

## Tahap Reconnaissance and Digital Footprinting

Target IP: 167.172.75.216

nmap

```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)-[~]  
$ nmap -Pn -T4 -A -v -oN nmapip.log 167.172.75.216  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 09:17 EDT  
NSE: Loaded 156 scripts for scanning.  
NSE: Script Pre-scanning.  
Initiating NSE at 09:17  
Completed NSE at 09:17, 0.00s elapsed  
Initiating NSE at 09:17  
Completed NSE at 09:17, 0.00s elapsed  
Initiating NSE at 09:17  
Completed NSE at 09:17, 0.00s elapsed  
Initiating Parallel DNS resolution of 1 host. at 09:17  
Completed Parallel DNS resolution of 1 host. at 09:17, 0.39s elapsed  
Initiating Connect Scan at 09:17  
Scanning 167.172.75.216 [1000 ports]  
Discovered open port 1723/tcp on 167.172.75.216  
Discovered open port 22/tcp on 167.172.75.216  
Discovered open port 21/tcp on 167.172.75.216  
Discovered open port 80/tcp on 167.172.75.216  
Completed Connect Scan at 09:17, 10.84s elapsed (1000 total ports)  
Initiating Service scan at 09:17  
Scanning 4 services on 167.172.75.216  
Completed Service scan at 09:17, 6.13s elapsed (4 services on 1 host)  
NSE: Script scanning 167.172.75.216.  
Initiating NSE at 09:17  
Completed NSE at 09:17, 5.14s elapsed  
Initiating NSE at 09:17  
Completed NSE at 09:17, 0.41s elapsed  
Initiating NSE at 09:17  
Completed NSE at 09:17, 0.00s elapsed  
Nmap scan report for 167.172.75.216  
Host is up (0.025s latency).  
Not shown: 996 filtered tcp ports (no-response)  
PORT      STATE SERVICE VERSION  
21/tcp    open  tcpwrapped  
1723/tcp  open  tcpwrapped
```

Gobuster

```
(kali@kali)-[~]  
$ gobuster dir -u http://167.172.75.216/ -w /home/kali/pentest/SecLists/Discovery/Web-Content/common.txt -o gobuster.log  
Gobuster v3.6  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
[+] Url: http://167.172.75.216/  
[+] Method: GET  
[+] Threads: 10  
[+] Wordlist: /home/kali/pentest/SecLists/Discovery/Web-Content/common.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.6  
[+] Timeout: 10s  
Starting gobuster in directory enumeration mode  
/Login (Status: 200) [Size: 905]  
/css (Status: 301) [Size: 173] [→ /css/]  
/dashboard (Status: 302) [Size: 28] [→ /login]  
/js (Status: 301) [Size: 171] [→ /js/]  
/login (Status: 200) [Size: 905]  
/logout (Status: 302) [Size: 28] [→ /login]  
/profile (Status: 302) [Size: 28] [→ /login]  
/register (Status: 200) [Size: 1399]  
Progress: 4727 / 4727 (100.00%)  
Finished
```

## Nuclei

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)~  
$ nuclei -u http://167.172.75.216/ -o nuclei.txt  
  
v3.2.7  
projectdiscovery.io  
[INF] Current nuclei version: v3.2.7 (outdated) [see options]  
[INF] Current nuclei-templates version: v9.8.7 (latest)  
[WRN] Scan results upload to cloud is disabled. [info] [info] invalid floating-point values: 0.0000000000000000e+000  
[INF] New templates added in latest release: 62  
[INF] Templates loaded for current scan: 8021  
[INF] Executing 8021 signed templates from projectdiscovery/nuclei-templates  
[INF] Targets loaded for current scan: 1  
[INF] Templates clustered: 1510 (Reduced 1432 Requests)  
[INF] Using Interactsh Server: oast.site  
[node-express-dev-env] [http] [medium] http://167.172.75.216/  
[options-method] [http] [info] http://167.172.75.216/ ["GET,HEAD"]  
[tech-detect:express] [http] [info] http://167.172.75.216/  
[http-missing-security-headers:x-content-type-options] [http] [info] http://167.172.75.216/  
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://167.172.75.216/  
[http-missing-security-headers:referrer-policy] [http] [info] http://167.172.75.216/  
[http-missing-security-headers:clear-site-data] [http] [info] http://167.172.75.216/  
[http-missing-security-headers:strict-transport-security] [http] [info] http://167.172.75.216/  
[http-missing-security-headers:content-security-policy] [http] [info] http://167.172.75.216/  
[http-missing-security-headers:permissions-policy] [http] [info] http://167.172.75.216/  
[http-missing-security-headers:x-frame-options] [http] [info] http://167.172.75.216/  
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://167.172.75.216/  
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://167.172.75.216/  
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://167.172.75.216/  
[ssh-auth-methods] [javascript] [info] 167.172.75.216:22 [{"publickey","password"}] token: Do you
```

## Uji SQLI

sqlmap -u "http://167.172.75.216/profile"

--cookie="auth\_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFrdW51bnR1a2VoliwiaWF0IjoxNzE2OTY4Mzg3fQ.tH2Leh9Z08TtUU2t-7UGZ-0iVvk4Dvax0QXTY8xjjWuc; username=akununtukeh" --delay 60 --schema --batch

