Engineering and Technology Journal e-ISSN: 2456-3358

Volume 09 Issue 07 July-2024, Page No.- 4427-4433

DOI: 10.47191/etj/v9i07.11, I.F. – 8.227

© 2024, ETJ

Identify Vulnerabilities on the Ministry of Health's Ayo Sehat Website Through Penetration Testing

Nur Siti Aisyah[1], Fasya Zulia Puspitasari[2], Kalpin Oktavianus Angga[3], Brili Rey Shandi[4]

[1,2,3,4] Information Systems Study Program, Faculty of Engineering and Informatics, Gajayana University Malang, Indonesia

ABSTRACT: This research identifies security vulnerabilities on the "Ayo Sehat Kemenkes" website managed by the Ministry of Health of the Republic of Indonesia through penetration testing using the ISSAF (Information Systems Security Assessment Framework) framework. The methods used include information gathering, network mapping, vulnerability identification, and exploitation. Tools such as CMD, Whois, Nmap, and Subgraph Vega are used in the testing process. The research results found several vulnerabilities with different levels of severity: a high level vulnerability in the form of a social security number which can cause the risk of identity theft, a medium level vulnerability in the form of a local file system path which provides information about the structure of directories and files on the web server, and a low level vulnerability in the form of lots of email addresses and password forms with an active autocomplete feature. These findings demonstrate the importance of preventative measures to improve website security and protect user data.

KEYWORDS: Vulnerability, Website, Penetration Testing, Security, Cybersecurity

I. INTRODUCTION

In the current digital era, the existence and use of web applications has become an integral part of various sectors, including health services by providing easier access for patients to search for health information online. Penetration testing is the simulation of attacks on a computer system, network, or web application to identify vulnerabilities and assess the level of security [1]. Penetration testing is carried out by simulating attacks that might be carried out by hackers to find security gaps on the website. Security vulnerabilities in web-based applications include *SQL Injection* , *Broken Authentication* , *XSS* , *Security Misconfiguration* , and *CSRF* [2]. By carrying out penetration testing, we can find out potential security risks that can be exploited by irresponsible parties.

The "Let's Get Healthy Ministry of Health" website is a platform managed by the Ministry of Health of the Republic of Indonesia, which aims to provide health information to the public at large. Health information includes structured data that describes specific health conditions [3]. This data is very important in managing health care, covering biomedical concepts and other aspects related to health care, such as information about diseases, health tips, online medical consultations, and the latest news about health. Health information plays a central role in the activities of health professionals as well as shaping consumer attitudes towards health services [4]. Through this website, users can access reliable information to support prevention activities and personal and family health management.

However, with the increasing use of web applications in the health sector, including the Ministry of Health's “Let's Get Healthy” website, new challenges have emerged in terms of cyber security. The need for higher security is especially important considering that the data managed is often sensitive, such as users' personal medical information. Many web applications, including those managed by government institutions, are not free from potential vulnerabilities that can be exploited by irresponsible parties. One of the main problems often found in web applications is the lack of attention to security testing during the development and implementation phases. In the case of the Ministry of Health's “Let's Be Healthy” website, various potential vulnerabilities can be identified through penetration testing. By conducting penetration testing, we can identify these potential security risks and take the necessary steps to protect sensitive data and maintain user trust.

II. LITERATURE REVIEW

A website vulnerability is a weakness or security gap in a web application that can be exploited by an attacker to gain unauthorized access, steal data, or damage the system [5]. The sources of these vulnerabilities vary, including errors in writing the code, insecure server configurations, or weaknesses in communication protocols [6]. Identification of vulnerabilities on websites is generally done through scanning and penetration testing [7]. Scanning often uses tools such as Nmap and Subgraph Vega to perform in-depth analysis of web infrastructure [8]. Online scanning is useful for detecting known vulnerabilities and requires relatively little time.

Penetration testing, or pentesting, is a more comprehensive method for identifying vulnerabilities. This testing involves simulating an attack by a third party to evaluate the system's strengths and weaknesses. The penetration testing phase includes planning, reconnaissance, information gathering, exploitation, and reporting. Automated tools and manual techniques are often used simultaneously to uncover exploitable weaknesses. By conducting regular penetration testing, organizations can maintain high security standards, protect sensitive data, and improve overall cybersecurity defenses [9]. Additionally, penetration testing plays an important role in ensuring the confidentiality, integrity and availability of data in today's digital era, where cyber threats continue to evolve.

