Journal of Information Systems and Informatics

Vol. 4, No. 4, December 2022 e-ISSN: 2656-4882 p-ISSN: 2656-5935

http://journal-isi.org/index.php/isi Published By DRPM-UBD

IT Support Website Security Evaluation Using Vulnerability Assessment Tools

Rio Armando[1], I G Ag Kom Agnam Melyantara [2], Rizma Elfariani[3], Desy Fitri Aulia Latuconsina[4], Muhammad Nasrullah[5]

[1, 2, 3, 4, 5] Program Studi Sistem Informasi, Institut Teknologi Telkom Surabaya, Surabaya, Indonesia
Email: [1]rioarmando@student.ittelkom-sby.ac.id, [2]agnam@student.ittelkom-sby.ac.id,
[3]rizmaelfariani@student.ittelkom-sby.ac.id, [4]desyaulia20@student.ittelkom-sby.ac.id,
[5]em.nashrul@gmail.com

Abstract

Vulnerability Assessment is one of the crucial stages that must be carried out to define and identify vulnerabilities in web systems so that they can be repaired and reduced. The XYZ institution is new, so the Vulnerability Assessment is to minimize attacks from irresponsible parties. In this study, a Vulnerability Assessment of the IT Support website was carried out on XYZ institution using the Nessus tool. This study used the Vulnerability Assessment Penetration Testing (VAPT) Life Cycle method, which has six stages: scope, planning, scanning & vulnerability Analysis, exploitation, Privilege Escalation, and Generating Report. The results of this study obtained various vulnerabilities ranging from Low to Critical on the IT Support website at XYZ institution so that the IT Support party at XYZ institution to update PHP versions, JQuery and several other preventive steps reviewed in the discussion section.

Keywords: Vulnerability Assessment, Website, VAPT Life Cycle.

1. INTRODUCTION

The rapid development of information technology has brought convenience to human life, one of which is websites [1]. This can be seen from the increasing number of website users for agency, educational, organizational, and personal purposes. The rapid growth of the web is due to several factors, including the development of infrastructure such as the internet, facilities for industrial workers to use the internet, and as an additional service to help them manage their business. Internet today is necessary in all aspects of their lives, for example, in a society that currently uses technology [2].

The development of websites in Indonesia has now developed very rapidly, which is due to the increase in internet service users from year to year. The website can also be easily accessed by many people who do not know where and when they are accessing it. With this kind of convenience, many organizations don't care whether the web server has met security standards and the system built is secure, or whether there is still interference [3]. Some websites that users frequent include search engines, e-commerce, social networks, forums, and news portals. However, despite the ease of service provided by these sites, it turns out that there are several security vulnerability issues, including cross-site scripting, information disclosure, authentication and authorization, session management, SQL injection, and CSRF [4]. The security of a website is one of the top priorities for an administrator or website user. Most users only focus on the design of the look and content that attracts as many visitors as possible. If a processor or user ignores the website's security, the user will be at a disadvantage because someone can retrieve essential data on the website or even spoil the appearance of the website [5], [15].

The increasing use of the web is a challenge for web developers to maintain security. This is because it does not rule out the possibility of hacking that can interfere [6]. A vulnerability in an IT system can be defined as a potential weakness of a system and, when exploited, can cause the system to come under attack [7]. These attacks have dangerous effects, such as theft and data leakage, the spreading of false information, system modifications, and system paralysis. To anticipate this, web developers need to conduct vulnerability assessments. The need for vulnerability assessment has been underestimated as it is only seen as a formal activity and is rarely carried out [9], [14]. Vulnerability assessment defines, identifies, classifies, and prioritizes vulnerabilities in web systems. Vulnerabilities in the network can be detected using specific tools or software. Vulnerability assessment methods can help detect vulnerabilities on the web. Developers and network administrators consider the assessment result to make preventive decisions and determine survivability when encountering an attack [8].

