Analysis and Implementation of the ISSAF Framework on OSSTMM on Website Security Vulnerabilities Testing in Polinema

1st Muhammad Alif Nabila[1], 2nd Putri Elfa Mas'udia[2], 3rd Rachmad Saptono [3]
[1,3] Digital Telecomunications Network Study Program,
Department of Electrical Engineering, State Polytechnic of Malang, 65141, Indonesia
[2] Telecommunication Engineering Study Program
Department of Electrical Engineering, State Polytechnic of Malang, 65141, Indonesia

[1]alifnabila48@gmail.com, [2]putri.elfa@polinema.ac.id, [3]rachmad.saptono@polinema.ac.id

***Abstract*—Along with the increasing number of websites circulating on the Internet, the security holes that arise are also increasing. The Electrical Engineering Department's website is no exception, especially on the Electrical Engineering Department's website which has never been audited to scan for security holes on the Electrical Engineering Department's website so the level of reliability of the Electrical Engineering Department's website cannot be known. On this basis, a study entitled "Analysis and Implementation of the ISSAF Framework for OSSTMM in Testing Website Security Gaps at Polynema" will be carried out. In this study, the authors tested security holes on the website at Polinema using the ISSAF and OSSTMM frameworks to scan for security holes on the Electrical Engineering Network website. Then from the test results, recommendations will be given to website managers to overcome existing security holes. Before giving recommendations, the author will try to update website security and re-test the updated website. This is done to prove whether updates made to website security can work effectively in overcoming security holes that were previously found. Based on the research that has been done, it is known that on the Electrical Engineering Department's website there are 21 security holes with 7 of them at medium level when testing for security holes using the ISSAF framework. And there are 17 security holes when testing security holes using the OSSTMM framework. The security holes include 10 open ports, DoS, brute-force, and there are security holes in the library used.**

***Keywords*— Website, Security Vulnerabilities, Penetration Testing, ISSAF, OSSTMM**

I. INTRODUCTION

Website is a collection of several web pages that contain various information in the form of text, images, audio, video, or files. The website is intended to display web pages that contain information and to store data which will later be stored on a web server so that it can be accessed anytime and anywhere. As time goes by, the website is growing and playing a role in everyday life, starting from looking for information, learning, media branding, to buying and selling activities. No wonder the growth in the number of websites is increasing rapidly [1].

Along with the growth in the number of websites that are increasing rapidly, the security gaps that arise are also increasing. Security vulnerabilities are the beginning of attacks on websites, from existing security gaps attackers will exploit existing loopholes to be able to enter the website system. In addition to being able to enter the system, security loopholes can also be used to damage the website directly or steal data on the website. This security vulnerability is crucial because it relates to personal data (privacy), integrity (integrity), access rights (authentication) , confidentiality (confidentiality), and availability (availability) [[2, 3].

In addition to relating to data security, security gaps also affect the reputation of a website, where the more security holes there are on a website, the reputation of the website will decrease. This will also affect visitors, where visitors will feel hesitant to visit a website with a low reputation because it is feared that the visitor's personal data is not safe. The attacks that are commonly carried out in penetration testing include SQL Injection, Cross-Site Scripting (XSS), Denial Of Service (DOS), brute force attacks, sniffing, clickjacking, Cross-Site Request Forgery (CSRF), and broken authentication and session. management [4, 5].

Therefore, according to [1], [6], and [7] penetration testing is very necessary to be able to find out the security holes that exist in a system in order to improve a system, including the website system. Penetration testing itself is an activity to evaluate the security of a system. Penetration testing is done by simulating an attack on a system to find out the security holes in the system. In addition, penetration testing is also carried out to find out what types of attacks can attack the system and can find out the impact that occurs due to these attacks. Penetration testing generates feedback that can be used by developers to improve or develop the security level of the system.

There are several frameworks that can be used to perform penetration testing, including the ISSAF framework, OSSTMM, ISO, NIST, OWASP, PTES, and so on. Research conducted by [8] uses the ISSAF framework to analyze website security, according to him, the ISSAF framework is suitable for doing penetration testing on websites because there are structured guidelines so that testing gets complete and clear directions. While the research conducted by [6] and [9] used the OSSTMM framework as a penetration testing method. The OSSTMM framework is considered better and more thorough in penetration testing because it is comprehensive globally because it does work on the front-end. The OSSTMM framework provides results in the form of RAV and STAR so that the results obtained can be presented more specifically [9].

Based on the description above, research will be conducted to conduct penetration testing using the ISSAF and OSSTMM frameworks to test the security vulnerabilities of the X website. Then the researcher will compare the two frameworks based on the penetration testing results of each framework. Researchers will also provide recommendations for handling vulnerabilities that exist on the X website based on security vulnerabilities detected during the research. With the recommendation from the researcher, it is hoped that the administrator of the X website can fix the security holes that exist on the website.

II. METHOD

A. *Research Stages*

stages are arranged so that this research can be carried out in detail. The stages of research that will be carried out in this study as shown in Fig. 1.

