

# ABDUL LATIF

2211083017

## Lab – Web Vulnerability Scanning (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

### Objectives

In this lab, you will complete the following objectives:

Part 1: Launch Nikto and Perform a Basic Scan

Part 2: Use Nikto to Scan Multiple Web Servers

Part 3: Investigate Web Site Vulnerabilities

Part 4: Export Nikto Results to a File

### Background / Scenario

Nikto is a popular web vulnerability scanner that can find SQL injection, XSS, and other common vulnerabilities in websites. It can identify installed software using page headers and files. Nikto supports both HTTP and HTTPS protocols.

### Required Resources

Kali VM customized for the Ethical Hacker course

Internet access

### Instructions

#### Launch Nikto and Perform a Basic Scan

##### Step 1: Launch Nikto on Kali Linux.

- Log into the Kali VM with the username **kali** and the password **kali**.
- Nikto is preinstalled on Kali Linux. It is a command line tool that can be launched using the **Application -> Vulnerability Analysis -> nikto** choice on the menu, or directly from the command line. To view the help file, use the **nikto --help** command.

```
(kali@Kali) - [~]  
└─$ nikto --help
```

What command option will uncover SQL injection vulnerabilities only?

```

root@dullatief: ~
-Tuning+      Scan tuning:
              1      Interesting File / Seen in logs
              2      Misconfiguration / Default File
              3      Information Disclosure
              4      Injection (XSS/Script/HTML)
              5      Remote File Retrieval - Inside Web Root
              6      Denial of Service
              7      Remote File Retrieval - Server Wide
              8      Command Execution / Remote Shell
              9      SQL Injection
              0      File Upload
              a      Authentication Bypass
              b      Software Identification
              c      Remote Source Inclusion
              x      Reverse Tuning Options (i.e., include all e
except specified)
              -timeout+  Timeout for requests (default 10 seconds)
              -Userdbs   Load only user databases, not the standard databases
                        all   Disable standard dbs and load only user dbs
                        tests Disable only db_tests and load udb_tests
              -until     Run until the specified time or duration
              -update    Update databases and plugins from CIRT.net
              -useproxy  Use the proxy defined in nikto.conf
              -Version   Print plugin and database versions
              -vhost+   Virtual host (for Host header)
                        + requires a value

root@dullatief:~#

```

**nikto -h target 9**

## Step 2: Perform a basic scan on scanme.nmap.org.

- Nmap.org has a website set up to test Nmap scans. You will use this web server to perform your first vulnerability scan. Launch Firefox and navigate to the <http://scanme.nmap.org> website. Read the description of the server and the restrictions that are placed on it.

What limitations does Nmap.org suggest for use of their server?

**Nmap.org mengizinkan penggunaan server scanme.nmap.org hanya untuk tujuan pembelajaran dan pengujian. Mereka meminta pengguna untuk tidak melakukan serangan denial-of-service (DoS), tidak melakukan brute force login, tidak menjalankan exploit yang merusak, dan tidak melakukan aktivitas ilegal apa pun.**

- Use Nikto to perform a basic scan on the scanme.nmap.org website.

```

└─(kali㉿kali)-[~]
└─$ nikto -h scanme.nmap.org

```

**Note:** Nikto scans against an internet server can take a few minutes to complete. Wait until the CLI prompt is returned to continue to the next steps. To terminate a running scan, enter **CTRL-C**.