```
kali@kali: ~  
File Actions Edit View Help  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal  
. It is the end user's responsibility to obey all applicable local, state and federal laws. Develop  
ers assume no liability and are not responsible for any misuse or damage caused by this program  
[*] starting @ 09:14:55 /2024-05-31/  
[09:14:55] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.c  
om/article.php?id=1') and without providing any POST parameters through option '--data'  
do you want to try URI injections in the target URL itself? [Y/n/q] Y  
Cookie parameter 'auth_token' appears to hold anti-CSRF token. Do you want sqlmap to automatically  
update it in further requests? [y/N] N  
[09:14:55] [INFO] testing connection to the target URL  
got a 302 redirect to 'http://167.172.75.216/login'. Do you want to follow? [Y/n] Y  
[09:15:55] [INFO] testing if the target URL content is stable  
[09:16:55] [WARNING] URI parameter '#1*' does not appear to be dynamic  
[09:17:55] [WARNING] heuristic (basic) test shows that URI parameter '#1*' might not be injectable  
[09:18:55] [INFO] testing for SQL injection on URI parameter '#1*'  
[09:18:55] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'  
[09:28:56] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'  
[09:30:56] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY claus  
e (EXTRACTVALUE)'  
[09:35:56] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'  
[09:40:56] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN  
)'  
[09:45:56] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'  
[09:50:57] [INFO] testing 'Generic inline queries'  
[09:51:57] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'  
[09:55:57] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'  
[09:59:57] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'  
[10:03:57] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'  
[10:08:57] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'  
[10:13:57] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'  
[10:18:58] [INFO] testing 'Oracle AND time-based blind'  
it is recommended to perform only basic UNION tests if there is not at least one other (potential)  
technique found. Do you want to reduce the number of requests? [Y/n] Y  
[10:23:58] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'  
[10:28:59] [WARNING] URI parameter '#1*' does not seem to be injectable  
[10:28:59] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values  
for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some  
kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g  
. '--tamper=space2comment') and/or switch '--random-agent'  
[10:28:59] [WARNING] HTTP error codes detected during run:  
404 (Not Found) - 72 times  
[*] ending @ 10:28:59 /2024-05-31/
```

## Uji XSS

terjadi error ketika password ada petik



### Login

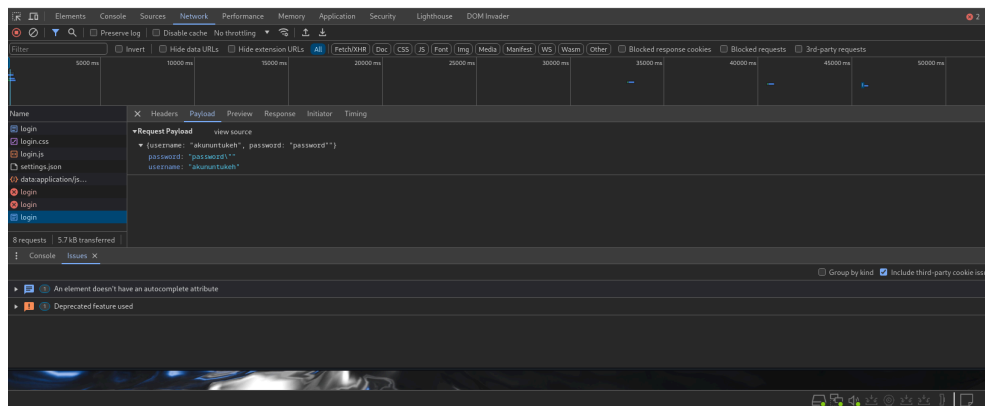
An error occurred. Please try again.

Username:

Password:

[Login](#)

Don't have an account? [Sign up here.](#)



terjadi error ketika username ada petik

### Login

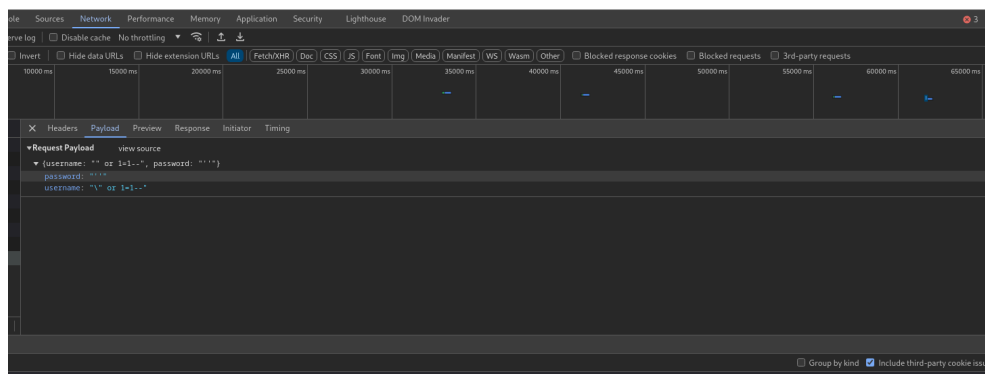
An error occurred. Please try again.

Username:

Password:

[Login](#)

Don't have an account? [Sign up here.](#)



ada error ketika memberikan input simbol

Home Dashboard Logout Contact Support

## Your Profile, akununtukeh

SyntaxError: Unexpected token '<', "<html><hea"... is not valid JSON

Phone:

Credit Card:

Secret Question:

Secret Answer:

Current Password (for verification):

Update Profile

New Password:

Secret Answer:

Change Password