JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 8, No. 2, Juni 2023, Pp. 647-655

WEBSITE SECURITY TEST AT THE UNIVERSITY OF MATARAM USING VULNERABILITY ASSESSMENT

Muh Adha*[1)], Zitnaa Dhiaaul KWA[2)], Alva Hendi Muhammad[3)]
1. Magister Teknik Informatika, Universitas Amikom Yogyakarta, Indonesia
2. Magister Teknik Informatika, Universitas Amikom Yogyakarta, Indonesia
3. Magister Teknik Informatika, Universitas Amikom Yogyakarta, Indonesia

Article Info
Kata Kunci: Website, Vulnerability, Hosted Scan

Keywords: Website, Vulnerability, Hosted Scan

Article history:
Received 27 January 2023
Revised 3 February 2023
Accepted 1 March 2023
Available online 1 June 2023

DOI :
https://doi.org/10.29100/jipi.v8i2.3830

* Corresponding author.
Corresponding Author
E-mail address:
muh.adha0@students.amikom.ac.id

ABSTRAK
Perkembangan internet dan teknologi telah memberikan dampak yang besar terhadap berbagai kebutuhan manusia. Menurut data dari Internet Live Stats ada lebih dari 5 miliar pengguna internet saat ini. Dengan banyaknya pengguna internet dan website, maka akan semakin banyak juga pihak yang menyalahgunakan internet dan website dalam tindak pidana. Sebuah website membutuhkan tingkat keamanan yang tinggi untuk mencegah penipuan dan manipulasi yang dil-akukan oleh pihak yang tidak bertanggung jawab. Dalam melindungi informasi yang terdapat pada website, kerentanan website menjadi perhatian penting agar tidak mudah dieksploitasi. Langkah-langkah yang dapat dilakukan adalah dengan memulai dengan menerapkan metode penetration testing untuk mengetahui kerentanan pada website yang dijadi-kan objek penelitian oleh penulis sehingga hasil dari proses pengujian dapat menjadi gambaran kondisi dan kerentanan apa saja yang ada. pada situs web target atau objek situs web. Pada penelitian ini website yang menjadi sasaran adalah unram.ac.id milik Universitas Mataram yang digunakan untuk operasional perusahaan dengan menggunakan beberapa tools pengujian yaitu Hosted Scan dalam pencarian ulang dan pengujian keamanan website sebelumnya. Pada penelitian ini ditemukan beberapa kerentanan pada level tinggi, sedang, dan rendah pada website target, sehingga dilakukan pen-gujian dan perbaikan pada website sehingga dapat meningkatkan keamanan layanan website yang akan digunakan untuk perusahaan. operasi.

ABSTRACT
The development of the internet and technology has had a big impact on various human needs. According to data from Internet Live Stats there are more than 5 billion internet users at the moment. With a large number of internet and website users, there will also be an increasing number of parties who abuse the internet and web-sites in criminal acts. A website requires a high level of security to prevent fraud and manipulation caused by irresponsible parties. In protecting the in-formation contained on the website, website vulnerabilities are an important concern so that they are not easy to exploit. The steps that can be taken are to start by applying the penetration testing method to know the vulnerabilities on websites that are used as research objects by the author so that the results of the testing process can be an overview of what condi-tions and vulnerabilities exist on the tar-get website or website object. In this study, the website that was targeted was un-ram.ac.id owned by University of Mataram which was used for the company's operations using several testing tools, name-ly Hosted Scan in re-searching and testing the security of the previous website. It was found in this study that there were several vunerabilities at high, medium, and low levels on the target website, so testing and repairs were carried out on the website so that it could increase the security of website services that will be used for company operations

I. PENDAHULUAN

The development of the internet and online services is a necessity that is inherent in everyday life carried out by humans today [1]. According to data from internet live stats [2], at this time internet users have reached more than 5 billion users. With so many internet users and online services, this can encourage the opening

of cybercrime as a medium for attacks. Thus, the security aspect becomes an important component in web application development to minimize the level of risk that can occur in a web application such as theft, manipulation, or loss of data [3].