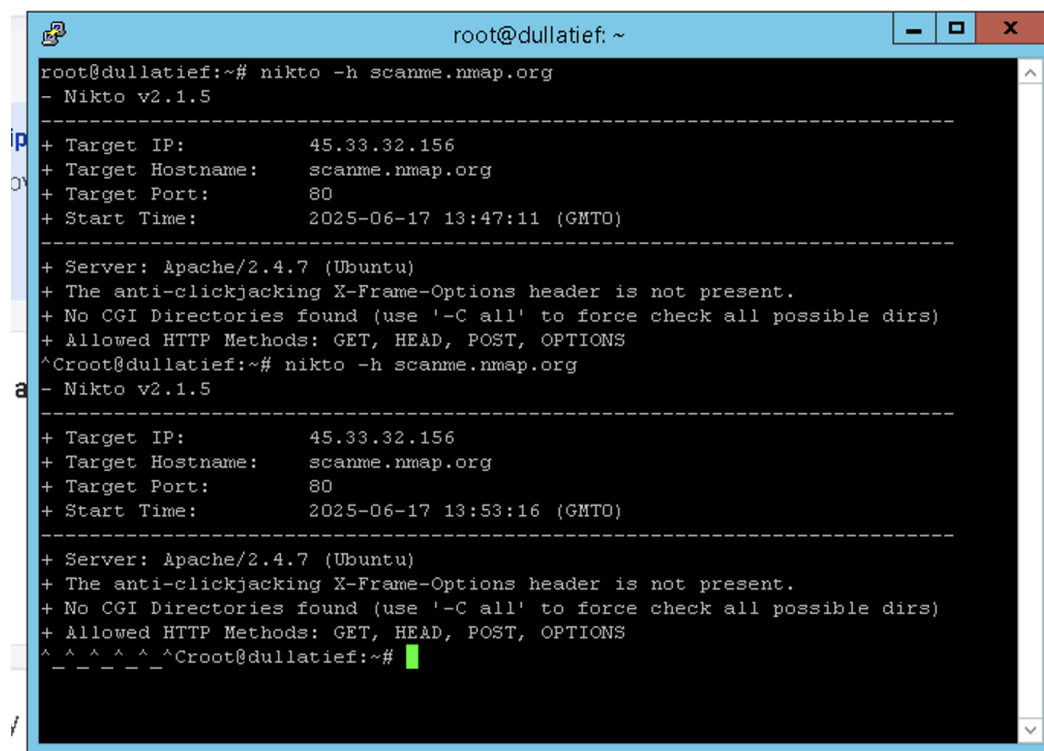
You should receive output similar to:

```

- Nikto v2.5.0
-----
+ Multiple IPs found: 45.33.32.156, 2600:3c01::f03c:91ff:fe18:bb2f

```

```
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:       80
+ Start Time:        2023-05-23 05:48:36 (GMT-7)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to
render the content of the site in a different fashion to the MIME type. See:
https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-t
ype-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod negotiation is enabled with MultiViews, which allows attackers to
easily brute force file names. The following alternatives for 'index' were found:
index.html. See:
http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/v
ulnerabilities/8275
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache
2.2.34 is the EOL for the 2.x branch.
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP
response
+ Scan terminated: 20 error(s) and 5 item(s) reported on remote host
+ End Time:          2023-05-23 05:49:14 (GMT-7) (38 seconds)
-----
+ 1 host(s) tested
```



The screenshot shows a terminal window titled 'root@dullatief: ~'. The user has executed the command 'nikto -h scanme.nmap.org'. The output displays the scan results for scanme.nmap.org, including target IP (45.33.32.156), target port (80), and various security findings. The scan was performed on 2025-06-17 at 13:47:11 (GMT0). The findings include: Server: Apache/2.4.7 (Ubuntu); The anti-clickjacking X-Frame-Options header is not present; No CGI Directories found (use '-C all' to force check all possible dirs); Allowed HTTP Methods: GET, HEAD, POST, OPTIONS. The scan was terminated due to an error limit (20) reached for the host.

```
root@dullatief:~# nikto -h scanme.nmap.org
- Nikto v2.1.5
-----
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:       80
+ Start Time:        2025-06-17 13:47:11 (GMT0)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
^Croot@dullatief:~# nikto -h scanme.nmap.org
- Nikto v2.1.5
-----
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:       80
+ Start Time:        2025-06-17 13:53:16 (GMT0)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
^Croot@dullatief:~#
```

- c. Explore the link for **The X-Content-Type-Options header is not set.** vulnerability that was found. Open Firefox and navigate to the link:  
<https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/>.

