Mitigation of Learning Management System Vulnerabilities using Penetration Testing Methods

Ridho Surya Kusuma[1], Rakhmat Prasetyo Agung Nugroho[2]
[1,2]Department of Informatic, Universitas Siber Muhammadiyah, Yogyakarta, Indonesia
Email: *ridhosuryakusuma@sibermu.ac.id

***Abstract*— This research delves into vulnerability testing of Learning Management Systems (LMS) using penetration methods, aiming to enhance the security resilience of LMS platforms against cyber threats. By employing a structured penetration testing framework encompassing stages such as reconnaissance, scanning, gaining access, maintaining access, and covering tracks, the study seeks to identify and address potential vulnerabilities within LMS systems. The research contributes to fortifying LMS platforms by simulating attacks and evaluating system weaknesses to provide insights for effective security enhancements.**

Keywords*— Vulnerability Testing, Penetration Methods, Learning Management Systems, Cybersecurity, Security Resilience.

I. INTRODUCTION

In the realm of cybersecurity, ensuring the robustness of systems is paramount to safeguard against potential threats. One of the key methodologies employed to assess the security posture of systems is penetration testing. Penetration testing, commonly referred to as pen-testing, is a proactive approach that simulates attacks on a system or network to identify vulnerabilities, misconfigurations, and security loopholes that malicious actors could exploit [1]. By conducting penetration testing, organizations can proactively identify weaknesses in their systems before they are exploited by real attackers [2].

Penetration testing is a crucial component of cybersecurity practices, aiming to evaluate the effectiveness of security measures implemented within a system [3]. It involves a systematic analysis of the system's defenses through simulated attacks to uncover vulnerabilities that could potentially be exploited [4]. This method is essential as it provides organizations with insights into their security posture, allowing them to address weaknesses before they are compromised by malicious entities [5].

Despite the importance of penetration testing, there is a need for comprehensive vulnerability testing methodologies tailored to specific systems, such as Learning Management Systems (LMS). LMS platforms, being critical for educational institutions, store vast amounts of sensitive data, making them prime targets for cyber threats. However, there is a lack of research focusing on vulnerability testing specifically designed for LMS using penetration methods.

The primary objective of this study is to conduct vulnerability testing of Learning Management Systems using penetration methods. By leveraging established penetration testing tools and methodologies, the research aims to identify and assess potential security vulnerabilities within LMS platforms. Through this research, insights will be gained into the effectiveness of penetration testing in enhancing the security posture of Learning Management Systems.

This research contributes to the existing body of knowledge by providing a focused investigation into vulnerability testing of Learning Management Systems using penetration methods. By applying penetration testing techniques to LMS platforms, this study seeks to enhance the understanding of how such systems can be fortified against cyber threats. The findings of this research are expected to offer valuable insights for educational institutions and cybersecurity professionals in securing Learning Management Systems effectively.

II. LITERATURE REVIEW

Numerous studies have explored penetration testing, a proactive method for evaluating system security by simulating attacks to identify vulnerabilities [6]. These investigations have underscored the importance of penetration testing in assessing cybersecurity readiness and resilience against potential threats [7]. Furthermore, research has highlighted the role of penetration testing in uncovering vulnerabilities such as poor system configurations, software flaws, and operational weaknesses that could compromise system security [8].

The theoretical foundation of this research is based on penetration testing, which involves conducting simulated attacks on a system to assess the effectiveness of its security measures [9]. Through methodologies like Black Box Testing, White Box Testing, and Gray Box Testing, penetration testing aims to identify and address security vulnerabilities within systems [10]. Additionally, frameworks like the Open Web Application Security Project (OWASP) method offer a structured approach to evaluating web-based application systems for security flaws [11]. This method includes a comprehensive list of the top 10 security vulnerabilities that could endanger the safety of web applications, aiding in the identification and mitigation of potential risks [11].

III. RESEARCH METHODOLOGY

The research methodology for this study will be based on a comprehensive penetration testing framework tailored to assess the security vulnerabilities of Learning Management Systems (LMS). The framework will encompass various stages designed to systematically evaluate the security posture of LMS platforms and identify potential weaknesses that could be exploited by malicious actors. By following a structured penetration testing framework, the research aims to provide a rigorous assessment of the security resilience of LMS against cyber threats. The following are the four main stages of penetration testing method implementation as shown in Figure 1.

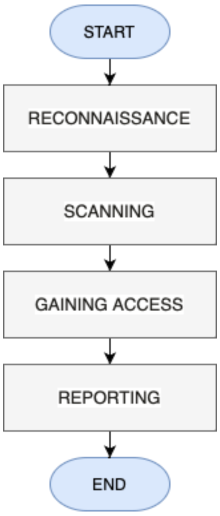


Fig. 1. Stages of Penetration Testing.

The following is a detailed explanation of the four stages:

- Reconnaissance Phase: The initial stage involves passive and active exploration to gather information about the target LMS system. This phase is crucial for understanding the system's architecture, components, and potential entry points for attacks Koroniotis et al. [12].
- Scanning Phase: In this stage, the researcher conducts active scanning of the LMS to identify open ports, services running, and potential vulnerabilities present in the system. Tools like Nmap and Nessus can be utilized for comprehensive scanning [13].
- Gaining Access*: Following the scanning phase, the researcher attempts to exploit identified vulnerabilities to gain unauthorized access to the LMS. This step involves using penetration testing tools to simulate attacks and assess the system's susceptibility to exploitation [13].
- Reporting Phase: this stage displays the overall results of the penetration check and documentation of any vulnerabilities found. These results can serve as a consideration for improvements and strengthen cybersecurity defences in the future.