2. METHODS

The research method or phase used is the Vulnerability Assessment and Penetration Testing Lifecycle[1]. In the VAPT life cycle, as shown in Figure 1.

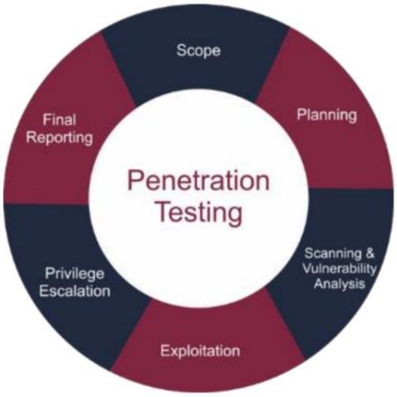


Figure 1. Penetration Testing

The explanation for the research stage is as follows:

1. Scope
   The first step is to establish the scope of the object of study. This study takes the IT support website of XYZ Institution as the object of research.
2. Planning
   The second stage is the planning phase, which is aimed at planning and collecting system information.
3. Scanning & Vulnerability Analysis
   The third stage is to use Nessus to find vulnerabilities on the IT Support website.
4. Exploitation
   The fourth stage is where exploits that can be exploited result from penetrating the target system.
5. Privilege Escalation
   The fifth stage is a standard method for attackers to gain unauthorized access to the system within certain limits.
6. Final Reporting
   The sixth stage is the final report stage which contains vulnerabilities on the IT Support website and their impacts and provides recommendations to fix vulnerabilities on the IT Support website.

3. RESULTS AND DISCUSSION

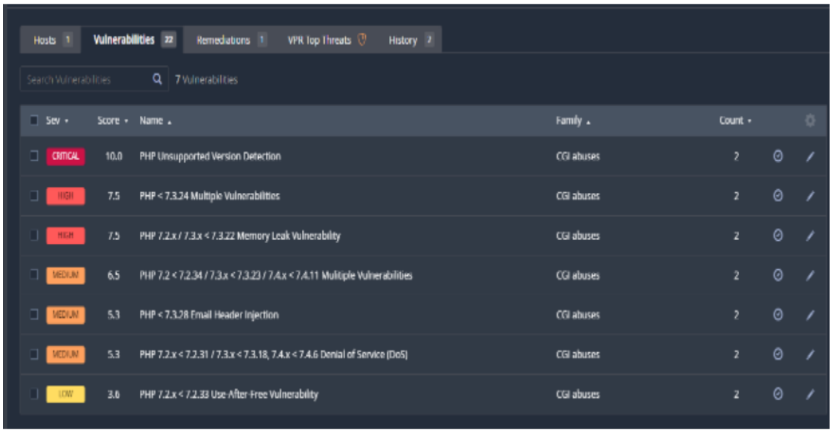
3.1 Nessus

Figure 2. Nessus

The tool used is Nessus. Nessus works by examining a set target, such as a set of hosts, or it could be a host in a particular focus. After completing the scan activity, it can view the resulting information in graphs or lines. The graphical interface for Nessus is built using the Gimp Toolkit (GTK). GTK is a free library widely used to build graphical interfaces under X. Computer security administrators choose Nessus because the distribution of these applications is always up to date (continually updated), the interface is web-based, easy to operate and free.[10]

3.2 Vulnerability Scanning

Vulnerability Scanning is carried out vulnerability scanning of IT Support websites at XYZ Institutions using the Nessus tool. The results of the vulnerability scan are shown in Figure 3.



Sev	Score	Name	Family	Count
CRITICAL	10.0	PHP Unsupported Version Detection	CGI abuses	2
HIGH	7.5	PHP < 7.3.24 Multiple Vulnerabilities	CGI abuses	2
HIGH	7.5	PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability	CGI abuses	2
MEDIUM	6.5	PHP 7.2 < 7.2.34 / 7.3.x < 7.3.23 / 7.4.x < 7.4.11 Multiple Vulnerabilities	CGI abuses	2
MEDIUM	5.3	PHP < 7.3.28 Email Header Injection	CGI abuses	2
MEDIUM	5.3	PHP 7.2.x < 7.2.31 / 7.3.x < 7.3.18, 7.4.x < 7.4.6 Denial of Service (DoS)	CGI abuses	2
LOW	3.6	PHP 7.2.x < 7.2.33 Use-After-Free Vulnerability	CGI abuses	2

Figure 3. Scan Results

Figure 3 shows a vulnerability scan conducted on the IT Support website at the XYZ Institution. The following are the types of vulnerabilities found in Table 1.