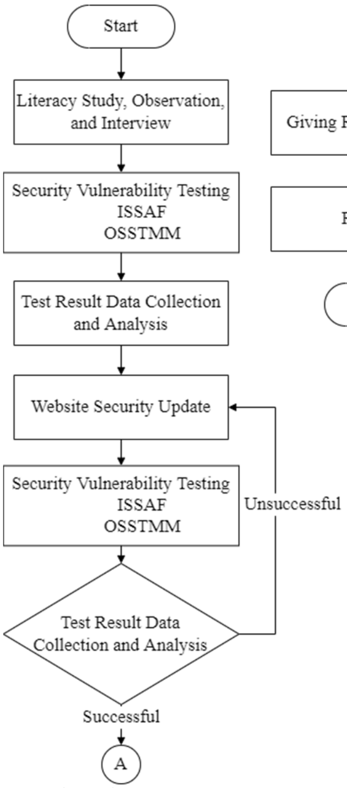

Start
Literacy Study, Observation, and Interview
Security Vulnerability Testing
ISSAF
OSSTMM
Test Result Data Collection and Analysis
Website Security Update
Security Vulnerability Testing
ISSAF
OSSTMM
Test Result Data Collection and Analysis
Unsuccessful
Successful
A
A
Giving Recommendation
Reporting
Finish

Figure 1. Research Design

1. Literacy Study, Observation, and Interview
2. Security Vulnerabilities Testing
3. Data Collection Test Results and Analysis
4. Website Security Update
5. Security Vulnerabilities Testing
6. Testing Data Collection and Analysis
7. Providing Recommendations
8. Reporting

B. *Penetration Testing Steps Penetration*

Testing steps are carried out using 2 different frameworks, namely the ISSAF framework and the OSSTMM framework. The steps for penetration testing will be shown in Fig. 2 and Fig. 3.

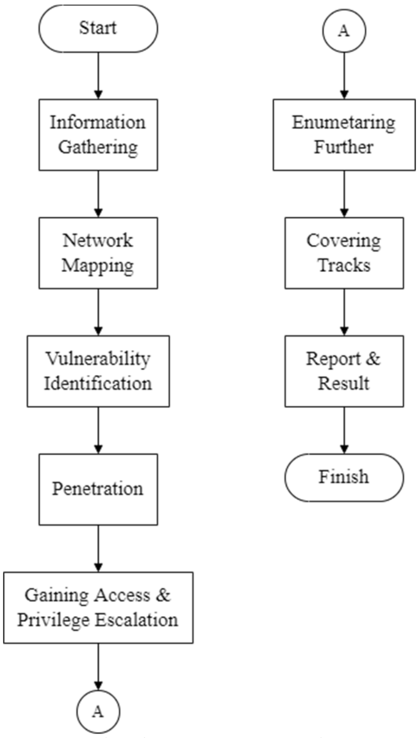


Figure 2. Testing Steps Using the ISSAF Framework

Fig. 2 is a penetration test step using the ISSAF framework, the following is a description of Figure 2:

1. Information Gathering is an early stage that aims to collect information about the target domain using the Whois tool.
2. Network Mapping is a network mapping related to ports and services used on the server. The tool used is Nmap.
3. Vulnerability Identification is to identify weaknesses on websites that can be exploited. The tool used is Acunetix.
4. Penetration is a security vulnerability test that is carried out by attacking the website. The attacks that will be carried out are and DoS Attack. The tool used is the Low Orbit Ion Cannon.
5. Gaining Access & Privilege Escalation is the stage of gaining access privileges by gaining access to the account. The attacks that can be done are Brute-force attacks and the tool used is WPScan.
6. Enumerating Further is a continuation of the previous stages which include decrypting passwords, sniffing traffic, and retrieving cookies. The tool used is Wireshark.
7. Covering Tracks is the stage of clearing traces so that they are not detected by website managers, this can be done by deleting logs or modifying logs.

8. Report & Result is the final stage to report the results of penetration testing in the form of any vulnerabilities found on the website and provide solutions to security vulnerabilities found.

Steps for penetration testing using the OSASTMM framework are shown in Fig. 3.

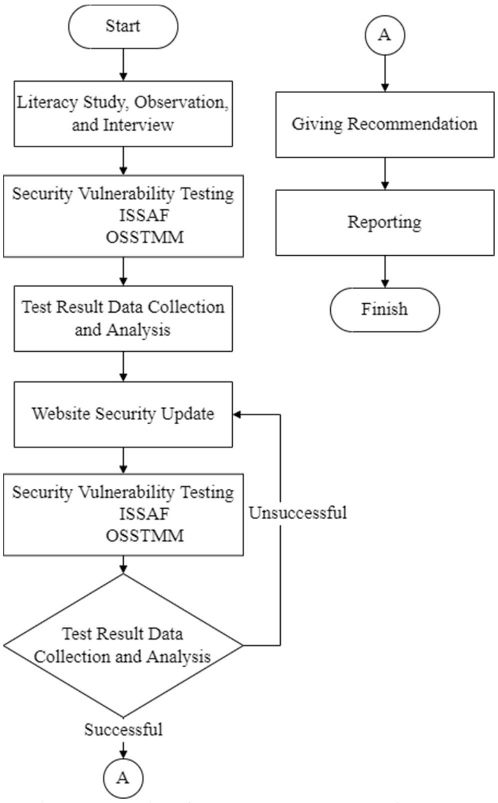

Start
Literacy Study, Observation, and Interview
Security Vulnerability Testing ISSAF OSSTMM
Test Result Data Collection and Analysis
Website Security Update
Security Vulnerability Testing ISSAF OSSTMM
Unsuccessful
Test Result Data Collection and Analysis
Successful
A
A
Giving Recommendation
Reporting
Finish