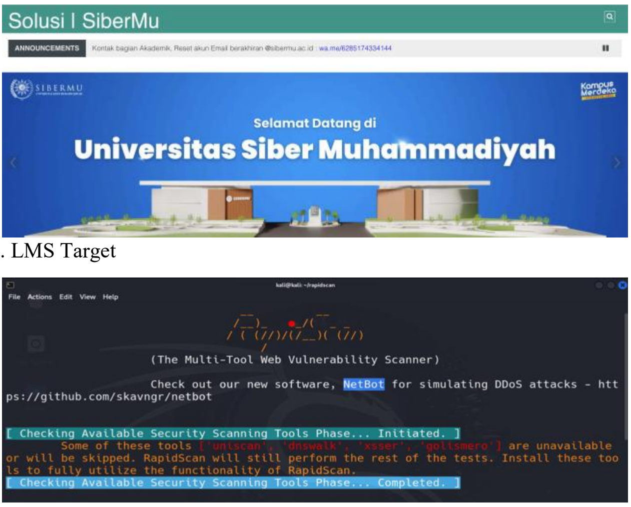
By following these structured stages of penetration testing within the context of Learning Management Systems, the research endeavors to provide valuable insights into the security vulnerabilities of LMS platforms and recommend mitigation strategies to enhance their resilience against potential cyber threats.

IV. RESULT

This section presents the results of the research consisting of the reconnaissance, scanning, gaining access and reporting stages in stages as follows.

A. Reconnaissance Phase

At this stage, the process of collecting initial information about the Learning Management System (LMS) being tested. The information includes domain name: solusi.sibermu.ac.id and penetration testing tool: Rapidscan. The following is a view of the LMS target and tools for the penetration testing process as shown in Figure 2.


Solusi I SiberMu
ANNOUNCEMENTS
Kontak bagian Akademik, Reset akun Email berakhiran @sibermu.ac.id : wa.me/6285174334144
SIBERMU
Kampus Merdeka
Selamat Datang di
Universitas Siber Muhammadiyah

a. LMS Target

```
kali@kali: ~/rapidscan
File  Actions  Edit  View  Help

                        (The Multi-Tool Web Vulnerability Scanner)

                        Check out our new software, NetBot for simulating DDoS attacks - htt
ps://github.com/skavngr/netbot

[ Checking Available Security Scanning Tools Phase... Initiated. ]
        Some of these tools ['uniscan', 'dnswalk', 'xsser', 'golismero'] are unavailable
or will be skipped. RapidScan will still perform the rest of the tests. Install these too
ls to fully utilize the functionality of RapidScan.
[ Checking Available Security Scanning Tools Phase... Completed. ]
```

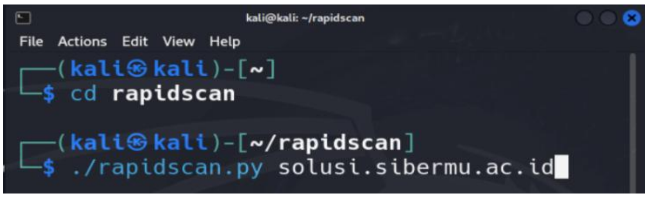
b. Rapidscan Tool

Fig. 2. a. The LMS Target and b. Rapidscan Tool

Figure 2 consists of part (a) showing the initial appearance of the LMS that will be the test target. Then, part (b) shows the vulnerability scanning process using the RapidScan tool. This tool is used to find weaknesses in the system that can be exploited by hackers to conduct cyber-attacks. The scan results will show whether the system is secure or still has security holes that need to be fixed. The purpose of this test is to ensure that the LMS is safe and protected from various cyber threats.

B. Scanning

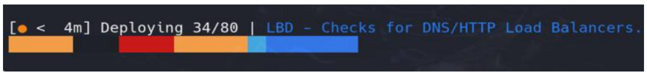
The scanning process is conducted to identify specific weaknesses in the LMS system. In this stage, various scanning tools such as XSSer, Uniscan, Wafw00f, SMB service over UDP, WHOis, Nikto, DMitry, Golismero SSL Scans, Harvester, SSLyze, DirB, Drupal Checker and port scanners to find exposed services, vulnerable ports, and out-of-date software. The following display commands run the rapidscan tool and the ongoing inspection process as shown in Figure 3.



```
kali@kali: ~/rapidscan
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ cd rapidscan

┌──(kali㉿kali)-[~/rapidscan]
└─$ ./rapidscan.py solusi.sibermu.ac.id
```

a. Command to Run The Rapidscan Tool



```
[● <  4m] Deploying 34/80 | LBD - Checks for DNS/HTTP Load Balancers.
```

b. Scanning Process

Fig. 3. a. Command to Run The Rapidscan Tool and b. Scanning Process

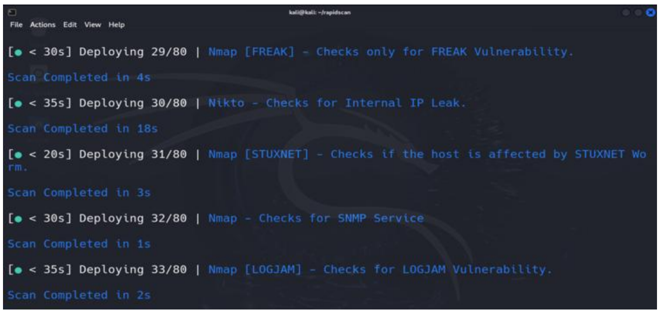
Figure 3 provides information about vulnerability scanning process which consists of Section (a): Displays the commands used to run the RapidScan tool. The command "./rapidscan.py solusi.sibermu.ac.id" instructs the tool to scan the targeted website.

