language (such as HTML, JavaScript, Java, etc.) that needs to be run through a browse (Yik Ern, Yan Shaw, & Jun Hao, 2019) r. These applications also typically use a server to store data and process requests from users. Web applications can be run on a server connected to the internet or on rented hosting.

In addition to accessibility, web applications are generally more secure than desktop applications because they do not need to be installed on the user's device. This reduces the risk of security vulnerabilities caused by incorrect installation or failed updates. However, web applications can still be exposed to other security risks such as DDoS attacks or security vulnerabilities in the server used to run the application.

There are several types of web application, in example(Khurana, 2020):

- Static web application
- Dynamic web application
- Single page apps
- Multi-Page web apps
- Progressive web applications
- Content management system

Content Management System

A content management system (CMS) is a software application that allows users to manage and publish digital content. The history of CMS can be traced back to the late 1990s, when web-based content management systems first emerged. These early systems were designed to make it easier for non-technical users to create and manage websites.

Since then, CMSs have evolved significantly, and today they are used by individuals, small businesses, and large organizations to manage a wide range of digital content, including text, images, audio, and video. Some popular

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 1, January 2023
https://doi.org/ 10.47709/cnahpc.v5i1.1991

Submitted : January 12, 2023
Accepted : January 19, 2023
Published : January 19, 2023

examples of CMS include WordPress, Joomla, and Drupal.

One of the key benefits of using a CMS is that it allows users to easily create and update content without requiring any knowledge of HTML or other programming languages. This makes it possible for non-technical users to maintain a professional-looking website without the need to hire a web developer.

Another benefit of CMS is that it enables users to manage multiple users and roles, which is useful for organizations that have a team of people working on their website. CMSs also typically have built-in features for search engine optimization, which can help improve the visibility of a website in search engine results.

In summary, a CMS is a powerful tool for managing and publishing digital content, and it has revolutionized the way that websites are created and maintained. In the following sections, we will delve deeper into the specific features and capabilities of WordPress, which is one of the most widely used CMSs.

WordPress

WordPress is a web platform of content management system (CMS) that is widely used for creating and managing websites. From a technical perspective, WordPress is based on a PHP and MySQL backend, which allows it to store and retrieve data from a database. This makes it easy to manage large amounts of content, such as blog posts, pages, and media files, and to display this content on the frontend of a website. WordPress also utilizes a template system, which separates the content of a website from its design, making it easy to change the look and feel of a site without affecting its content. Additionally, WordPress has a large selection of plugins and themes that allow users to extend and customize its functionality, making it a highly flexible and scalable platform for building websites. Due to ease-of-use WordPress is applicable for both developers and non-technical users alike, as it offers a wide range of features and customization options. Like other application, WordPress also requires to be periodically maintained and monitor It's important to monitor your website health and performance. Regular monitoring will help you discover issues as soon as they and appear, and often before they become serious(Burgess, 2015). Vulnerable plugins and themes are the #1 reason WordPress websites get hacked(ITHEMES, 2023). Therefore, vulnerabilities from third-party code remain as one of the biggest threats to websites build on WordPress.(Sild, 2021)

Vulnerability Assessment

Vulnerability assessment is the process of identifying computer system vulnerabilities that can be exploited by hackers. The purpose of vulnerability assessment is to determine what vulnerabilities exist in the system and take action to mitigate them, to protect the system from hacker attacks. Vulnerability Assessment is a search for system security gaps that can lead to failure of the information technology process(Susanto, Rizko, & Purbohadi, 2020).

The process of vulnerability assessment consists of three stages: pre-activity, activity, and post-activity. Pre-activity is the preparation stage before conducting the vulnerability assessment, which includes planning, tool selection, and system configuration. Activity is the stage of carrying out the vulnerability assessment, which includes scanning system vulnerabilities, identifying vulnerabilities, and evaluating vulnerabilities. Post-activity is the stage after the vulnerability assessment has been completed, which includes presenting the results, recommendations, and follow-up actions.

Below are the summary vulnerability assessment steps (Imperva, 2022):

- Vulnerability identification (testing)
- Vulnerability analysis
- Risk assessment
- Remediation

Fig. 1 Vulnerability Assessment Test (Imperva, 2022)

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 1, January 2023
https://doi.org/ 10.47709/cnahpc.v5i1.1991

Submitted : January 12, 2023
Accepted : January 19, 2023
Published : January 19, 2023

The methodology used in vulnerability assessment varies depending on the type of system being assessed, the tools used, and the purpose of the assessment. Some commonly used methodologies are manual assessment, automated assessment, and hybrid assessment.