Figure 3. Testing Steps Using the OSSTMM Framework

Fig. 3 is a penetration testing step using the OSSTMM framework, the following is a description of Figure 3:

1. Assets, defines the target to be protected which is called an asset.
2. Engagement Zone, knowing the environment around the Asset which can be in the form of a protection mechanism, process, or service.
3. Scope, knowing everything outside the Engagement Zone that is needed to maintain Assets.
4. Vector determines the direction of Asset interaction to determine the direction from which the test is carried out.
5. Channel, identify the equipment needed to perform the test based on the interaction levels on the Vector.
6. Type of Test determines the type of approach to be taken (blind, double blind, gray box, double gray box, tandem, reversal).
7. Security Testing, testing security vulnerabilities using several tools such as Nmap, Nikto, and Low Orbit Ion Cannon, to be able to find out security vulnerabilities that exist on the website.
8. RAV & STAR, make assessments in the form of Risk Assessment Value (RAV) and Security Testing Audit Report (STAR). Where RAV produces a security value while STAR produces status and comments on the security testing performed.
9. Recommendations, formulate several recommendations on the results of security testing that has been carried out.

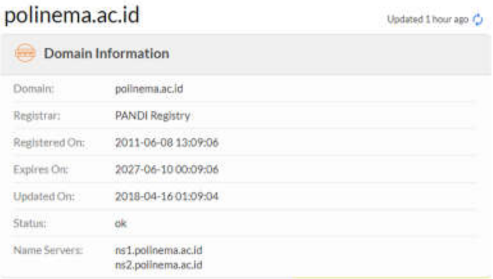
III. RESULTS AND DISCUSSION

A. *ISSAF Testing The*

following are the results of testing the *website* Electrical Engineering Network framework ISSAF.

1. Information Gathering

The results of scanning information gathering using the whois tool as shown in Fig. 4.


polinema.ac.id

Updated 1 hour ago

Domain Information

Domain:	polinema.ac.id
Registrar:	PANDI Registry
Registered On:	2011-06-08 13:09:06
Expires On:	2027-06-10 00:09:06
Updated On:	2018-04-16 01:09:04
Status:	ok
Name Servers:	ns1.polinema.ac.id ns2.polinema.ac.id

Figure 4 Information Gathering Test Results

It can be seen that the jte.polinema.ac.id website has the main domain polinema.ac.id. The jte.polinema.ac.id domain was registered by the PANDI Registry domain company which was registered on 08-06-2011 and is valid until 10-06-2017 and was updated on 16-04-2018.

2. Network Mapping

The results of the network mapping scan using the nmap tool as shown in Fig. 5.

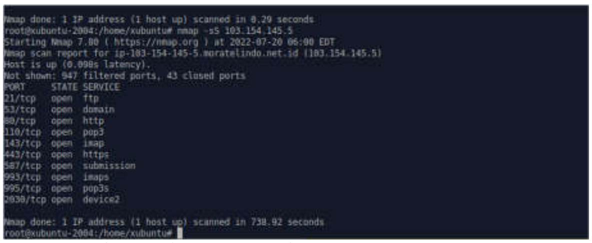
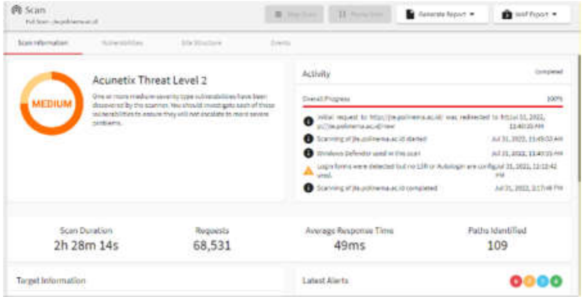

```
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
root@xubuntu-2004:/home/xubuntu# nmap -sS 103.154.145.5
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-20 06:00 EDT
Nmap scan report for ip-103-154-145-5.moratelindo.net.id (103.154.145.5)
Host is up (0.098s latency).
Not shown: 947 filtered ports, 43 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
2030/tcp open  device2

Nmap done: 1 IP address (1 host up) scanned in 738.92 seconds
root@xubuntu-2004:/home/xubuntu# 
```

Figure 5 Network Mapping Test Results

There are 10 open ports, can be described in Table I.

3. Vulnerability Identification

The results of the vulnerability identification scan using the acunetix tool as shown in Fig. 6.



Acunetix Threat Level 2

Scan Duration	Requests	Average Response Time	Paths Identified
2h 28m 14s	68,531	49ms	109

Figure 6 Vulnerability Identification Test.

Results The scan results show that there is a security vulnerability with a medium level of vulnerability, which means the jte.polinema.ac.id website is quite vulnerable to external attacks. There are 7 kinds of security vulnerabilities with a medium level of vulnerability, including application error messages, development configuration files, slow HTTP denial of service attacks, User credentials are sent in clear text, vulnerable javascript libraries, WordPress XML-RPC authentication brute force.