Part (b): Shows the scanning process in progress. The progress bar shows the percentage of scan completion, and the text below it describes the type of check being performed, which is checking for the presence of Load Balancers (LBDs) for DNS and HTTP services.

Overall, this figure illustrates the first step in conducting a security assessment of a website. By running RapidScan, we can identify potential weaknesses or vulnerabilities on the website before they are exploited by irresponsible parties.

C. Gaining Access

Based on the results of the scan of the vulnerabilities found in the LMS system. This process aims to test for unauthorised access into the system. The techniques used can involve vulnerability exploitation, brute force, or the use of a discovered backdoor. This penguin measures the extent to which an attacker can access sensitive system data and resources as shown in Figure 4.



```
[● < 30s] Deploying 29/80 | Nmap [FREAK] - Checks only for FREAK Vulnerability.

Scan Completed in 4s

[● < 35s] Deploying 30/80 | Nikto - Checks for Internal IP Leak.

Scan Completed in 18s

[● < 20s] Deploying 31/80 | Nmap [STUXNET] - Checks if the host is affected by STUXNET Wo
rm.

Scan Completed in 3s

[● < 30s] Deploying 32/80 | Nmap - Checks for SNMP Service

Scan Completed in 1s

[● < 35s] Deploying 33/80 | Nmap [LOGJAM] - Checks for LOGJAM Vulnerability.

Scan Completed in 2s
```

Fig. 4. Penetration Testing Process until 80 steps

Figure 4 shows a brief overview of how the penetration testing process is automated using specialised tools. This process involves using various tools to check for vulnerabilities or security weaknesses in a system or network. In this image, we see some of the initial steps of testing performed using the Nmap and Nikto tools.

Nmap is used to perform different types of scans, such as checking for FREAK and STUXNET vulnerabilities, as well as the presence of SNMP services. While Nikto is used to check for internal IP leaks. Each step of the scan will take a different amount of time, as indicated by the number in square brackets at the beginning of each line.

D. Reporting

After completing the exploitation, the final step is to document all the findings from the testing process. This report includes all the vulnerabilities found, the means used to exploit the system, as well as recommended fixes to prevent similar attacks in the future. This report is very important as a reference for LMS managers to improve the security of their system as shown in Table 1.

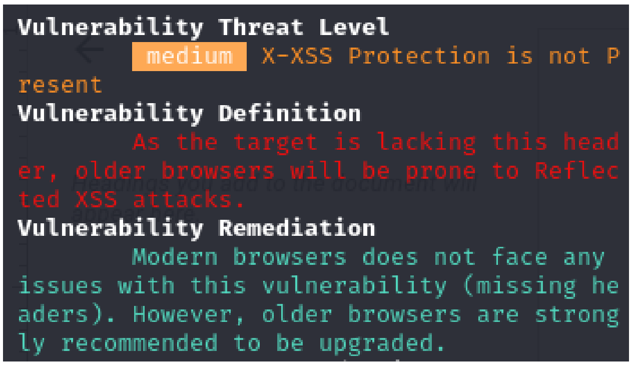
TABLE I. VULNERABILITY REPORT FOR LMS

No.	Vulnerability	
	Threat	***Level***
1.	X-XSS Protection is not Present	Medium
2.	Secure Client Initiated Renegotiation is supported	Medium
3.	SNMP Service Detected	Medium
4.	RDP Server Detected over UDP	High
5.	Found Subdomains with AMass	Medium
6.	Some vulnerable headers exposed	Medium
7.	Found Subdomains with Fierce.	Medium
8.	TCP Ports are Open	Low
9.	Some ports are open. Perform a full-scan manually	Low
10.	Open Directories Found with DirB	Medium

Table 1 summarises the results of the security scan, showing a number of weaknesses that need to be corrected immediately. No: Sequence number of the vulnerability finding; Vulnerability: A brief description of the type of vulnerability found; Threat: The level of threat posed by the vulnerability; Level: The severity of the vulnerability, usually measured on a scale of low, medium, or high.

Based on the Vulnerability analysis table:

1) X-XSS Protection is not Present: The LMS has no protection against Cross-Site Scripting (XSS) attacks as shown in Figure 5.



```
Vulnerability Threat Level
        medium   X-XSS Protection is not P
resent
Vulnerability Definition
        As the target is lacking this head
er, older browsers will be prone to Reflec
ted XSS attacks.
Vulnerability Remediation
        Modern browsers does not face any
issues with this vulnerability (missing he
aders). However, older browsers are strong
ly recommended to be upgraded.
```

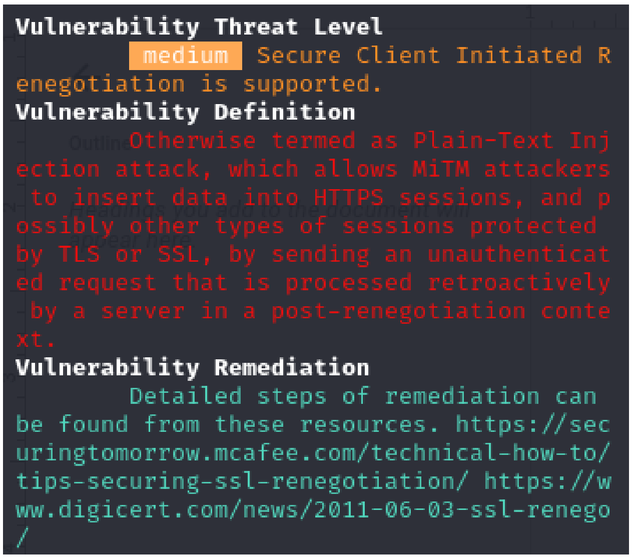
Fig. 5. Vulnerability: X-XSS Protection

Figure 5 describes a security vulnerability called Cross-Site Scripting (XSS) in an online learning system (LMS). This vulnerability occurs because the LMS does not have a protection feature against XSS attacks.