Tools used in penetration testing include Nmap for network scanning, and Subgraph Vega for analyzing web vulnerabilities. Nmap can perform fast, UDP-intensive, and TCP-intensive scanning, while Subgraph Vega is used for more specific vulnerability exploitation. The 'Let's Get Healthy Ministry of Health' website is a platform managed by the Ministry of Health of the Republic of Indonesia. This site makes health information available to the general public, including sensitive personal medical data. Therefore, it is important to identify and address potential vulnerabilities through penetration testing. Proper testing methods can help in uncovering security gaps and protecting user data from unwanted threats.

III. METHOD

This research uses an exploratory method with a qualitative approach to identify security vulnerabilities on a website through penetration testing. The methodology used is based on ISSAF (Information System Security Assessment Framework), which provides a structured framework for conducting penetration testing. ISSAF is a methodology used to assess the security of information systems, particularly websites, by identifying vulnerabilities and recommending improvements [10]. To ensure that the writing of this research follows the necessary stages, we use a research flow. Figure 1. below shows the research flow chart:

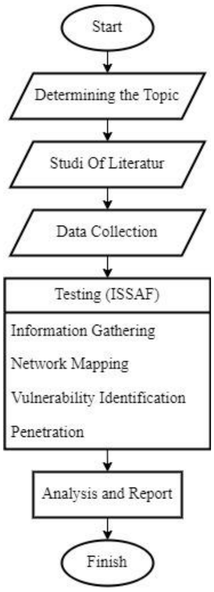


Figure 1. Research Flow

1. Determining the Topic

The first step of this research is to determine the topic to be investigated. The topic chosen determines the topic to be investigated. The topic chosen was "Identification of Vulnerabilities on the "Let's Healthy Ministry of Health" Website through penetration testing.

2. Study of literature

At this stage, collection and analysis of literature relevant to the research topic is carried out.

3. Data collection

Data is collected through various sources including technical data regarding system architecture to support the penetration testing process.

4. Testing Using the ISSAF Method

The penetration testing process is carried out based on the ISSAF methodology, which includes the following stages:

a. Information Gathering

This stage involves gathering the information necessary to understand the structure and architecture of the website. The techniques used include using CMD and Who is to obtain information on the domain, server and technology used.

b. Network Mapping

Network mapping is carried out to identify network topology including connected hardware and software. Nmap is used to perform network scanning (Quick Scan, Intensive UDP, Intensive TCP) to identify active hosts and services.

c. Vulnerability Identification

At this stage vulnerabilities in the system are identified using tools such as Subgraph Vega.

d. Penetration

Exploitation is carried out to test whether a discovered vulnerability can be exploited by an attacker, the goal is to evaluate the level of risk associated with each vulnerability.

5. Analysis and Reports

The results of penetration testing are analyzed to determine the level of risk and impact of each vulnerability found, categorized into high risk, medium risk and low risk based on its impact on data security and website operations. A final report is prepared to present the findings of the analysis.

In the pentest testing process with the ISSAF framework, it can be concluded that the following stages will be carried out, the tools used and the functions of the tools can be seen in Table 1. As follows:

Table 1. ISSAF Method

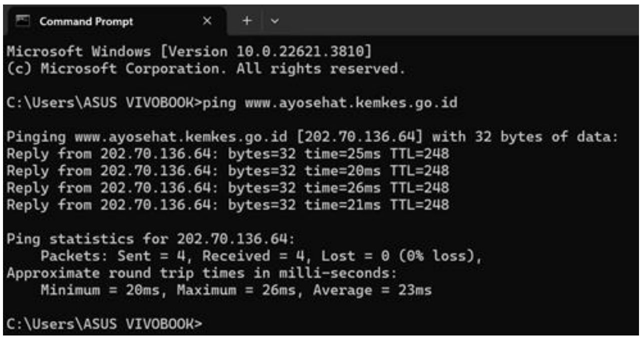
Stages	Tools	Description
Information Gathering	CMD, Whois	Gather basic information about the target
Network Mapping	Nmap (Quick Scan, Intense Scan Plus UDP, Intense Scan All TCP Ports)	Network mapping for identification of running activities and services
Vulnerability Identification	Subgraph Vega	Identify vulnerabilities in applications and systems
Penetration	Subgraph Vega	Exploit identified vulnerabilities to verify the existence and extent of vulnerabilities

IV. RESULT AND DISCUSSION

The website used to identify this vulnerability is ", at the website security testing stage using the ISSAF method with 4 stages, which are explained as follows:

1. Information Gathering

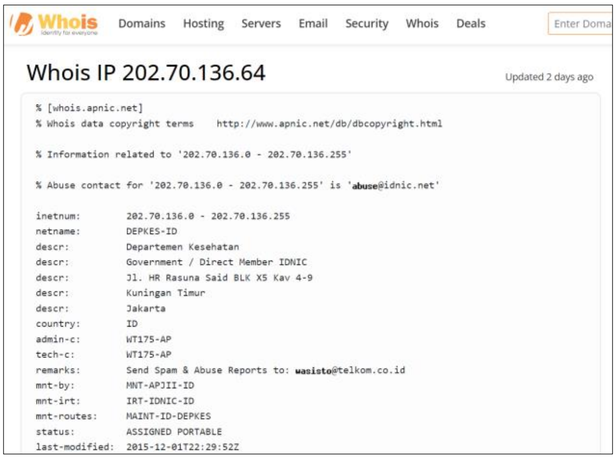
At this stage, the main objective is to collect as much publicly available information as possible about the target website, namely www.ayosehat.kemkes.go.id. This information can be used to develop attack strategies in subsequent stages. The method used in this stage includes the use of Command Line (CMD) in Figure 2. and the WHOIS service in Figure 3. As follows:



```
Microsoft Windows [Version 10.0.22621.3810]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ASUS VIVOBOOK>ping www.ayosehat.kemkes.go.id

Pinging www.ayosehat.kemkes.go.id [202.70.136.64] with 32 bytes of data:
Reply from 202.70.136.64: bytes=32 time=25ms TTL=248
Reply from 202.70.136.64: bytes=32 time=20ms TTL=248
Reply from 202.70.136.64: bytes=32 time=26ms TTL=248
Reply from 202.70.136.64: bytes=32 time=21ms TTL=248

Ping statistics for 202.70.136.64:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 26ms, Average = 23ms

C:\Users\ASUS VIVOBOOK>
```

Figure 2. Command Line (CMD)

From the results of the "ping" command to the address www.ayosehat.kemkes.go.id, the IP address of the website was obtained, namely 202.70.136.64. These results show that the www.ayosehat.kemkes.go.id server can be accessed stably and has a good response time, with an average latency of around 23 milliseconds and without data packet loss.



Whois IP 202.70.136.64

Updated 2 days ago

```
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '202.70.136.0 - 202.70.136.255'

% Abuse contact for '202.70.136.0 - 202.70.136.255' is 'abuse@idnic.net'

inetnum:        202.70.136.0 - 202.70.136.255
netname:        DEPKES-ID
descr:          Departemen Kesehatan
descr:          Government / Direct Member IDNIC
descr:          Jl. HR Rasuna Said BLK X5 Kav 4-9
descr:          Kuningan Timur
descr:          Jakarta
country:        ID
admin-c:        WT175-AP
tech-c:         WT175-AP
remarks:        Send Spam & Abuse Reports to: wasisto@telkom.co.id
mnt-by:         MNT-APJII-ID
mnt-irt:        IRT-IDNIC-ID
mnt-routes:     MAINT-ID-DEPKES
status:         ASSIGNED PORTABLE
last-modified:  2015-12-01T22:29:52Z
```

Figure 3. Whois

From Figure 3. The Whois results show information regarding the website www.ayosehat.kemkes.go.id with the IP address 202.70.136.64 in Table 2. As follows:

Table 2. Whois information

Information	Details
Organization	Department of Health
Organization Type	Government / Direct Member IDNIC
Address	Jl. HR Rasuna Said BLK X5 Kav 4-9, East Kuningan, Jakarta, Indonesia
Administrative Contact	Wasisto Tririno R
Administrative Contact Email	email@telkom.co.id

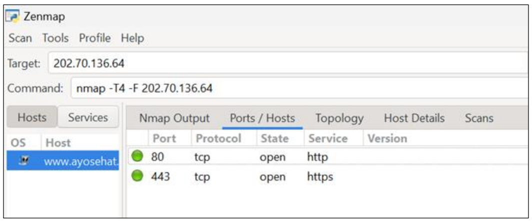
Administrative Contact Address	Multimedia Tower lt. 4, Jl Kebon Sirih No. 12, DKI Jakarta
Administrative Contact Phone	+62-21-70255504
Administrative Contact Fax	+62-21-3864004
IP Address Status	ASSIGNED PORTABLE
Route Maintainer	MAINT-ID-DEPKES
Maintainer	MNT-APJII-ID, IRT-IDNIC-ID
Contact For Abuse Reports	email@telkom.co.id, email@idnic.net

The Department of Health is a government organization in Indonesia which has the IP address 202.70.136.64. They are direct members of IDNIC (Indonesia Network Information Center). Their physical address is located in Jakarta. Wasisto Tririno R is the main administrative contact with the contact details listed above. To report misuse or problems related to this IP, you can contact the email listed.