In one of the sources written by other researchers, it has been said that there is no website application without the risk of vulnerability to cyber attacks. Along with the development of the times, currently, the website is a medium of information and communication that is used by many companies to support business operations [4]. Therefore, the information available on the website needs to be safeguarded comprehensively so that it cannot result in integrity violations or data theft [5]. Knowing the security vulnerability gaps can be done by utilizing the penetration testing method which is part of the system testing process with the hope of knowing the available security holes [6].

One method is part of penetration testing, namely information gathering, where information gathering is the first step carried out at the penetration testing stage to find out information about the target website being tested [61232-1057-162953-1-10-20200728] [4]. Meanwhile, the next step is a vulnerability assessment which is a method for scanning loopholes on websites, to find out the vulnerabilities that exist on the website by carrying out vulnerability scanning which can be used to detect vulnerabilities such as SQL injection, cross-site scripting, and other vulnerabilities. In implementing vulnerability scanning, several tools are available that can be optimized in vulnerability scanning activities such as Acunetix, OWASP ZAP, Vega, and others. Furthermore, the steps that can be carried out are testing the vulnerability of the loopholes found in the scanning process, through exploitation to prove a test (penetration testing) [5].

In conducting this study, several references were taken from previous studies as a reference in conducting the research to be carried out. Previous researchers conducted by [6], in his research conducted testing for security holes on the scientific journal website of the University of Muhammadiyah Purwokerto using the OpenVAS and Acunetix WVS tools. The method used is applied research that focuses on the analysis of evaluation results so that it is expected to produce information that is used as input or to make certain decisions according to the urgency of the target. This study uses 3 core stages of the VA process, namely determining project boundaries, implementing VA, and analyzing VA results. VA was carried out using OpenVAS software and Acunetix WVS. The VA process on the UMP scientific journal website based on OJS version 2.4.8.0 went well and resulted in findings of weaknesses or vulnerabilities. OpenVAS found 9 data gaps, while Acunetix WVS found 166 data gaps.

Further research was carried out by [7], in his research conducted a security analysis on e-learning website applications at ABC University with VA. His research aims to detect vulnerabilities, describe vulnerabilities, assess vulnerabilities based on the Common Vulnerability Scoring System, and provide solutions. The research stages used are VA and Penetration Testing Life Cycle. Based on the results of the vulnerability scan, low vulnerability, moderate vulnerability, high vulnerability, and critical vulnerability were found. Each vulnerability certainly has a different vulnerability impact, but the critical vulnerability, namely Elasticsearch Transport Protocol Unspecified Remote Code Execution, has the most serious impact with a base score of 9.8.

Further research conducted by [8], in his research testing security on the OJS website with VA, his research aims to identify security holes in the open journal system (OJS) website. This research uses the open web application security project (OWASP). The tests that have been carried out have successfully identified 70 high vulnerabilities, 1929 medium, and 4050 low in OJS. The total vulnerability value in OJS that was tested was 6049. The results of the tests carried out showed that OJS version 2.4.7 has many vulnerabilities, not recommended to use. Use the latest version issued by the OJS Public Knowledge Project (PKP).

Next, similar research was conducted by [9]. In his study of analyzing security gaps on websites using VA, the purpose of this study was to find gaps in vulnerabilities and risks on a website and to raise awareness about the importance of information security. In conducting a security evaluation applied the Vulnerability Assessment method to identify website assets and then analyze the vulnerabilities found. Based on website security testing using the Vulnerability Assessment method, it can be concluded that after carrying out a series of tests, two tests have an unsafe status including XML-RPC and Port 80 Service HTTP (Hyper Text Transfer Protocols). The existence of these vulnerabilities can threaten website security if repairs are not carried out, because the researchers have recommended repair solutions.

Subsequent research by [10]. In his research, the aim was to test and analyze the extent to which the security of the ITP website and provide troubleshooting suggestions from the results of the analysis. Testing was carried out using the Acunetix Vulnerability Scanner tool. The method used is analysis descriptive, namely, the data obtained served in the form of sentences that are described, thus providing clarity of the results of the analysis carried out. From the data obtained, the ITP website is at threat level 3 which includes category high. In this study, there were 714 alerts or gaps found consisting of 94 at the high level, 25 at the medium level, 46 at the low level, and 549 at the informational level. Based on the analysis, repairs and tests carried out in this study on the ITP website, the

threat level is already at level 1, which can be concluded that the ITP website is classified as safe from security holes.