Hackers can infiltrate malicious code into LMS web pages. This malicious code can be used to steal users' personal data, such as passwords or other personal information. In addition, hackers can also redirect users to malicious websites. The risk of this vulnerability is moderate and mainly affects users using older versions of browsers. To resolve this issue, it is recommended to update the browser to the latest version.

The bottom line is that an LMS that does not have XSS protection is highly vulnerable to cyberattacks. Therefore, it is important for LMS managers to fix this vulnerability immediately to ensure the security of user data.

2) Secure Client Initiated Renegotiation is supported: Although it sounds positive, this feature can actually be exploited under some specific conditions to perform protocol downgrade attacks as in Figure 6.



```
Vulnerability Threat Level
        medium  Secure Client Initiated R
enegotiation is supported.
Vulnerability Definition
        Otherwise termed as Plain-Text Inj
ection attack, which allows MiTM attackers
 to insert data into HTTPS sessions, and p
ossibly other types of sessions protected
by TLS or SSL, by sending an unauthenticat
ed request that is processed retroactively
 by a server in a post-renegotiation conte
xt.
Vulnerability Remediation
        Detailed steps of remediation can
be found from these resources. https://sec
uringtomorrow.mcafee.com/technical-how-to/
tips-securing-ssl-renegotiation/ https://w
ww.digicert.com/news/2011-06-03-ssl-renego
/
```

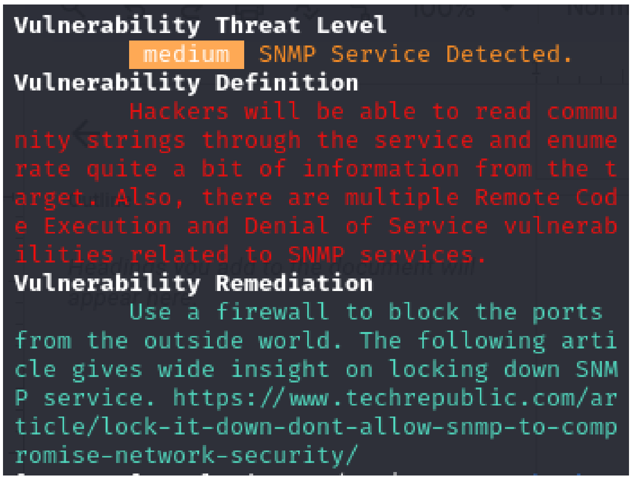
Fig. 6. Vulnerability: Secure Client

Figure 6 describes a security vulnerability called ‘Secure Client Initiated Renegotiation’. Although the name sounds safe, this feature can actually be utilised by hackers under certain conditions to perform protocol downgrade attacks.

The hackers can insert data into a supposedly secure HTTPS session, allowing them to ‘listen in’ on data traffic that should be encrypted. This attack is also referred to as a Plain-Text Injection attack. The threat level of this vulnerability is medium. To address this issue, there are several remediation steps that can be taken. The detailed steps can be found in the resources listed at the bottom of the image.

In essence, the Secure Client Initiated Renegotiation feature, which is supposed to increase security, can actually become a security hole if not configured properly. Therefore, it is important for system managers to understand the risks and implement appropriate remediation measures.

3) SNMP Service Detected: Simple Network Management Protocol (SNMP) is a protocol used to monitor and manage network devices. If not configured properly, the SNMP service can be exploited by hackers. They can read sensitive information from network devices, such as configuration, data traffic, and even execute malicious commands. The biggest risk of this vulnerability is the potential for remote attacks that could result in disruption of network services or even system takeover. SNMP service detected as in Figure 7.



```
Vulnerability Threat Level
        medium  SNMP Service Detected.
Vulnerability Definition
        Hackers will be able to read commu
nity strings through the service and enume
rate quite a bit of information from the t
arget. Also, there are multiple Remote Cod
e Execution and Denial of Service vulnerab
ilities related to SNMP services.
Vulnerability Remediation
        Use a firewall to block the ports
from the outside world. The following arti
cle gives wide insight on locking down SNM
P service. https://www.techrepublic.com/ar
ticle/lock-it-down-dont-allow-snmp-to-comp
romise-network-security/
```

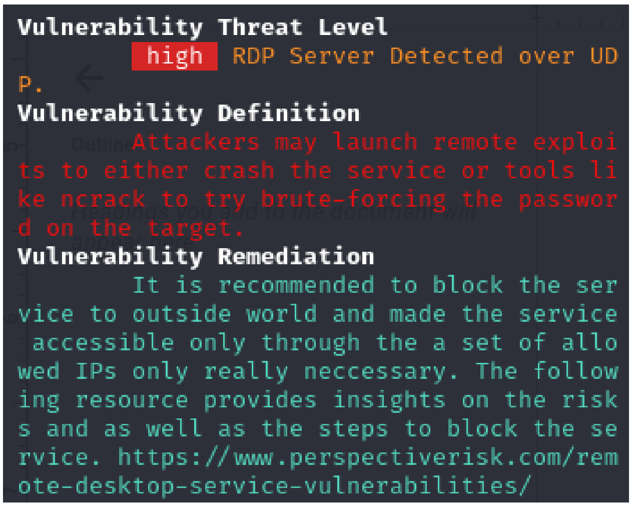
Fig. 7. Vulnerability: SNMP Service Detected

Figure 7 shows a security vulnerability in a system, namely the discovery of SNMP (Simple Network Management Protocol) services. This vulnerability is classified as moderate and has the potential to pose a considerable risk.