TABLE I
THE PORTS DETECTED IN THE NETWORK MAPPING TEST

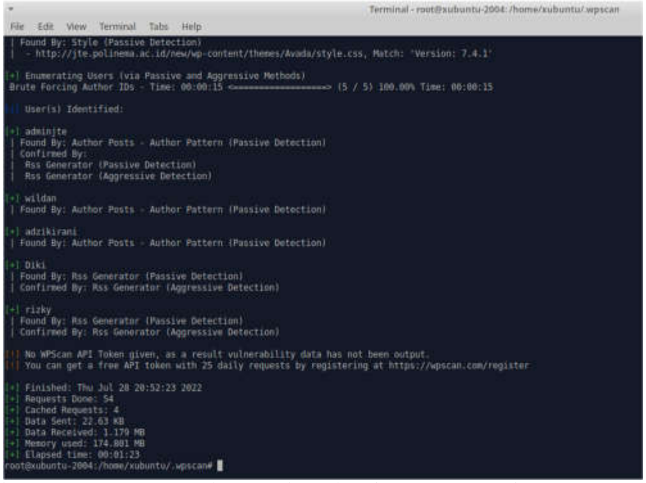
Port	State	Service	Describtion
21/tcp	Open	ftp	Is a port for data transfer services
53/tcp	Open	domain	Is a port for domain services from websites
80/tcp	Open	http	Is a port for the http protocol used by websites
110/tcp	Open	pop3	Is a port for mail server services
143/tcp	Open	imap	Is a port for mail server services
443/tcp	Open	https	Is a port for the https protocol (http with security) used by websites
587/tcp	Open	submission	Is a port default for sending email
993/tcp	Open	imaps	Is a port for mail server services with security
995/tcp	Open	pop3s	Is a port for mail server services with security
2030/tcp	Open	device2	Is a port for TCP / IP services so that the server can communicate with clients via the internet network.

4. Penetration

The results of the Denial of Service (DOS) penetration test performed using the LOIC tool can be viewed using the ping tool. From the results of the ping, it was found that the jte.polinema.ac.id website was quite vulnerable to DOS attacks. It is evident from the results of the ping before DOS penetration that the average response time is 80.8ms and the percentage of success is 100%, while the data from the ping results during the DOS penetration get an average response time of 1078.25ms and the percentage of success is 66.67%. Referring to the standard response time used in this study, the service quality of the jte.polinema.ac.id website is of good value with an average response time of 80.8ms. However, when DOS penetrated, the service quality of the jte.polinema.ac.id website became poor with an average response time of 1078.25ms.

5. Gaining Access & Privilege Escation

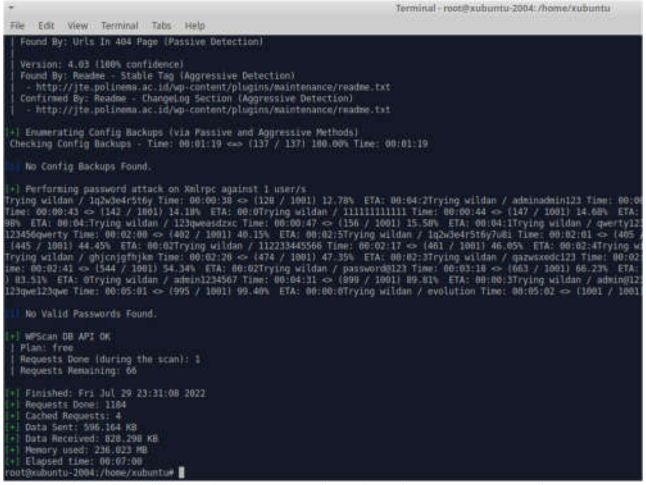
The results of the gaining access & privilege escalation stage carried out using the WPScan tool with the brute-force method as shown in Fig. 7.



```
 | Found By: Style (Passive Detection)
 |  - http://jte.polinema.ac.id/new/wp-content/themes/Avada/style.css, Match: 'Version: 7.4.1'

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:15 <====================> (5 / 5) 100.00% Time: 00:00:15

[i] User(s) Identified:

[+] adminjte
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Rss Generator (Aggressive Detection)

[+] wildan
 | Found By: Author Posts - Author Pattern (Passive Detection)

[+] adzikirani
 | Found By: Author Posts - Author Pattern (Passive Detection)

[+] Diki
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Rss Generator (Aggressive Detection)

[+] rizky
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Rss Generator (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Thu Jul 28 20:52:23 2022
[+] Requests Done: 54
[+] Cached Requests: 4
[+] Data Sent: 22.63 KB
[+] Data Received: 1.179 MB
[+] Memory used: 174.801 MB
[+] Elapsed time: 00:01:23
root@xubuntu-2004:/home/xubuntu/.wpscan# 
```

Figure 7 Username Scanning Results Using the WPScan Tool.