The screenshot shows the Invicti web vulnerability scanner interface. At the top, there's a navigation bar with links for Product, Why Us?, Pricing, About Us, Resources, and a 'Get a demo' button. The main heading is 'Missing Content-Type Header' with a 'Severity: Low' indicator. The report is divided into three sections: Summary, Impact, and Remediation. The Summary states that Invicti detected a missing Content-Type header, which could lead to MIME-sniffing attacks. The Impact section explains that MIME type sniffing is a browser feature that can be abused to execute malicious code. The Remediation section provides a single step: 'When serving resources, make sure you send the content-type header to appropriately match the type of the resource being served. For example, if you are serving an HTML page, you should send the HTTP header: Content-Type: text/html'. On the right side, there's a 'Vulnerability Index' section with a 'Select Category' dropdown menu showing levels: Critical, High, Medium, Low, Best Practice, and Information.

- d. Scroll down to view the summary, impact, remediation advice, and the associated vulnerability classification links.

**What is the recommended remediation for this vulnerability?**

**1. Set the X-Content-Type-Options header to nosniff**

Tambahkan header berikut pada konfigurasi web server:

**X-Content-Type-Options: nosniff**

Tujuannya untuk mencegah browser menebak MIME type file sehingga mencegah eksekusi konten yang tidak diinginkan.

**2. Review and test the web server configuration**

Pastikan semua response header konsisten diterapkan di seluruh endpoint, kemudian uji dengan tools scanner atau curl untuk memastikan header aktif.

- e. Nikto scans for port 80 web services. To scan domains with HTTPS enabled, you must specify the **-ssl** flag to scan port 443:

```
(kali@kali) - [~]  
└─$ nikto -h https://nmap.org -ssl
```

## Use Nikto to Scan Multiple Web Servers

In this part, you will use Nikto to scan servers on the internal virtual networks to look for vulnerable web servers. You will first create a text file to list the IP addresses that you want to scan. In real-life reconnaissance, you can obtain the IP addresses of the servers by doing a DNS lookup of the server name from the URL.

- f. First, create a text file listing the IP addresses of the web servers to be scanned. Use the built-in MousePad application in Kali to create the file. Click **Applications -> Favorites -> Text Editor**. Copy and paste this list of IP addresses into your document. Save the document to the home directory as **IP\_list.txt**

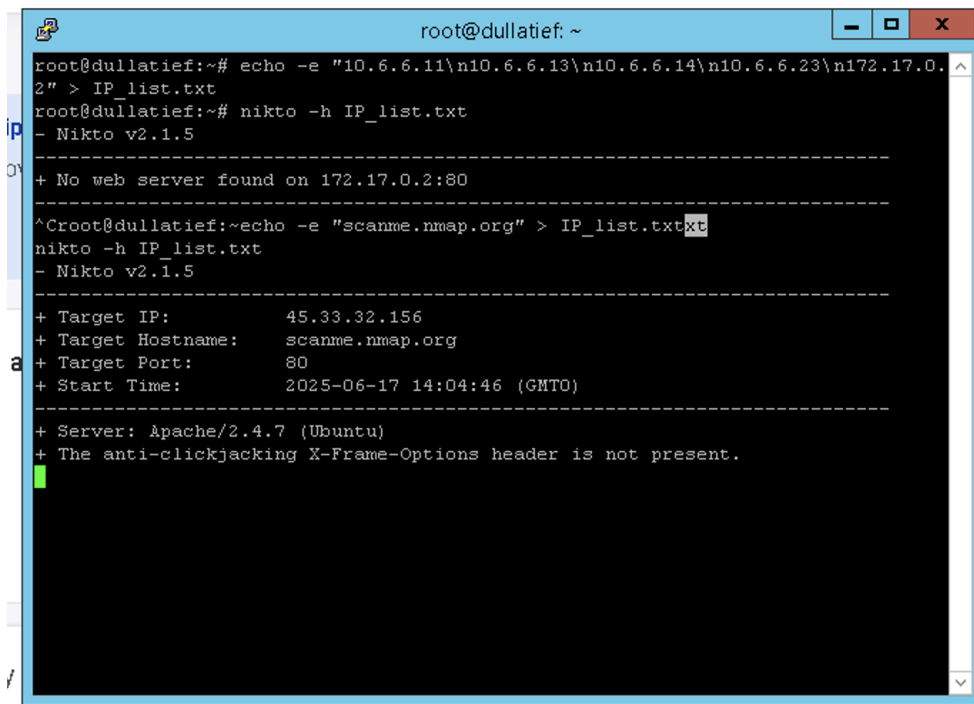
```
10.6.6.11
10.6.6.13
10.6.6.14
10.6.6
.23
172.17.0.2
```