2. Network Mapping

At this stage, scanning is carried out using the Nmap application. Following are the results of scanning with Nmap:

1. Quick Scan



Zenmap

Target: 202.70.136.64

Command: nmap -T4 -F 202.70.136.64

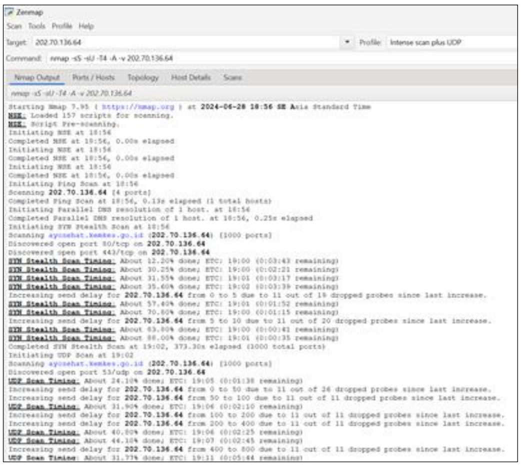
OS	Host
	www.ayosehat

	Port	Protocol	State	Service	Version
●	80	tcp	open	http	
●	443	tcp	open	https	

Figure 4. Quick Scan Results

A scan of the IP '202.70.136.64' shows that the host 'www.ayosehat.kemkes.go.id' has two open ports: post 80 (HTTP) and port 443 (HTTPS). Scanning is done with the command “nmap -T4 -F”, which means fast scanning with high speed priority.