The results of username scanning using the WPScan tool showed that there were 5 accounts found, the accounts were adminjte, wildan, adzikirani, Diki, and rizky.



```
 | Found By: Urls In 404 Page (Passive Detection)
 |
 | Version: 4.03 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://jte.polinema.ac.id/wp-content/plugins/maintenance/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://jte.polinema.ac.id/wp-content/plugins/maintenance/readme.txt

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:01:19 <=> (137 / 137) 100.00% Time: 00:01:19

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 1 user/s
Trying wildan / 1q2w3e4r5t6y Time: 00:00:38 <> (128 / 1001) 12.78%  ETA: 00:04:2Trying wildan / adminadmin123 Time: 00:0
Time: 00:00:43 <> (142 / 1001) 14.18%  ETA: 00:0Trying wildan / 111111111111 Time: 00:00:44 <> (147 / 1001) 14.68%  ETA:
98%  ETA: 00:04:Trying wildan / 123qweasdzxc Time: 00:00:47 <> (156 / 1001) 15.58%  ETA: 00:04:1Trying wildan / qwerty12
123456qwerty Time: 00:02:00 <> (402 / 1001) 40.15%  ETA: 00:02:5Trying wildan / 1q2w3e4r5t6y7u8i Time: 00:02:01 <> (405
 (445 / 1001) 44.45%  ETA: 00:02Trying wildan / 112233445566 Time: 00:02:17 <> (461 / 1001) 46.05%  ETA: 00:02:4Trying w
Trying wildan / ghjcnjgfhjkm Time: 00:02:20 <> (474 / 1001) 47.35%  ETA: 00:02:3Trying wildan / qazwsxedc123 Time: 00:02
ime: 00:02:41 <> (544 / 1001) 54.34%  ETA: 00:02Trying wildan / password@123 Time: 00:03:18 <> (663 / 1001) 66.23%  ETA:
) 83.51%  ETA: 0Trying wildan / admin1234567 Time: 00:04:31 <> (899 / 1001) 89.81%  ETA: 00:00:3Trying wildan / admin@12
123qwe123qwe Time: 00:05:01 <> (995 / 1001) 99.40%  ETA: 00:00:0Trying wildan / evolution Time: 00:05:02 <> (1001 / 1001

[i] No Valid Passwords Found.

[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 1
 | Requests Remaining: 66

[+] Finished: Fri Jul 29 23:31:08 2022
[+] Requests Done: 1184
[+] Cached Requests: 4
[+] Data Sent: 596.164 KB
[+] Data Received: 828.298 KB
[+] Memory used: 236.023 MB
[+] Elapsed time: 00:07:00
root@xubuntu-2004:/home/xubuntu# 
```

Figure 8 Results of Scanning Passwords Using the WPScan Tool.

Scanning passwords for previously found accounts (wildan) yielded the above data. As for the data above, the results of the scan "No Valid Passwords Found" are shown, which means that no suitable password was found for the "wildan" account. These results do not mean that the jte.polinema.ac.id website does not have security holes from brute-force attacks, security holes from brute-force attacks still exist but the use of passwords from "wildan" accounts is too difficult to track.

6. Enumetaring Further

The results of sniffing traffic using the Wireshark tool can be seen in the image below:

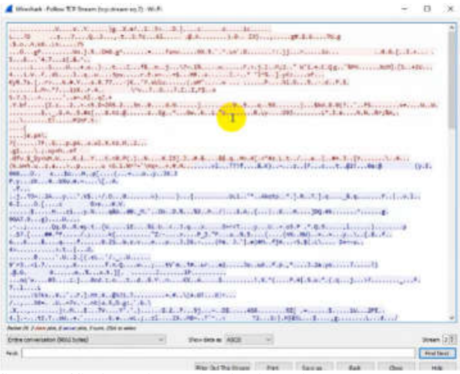


Figure 9 Sniffing Traffic by using Wireshark tools.

Fig. 9 shows the contents of the package. The contents of the package are encrypted data because the transmission on the jte.polinema.ac.id website already uses the HTTPS protocol which uses data encryption. Because the data has been encrypted, the data transmitted by the jte.polinema.ac.id website is safe.

7. Covering Tracks

After being able to access log files and delete existing history, the traces left can be declared lost.

8. Report & Result

Based on the website security vulnerability testing using the ISSAF framework that has been carried out, several security vulnerabilities have been found as follows:

- There are 10 open ports, but 6 of them are not used in website services so that they can be used as access to exploit the website. The 6 ports are port 21 (ftp), 110 (pop3), 143 (imap), 587 (submission), 993 (imaps), 995 (pop3s).
- There is an application error message that can show sensitive information related to the website system.
- There is a configuration file that can be accessed via the internet.
- There is a vulnerability to Slow DOS attacks.
- User credentials are transmitted over an open channel without any encryption, making them vulnerable to sniffing attacks.
- There are JavaScript libraries that contain security holes. Generally due to a bug in the library used.
- WordPress XML-RPC authentication brute force marked with the xmlrpc.php file can be accessed through the website.

B. OSSTMM Testing

following is the result of testing the website security vulnerability of the Electrical Engineering Network using the OSSTMM framework.

1. Asset

for testing website security holes in this experiment is the website jte.polinema.ac.id. So, the asset in this experiment is the website jte.polinema.ac.id.

2. Engagement Zone

There are 2 aspects found in the engagement zone, namely:

a. Protection

mechanism Protection mechanism can be interpreted as any protection contained on the website. From observations and interviews that have been carried out, it is known that the protection currently available on the jte.polinema.ac.id website is the HTTPS protocol. Where in this protocol has used a Secure Socket Layer (SSL) certificate to encrypt the data transmission that occurs on the website.

a. Services

The services provided by the jte.polinema.ac.id website are standard website services that contain general information about the Department of Electrical Engineering.

3. Scope

There are several things outside the engagement zone related to the website, including regulations and hosting.