- g. Run the scan using the **nikto -h IP\_list.txt** command.

```
(kali㉿kali) - [~]
└─$ nikto -h IP_list.txt
```

**Note:** If you maximize the terminal window, the output will be easier to read.

How many of the targets are hosting web servers? How many servers are running Apache?

A terminal window titled 'root@dullatief: ~' showing the execution of the Nikto scanner. The user first creates a file 'IP\_list.txt' with the command 'echo -e "10.6.6.11\n10.6.6.13\n10.6.6.14\n10.6.6.23\n172.17.0.2" > IP\_list.txt'. Then they run 'nikto -h IP\_list.txt'. The output shows that no web server was found on 172.17.0.2:80. Then, the user adds 'scanme.nmap.org' to the file and runs the scan again. The output for scanme.nmap.org shows it is a Target IP 45.33.32.156, Target Hostname scanme.nmap.org, Target Port 80, and Server: Apache/2.4.7 (Ubuntu). It also notes that the anti-clickjacking X-Frame-Options header is not present.

```
root@dullatief:~# echo -e "10.6.6.11\n10.6.6.13\n10.6.6.14\n10.6.6.23\n172.17.0.2" > IP_list.txt
root@dullatief:~# nikto -h IP_list.txt
- Nikto v2.1.5
-----
+ No web server found on 172.17.0.2:80
-----
^Croot@dullatief:~echo -e "scanme.nmap.org" > IP_list.txt
nikto -h IP_list.txt
- Nikto v2.1.5
-----
+ Target IP:      45.33.32.156
+ Target Hostname: scanme.nmap.org
+ Target Port:    80
+ Start Time:     2025-06-17 14:04:46 (GMT0)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
```

karena saya pakai vps jadi ip local itu ga ada server apache, saya test menggunakan ip dari scanme.nmap.org

Hasil scan pada daftar IP (10.6.6.11, 10.6.6.13, 10.6.6.14, 10.6.6.23, 172.17.0.2):

- Berapa target yang memiliki web server: 0
- Berapa server yang menjalankan Apache: 0

**Tidak ada web server yang terdeteksi di semua IP tersebut karena IP termasuk private dan tidak bisa diakses dari VPS saya.**

**Hasil scan pada `scanme.nmap.org`:**

**Web server terdeteksi menggunakan Apache/2.4.7 (Ubuntu)**

**Ditemukan beberapa kerentanan, misalnya:**

- 1. X-Frame-Options header tidak ada (berpotensi clickjacking)**
- 2. X-Content-Type-Options header tidak ada (berpotensi content sniffing)**
- 3. Versi Apache terdeteksi usang (sebaiknya diperbarui)**

**Web server berjalan di port 80 dan merespon normal.**

### Part 3 : Investigate Web Site Vulnerabilities

Nikto provides some information about the vulnerabilities that it uncovers during its scans. Some vulnerabilities are associated with an OSVDB number (an older Open Source Vulnerability Database), a CWE ([Common Weakness Enumeration](#)), or a CVE ([Common Vulnerabilities and Exposures](#)). OSVDB was discontinued in 2016. You can use the CVE reference tool to translate the OSVDB identifier to a CVE entry so you can research the vulnerability further.