A recent similar study was conducted by [11].In his research, vulnerability assessment can identify various kinds of gaps that allow the entry of attacks. This method can help certain parties to take precautions against attacks or damage caused by cybercrime. Network mapping, also known as Nmap, can help webmasters to carry out vulnerability assessments. This study uses Kali Linux OS to run Nmap. The tested target host supports POST, OPTIONS, GET, and HEAD methods. The results of the VA test with Nmap also show that the target is detected as an HTTP open proxy. The targets which tested not detected cross-site scripting. And the target host is also not detected by SQL injection.

Some of the previous studies summarized above have the same characteristics and must be basis for conducting this research. In this study, the authors will conduct security testing on the website owned by University of Mataram by analyzing the features and data structures available in the application. Available data such as goods transactions and financial data to support operational processes in the company [12]. The categories of some of the data are confidential, and may not be disseminated. So, the website needs to be tested for vulnerabilities to avoid data manipulation or theft from parties who do not have rights and responsibilities on the website. This website has never been tested for security holes. Therefore, the authors conducted research on the website which aims to find out the weaknesses and security gaps of the website from possible attacks so that the weaknesses found can be corrected so that website services are getting better and as a form of preventive action against data theft.

II. METHOD

The Open Vulnerability Assessment System (OpenVAS) and Owasp ZAP Vulnerability Scanner are software used for vulnerability assessments. OpenVAS is one of the software that has the ability to perform comprehensive scanning in handling system vulnerabilities against disturbances that often or have occurred based on signatures or anomalies (statistics). Owasp ZAP is an automated web application security testing tool that can audit web applications by checking for vulnerabilities such as SQL Injection, cross site scripting and other vulnerability.

The research methodology identifies all the stages used in making a work structure or commonly known as a framework. The framework is used to make the stages that will be completed in the research so that these stages affect each stage in achieving the research objectives [13]. The purpose of this study is to analyze the vulnerabilities found on the University of Mataram website using the Hosted Scan Vulnerability Scanner tool. HostedScan is one of the most successful programs on the market for detecting SQL injection and XSS vulnerabilities [14]. The data that has been obtained will be examined for security vulnerabilities that are found one by one based on the type of security vulnerabilities. Grouping the types of security holes make it easy to analyze. This information is used as the basis for knowing what causes it and providing solutions to this security gap problem.

The research method used in this research is the Vulnerability Assessment (VA) method, this method is divided into four stages [15]. The research method or stages used are the Vulnerability Assessment and Penetration Testing Life Cycle (VAPT-LC), which is the part that explains the main phases in the VAPT [16] [17]. In the VAPT Life Cycle there are six stages which can be seen in Figure 1 below :

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 8, No. 2, Juni 2023, Pp. 647-655

Figure 1: Stages of the VA Method

Based on the picture above, it can be explained that the method has six stages. Identifyng Scope Stage, at this stage, the researcher determines the scope of the research to be studied, in this study the researcher uses the E-learning Web application at University of Mataram as the object of the research to be carried out [18]. Information Gathering stage, this stage is the stage that researchers use to gather information about the target system with the tools whois, dig, nslookup, NMAP .VA Scanning Stage, is a step that researchers use to look for vulnerabilities on the Mataram University Web by using the Nessus tool [19]. This VA Identification Activities is carried out using existing applications on the Kali Linux operating system. False Positive Analysis, this stage where the results of the scan, researchers will get a list of vulnerabilities from the Web. One of the main activities that must be carried out with the output being a false positive analysis is eliminating or ensuring that the vulnerabilities found are not false vulnerabilities. Vulnerability Exploitation, this stage is a stage that aims to penetrate the target system based on available exploits for identified vulnerabilities or publicly available exploits of known vulnerabilities that can be exploited. Generating report, this stage is the stage of making a report that contains vulnerabilities on the Web, along with their impacts, and provides recommendations for fixing vulnerabilities on the University of Mataram Web.