There are several types of Vulnerability Assessment (McNab, 2004):

- Network vulnerability assessment is an assessment of the security of a network infrastructure, which includes both hardware and software components.
- Host-based vulnerability assessment is an assessment of the security of individual systems, including both the hardware and software components.
- Web application vulnerability assessment is an assessment of the security of web applications, which includes the source code, server configuration, and application configuration.
- Penetration testing is an assessment of system security by attempting to hack into the system.
- Compliance assessment is an assessment of a system's compliance with industry standards or regulations.

This research will be using Network vulnerability assessment. Network scanner-based vulnerability assessment is a type of vulnerability assessment that is performed using tools such as Nmap or Nessus to scan for vulnerabilities in a computer network. These tools can automatically scan a computer network and identify vulnerabilities on that network. Nmap performs a large number of IP fingerprinting test to guess the remote operating platform(McNab, 2004), and also scan the other parameter based on current Nmap database.

The process of network scanner-based vulnerability assessment typically includes selecting the tool to be used, configuring the tool according to the conditions of the network to be scanned, and conducting the vulnerability scan. The results of network scanner-based vulnerability assessment are usually in the form of a report that lists the vulnerabilities found, the level of vulnerability of each vulnerability, and recommendations for actions that can be taken to mitigate the vulnerabilities.

The advantage of network scanner-based vulnerability assessment is that it can be done automatically and can provide accurate results. However, its disadvantage is that it depends on the capabilities of the tool used, so not all vulnerabilities can be detected. Nmap and WPScan, which will be used in this writing, are part of Network scanner-based vulnerability assessment.

3. METHOD

The methodology used in this study follows the design scheme outlined in Figure 2. Below:

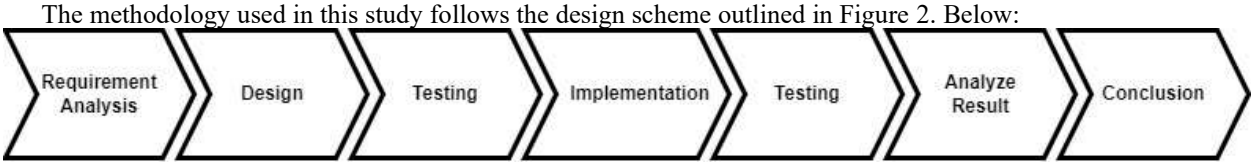

Fig. 2 Methodology

Requirement Analysis

The analysis will be carried out through several stages:

- Conducting direct observation in order to gain more in-depth understanding about the needs.
- Understand all the conditions of needs in the field related to the needs of vulnerability assessment
- Analyzing the results of observation

Design

Design process is done through several stages, which are:

- Selection of web server as testing target.
- Selection of tools for vulnerability scanning.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 1, January 2023
https://doi.org/ 10.47709/cnahpc.v5i1.1991

Submitted : January 12, 2023
Accepted : January 19, 2023
Published : January 19, 2023

Testing

Carry out the process of identifying and evaluating security weaknesses in the system by utilizing selected tools specifically designed for vulnerability assessment to perform a thorough scan

Implementation

To run Nmap and WPScan, the following implementation steps are required.

- **Installation and Configuration of Linux**
  The installation of Kali Linux is performed on a virtual machine (VM) on the local system. Kali Linux is chosen because it is one of the most popular Linux distros in the cyber security world. The server is installed with the following specifications:
  Processor : 4 cores
  RAM : 16 GB
  Hard Disk : 100GB

- **Installation of Nmap**
  After Kali Linux is installed, the next step is to perform the installation of Nmap which is available on the Kali Linux repository. After the installation is completed, the Nmap service must be manually initiated by executing commands through the terminal.

- **Installation of WPScan**
  The next step is to perform the installation of WPScan which is available on Github. The installation begins with installing git which is available on the Kali Linux repository. After git installation is completed, the next step is to perform a git clone for WPScan and then proceed with installing bundler. WPScan must be manually initiated by executing commands through the terminal.

Analyze Result

Analyzing the results obtained from running Nmap and WPScan involves reviewing and interpreting the data generated by the tools during the vulnerability scan. This process includes identifying and evaluating security weaknesses present in the target system, as well as identifying potential vulnerabilities.

Conclusion

The next step is to draw conclusions about the security posture of the target system based on the findings, where it includes summarizing the vulnerabilities that have been discovered and their potential impact on the system security. It is also important to make recommendations for remediation and mitigation of identified vulnerabilities and validate the findings to ensure the accuracy and reliability of the results. The analysis and interpretation of the result is key to understanding the security of the target system, and inform the decision to strengthen the security system

4. RESULT

Summary of Scan Results

In this subchapter, the results of the testing and analysis of vulnerability scans will be presented in general.