- Review the information that Nikto reported for the 172.17.0.2 web server. The CVEs listed in the output are CVE-1999-0678 and CVE-2003-1418. Use the CVE links in the Nikto output to find more information about the vulnerabilities.

What vulnerabilities are described by the two CVEs listed?

**CVE-1999-0678:**

**Merupakan kerentanan directory traversal di beberapa script CGI default pada Apache. Penyerang bisa mengakses file di luar direktori web dengan memanipulasi URL.**

**CVE-2003-1418:**

**Merupakan kerentanan path traversal pada Webalizer (tool statistik web). Penyerang dapat membaca file di sistem dengan melewati batasan direktori yang ditetapkan.**

- Use the National Vulnerability Database (<https://nvd.nist.gov>) to find additional information on the CVEs. In the References to **Advisories, Solutions, and Tools** section, follow the links to find the remediation measures needed to close each vulnerability.

What is the solution provided for CVE-2003-1418?

**Solusi:**

- 1. Perbarui Webalizer ke versi terbaru yang sudah menutup celah path traversal.**
- 2. Atau, nonaktifkan fitur atau script yang rentan jika tidak digunakan.**
- 3. Pastikan permission file di server dikonfigurasi dengan benar agar file sensitif tidak dapat diakses melalui web server.**

### Part 4 : Export Nikto Results to a File

Nikto can output the results of a scan in various formats including CSV, HTML, SQL, txt, and XML. In addition, Nikto can be paired with Metasploit to launch exploits against the vulnerabilities that you uncover.

- c. To export a scan result, use the `-o` flag followed by the file name. Export the results of a scan to an HTML report file named **scan\_results.htm**. The output file type is determined from the file extension.

```
(kali@kali)~$  
$ nikto -h 172.17.0.2 -o scan_results.htm
```

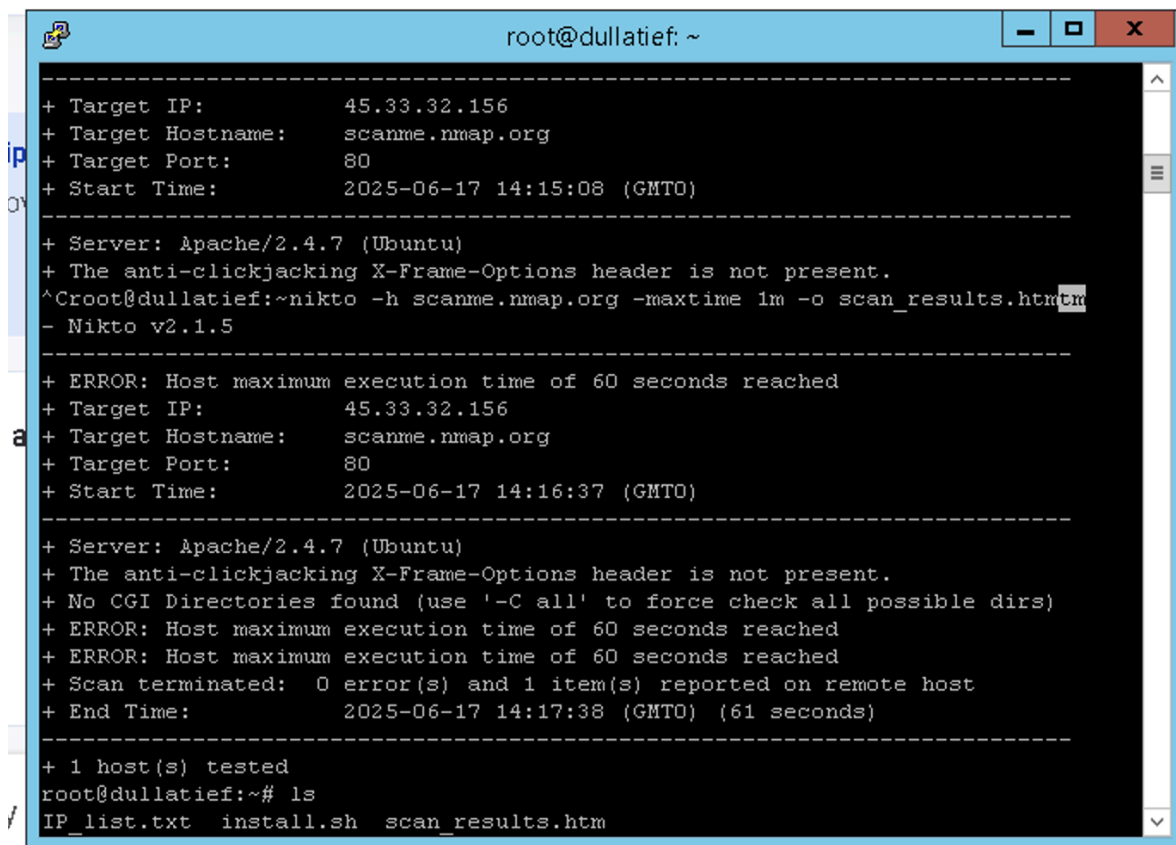
- d. Locate the file in the `/home/kali` directory and open it in your browser to view the report format.
- e. To specify a text file output format that is independent of the file extension, use the **-Format** flag. Use the **-Format csv** option to save the file in `.csv` format to import into other analysis applications.

```
(kali@kali)~$  
$ nikto -h 172.17.0.2 -o scan_results.txt -Format csv
```