2. Intense Scan Plus UDP



Zenmap

Target: 202.70.136.64 Profile: Intense scan plus UDP

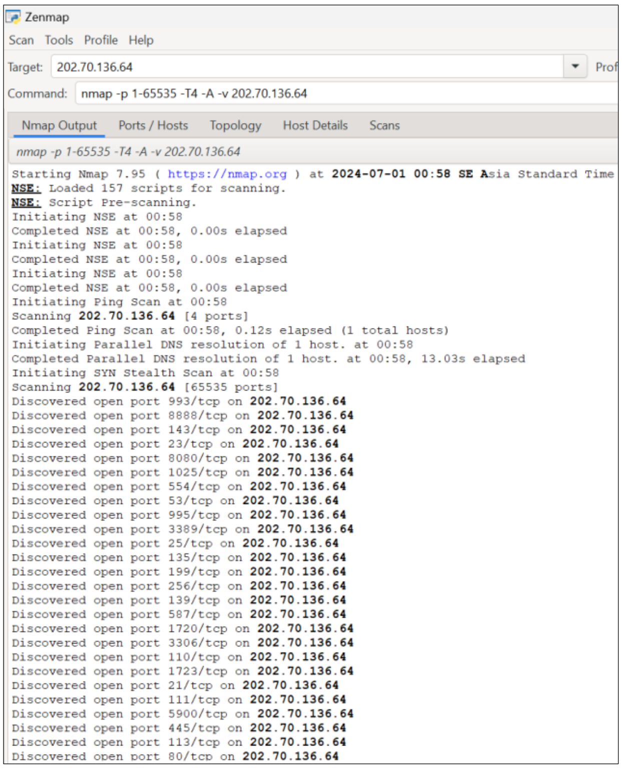
Command: nmap -sS -sU -T4 -A -v 202.70.136.64

```
nmap -sS -sU -T4 -A -v 202.70.136.64
Starting Nmap 7.95 ( https://nmap.org ) at 2024-06-28 18:56 SE Asia Standard Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:56
Completed NSE at 18:56, 0.00s elapsed
Initiating NSE at 18:56
Completed NSE at 18:56, 0.00s elapsed
Initiating NSE at 18:56
Completed NSE at 18:56, 0.00s elapsed
Initiating Ping Scan at 18:56
Scanning 202.70.136.64 [4 ports]
Completed Ping Scan at 18:56, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:56
Completed Parallel DNS resolution of 1 host. at 18:56, 0.25s elapsed
Initiating SYN Stealth Scan at 18:56
Scanning ayosehat.kemkes.go.id (202.70.136.64) [1000 ports]
Discovered open port 80/tcp on 202.70.136.64
Discovered open port 443/tcp on 202.70.136.64
SYN Stealth Scan Timing: About 12.20% done; ETC: 19:00 (0:03:43 remaining)
SYN Stealth Scan Timing: About 30.25% done; ETC: 19:00 (0:02:21 remaining)
SYN Stealth Scan Timing: About 31.55% done; ETC: 19:01 (0:03:17 remaining)
SYN Stealth Scan Timing: About 35.60% done; ETC: 19:02 (0:03:39 remaining)
Increasing send delay for 202.70.136.64 from 0 to 5 due to 11 out of 19 dropped probes since last increase.
SYN Stealth Scan Timing: About 57.40% done; ETC: 19:01 (0:01:52 remaining)
SYN Stealth Scan Timing: About 70.80% done; ETC: 19:00 (0:01:15 remaining)
Increasing send delay for 202.70.136.64 from 5 to 10 due to 11 out of 20 dropped probes since last increase.
SYN Stealth Scan Timing: About 83.80% done; ETC: 19:00 (0:00:41 remaining)
SYN Stealth Scan Timing: About 88.00% done; ETC: 19:01 (0:00:35 remaining)
Completed SYN Stealth Scan at 19:02, 373.30s elapsed (1000 total ports)
Initiating UDP Scan at 19:02
Scanning ayosehat.kemkes.go.id (202.70.136.64) [1000 ports]
Discovered open port 53/udp on 202.70.136.64
UDP Scan Timing: About 24.10% done; ETC: 19:05 (0:01:38 remaining)
Increasing send delay for 202.70.136.64 from 0 to 50 due to 11 out of 26 dropped probes since last increase.
Increasing send delay for 202.70.136.64 from 50 to 100 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 31.90% done; ETC: 19:06 (0:02:10 remaining)
Increasing send delay for 202.70.136.64 from 100 to 200 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 202.70.136.64 from 200 to 400 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 40.80% done; ETC: 19:06 (0:02:25 remaining)
UDP Scan Timing: About 44.10% done; ETC: 19:07 (0:02:45 remaining)
Increasing send delay for 202.70.136.64 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 31.77% done; ETC: 19:11 (0:05:44 remaining)
```

Figure 5. Intense Scan Plus UDP results

In the scan output, Nmap against ayosehat.kemkes.go id (202.70.136.64). An intensive scan is carried out which includes the SYN Stealth Scan method for TCP ports and UDP Scan for UDP ports. As a result, it was found that ports 80 (HTTP) and 443 (HTTPS) were open, indicating that there were web services that could be accessed via the HTTP and HTTPS protocols. In addition, port 53 (DNS) was also detected as open. The UDP scanning process took longer due to its not directly connected nature like TCP, with some increase in send delay due to lost packets. This scan provides a deep understanding of the target network infrastructure, which is important for security evaluation and identification of potential vulnerabilities.

3. Intense Scan All TCP Ports



Zenmap

Target: 202.70.136.64

Command: nmap -p 1-65535 -T4 -A -v 202.70.136.64

```
nmap -p 1-65535 -T4 -A -v 202.70.136.64
Starting Nmap 7.95 ( https://nmap.org ) at 2024-07-01 00:58 SE Asia Standard Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:58
Completed NSE at 00:58, 0.00s elapsed
Initiating NSE at 00:58
Completed NSE at 00:58, 0.00s elapsed
Initiating NSE at 00:58
Completed NSE at 00:58, 0.00s elapsed
Initiating Ping Scan at 00:58
Scanning 202.70.136.64 [4 ports]
Completed Ping Scan at 00:58, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:58
Completed Parallel DNS resolution of 1 host. at 00:58, 13.03s elapsed
Initiating SYN Stealth Scan at 00:58
Scanning 202.70.136.64 [65535 ports]
Discovered open port 993/tcp on 202.70.136.64
Discovered open port 8888/tcp on 202.70.136.64
Discovered open port 143/tcp on 202.70.136.64
Discovered open port 23/tcp on 202.70.136.64
Discovered open port 8080/tcp on 202.70.136.64
Discovered open port 1025/tcp on 202.70.136.64
Discovered open port 554/tcp on 202.70.136.64
Discovered open port 53/tcp on 202.70.136.64
Discovered open port 995/tcp on 202.70.136.64
Discovered open port 3389/tcp on 202.70.136.64
Discovered open port 25/tcp on 202.70.136.64
Discovered open port 135/tcp on 202.70.136.64
Discovered open port 199/tcp on 202.70.136.64
Discovered open port 256/tcp on 202.70.136.64
Discovered open port 139/tcp on 202.70.136.64
Discovered open port 587/tcp on 202.70.136.64
Discovered open port 1720/tcp on 202.70.136.64
Discovered open port 3306/tcp on 202.70.136.64
Discovered open port 110/tcp on 202.70.136.64
Discovered open port 1723/tcp on 202.70.136.64
Discovered open port 21/tcp on 202.70.136.64
Discovered open port 111/tcp on 202.70.136.64
Discovered open port 5900/tcp on 202.70.136.64
Discovered open port 445/tcp on 202.70.136.64
Discovered open port 113/tcp on 202.70.136.64
Discovered open port 80/tcp on 202.70.136.64
```