To address this issue, it is recommended to block access to SNMP ports from outside the network using a firewall. In addition, the SNMP configuration also needs to be tightened to limit access and the type of information that can be read. More information on how to secure SNMP services can be found in the article listed in the image.

In essence, the presence of poorly configured SNMP services can be an entry point for hackers to attack your network systems. Therefore, it is important to take immediate remedial action to prevent exploitation.

4) RDP Server Detected over UDP: A Remote Desktop Protocol (RDP) server running over UDP was found as shown in Figure 8.



```
Vulnerability Threat Level
        high  RDP Server Detected over UD
P.
Vulnerability Definition
        Attackers may launch remote exploi
ts to either crash the service or tools li
ke ncrack to try brute-forcing the passwor
d on the target.
Vulnerability Remediation
        It is recommended to block the ser
vice to outside world and made the service
 accessible only through the a set of allo
wed IPs only really neccessary. The follow
ing resource provides insights on the risk
s and as well as the steps to block the se
rvice. https://www.perspectiverisk.com/rem
ote-desktop-service-vulnerabilities/
```

Fig. 8. Vulnerability: RDP Server Detected

Figure 8 shows a very serious security vulnerability, namely the discovery of a Remote Desktop Protocol (RDP) server running on top of the

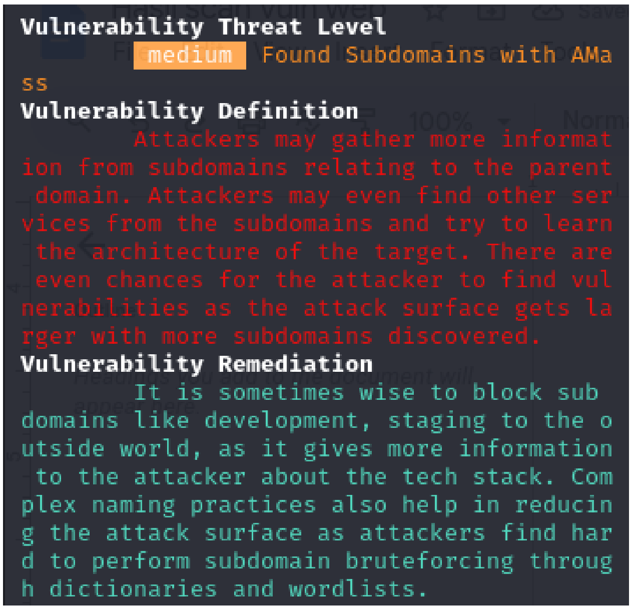
UDP protocol. This is an insecure and very risky configuration.

RDP is commonly used to access computers remotely. When RDP runs on top of UDP, it opens a gap for hackers to perform various attacks, such as dropping the RDP service, or trying to guess the administrator's password using tools like ncrack. The biggest risk of this vulnerability is the potential for a full system takeover by hackers.

To solve this problem, it is recommended to block access to the RDP service from outside the network and only allow access from specific IPs that really need it. In addition, it is important to strengthen password security and use two-factor authentication. More information on how to secure RDP services can be found in the resources listed in the image.

In essence, the presence of an RDP server running on top of UDP is a serious threat to system security. Therefore, remedial action should be taken immediately to prevent exploitation by irresponsible parties.

5) Found Subdomains with AMass: Found new subdomains that have not been previously identified as in Figure 9.



```
Vulnerability Threat Level
        medium  Found Subdomains with AMa
ss
Vulnerability Definition
        Attackers may gather more informat
ion from subdomains relating to the parent
 domain. Attackers may even find other ser
vices from the subdomains and try to learn
 the architecture of the target. There are
 even chances for the attacker to find vul
nerabilities as the attack surface gets la
rger with more subdomains discovered.
Vulnerability Remediation
        It is sometimes wise to block sub
domains like development, staging to the o
utside world, as it gives more information
 to the attacker about the tech stack. Com
plex naming practices also help in reducin
g the attack surface as attackers find har
d to perform subdomain bruteforcing throug
h dictionaries and wordlists.
```

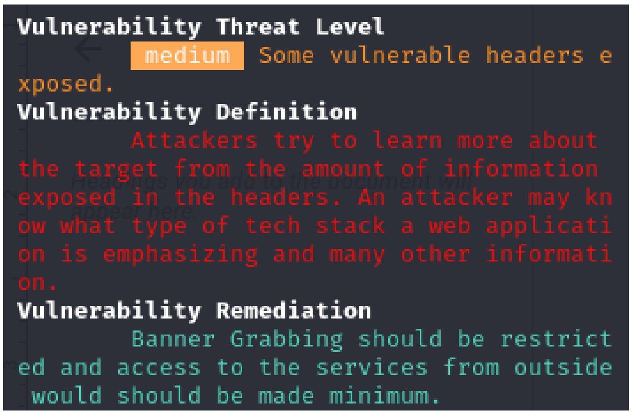
Fig. 9. Vulnerability: Found Subdomains

Figure 9 shows a security vulnerability associated with the discovery of new subdomains on a system. These subdomains were previously unidentified and could provide an entry point for attackers.

To address this issue, it is recommended to block access to non-essential subdomains, such as subdomains for development or testing. In addition, the use of complex subdomain names can also make it difficult for attackers to find and exploit these subdomains.

In essence, the existence of new subdomains is an indication of a potential security threat. Therefore, it is important to carefully manage subdomains and implement appropriate security measures to protect systems from attacks..