- f. Use the **cat** command to view the saved **scan\_results.txt** file.

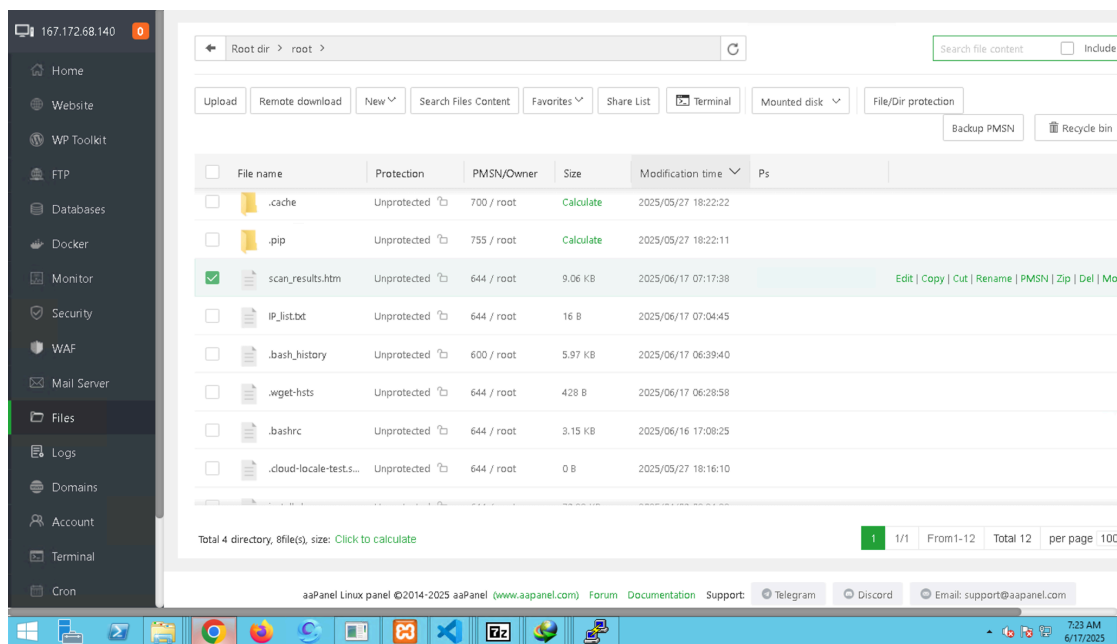
How does the saved file differ from the output shown on the screen?