Figure 6. Intense Scan Results for All TCP Ports

In this section, an intensive scan is carried out to check all TCP ports on the target 202.70.136.64 which is the domain www.ayosehat.kemkes.go.id. This scan aims to identify open ports and services running on them, as well as identifying the operating system and devices used. The following are the results of the scan carried out using Nmap in Table 3. Below:

Table 3. Intense Scan Results for All TCP Ports

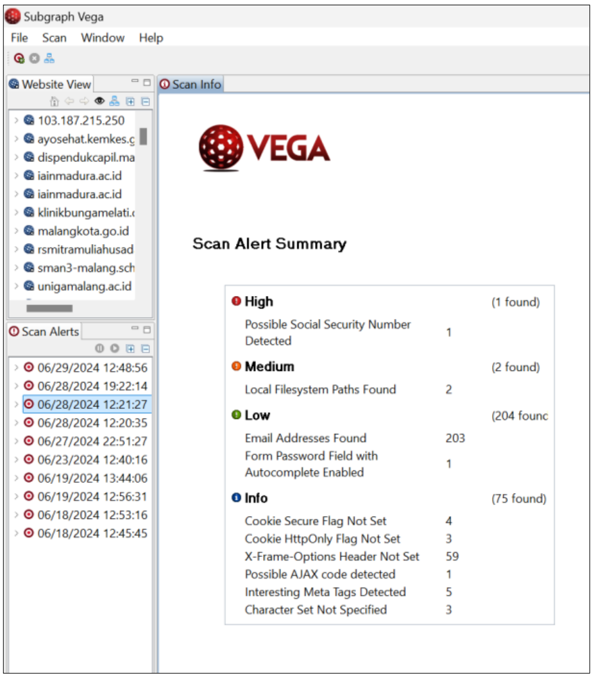
Category	Details
Target	202.70.136.64 (www.ayosehat.kemkes.go.id)
Command	nmap -p 1-65535 -T4 -A -v 202.70.136.64

Scan Start Time	16:00
Scan Duration	16.54 seconds
HostStatus	Active (latency 0.24s)
Total Ports Scanned	65535
TCP Port Not Displayed	65531 filtered TCP ports (no response), 4 filtered TCP ports (net-unreach)
Oscan Results	Not available because there are no open and closed ports
Device Type	Firewalls, Load Balancers, Routers, WAP
CPE OS	F5 Networks TMOS, Cisco ASA, Cisco PIX OS, Cisco IOS, Compaq embedded, etc.
Aggressive OS Guessing	F5 Networks TMOS (92%), Cisco ASA 8.X (86%), Cisco IOS 12.X (86%), Cisco PIX OS 6.X (86%), Compaq embedded (85%), F5 BIG-IP LTM (92%), Cisco ASA 5510 (86%)
Network Distance	8 hops

From the results of this scan, it can be seen that almost all TCP ports are filtered, which indicates the presence of a firewall or other security device that prevents direct access. Identification of operating systems and devices shows the possibility of using various types indicating several network layers that are traversed before reaching the target.