6) Some vulnerable headers exposed: Some HTTP headers sent by the LMS server contain information that can be exploited by attackers to perform attacks such as clickjacking or information disclosure as shown in Figure 10.



```
Vulnerability Threat Level
        medium  Some vulnerable headers e
xposed.
Vulnerability Definition
        Attackers try to learn more about
the target from the amount of information
exposed in the headers. An attacker may kn
ow what type of tech stack a web applicati
on is emphasizing and many other informati
on.
Vulnerability Remediation
        Banner Grabbing should be restrict
ed and access to the services from outside
 would should be made minimum.
```

Fig. 10. Vulnerability: Headers Exposed

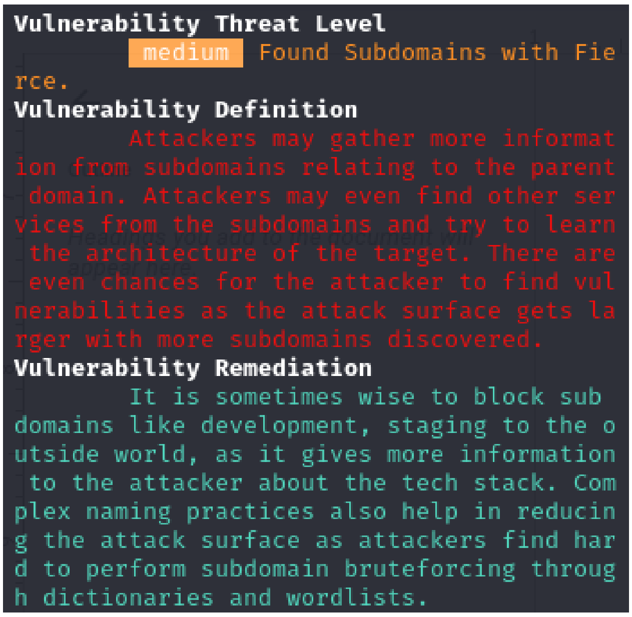
Figure 10 shows a security vulnerability in a system, where some HTTP headers that should be hidden are left exposed. This vulnerability is classified as moderate and has the potential to be abused by attackers.

HTTP headers are parts of HTTP messages that contain additional information about the request or response. If these headers are not configured properly, an attacker can extract sensitive information about the system, such as the type of technology used, software version, and other information. This information can be used to perform further attacks, such as clickjacking or information disclosure. The biggest risk of this vulnerability is the potential for larger, targeted attacks.

To solve this problem, it is recommended to limit the information displayed on HTTP headers. One way is to restrict access to services from outside the network and minimise the information provided in the header. More information on how to secure HTTP headers can be found in relevant security resources.

The bottom line is that the presence of exposed HTTP headers can provide valuable information to attackers. Therefore, it is important to configure HTTP headers correctly to make the system more secure.

7) Found Subdomains with Fierce: found new subdomains that can be attack points as shown in Figure 11.



```
Vulnerability Threat Level
        medium  Found Subdomains with Fie
rce.
Vulnerability Definition
        Attackers may gather more informat
ion from subdomains relating to the parent
 domain. Attackers may even find other ser
vices from the subdomains and try to learn
 the architecture of the target. There are
 even chances for the attacker to find vul
nerabilities as the attack surface gets la
rger with more subdomains discovered.
Vulnerability Remediation
        It is sometimes wise to block sub
domains like development, staging to the o
utside world, as it gives more information
 to the attacker about the tech stack. Com
plex naming practices also help in reducin
g the attack surface as attackers find har
d to perform subdomain bruteforcing throug
h dictionaries and wordlists.
```

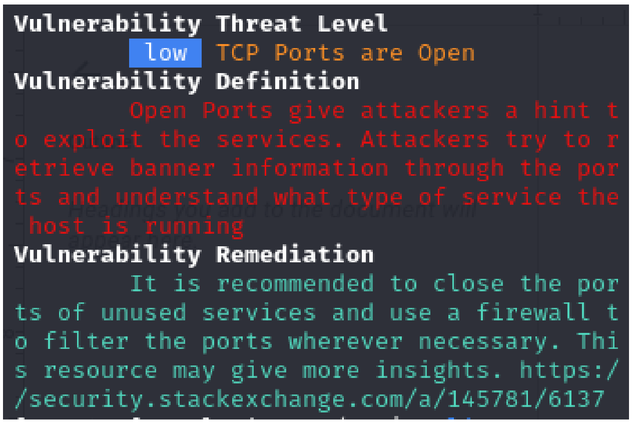
Fig. 11. Vulnerability: Subdomains with Fierce

Figure 11 shows a security vulnerability associated with the discovery of a new subdomain on a system. This vulnerability was detected by a tool called Fierce. These new subdomains can be a point of attack for hackers.

To solve this problem, it is recommended to block access to non-essential subdomains, such as subdomains for development or testing. In addition, using complex subdomain names can also make it difficult for attackers to find and exploit these subdomains.

In essence, the existence of new subdomains is an indication of a potential security threat. Therefore, it is important to carefully manage subdomains and implement appropriate security measures to protect systems from attacks.