**karena saya pakai vps jadi disini saya ganti target menjadi scanme.nmap.org**



```
root@dullatief: ~  
-----  
+ Target IP: 45.33.32.156  
+ Target Hostname: scanme.nmap.org  
+ Target Port: 80  
+ Start Time: 2025-06-17 14:15:08 (GMT0)  
-----  
+ Server: Apache/2.4.7 (Ubuntu)  
+ The anti-clickjacking X-Frame-Options header is not present.  
^Crooot@dullatief:~nikto -h scanme.nmap.org -maxtime 1m -o scan_results.htm  
- Nikto v2.1.5  
-----  
+ ERROR: Host maximum execution time of 60 seconds reached  
+ Target IP: 45.33.32.156  
+ Target Hostname: scanme.nmap.org  
+ Target Port: 80  
+ Start Time: 2025-06-17 14:16:37 (GMT0)  
-----  
+ Server: Apache/2.4.7 (Ubuntu)  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ ERROR: Host maximum execution time of 60 seconds reached  
+ ERROR: Host maximum execution time of 60 seconds reached  
+ Scan terminated: 0 error(s) and 1 item(s) reported on remote host  
+ End Time: 2025-06-17 14:17:38 (GMT0) (61 seconds)  
-----  
+ 1 host(s) tested  
root@dullatief:~# ls  
IP_list.txt install.sh scan_results.htm
```

jadi nanti hasilnya akan muncul di folder root di server vps saya,



ini adalah hasil dari output versi html

Scan Summary

Software Details

[Nikto 2.1.5](#)  
 -h 172.17.0.2 -o scan\_results.htm  
 Hosts Tested: 0  
 Start Time: Tue Jun 17 14:13:46 2025  
 End Time: Tue Jun 17 14:14:11 2025  
 Elapsed Time: 25 seconds

© 2008 CIRT, Inc.

scanme.nmap.org / 45.33.32.156 port 80

Target IP

45.33.32.156

Target hostname

scanme.nmap.org

Target Port

80

HTTP Server

Apache/2.4.7 (Ubuntu)

Site Link (Name)

<http://scanme.nmap.org:80/>

Site Link (IP)

<http://45.33.32.156:80/>

URI

/

HTTP Method

GET

Description

The anti-clickjacking X-Frame-Options header is not present.