Table 1. Vulnerability Type

No	Vulnerability	Score	Category
1.	Unsupported PHP Versions	10.0	Critical
2.	PHP 7.3.x < 7.3.24 has Some Vulnerabilities	7.5	Hight
3.	PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability	7.5	Hight
4.	JQuery 1.2 < 3.5.0 Multiple XSS	6.5	Middle
5.	Web Applications Vulnerable to Clickjacking	5.3	Middle
6.	WordPress User Enumeration	5.3	Middle
7.	Web Server Enables Password Auto-Completion	3.6	Low

The list of vulnerabilities in the table has a different impact for each. Vulnerabilities can be described as follows:

1. **Unsupported PHP**
   Php installation on the remote host is no longer supported, and there are no new security patches for products to be released by the vendor. As a result, it is likely to contain security vulnerabilities.

2. **PHP 7.3.x < 7.3.24 has Some Vulnerabilities**
   According to the self-reported version number, the version of PHP running on the remote web server is 7.3. before 7.3.24 or 7.4.x before 7.4.12. Therefore, it is affected by some vulnerabilities.
3. **PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability**
   The version of PHP running on the remote web server is 7.2.x or 7.3.x prior to 7.3.21. Therefore, this is affected by a memory leak vulnerability in the LDAP component. An unauthenticated, remote attacker can exploit this issue to cause a denial-of-service condition.
4. **JQuery 1.2 < 3.5.0 Multiple XSS**
   The version of jQuery that is hosted on a remote web server is greater than or equal to 1.2 and before 3.5.0
5. **Web Applications Vulnerable to Clickjacking**
   The remote web server does not send X-Frame-Options response headers or content security policy response headers in all content responses. This could potentially expose the site to clickjacking attacks or UI fixes.
6. **Wordpress User Enemuration**
   WordPress versions hosted on remote web servers are affected by user enumeration vulnerabilities. Unauthenticated, remote attackers can use this to learn valid WordPress usernames. This information can be used to mount further attacks.
7. **Web Server Enables Password Auto-Completion**
   The remote web server contains at least one HTML from a field with the input of type 'password' where 'autocomplete' is not set to 'off'.

3.3 Reporting

Reporting is a preliminary to final report as a suggestion for website improvement steps. After the identification process, several vulnerabilities were found on the website, namely critical, high, medium, and low, and of course, each vulnerability has a different solution. Therefore, the stage of making the report will provide recommendations for solutions in the form of reports in Table 2 [6].

Table 2. Reporting Vulnerability Assessment [11]

No	Vulnerability	Solution
1.	PHP Unsupported Version	Upgrade to a currently supported PHP version
2.	PHP 7.3. x < 7.3.24 Multiple Vulnerabilities	Upgrade to PHP version 7.3.24 or later
3.	PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability	Upgrade to PHP version 7.3.22 or later

No	Vulnerability	Solution
4.	JQuery 1.2 < 3.5.0 Multiple XSS	Upgrade to JQuery version 3.5.0 or later
5.	Web Application Vulnerable to Clickjacking	Return the HTTP header X-FrameOptions or Content-SecurityPolicy (with the 'frame-ancestors' directive) with the page response. This prevents page content from being rendered by other sites when using frame HTML tags or iframes
6.	WordPress User Enumeration	Block requests to sensitive user information on the server using .htaccess or WAF files blocks all requests made to '/wp-JSON/wp/v2/users/' and the 'author' parameter (via GET and POST requests)
7.	Web Server Enables Password Auto-Completion	Add the 'autocomplete=off' attribute to this field to prevent the browser from storing credentials in the cache

3.4 Percentage Vulnerability Scanning

This percentage is obtained from the number of vulnerabilities found when conducting a vulnerability scan using Nessus, and this percentage is to make it easier to find the level of vulnerability on the IT support website XYZ so that the percentage of vulnerability scan can be used as material for website security assessment. The percentage of vulnerability is shown in Figure 4 [1].