8) TCP Ports are Open: Some unnecessary TCP ports are open, which can be the target of attacks like Figure 12.



```
Vulnerability Threat Level
        low  TCP Ports are Open
Vulnerability Definition
        Open Ports give attackers a hint t
o exploit the services. Attackers try to r
etrieve banner information through the por
ts and understand what type of service the
 host is running
Vulnerability Remediation
        It is recommended to close the por
ts of unused services and use a firewall t
o filter the ports wherever necessary. Thi
s resource may give more insights. https:/
/security.stackexchange.com/a/145781/6137
```

Fig. 12. Vulnerability: TCP Ports are Open

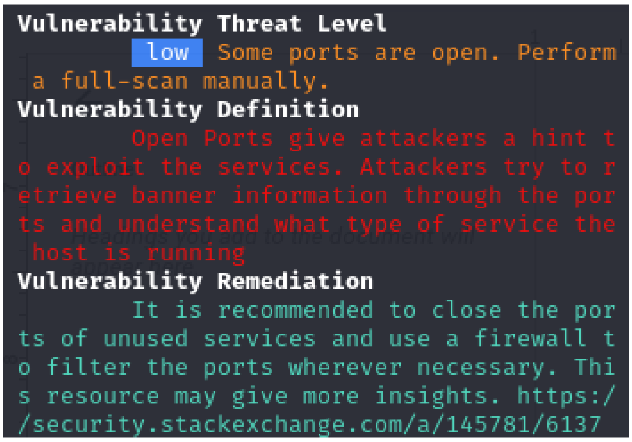
Figure 12 shows a security vulnerability in a system, where there are several TCP ports that are not needed but remain open. Although the threat level is relatively low, this condition still needs to be considered.

TCP ports are communication channels used by applications to interact with each other. If too many ports are open, this can give an attacker additional information about what services are running on the system. Knowing this information, the attacker can determine what type of attack would be most effective. Although the threat level is low, open ports can still be an entry point for larger attacks if not handled properly.

To solve this problem, it is recommended to close unused ports and use a firewall to restrict access to ports that are still needed. This way, the attack surface can be reduced and the risk of exploitation minimised. More information on how to manage TCP ports can be found in the resources listed in the figure.

The bottom line is that the presence of open TCP ports can provide valuable information to attackers. Therefore, it is important to manage TCP ports properly to make the system more secure.

9) Some ports are open. Perform a full-scan manually: Some ports are open and need to be scanned manually to identify services running on those ports as shown in Figure 13.



```
Vulnerability Threat Level
        low  Some ports are open. Perform
 a full-scan manually.
Vulnerability Definition
        Open Ports give attackers a hint t
o exploit the services. Attackers try to r
etrieve banner information through the por
ts and understand what type of service the
 host is running
Vulnerability Remediation
        It is recommended to close the por
ts of unused services and use a firewall t
o filter the ports wherever necessary. Thi
s resource may give more insights. https:/
/security.stackexchange.com/a/145781/6137
```

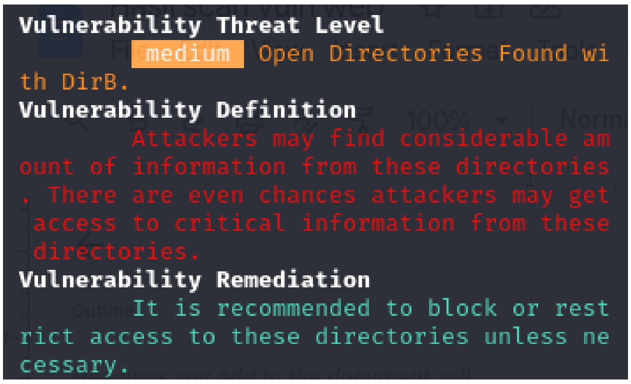
Fig. 13. Vulnerability: Some Ports are Open

Figure 13 shows a security vulnerability in a system, where there are several TCP ports that are not needed but remain open. Although the threat level is relatively low, this condition still needs to be considered.

To solve this problem, it is recommended to close unused ports and use a firewall to restrict access to ports that are still needed. This way, the attack surface can be reduced and the risk of exploitation minimised. More information on how to manage TCP ports can be found in the resources listed in the figure.

The bottom line is that the presence of open TCP ports can provide valuable information to attackers. Therefore, it is important to manage TCP ports properly to make the system more secure. This vulnerability indicates that the system has more potential entry points for attackers than it should. By closing unused ports and performing manual scans, security risks can be significantly reduced.

10) Open Directories Found with DirB: Found directories that should not be publicly accessible, which could contain sensitive files such as Figure 14.



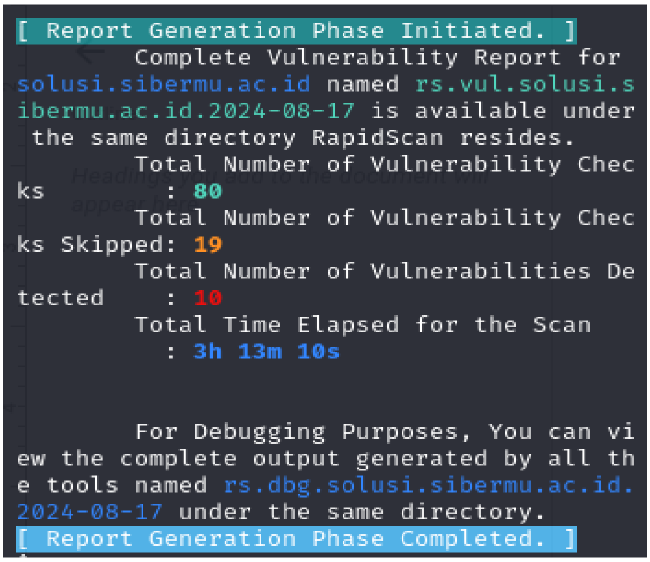
```
Vulnerability Threat Level
        medium   Open Directories Found wi
th DirB.
Vulnerability Definition
        Attackers may find considerable am
ount of information from these directories
. There are even chances attackers may get
 access to critical information from these
 directories.
Vulnerability Remediation
        It is recommended to block or rest
rict access to these directories unless ne
cessary.
```

Fig. 14. Vulnerability: Open Directories Found with DirB

Figure 14 shows a security vulnerability in a system, namely the discovery of directories (folders) that should not be publicly accessible but can be. These directories potentially contain important or sensitive files that could be misused if they fall into the wrong hands. To solve this problem, it is recommended to restrict access to these directories or move them to a more secure location. In addition, it is also important to conduct regular audits of existing directories to ensure that no other directories are accidentally open to the public.