System analysis is carried out to obtain information from the system which aims to analyze system weaknesses. The steps involved in collecting information are using the CEH module [20]. Some of the variables implemented are :

a. Footprinting and Network Discover.
   This phase is to find the design structure of network security at the intended targets as a barometer of the methodology:
   - **Whois** : is a procedure for obtaining information about a domain, address, telephone number, email address, when this domain was registered and when this domain will expire.
   - **Nslookup** : is a useful tool to find out the IP of a domain. Besides that, it can also be useful for diagnosing network problems related to DNS.
   - **Scanning port** : is an application procedure designed to investigate server or host open ports. Applications are often used by administrators to verify network security.
   - **HttpRecon** : is a procedure for collecting information on a network, a web server, which is a hypertext transfer protocol.

b. Scanning Vulnerability

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 8, No. 2, Juni 2023, Pp. 647-655

The purpose of scanning vulnerabilities is to find security holes in the target including SQL Injection, Cross Site Scripting (XSS), Remote OS Command, Path Transversal, Private IP Disclosure. on an operating system or application.

c. Reporting

It is a report from the beginning to the end in the form of a document file as a recommendation for steps to prevent improvement in the system of both companies, educational institutions and organizations.

III. RESULT AND DISCUSSION

The stage of determining the boundaries of the research is necessary so that the VA is not too broad so that it involves things that are not necessary and not too narrow so that it misses important things. To determine system boundaries, 3 things need to be taken into consideration, namely understanding the business processes and systems to be tested, understanding system complexity, and determining time and costs.

Before carrying out the Vulnerability Assessment process, a device is prepared that has the following minimum specifications:

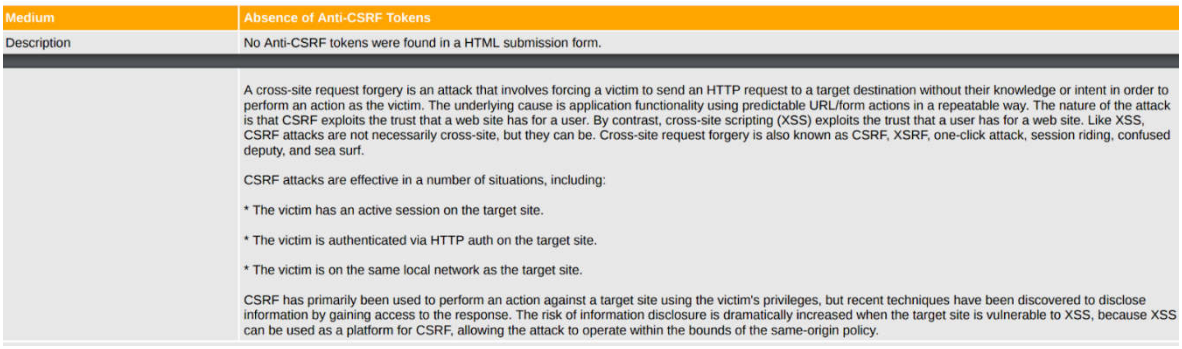
- Type: Linux
- Memory: 4GB RAM
- Hard Disk: 500GB

The next stage is the VA process using OpenVAS and ZAP. The scanning results get weak data on the University of Mataram website. The data on weaknesses obtained amounted to 14 data on weaknesses with details of 7 data being at the medium level and 7 data being at the low level, while at the high level there were no weaknesses as shown in table 1 below:

Table I: Scanning Results Using Owasp ZAP

Host	High	Medium	Low
Mataram University Website Server	0	4	7

Figure 2 shows one of the weaknesses at the medium level detected by the Owasp ZAP software, namely the Absence of Anti-CSRF Tokens.



Medium	Absence of Anti-CSRF Tokens
Description	No Anti-CSRF tokens were found in a HTML submission form.
	A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

Instances	102
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Figure 2: Weakness data sample at the Owasp ZAP medium level

Weaknesses at the low level also found several 7 data. Figure 3 shows one of the weaknesses at the low level detected by the Owasp ZAP software, namely the weak Cross-Domain JavaScript Source File Inclusion section.