3. Vulnerability Identification

At this stage, a vulnerability scan was carried out on the "Ayo Seha Ministry of Health" website using the Subgraph Vega application. This step aims to identify potential vulnerabilities that exist on the website. So that security risks that may arise can be identified. Subgraph Vega is an effective tool in finding a wide range of vulnerabilities including Cross-Site Scripting (XSS), SQL, Injection and other security issues. The results of this scan will provide a detailed picture of the website's security status and areas that require further attention, following Figure 7 Scanning via Subgraph Vega:



103.187.215.250
ayosehat.kemkes.g
dispendukcapil.ma
iainmadura.ac.id
iainmadura.ac.id
klinikbungamelati.
malangkota.go.id
rsmitramuliahusad
sman3-malang.sch
unigamalang.ac.id

06/29/2024 12:48:56
06/28/2024 19:22:14
06/28/2024 12:21:27
06/28/2024 12:20:35
06/27/2024 22:51:27
06/23/2024 12:40:16
06/19/2024 13:44:06
06/19/2024 12:56:31
06/18/2024 12:53:16
06/18/2024 12:45:45

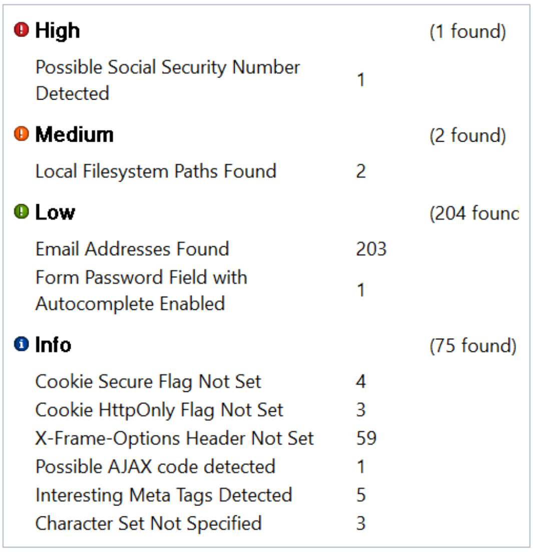
Scan Alert Summary

High		(1 found)
Possible Social Security Number Detected	1	
Medium		(2 found)
Local Filesystem Paths Found	2	
Low		(204 founc
Email Addresses Found	203	
Form Password Field with Autocomplete Enabled	1	
Info		(75 found)
Cookie Secure Flag Not Set	4	
Cookie HttpOnly Flag Not Set	3	
X-Frame-Options Header Not Set	59	
Possible AJAX code detected	1	
Interesting Meta Tags Detected	5	
Character Set Not Specified	3	

Figure 7. Vega Subgraph Scanning Process

4. Penetration

At this stage, exploitation of vulnerabilities that have been identified on the "Let's Healthy Ministry of Health" website is carried out. This step aims to test the extent to which these vulnerabilities can be exploited by irresponsible parties. The exploit was carried out using various techniques and tools, including Subgraph Vega to simulate a real attack. The results of this stage provide in-depth insight into the risk level and potential impact of each existing vulnerability. Based on the scan results, several vulnerabilities were found which are categorized in Figure 8. As follows:



High		(1 found)
Possible Social Security Number Detected	1	
Medium		(2 found)
Local Filesystem Paths Found	2	
Low		(204 founc
Email Addresses Found	203	
Form Password Field with Autocomplete Enabled	1	
Info		(75 found)
Cookie Secure Flag Not Set	4	
Cookie HttpOnly Flag Not Set	3	
X-Frame-Options Header Not Set	59	
Possible AJAX code detected	1	
Interesting Meta Tags Detected	5	
Character Set Not Specified	3	

Figure 8. Vega Subgraph Scanning Results

In these results, using Subgraph Vega for the vulnerability identification process, it is divided into 3 levels, namely high, medium and low. Levels in the following table:

Table 4. High Level Vulnerabilities

No	Levels	Type	Information	Number of Vulnerabilities
1	High	Possible Social Security Number Detected	Detected social security numbers that can pose serious risks of identity theft and privacy violations.	1

Table 4 shows vulnerabilities with a high severity level. The type of vulnerability detected is the presence of social security numbers which can cause the risk of identity theft and privacy violations. In this case, there was 1 vulnerability detected .

Table 5. Medium Level Vulnerability

No	Levels	Type	Information	Number of Vulnerabilities
1	Medium	Local Filesystem Paths Found	Local file system paths are discovered that can provide an attacker with valuable information about the directory and file structure on the web server.	2

Table 5 shows vulnerabilities with a medium severity level. The type of vulnerability discovered is a local file system path that could provide an attacker with important information regarding the directory and file structure on the web server. In this case, there are 2 vulnerabilities detected.