Nmap Findings

From the scan results using Nmap, 21257 open ports were found The number of open ports on a web server can have a significant impact on its security. When a server has many open ports, it increases the attack surface for an attacker and makes it more susceptible to various types of attacks.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 1, January 2023
https://doi.org/ 10.47709/cnahpc.v5i1.1991

Submitted : January 12, 2023
Accepted : January 19, 2023
Published : January 19, 2023

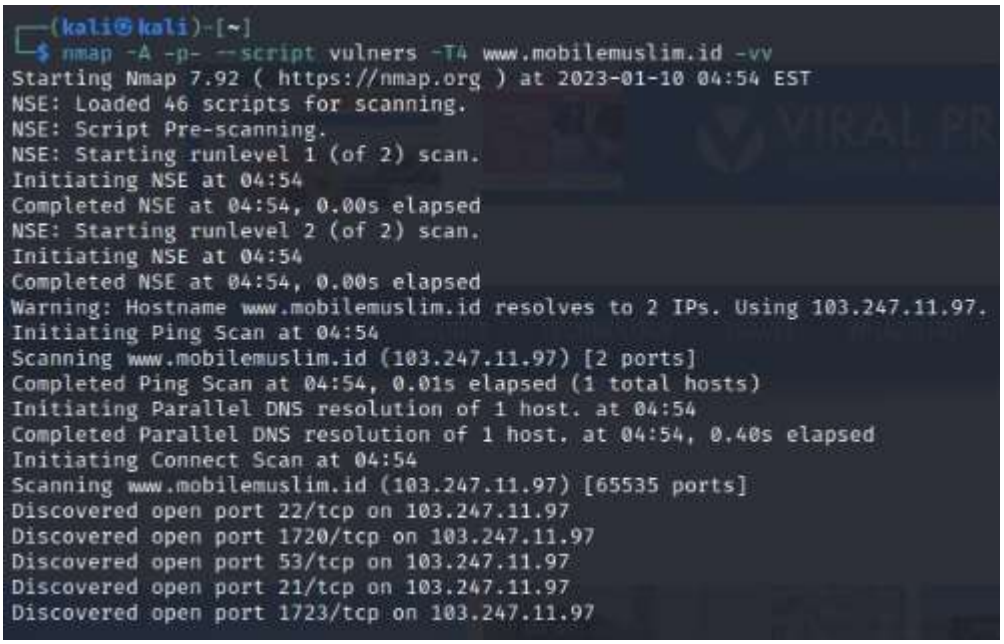

Fig. 3 Nmap Operations

WPScan Findings

From the scan results using WPScan, the following vulnerabilities were found:

- robots.txt found: This may not necessarily indicate a vulnerability, but having the robots.txt file publicly available could reveal information about the website's structure and potentially sensitive areas that should not be indexed by search engines.
- XML-RPC seems to be enabled: This feature can increase the attack surface for an attacker, as it allows remote communication with the website, including the ability to execute certain actions and potentially exploit vulnerabilities in the XML-RPC interface.
- WordPress readme found: This may not necessarily indicate a vulnerability, but it could reveal information about the version of WordPress being used, which could be used by an attacker to target known vulnerabilities in that specific version.
- Upload directory has listing enabled: This could allow an attacker to easily enumerate all files that have been uploaded to the website, potentially revealing sensitive information or allowing them to find and exploit vulnerabilities in those files.
- The external WP-Cron seems to be enabled: This feature allows scheduling tasks to be executed on the website, however, if it's not configured properly, it could be used by an attacker to perform malicious actions on the website.
- WordPress version 6.1.1 identified: Knowing the version of WordPress the website is running on can help an attacker to find and exploit vulnerabilities specific to that version. If a website is running an older version, it is possible that it is missing security updates and patches that were released for later versions.
- WordPress theme in use: This could potentially indicate that the website is using a theme with known vulnerabilities. Knowing the theme can help an attacker to find and exploit vulnerabilities specific to that theme.

It is important for a website administrator to address these vulnerabilities as soon as possible, by either disabling unnecessary features, configuring them properly or applying necessary patch updates. Keeping the WordPress, plugins and themes updated can significantly reduce the vulnerabilities.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 1, January 2023
https://doi.org/ 10.47709/cnahpc.v5i1.1991

Submitted : January 12, 2023
Accepted : January 19, 2023
Published : January 19, 2023

```
wpscan --url https://www.mobilemuslim.id -e
_______________________
        _       ___   __
        \ \        / /  _ \ / ___|
         \ \  /\  / /| |_) | (_     __  _ _ _ _ ®
          \ \/  \/ / |  _/ \__ \ / _|/ ` | ' \
           \  /\  /  | |     _) | (| (| | | | |
            \/  \/   ||    |_/ \_|\,|| ||

        WordPress Security Scanner by the WPScan Team
                       Version 3.8.22
      Sponsored by Automattic - https://automattic.com/
      @WPScan, @ethicalhack3r, @erwan_lr, @firefart
_______________________

[+] URL: https://www.mobilemuslim.id/ [103.247.11.97]
[+] Started: Tue Jan 10 04:44:22 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entry: server: Apache
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: https://www.mobilemuslim.id/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: https://www.mobilemuslim.id/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
```

Fig. 3 WPScan Operations

5. DISCUSSION

The results of the NMAP and WPScan tests reveal several vulnerabilities on the website. The NMAP test identified 21257 open ports, which can have a significant impact on the website's security. Having a large number of open ports increases the attack surface for an attacker and makes the server more vulnerable to various types of attacks. For example, an attacker could use an open port to access the server and execute malicious code, install malware, or steal sensitive information. Additionally, open ports can also be used to launch a Denial of Service (DoS) attack, which can overload the server and make it unavailable to legitimate users.