In essence, the existence of publicly accessible directories is a serious threat to system security. Therefore, it is important to take immediate remedial action to prevent exploitation by irresponsible parties.

The complete vulnerability report for solusi.sibermu.ac.id as shown in Figure 15.



```
[ Report Generation Phase Initiated. ]
        Complete Vulnerability Report for
solusi.sibermu.ac.id named rs.vul.solusi.s
ibermu.ac.id.2024-08-17 is available under
 the same directory RapidScan resides.
        Total Number of Vulnerability Chec
ks      : 80
        Total Number of Vulnerability Chec
ks Skipped: 19
        Total Number of Vulnerabilities De
tected     : 10
        Total Time Elapsed for the Scan
          : 3h 13m 10s


        For Debugging Purposes, You can vi
ew the complete output generated by all th
e tools named rs.dbg.solusi.sibermu.ac.id.
2024-08-17 under the same directory.
[ Report Generation Phase Completed. ]
```

Fig. 15. Summaries of All Vulnerability Scanning

Figure 15 shows a summary of the vulnerability scan results against the website solusi.sibermu.ac.id. This scan was conducted on 17 August 2024 and lasted for 3 hours 13 minutes 10 seconds. Out of a total of 80 types of vulnerability checks performed, 19 checks were skipped and 10 vulnerabilities were found.

This report provides an overview of the vulnerability level of the website solusi.sibermu.ac.id and provides further information for remedial action.

Conclusion

Based on the results of a vulnerability scan of the website solusi.sibermu.ac.id, several security issues were found that need to be addressed immediately. These include publicly accessible directories, unnecessarily open ports, and other possible vulnerabilities.

The full scan report is available and provides details on the types of vulnerabilities found, as well as recommended fixes. By fixing these vulnerabilities, the security of the solusi.sibermu.ac.id website can be improved and the risk of cyber-attacks minimised. The results of this scan show that there are still some areas that need to be fixed to improve the security of the solusi.sibermu.ac.id website..

References

[1] M. Ghanem and T. Chen, "Reinforcement learning for efficient network penetration testing", Information, vol. 11, no. 1, p. 6, 2019. https://doi.org/10.3390/info11010006

[2] T. Gunawan, M. Lim, N. Zulkurnain, & M. Kartiwi, "On the review and setup of security audit using kali linux", Indonesian Journal of Electrical Engineering and Computer Science, vol. 11, no. 1, p. 51, 2018. https://doi.org/10.11591/ijeecs.v11.i1.pp51-59

[3] C. Susanto, K. Rizko, & D. Purbohadi, "Security assessment using nessus tool to determine security gaps on the repository web application in educational institutions", Emerging Information Science and Technology, vol. 1, no. 2, 2020. https://doi.org/10.18196/eist.128

[4] N. Pirsa and S. Sumijan, "Vulnerability assessment of web applications using penetration testing", International Journal of Recent Technology and Engineering, vol. 8, no. 4, p. 1552-1556, 2019. https://doi.org/10.35940/ijrte.b2133.118419

[5] J. Goel and B. Mehtre, "Vulnerability assessment &amp; penetration testing as a cyber defence technology", Procedia Computer Science, vol. 57, p. 710-715, 2015. https://doi.org/10.1016/j.procs.2015.07.458

[6] M. Ghanem and T. Chen, "Reinforcement learning for efficient network penetration testing", Information, vol. 11, no. 1, p. 6, 2019. https://doi.org/10.3390/info11010006

[7] N. Koroniotis, N. Moustafa, B. Turnbull, F. Schiliro, P. Gauravaram, & H. Janicke, "A deep learning-based penetration testing framework for vulnerability identification in internet of things environments",, 2021. https://doi.org/10.48550/arxiv.2109.09259

[8] A. Bacudio, X. Yuan, B. Chu, & M. Jones, "An overview of penetration testing", International Journal of Network Security & Its Applications, vol. 3, no. 6, p. 19-38, 2011. https://doi.org/10.5121/ijnsa.2011.3602

[9] B. Arfaj, S. Mishra, & M. Alshehri, "Efficacy of unconventional penetration testing practices", Intelligent Automation & Soft Computing, vol. 31, no. 1, p. 223-239, 2022. https://doi.org/10.32604/iasc.2022.019485

[10] H. Lu and Y. Yang, "Research on wifi penetration testing with kali linux", Complexity, vol. 2021, no. 1, 2021. https://doi.org/10.1155/2021/5570001

[11] B. Arromdoni, "Web application vulnerability analysis using the owasp method (case study: ojs csfd uin sunan kalijaga yogyakarta)",, 2024. https://doi.org/10.4028/p-fosz2d

[12] N. Koroniotis, N. Moustafa, B. Turnbull, F. Schiliro, P. Gauravaram, & H. Janicke, "A deep learning-based penetration testing framework for vulnerability identification in internet of things environments",, 2021. https://doi.org/10.48550/arxiv.2109.09259

[13] Kongara, D., & Krishnama, S., "A process of penetration testing using various tools", MJCS, p. 94-104, 2023. https://doi.org/10.58496/mjcs/2023/014.