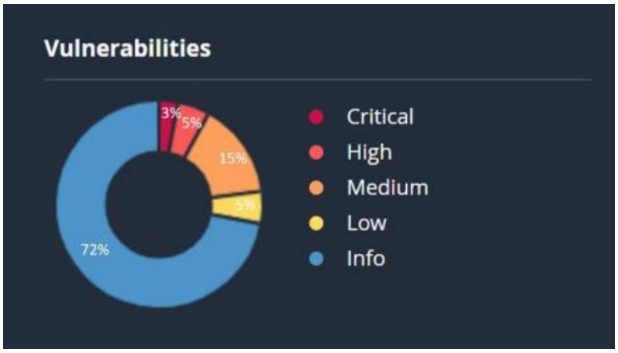


Figure 4. Percentage of Vulnerability Scanning

Figure 4 illustrates that the percentage of vulnerability scans comes from the number of vulnerabilities found. However, there is only one critical vulnerability, an unsupported PHP version. This is evidenced by the very high level of vulnerability demonstrated by unsupported PHP versions based on confidentiality, integrity, availability, and the following calculations:

1. Vulnerability in PHP Unsupported Version can be seen from Attack Vector (AV), Attack Complexity (AC), Privilege Required (PR), User Interaction (UI), Confidentiality (C), Integrity (I), and Availability (A) [1].
2. There are eight assessment aspects: Attack Vector: Privileges Required, Attack Complexity: Low, Privileges Required: None, User Interaction: None, Scope: Changed, Confidentiality: High, Integrity: High, and Availability: High. The following is a table of assessment aspects shown by Metric Values in Table 3 [1].

Table 3. Metric Values [12]

Metric k	Metric Values	Number Value
Attack Vector	Privileges Required	0,85
Attack Complexity	Low	0,77
Privileges Required	None	0,85
User Interaction	None	0,85
Scope	Changed	6,42
Confidentiality	High	0,56
Integrity	High	0,56
Availability	High	0,56

1. Calculating Exploitability with formulas:
   8,22 × AV × AC × PR × UI get results 8,22 × 0,85 × 0,77 × 0,85 × 0,85 = 3,887042775.

2. Calculating Impact Sub with the formula:
   1 - [(1 - Confidentiality) × (1-Integrity) × (1-Availability)] get results 1-(1-0,56) × (1-0,56) × (1-0,56) = 0,914816.

3. Calculate the Impact Scope with formulas:
   6.42 × ISS get results 6,42×0,914816 = 6,04773049.

4. Calculate Base score with the formula:
   Minimum [1.08 x (Impact Scope + Exploitability), 10]) get results Minimum (6,04773049 + 3,887042775) = 10,7295551262, 10.

Based on the above calculations, the overall risk level on the site falls into the "High" category, with the highest threat level score represented by a critical vulnerability, which is 10. Therefore, this value is used as a reference for the overall risk, so it can be concluded that the XYZ Institutional IT Support website is very vulnerable because it has a severe impact through its vulnerability that affects confidentiality, integrity, and availability [1], [13], [16].

4. CONCLUSION

The XYZ Institutional IT Support website has several vulnerabilities; namely, 3% of vulnerabilities are critical, 5% are high, 15% are medium, and 5% are low. PHP Unsupported Version, JQuery, ClickJacking, User Enumeration and Password Auto-Completion vulnerabilities. To reduce these vulnerabilities, website managers can take preventive steps by updating the PHP version, updating JQuery, returning the X-Frame Options HTTP header function, blocking requests for sensitive user information, and disabling the AutoComplete Password feature.