Table 6. Low Level Vulnerability

No	Levels	Type	Information	Number of Vulnerabilities
1	Low	Email Addresses Found	Many email addresses are found in website content	203
2	Low	Form Password Field with Autocomplete Enabled	Password form with autocomplete feature enabled	1

Table 6 shows vulnerabilities with a low severity level:

1) The first type of vulnerability was the large number of email addresses found in the website content, with a total of 203 email addresses detected.
2) type of vulnerability is a password form that was discovered with one vulnerability detected.

Low level vulnerabilities usually pose less risk than high or medium level vulnerabilities, but still need to be considered and addressed to prevent potential security threats.

CONCLUSION

This research has succeeded in identifying vulnerabilities on the 'Ayo Sehat Kemenkes' website using the penetration testing method with the ISSAF (Information Systems Security Assessment Framework) framework. From the test results, several vulnerabilities were found with varying degrees of severity. High-level vulnerabilities include having social security numbers detected, which could lead to serious risks of identity theft and privacy breaches. There is 1 vulnerability at this level. At the moderate level, 2 vulnerabilities were discovered in the form of local file system paths that could provide attackers with valuable information about the directory and file structure on the web server. Meanwhile, at the low level, 203 email addresses were found in the website content and 1 vulnerability related to the password form with the autocomplete feature activated, which posed additional security risks. This analysis shows that the 'Let's Be Healthy Ministry of Health' website has several vulnerabilities that have the potential to endanger the security of user data and system integrity. By identifying and addressing these vulnerabilities, remedial steps can be taken to improve security and maintain user trust.

REFERENCES

1. B. Bhardwaj And S. Tiwari, “Penetration Testing And Data Privacy: An In-Depth Review,” *Journal Of Cyber Security In Computer System*, Vol. 2, Pp. 18–22, Jun. 2023, Doi: 10.46610/Jcscs.2023.V02i01.003.
2. K. Vengurlekar, “Loop Holes In Web Based Security,” *International Journal Of Advanced Research In Science, Communication And Technology*, Pp. 329–335, Jun. 2022, Doi: 10.48175/Ijarsct-5347.
3. I. Oktaviani, D. Rahmawati, And Y. Nataya, “Prevalensi Dan Faktor Risiko Anemia Pada Anak Di Negara Maju,” *Jurnal Kesehatan Masyarakat Indonesia*, Vol. 16, P. 218, Jun. 2021, Doi: 10.26714/Jkmi.16.4.2021.218-226.
4. C. T. Lopes, “Health Information Retrieval -- State Of The Art Report,” May 2022, [Online]. Available: Http://Arxiv.Org/Abs/2205.09083
5. B. Ghozali, "Detecting Website Application Security Vulnerabilities Using The Owasp (Open Web Application Security Project) Method For Risk Assessment Detect Web Application Security Flaws Using The Owasp (Open Web Application Security Project) Method For Risk Assessment," *Posted: 09 February* , 2018.
6. D. Ariyana, S. Ningtyas, A. Fauzi, And R. Ramadhan, "Implementation of an Online Scanner Method to Find Vulnerabilities in Website Servers: Case Study: Gramedia.Com Website," Vol. 1, Pp. 16–25, June. 2023, Doi: 10.56855/Jeep.V1i1.304.
7. S. Comm. , MT , AERS Comm. , MMMDA Marcello Singadji, "Web Security Scanning to Increase Awareness of Web Security Vulnerabilities Using Nuclei," *Indigenous Journal-Jurnal of Arts, Design & Culture, South Tangerang Arts Council* , Vol. 4, no. 1, 2022.
8. Y. Hidayat And B. Arifwidodo, “Implementasi Web Server Menggunakan Infrastructure As Code Terraform Berbasis Cloud Computing,” *Format Jurnal Ilmiah Teknik Informatika*, Vol. 10, P. 192, Jun. 2021, Doi: 10.22441/Format.2021.V10.I2.010.
9. B. Bhardwaj And S. Tiwari, “Penetration Testing And Data Privacy: An In-Depth Review,” *Journal Of Cyber Security In Computer System*, Vol. 2, Pp. 18–22, Feb. 2023, Doi: 10.46610/Jcscs.2023.V02i01.003.
10. R. Ashar, “Analysis Of Open Website Security Using Owasp And Issaf Methods,” *Jurnal Informasi Dan Teknologi*, Pp. 187–194, Jun. 2022, Doi: 10.37034/Jidt.V4i4.233.