Low	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	http://languagecenter.unram.ac.id/
Method	GET
Parameter	//platform.twitter.com/widgets.js
Attack	
Evidence	<script async src="//platform.twitter.com/widgets.js" charset="utf-8"></script>
URL	http://spi.unram.ac.id/
Method	GET
Parameter	http://maps.google.com/maps/api/js?libraries=geometry%2Cplaces%2Cweather%2Cpanoramio%2Cdrawing&language=en&ver=6.1.1
Attack	
Evidence	<script type='text/javascript' src='http://maps.google.com/maps/api/js?libraries=geometry%2Cplaces%2Cweather%2Cpanoramio%2Cdrawing&language=en&ver=6.1.1' id='wpgmp-google-api-js'></script>
Instances	104
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017

Figure 3: Weakness sample data at low-level Owasp ZAP

The second scanning process using OpenVAS produces weak data on the University of Mataram website. The weakness data found amounted to 2 weakness data with details 1 data is at the medium level and also 1 data is at a low level, while at the high level no weaknesses were found as in table 2 below.

Table II: Results of scanning using OpenVAS

Host	High	Medium	Low
Unram.ac.id	0	1	1

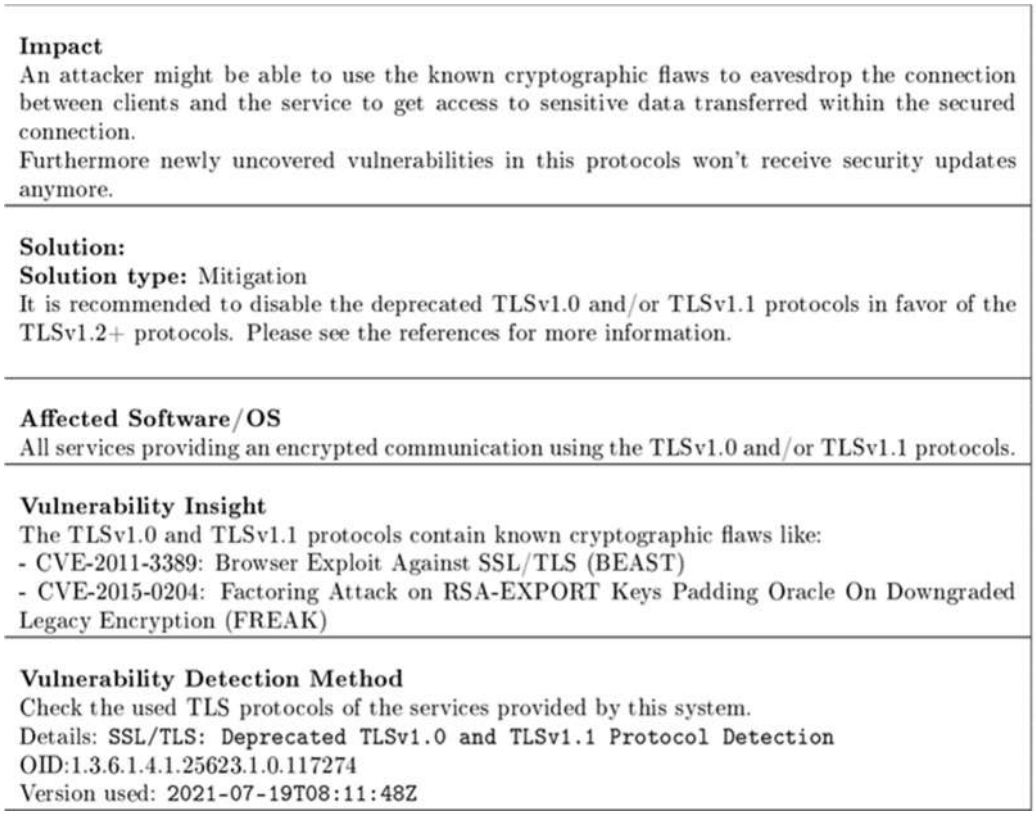
Weakness data generated from scanning using OpenVAS can be grouped into several warnings found, this is to make it easier to conclude which part has the most weaknesses and needs more attention for improvement. The weak data group is shown in table 3 below.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 8, No. 2, Juni 2023, Pp. 647-655

Table III: Data Group Weaknesses Scan Results Using OpenVAS

Alert Group	Severity	Alert Count
443/tcp	Medium	1
General/tcp	Low	1

From table 3 it can be concluded data weakness on the medium "443/tcp", means that an attacker might be able to use known cryptography to eavesdrop on connections between clients and services to gain access to sensitive data transferred in a secure connection. In addition, newly discovered vulnerabilities in this protocol will not receive security updates. Figure 4 shows one of the weak data at the medium level detected by OpenVAS, namely in the 443/tcp group.



Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2021-07-19T08:11:48Z`

Figure 4: Weakness data sample at the OpenVAS medium level

The scanning results between Owasp ZAP and OpenVAS shows a sizable difference. with the same scanning target, namely the University of Mataram website, firstly in terms of time if using Owasp ZAP is much shorter, which is approximately only 40 minutes, while using OpenVAS it takes 2 hours and 25 minutes. The results from the scanning report produced are also very different, OwaspZAP produces 14 detected data weaknesses, while OpenVAS found 2 data weaknesses. An overview of the comparison of scan results is shown in table 4 below:

Table IV: Comparison of Scanning Results

Software	Scan Time (minutes)	Results		
		High	Medium	Low
Owasp ZAP	40	0	7	7
Open VAS	145	0	1	1

In the table below, we will discuss comparisons with previous research where in this study the same Vulnerability Assessment method was used with different tools and objects. Comparison with previous research can be seen in

table 5 below :

Tabel V : Comparison of Previsious Research

	Comparison of Previous Research			
	Feri Wibowo (2019)		Muh Adha (2023)	
	Universitas Muhammadiyah Purwkerto		Universitas Mataram	
Tools	Open VAS	Acunetix WVS	Owasp ZAP	Open VAS
Waktu (menit)	60	954	40	145
Host	Server Website Jurnal	Server Website Jurnal	unram.ac.id	unram.ac.id
High	0	0	0	0
Medium	7	149	4	1
Low	2	17	7	1

IV. CONCLUSSION

Based on the results of the VA process on the Mataram University website running well and producing findings of weaknesses or vulnerabilities. Owasp ZAP found 14 data vulnerabilities, while OpenVAS found 2 data vulnerabilities. with a relatively long comparison of scanning time, namely, Owasp ZAP takes 40 minutes while OpenVAS takes 145 minutes. This weak data can be used as input for the University of Mataram information systems team to immediately close or fix existing security holes.

V. PUSTAKA

[1] M. M. P. Fredik Melkias Boiliu, "PERAN PENDIDIKAN AGAMA KRISTEN DI GEREJA TERHADAP PERBERDAYAAN EKONOMI EKONOMI KREATIF JEMAAT DI ERA DIGITAL," *Jurnal Pengabdian Tri Bhakti,* vol. 2, no. 2, pp. 118-132, Desember 2020.

[2] M. E. P. V. S. Gisela Hennita, "ANALISIS KOMUNIKASI PERSUASIF PADA AKUN INSTAGRAM FRELYSHOP DALAM MENINGKATKAN BRAND IMAGE," *Jurnal Ilmu Komunikasi,* vol. 3, no. 2, pp. 227-240, Agustus 2020.

[3] A. R. Fania Sofiyani, "PENENTUAN STRATEGI MITIGASI RISIKO KRITIS ASET IS/IT PERKARA BERDASARKAN ISO/IEC 27002:2013," *Journal of Information System,* vol. 4, no. 1, pp. 1-18, Mei 2019.

[4] G. M. A. S. D. M. S. A. I Gede Ary Suta Sanjaya, "EVALUASI KEAMANAN WEBSITE LEMBAGA X MELALUI PENETRATION TESTING MENGGUNAKAN FRAMEWORK ISSAF," *JURNAL ILMIAH MERPATI,* vol. 8, no. 2, pp. 113-124, Agustus 2020.

[5] H. A. P. W. Feri Wibowo, "UJI VULNERABILITY PADA WEBSITE JURNAL ILMIAH UNIVERSITAS MUHAMMADIYAH PURWOKERTO MENGGUNAKAN OPENVAS DAN ACUNETIX WVS," *JURNAL INFORMATIKA,* vol. 6, no. 2, pp. 212-218, SEPTEMBER 2019.

[6] H. A. P. W. Feri Wibowo, "Uji Vulnerability Pada website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix wvs," *JURNAL INFORMATIKA,* vol. 6, no. 2, pp. 212-218, September 2019.