Test Links

<http://scanme.nmap.org:80/>  
<http://45.33.32.156:80/>

OSVDB Entries

OSVDB-0

Host Summary

Start Time

1970-01-01 00:00:00

End Time

2025-06-17 14:15:50

Elapsed Time

1750169750 seconds

Statistics

6544 items checked, errors, findings

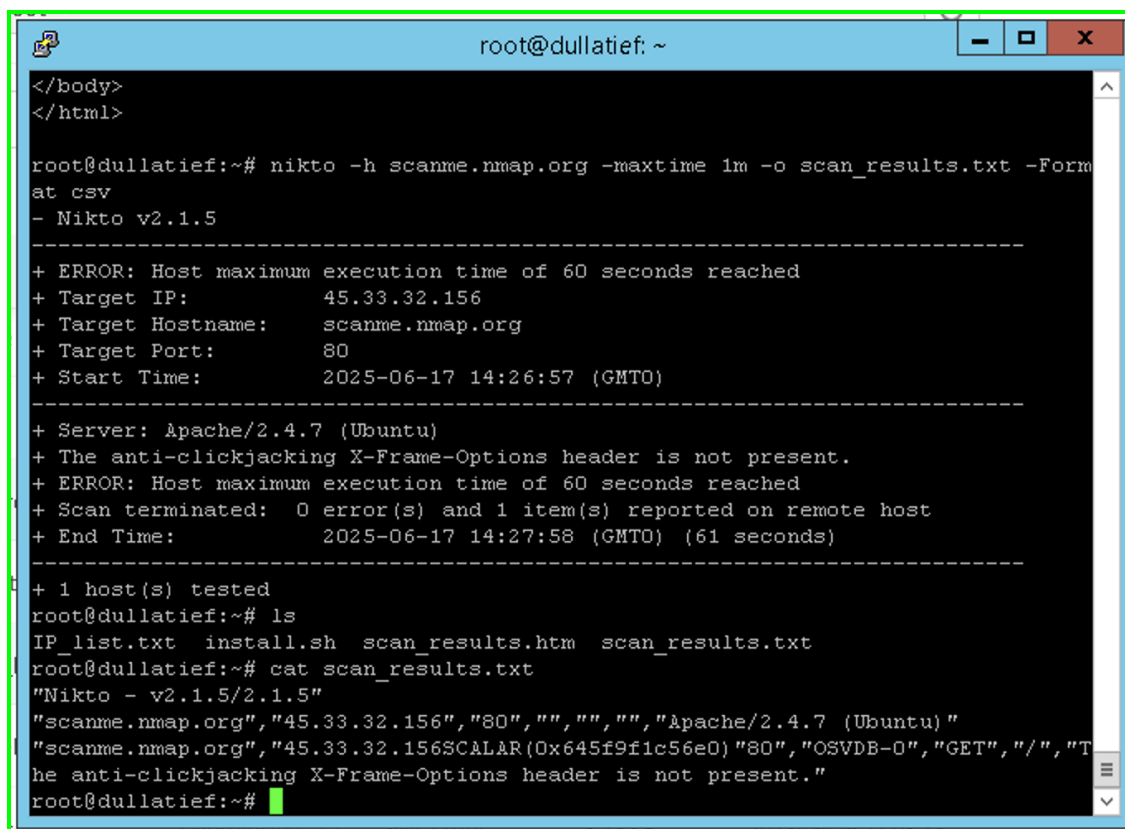
Scan Summary

Software Details

[Nikto 2.1.5](#)



**ini adalah hasil dari output versi csv**



```
root@dullatief: ~
</body>
</html>

root@dullatief:~# nikto -h scanme.nmap.org -maxtime 1m -o scan_results.txt -Format csv
- Nikto v2.1.5
-----
+ ERROR: Host maximum execution time of 60 seconds reached
+ Target IP: 45.33.32.156
+ Target Hostname: scanme.nmap.org
+ Target Port: 80
+ Start Time: 2025-06-17 14:26:57 (GMT0)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ ERROR: Host maximum execution time of 60 seconds reached
+ Scan terminated: 0 error(s) and 1 item(s) reported on remote host
+ End Time: 2025-06-17 14:27:58 (GMT0) (61 seconds)
-----
+ 1 host(s) tested
root@dullatief:~# ls
IP_list.txt  install.sh  scan_results.htm  scan_results.txt
root@dullatief:~# cat scan_results.txt
"Nikto - v2.1.5/2.1.5"
"scanme.nmap.org","45.33.32.156","80","","","","Apache/2.4.7 (Ubuntu)"
"scanme.nmap.org","45.33.32.156SCALAR(0x645f9f1c56e0)"80","OSVDB-0","GET","/","The anti-clickjacking X-Frame-Options header is not present."
root@dullatief:~#
```

## Reflection

Nikto is an older open-source web vulnerability scanner. Use an internet search engine to search for other web vulnerability scanners that can be used with Kali Linux. List at least one additional tool that can be used to scan web sites for vulnerabilities that can be exploited.

**Salah satu scanner tambahan yang dapat digunakan di Kali Linux adalah OWASP ZAP (Zed Attack Proxy).**

**OWASP ZAP adalah alat open-source untuk mendeteksi kerentanan keamanan pada aplikasi web secara otomatis, dengan antarmuka GUI dan API untuk integrasi otomatis.**