REFERENCES

[1] A. Budiman, S. Ahdan and M. Aziz, "Analisis Celah Keamanan Aplikasi Web E-Learning Universitas ABC Dengan Vulnerability Assesement," Jurnal Ilmu Komputer Unila, 2021.

[2] Priatno and N. P. Ramadhani, "Sistem Informasi Peminjaman Pada Koperasi Kredit Sejahtera Cibinong," Jurnal Esensi Infokom, vol. 2, no. 2, pp. 54-60, 2018.

[3] Guntoro, L. Costaner and Musfawati, "Analisis Keamanan Web Server Open Journal System (OJS) Menggunakan Metode ISSAF Dan OWASP (Studi Kasus OJS Universitas Lancang Kuning)," JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika), Vols. Volume 05, Nomor 01,, 2020.

[4] L. M. Gultom, "Analisis Celah Keamanan Website Instansi Pemerintahan Di Sumatera Utara," Jurnal Teknovasi, 2017.

[5] Y. Mulyanto, E. Haryanti and Jumirah, "Analisis Keamanan Websitesman 1 Sumbawa Menggunakan Metode Vulnerability Asesement," JINTEKS (Jurnal Informatika Teknologi dan Sains), p. Vol. 3 No. 3, 2021.

[6] I. Riadi, A. Yudhana and Y. W, "Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment," Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), vol. 7, no. 4, pp. 853-860, 2020.

[7] N. R., " Analisa Keamanan Internet Menggunakan Nessus Dan Ethereal Universitas Putra Indonesia "YPTK" Padang," J. Teknol. Inf. dan Pendidik., vol. 10, no. 3, pp. 11–25,, 2017.

[8] M. Orisa and M. Ardita, "Vulnerability Assesment Untuk Meningkatkan Kualitas Keamanan Web," Jurnal MNEMONIC, vol. 4, no. 1, pp. 16-19, 2021.

[9] A. Zirwan, "Pengujian dan Analisis Keamanan Website Menggunakan Acunetix Vulnerability Scanner," Jurnal Informasi & Teknologi, vol. 4, 2022.

[10] D. Juardi, "Kajian Vulnerability Keamanan Jaringan Internet Menggunakan Nessus," SYNTAX Jurnal Informatika, 2017.

[11] © 2022 Tenable®, Inc., "Tenable," [Online]. Available: https://www.tenable.com/plugins/was/112657.

[12] Forum of Incident Response and Security Teams, "Common Vulnerability Scoring System v3.1: Specification Document," [Online]. Available: https://www.first.org/cvss/v3.1/specification-document.

[13] M. Nasrullah, S. Suryawan, N. Istyanto, and T. Kristanto, "Risk Priority Analysis for Change Management on E-Government using RIPC4 and AHP", journalisi, vol. 4, no. 1, pp. 16-29, Mar. 2022.

[14] M. Nasrullah, N. D. Angresti, S. H. Suryawan, and Faizal Mahananto, "Requirement Engineering terhadap Virtual Team pada Proyek Software Engineering", JAIIT, vol. 3, no. 1, pp. 1–10, May 2021.

[15] T. Kristanto, M. Sholik, D. Rahmawati, and Muhammad Nasrullah, "Analisis Manajemen Keamanan Informasi Menggunakan Standard ISO 27001: 2005 Pada Staff IT Support Di Instansi XYZ", JISA (Jurnal Informatika dan Sains), vol. 2, no. 2, pp. 30-33, December 2019.

[16] T. Kristanto, W. Maulana Hadiansyah and M. Nasrullah, "Analysis of Higher Education Performance Measurement Using Academic Scorecard and Analytical Hierarchy Process," 2020 Fifth International Conference on Informatics and Computing (ICIC), 2020, pp. 1-6, doi: 10.1109/ICIC50835.2020.9288628.