[7] S. A. M. A. Arief Budiman, "ANALISIS CELAH KEAMANAN APLIKASI WEB E-LEARNING UNIVERSITAS ABC DENGAN VULNERABILITY ASSESMENT," *Jurnal Komputasi,* vol. 9, no. 2, pp. 1-10, 2021.

[8] A. Y. Y. Imam Riadi, "ANALISIS KEAMANAN WEBSITE OPEN JOURNAL SYSTEM MENGGUNAKAN METODE VULNERABILITY ASSESMENT," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK),* vol. 7, no. 4, pp. 853-860, Agustus 2020.

[9] D. S. F. N. K. Ari Marta Tania, "Keamanan Website Menggunakan Vulnerability Assesment," *INFORMATIC FOR EDUCATORS AND PROFESSIONALS,* vol. 2, no. 2, pp. 171-180, Juni 2018.

[10] A. Zirwan, "Pengujian dan Analisis Keamanan Website Menggunakan Acunetix Vulnerability Scanner," *Jurnal Informasi dan Teknologi,* vol. 4, no. 1, pp. 70-75, 2022.

[11] M. A. Mira Orisa, "VULNERABILITY ASSESMENT UNTUK MENINGKATKAN KUALITAS KEAMANAN WEB," *JURNAL MNEMONIC,* vol. 4, no. 1, pp. 16-19, Februari 2021.

[12] M. I. H. Syamgusti Ningsih, "ANALISIS FAKTOR-FAKTOR PENGHAMBAT MIGRASI SISTEM APLIKASI SOFI DALAM TRANSAKSI PEMBELIAN KREDIT DI KOPERASI KARYAWAN BETON MAKMUR," *JURNAL BISNIS MAHASISWA,* 21 Oktober 2021.

[13] S. K. A. P. W. Shahnilna F Bayastura, "ANALISIS DAN PERANCANGAN TATA KELOLA TEKNOLOGI MENGGUNAKAN FRAMEWORK COBIT 2019 PADA PT. XYZ," *JIKO (Jurnal Informatika dan Komputer),* vol. 4, no. 1, pp. 68-75, April 2021.

[14] M. Ula, "EVALUASI KINERJA SOFTWARE WEB PENETRATION TESTING," *TECHSI,* vol. 11, no. 3, Oktober 2019.

[15] R. L. Rahardian, "ANALISIS KEAMANAN WEB NEW KUTA GOLF MENGGUNAKAN METODE VULNERABILITY ASSESMENTS DAN PERHITUNGAN SECURITY METRIKS," *JURNAL INFORMATIKA DAN TEKNOLOGI KOMPUTER,* vol. 2, no. 3, pp. 256-265, November 2022.

[16] U. Y. K. S. H. M. F. Muhammad Rifki Oktova, "HARDENING CLOUDFRI DENGAN METODE SECURITY HARDENING PADA WEBSITE SAP.CLOUDFRI.ID," *E-Proceeding of Engineering,* vol. 8, no. 5, p. 9202, Oktober 2021.

[17] A. M. E. Marzuki Hasibuan, "Penetration Testing Sistem jaringan Komputer Menggunakan Kali Linux Untuk Mengetahui Kerentanan Keamanan Server Dengan Metode Black Box," *Jurnal Teknik Informatika,* 8 Desember 2022.

[18] H. B. S. I. W. W. P. Akmal Ilmi, "EVALUASI RISIKO CELAH KEAMANAN MENGGUNAKAN METODOLOGI OPEN-SOURCE SECURITY TESTING METHODOLOGY MANUAL (OSSTMM) PADA APLIKASI WEB TERBARU FAKULTAS ILMU KOMPUTER UPN VETERAN JAKARTA," *JURNAL INFORMATIKA,* vol. 18, no. 2, pp. 190-197, Agustus 2022.

[19] M. Aziz, "VULNERABILITY ASSESMENT UNTUK MENCARI CELAH KEAMANAN WEB APLIKASI E-LEARNING PADA UNIVERSITAS XYZ," *JECSIT,* vol. 1, no. 1, pp. 101-109, 2021.

[20] R. A. D. M. A. Sahren, "Penetration Testing Untuk Deteksi Vulnerability Sistem Informasi Kampus," *Prosiding Seminar Nasional Riset Information Science,* vol. 1, pp. 994-1001, September 2019.