4. Vector

website jte.polinema.ac.id itself provides information that can be accessed by the public via the internet, so testing for security holes can be done by accessing the jte.polinema.ac.id website using the internet network. So it can be concluded that the vector in this study is from the outside to the scope, namely from the internet network to the jte.polinema.ac.id website

5. Channel

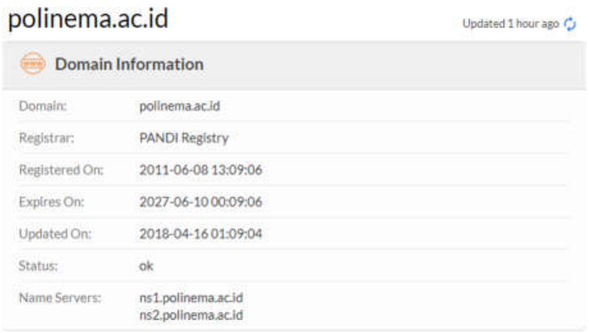
Assets in the research are the website of the Department of Electrical Engineering which can be accessed from anywhere via the internet. The engagement zone of the asset contains the HTTPS protocol and services in the form of providing information that can be accessed by the public through the internet network. On the scope there is also a hosting where hosting access is also through the internet network. Based on the explanation, all asset scopes can be accessed through the internet network, so that the most appropriate type of channel used in this research is the Data Network Channel.

6. Type of Test

In this study, analysts are provided with limited knowledge related to assets and defense of targets and targets are also prepared for audit. So the right type of test used in this study is the Gray Box Test or often also called the vulnerability test which aims to conduct a self-assessment of the target.

7. Security Testing

The results of security testing using the whois, nmap, and nikto tools as shown in Fig. 10.



polinema.ac.id

Updated 1 hour ago

Domain Information

Domain:	polinema.ac.id
Registrar:	PANDI Registry
Registered On:	2011-06-08 13:09:06
Expires On:	2027-06-10 00:09:06
Updated On:	2018-04-16 01:09:04
Status:	ok
Name Servers:	ns1.polinema.ac.id ns2.polinema.ac.id

Figure 10 Test Results Using the Whois Tool.

It can be seen that the jte.polinema.ac.id website has the main domain polinema.ac.id. The jte.polinema.ac.id domain is registered by the PANDI Registry domain company which was registered on 08-06-2011 and is valid until 10-06-2017 and has been updated on 16-04-2018.

Scanning using the nmap tool shows that there are 10 open ports, including:

TABLE II
TABLE OF PORTS DETECTED IN NETWORK MAPPING TESTING

Port	State	Service	Description
21/tcp	Open	ftp	It is a port for data transfer services
53/tcp	Open	domain	Is a port for domain services from the website
80/tcp	Open	http	Is a port for the http protocol used by the website
110/tcp	Open	pop3	Is a port for mail server services
143/tcp	Open	imap	Is a port for mail server services
443/tcp	Open	https	Is a port for the https protocol (http with security) used by the website Is a port for the https protocol (http with security) used by the website
587/tcp	Open	submission	It is default port for sending email
993/tcp	Open	imaps	Is a port for mail server services with security
995/tcp	Open	pop3s	Is a port for mail server services with security
2030/tcp	Open	device2	Is a port for TCP / IP services so that the server can communicate with clients via the internet network.

From the security vulnerability scan carried out using the Nikto tool, 6544 items have been checked with 0 errors and 26 items have been reported as shown in the image above. This indicates that there are 26 security holes on the jte.polinema.ac.id website.

Prior to DOS penetration, a ping was made to the jte.polinema.ac.id website to find out how the response from the jte.polinema.ac.id website was as well as a comparison of ping results during DOS penetration. pinged data before DOS penetration gets an average response time of 80.8ms and a success percentage of 100%, while the ping results data during DOS penetration gets an average response time of 1078.25ms and a success percentage of 66.67%. Referring to the standard response time used in this study, the service quality of the jte.polinema.ac.id website is of good value with an average ping response of 80.8ms. However, when DOS penetrated, the service quality of the jte.polinema.ac.id website became poor with an average response time of 1078.25ms.

8. RAV & STAR

To calculate the RAV value, several categories of OpSec, Loss Control, and Limitations factors are needed which will be mentioned in the table below:

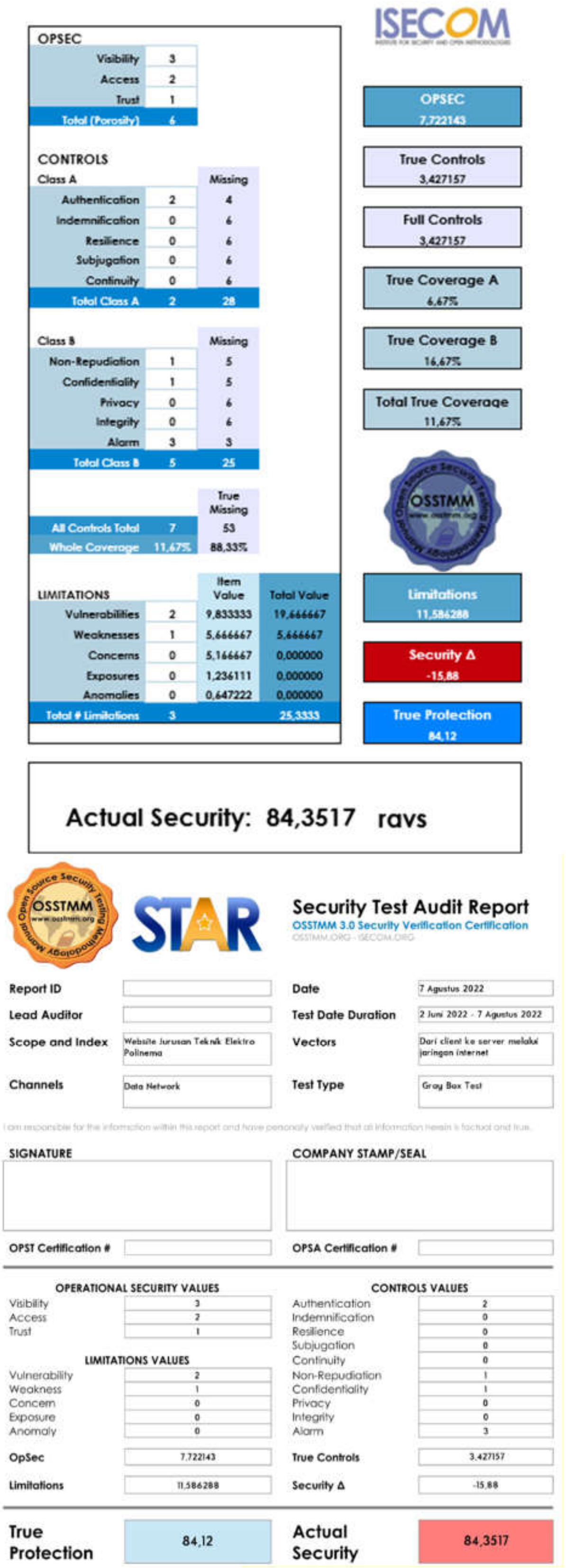
TABLE III
RAV COMPONENTS SUMMARY

No	Category	Description	Amount	Total
1	Visibility	1 Access to asset	1	3
		Web Server	1	
		Port	1	
2	Access	There are 2 ports with open status, namely port 53 and port 80	10	10
3	Trust	Spoofing IP Address	1	1
4	Authentication	There is authentication because it uses the HTTPS protocol	1	2
		The admin login system already uses 2-way authentication using email	1	
5	Non-Repudiation	Website visitors cannot change, delete, or add content on the website	1	1
6	Confidentility	Asset transmission is equipped with authentication and encryption via HTTPS protocol	1	1
7	Alarm	There is a notification when there is a login failure by the admin	1	3
		There is a notification when the data input has been successful	1	
		There is a notification when there is a text format error on the input form	1	
8	Vulnerablity	No anti-clickjacking X-Frame-Options header	6	17
		Header leaks inotes via ETags, header found with file /, fields: 0x62ea0c54 0x26a	1	
9	Weakness	Not all data input forms use authentication	1	1

From the table above, the value of each category will be summarized for later calculation of the RAV value.

TABLE IV
RAV VALUE SUMMARY TABLE

Actual Security			Amount
Opsec		Visibility	3
		Access	10
		Trust	1
Controll	Class A (Interactive)	Authentication	2
		Indemnification	0
		Resilience	0
		Subjugation	0
		Continuity	0
	Class B (Process)	Non-Repudiation	1
		Confidentiality	1
		Privacy	0
		Integrity	0
		Alarm	3
Limitations		Vulnerability	17
		Weakness	1
		Concerns	0
		Exposures	0
		Anomaly	0



ISECOM

OPSEC	
Visibility	3
Access	2
Trust	1
Total (Porosity)	6

CONTROLS

Class A		Missing
Authentication	2	4
Indemnification	0	6
Resilience	0	6
Subjugation	0	6
Continuity	0	6
Total Class A	2	28

Class B		Missing
Non-Repudiation	1	5
Confidentiality	1	5
Privacy	0	6
Integrity	0	6
Alarm	3	3
Total Class B	5	25

		True Missing
All Controls Total	7	53
Whole Coverage	11,67%	88,33%

LIMITATIONS		Item Value	Total Value
Vulnerabilities	2	9,833333	19,666667
Weaknesses	1	5,666667	5,666667
Concerns	0	5,166667	0,000000
Exposures	0	1,236111	0,000000
Anomalies	0	0,647222	0,000000
Total # Limitations	3		25,3333

OPSEC	7,722143
True Controls	3,427157
Full Controls	3,427157
True Coverage A	6,67%
True Coverage B	16,67%
Total True Coverage	11,67%
Limitations	11,586288
Security Δ	-15,88
True Protection	84,12

Actual Security: 84,3517 ravs

STAR

Security Test Audit Report

OSSTMM 3.0 Security Verification Certification

OSSTMM.ORG - ISECOM.ORG

Report ID		Date	7 Agustus 2022
Lead Auditor		Test Date Duration	2 Juni 2022 - 7 Agustus 2022
Scope and Index	Website Jurusan Teknik Elektro Polinema	Vectors	Dari client ke server melalui jaringan internet
Channels	Data Network	Test Type	Gray Box Test

I am responsible for the information within this report and have personally verified that all information herein is factual and true.

SIGNATURE

COMPANY STAMP/SEAL

OPST Certification #

OPSA Certification #

OPERATIONAL SECURITY VALUES		CONTROLS VALUES	
Visibility	3	Authentication	2
Access	2	Indemnification	0
Trust	1	Resilience	0
		Subjugation	0
LIMITATIONS VALUES		Continuity	0
Vulnerability	2	Non-Repudiation	1
Weakness	1	Confidentiality	1
Concern	0	Privacy	0
Exposure	0	Integrity	0
Anomaly	0	Alarm	3
OpSec	7,722143	True Controls	3,427157
Limitations	11,586288	Security Δ	-15,88
True Protection	84,12	Actual Security	84,3517

Figure 11. STAR Calculation Result

The RAV value obtained from the test results is 84.3517. This value is already higher than the RAV value from the previous test results. Although the security holes found have been greatly reduced compared to before, the RAV value obtained is still below 100. This means that the control on the website is less than what is needed. Therefore, to increase the RAV value, it is necessary to add control to the website.