Another vulnerability is the older version of software run on open port that is known to have vulnerabilities. This can be easily exploited by attackers if it is not updated. The WPScan findings also revealed vulnerabilities related to features, configurations, and themes in the WordPress web application. These findings highlight the level of vulnerabilities present in the website's WordPress application and the need for remediation measures to be taken to address them.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 1, January 2023
https://doi.org/ 10.47709/cnahpc.v5i1.1991

Submitted : January 12, 2023
Accepted : January 19, 2023
Published : January 19, 2023

6. CONCLUSION

The conclusion of this test is that the website has vulnerabilities that were identified using NMAP and WPScan. The NMAP findings primarily pertain to open ports, while the WPScan findings pertain to configurations and features. The website administrator must take prompt action to address these vulnerabilities. On the network side, firewalls should be configured to block or limit access to open ports, and appropriate security measures such as intrusion detection systems and network segmentation should be implemented. In the WordPress application, disabling unnecessary features, configuring them correctly, and applying necessary patch updates are necessary. Additionally, regularly updating WordPress, plugins, and themes can significantly reduce vulnerabilities and improve the website's security posture..

7. REFERENCES

Borky, J. M., & Bradley, T. H. (2019). Protecting Information with Cybersecurity. In *Effective Model-Based Systems Engineering* (pp. 345–404). Springer International Publishing. https://doi.org/10.1007/978-3-319-95669-5_10

Burgess, C. (2015). The Definitive Guide to WordPress Maintenance. Retrieved December 20, 2022, from SitePoint website: https://www.sitepoint.com/definitive-guide-to-wordpress-maintenance/

ComputerHope. (2022). When was the first computer invented? Retrieved January 2, 2023, from ComputerHope website: https://www.computerhope.com/issues/ch000984.htm

Imperva. (2022). Vulnerability Assessment. Retrieved January 9, 2023, from Imperva website: https://www.imperva.com/learn/application-security/vulnerability-assessment/

ISACA. (2019). *State of Cybersecurity 2019 Part 1: Current Trends in Workforce Development*.

ITHEMES. (2023, January). WordPress Vulnerability Report – January 11, 2023. Retrieved January 19, 2023, from ITHEMES website: https://ithemes.com/blog/wordpress-vulnerability-report-january-11-2023/

Khurana, A. (2020). What is Web Application Development-A Beginner's Guide.

Malinova, A., Rahneva, O., & Golev, A. (2014). *Developing Business Web Applications* (H. Krushkov & N. Pavlo, Eds.). Retrieved from https://www.researchgate.net/publication/327285875

McNab, C. (2004). *Network Security Assessment: Know Your Network*. O'Reilly Media.

Moran, M. (2022). WordPress Hacking Statistics (How Many Websites Get Hacked?). Retrieved January 8, 2023, from Colorlib website: https://colorlib.com/wp/wordpress-hacking-statistics/

Sild, O. (2021). *Security vulnerabilities of WordPress ecosystem in 2020*.

Susanto, C. O. N., Rizko, K. N. F., & Purbohadi, D. (2020). Security Assessment Using Nessus Tool to Determine Security Gaps on the Repository Web Application in Educational Institutions. *Emerging Information Science and Technology*, *1*(2). https://doi.org/10.18196/eist.128

Tania, A. M., Setiyadi, D., & Khasanah, F. N. (2018). Keamanan Website Menggunakan Vulnerability Assessment. *INFORMATICS FOR EDUCATORS AND PROFESSIONALS*, *2*(2), 171–180.

W3Techs. (2023). Usage Statistics and Market Share of WordPress,. Retrieved January 5, 2023, from W3Techs website: 18/01/2023https://w3techs.com/technologies/details/cm-wordpress

Yik Ern, T., Yan Shaw, C., & Jun Hao, G. (2019). Game Management System. *ASIA PACIFIC UNIVERSITY OF TECHNOLOGY AND INNOVATION*.

Zen, B. P., Gultom, R. A. G., & Reksoprodjo, A. H. S. (2020). Security Assessment Analysis Using Penetration Testing Methods In Maintaining The Security Capability Of National Defense Information Technology. *Jurnal Teknologi Penginderaan*.

* Corresponding author