9. Recommendations

From the tests that have been carried out, the results obtained are better than the previous tests. This indicates that the website security update that has been carried out is working effectively. However, even though the website security has been updated, the RAV value which is the reference for evaluating website security is still below 100, which means that the control on the website is still lacking. To get the ideal RAV value, a control can be added on the website so that the interaction and control can be balanced.

a. Giving Recommendations

Based on the research that has been done, researchers can recommend several things to the jte.polinema.ac.id website admin related to the jte.polinema.ac.id website security system. Some of these things are:

- Cover open ports that are not used on website services. This is done in order to block entry from outsiders who want to exploit the jte.polinema.ac.id website.
- Use the reverse proxy method to prevent DOS attacks.
- Disabling xmlrpc.php because xmlrpc.php becomes a security vulnerability in the form of vulnerability to brute-force attacks.
- Add Content Security Policy (CSP) on the web server to prevent Cross Site Script (XSS) attacks.
- Always update the web server software to always get updates, both regarding bug fixes, feature updates, or the addition of new features.
- Apply authentication on each input form.
- Add control to website services so that interaction and control on the website can be balanced.

IV. CONCLUSION

Testing website security vulnerabilities in Polinema using the ISSAF framework found 21 security vulnerabilities with 7 of them being medium level. And testing using the OSSTMM framework found 17 security holes. In testing the website security vulnerabilities in Polinema, it is better to use the ISSAF framework because it is more detailed with a total of 21 security vulnerabilities. The handling of website security vulnerabilities in Polinema is done by closing open ports, adding a reverse proxy, disabling xmlpc.php, adding Content Security Policy (CSP), and updating the web server software.

V. REFERENCES

[1] A. W. Wardhana and H. B. Seta, “Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF pada Website Universitas XYZ,” Jurnal Informatik, vol. 17, no. 3, pp. 226,237, 2021.

[2] Y. I. Fernando and R. Abdillah, “Security Testing Sistem Penerimaan Mahasiswa Baru Universitas XYZ Menggunakan Open Source Security Testing Methodology Manual (OSSTMM),” Jurnal CoreIT, pp. 33-40, 2016.

[3] A. Rochman, R. R. Salam and S. A. Maulana, “Analisis Keamanan Website Dengan Information System Security

Assessment Framework (ISSAF) dan Open Web Application Security Project (OWASP) di Rumah Sakit XYZ," Jurnal Indonesia Sosial Teknologi, Vols. vol. 2, no. 4,.

[4] Guntoro, L. Costaner and Musfawati, "Analisis Kemanan Web Server Open Journal System (OJS) Menggunakan Metode ISSAF dan OWASP (Studi Kasus OJS Universitas Lancang Kuning)," Jurnal Ilmiah Penelitian dan Pembelajaran Informatika, pp. 45-55, 2020.

[5] P. Herzog, " The Open Source Security Testing Methodology Manual 3.0," New York: ISECOM, 2010.

[6] M. A. Z. Rizky and Yuhandri, "Optimalisasi dalam Penetrasi Testing Keamanan Website Menggunakan Teknik SQL Injection dan XSS," Jurnal Sistim Informasi dan Teknologi, pp. 215-220, 2021.

[7] M. Arman, "Metode Pertahanan Web Server Terhadap Distributed Slow HTTP DoS Attack," Jurnal Teknik Informatika dan Sistem Informasi, pp. 56-70, 2020.

[8] B. Arifwidodo, Y. Syuhada and S. Ikhwan, "Analisis Kinerja Mikrotik Terhadap Serangan Brute Force dan DDoS," Techno.COM, pp. 392-399, 2021.

[9] W. Agustiara, A. Pratama and S. Junaidi, "Analisis Keamanan Protokol Secure Socket Layer Terhadap Serangan Packet Sniffing pada Website Portal Berita Harian Umum Koran Padang," Jurnal Teknik Informatika Kaputama, vol. 6, no. 1, pp. 10-15, 2022.

[10] M. S. Hisbuan and L. M. Gultom, "Analisis Serangan Deface Menggunakan Backdoor Shell Pada Website," Techno.COM, vol. 17, no. 4, pp. 415-423, 2018.

[11] D. Aleyka and P. Mishra, "Study on Manual Auditing for Web Application Vulnerability Detection," Annals of R.S.C.B., vol. 25, no. 4, pp. 19612-19618, 2021.

[12] S. U. Sunaringtyas and D. S. Prayoga, "Implementasi Penetration Testing Execution Standard Untuk Uji Penetrasi Pada Layanan Single Sign-On," Edu Komputika Journal, vol. 8, no. 1, pp. 48-56, 2021.

[13] R. T. Dirgahayu, Y. Prayudi and A. Fajaryanto, "Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server," Jurnal Ilmiah NERO, vol. 1, no. 3, pp. 190-197, 2015.

[14] F. Abu-Dabaseh and E. Alshammari, "Automated Penetration Testing: An Overview," Computer Science & Information Technology, pp. 121-129, 2018.

[15] E. S. P. Taringan, "Security Testing Dengan Menggunakan Metode OSSTMM Pada Web Institut Teknologi Telkom Purwokerto," Institut Teknologi Telkom Purwokerto, Purwokerto, 2018.