

Laporan Pengerjaan Lab Praktikum Ethical hacking



Nama : Ditya Wahyu Ramadhan
NRP : 502722 1051

Date: May 28th, 2024
Project: lab-3

Daftar ISI

Disclaimer	2
Contact Information	2
Flow	3
Scope	3
Pengecualian Ruang Lingkup	3
Lingkup dan Batasan Waktu	3
Dokumentasi	4

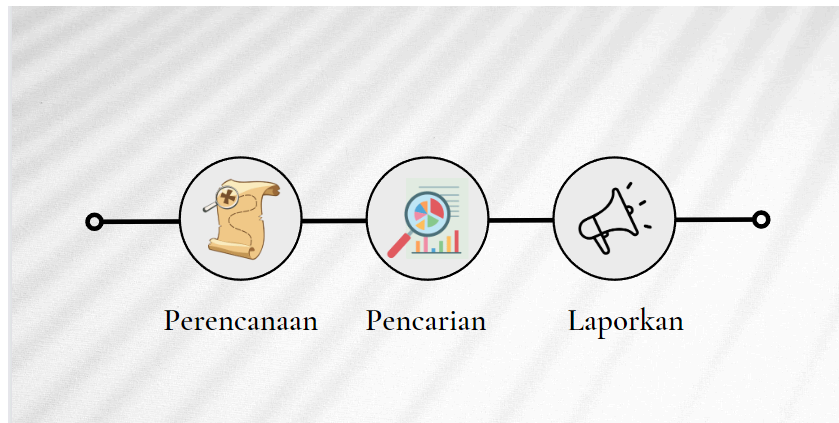
Disclaimer

Pengerjaan Praktikum-3 kali ini dilaksanakan selama periode 5 hari, dimulai dari tanggal 28 Mei hingga 1 juni. Oleh karena itu, saya mengakui bahwa terdapat kemungkinan adanya kesalahan dalam pelaksanaan praktikum ini. Saya dengan tulus memohon maaf atas segala kekurangan yang terjadi.

Contact Information

Name	Title	Contact Information
Peserta		
Ditya Wahyu Ramadhan	Penjaga Toko Lies jaya	Email: dityawahyu783@gmail.com

Flow



Scope

Details
- 167.172.75.216

Pengecualian Ruang Lingkup

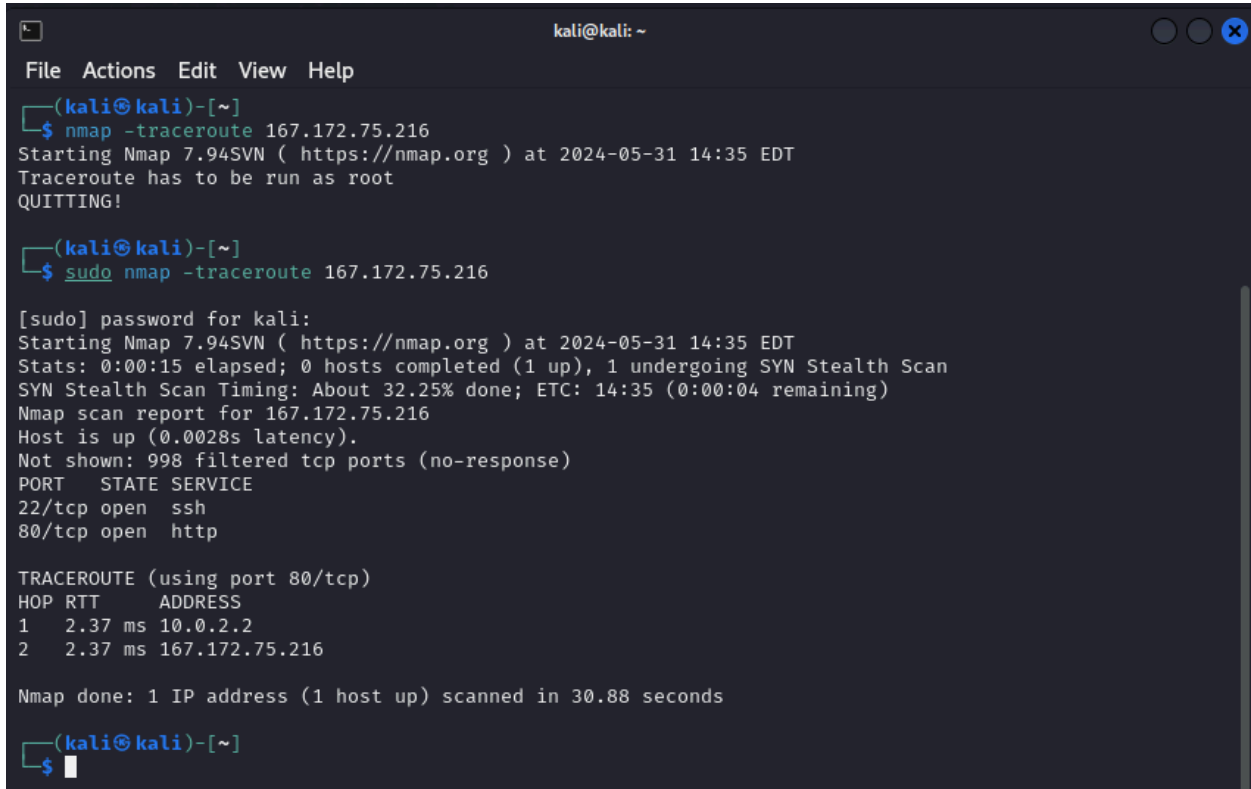
1. Tidak diperbolehkan untuk melakukan serangan yang dapat merusak data atau infrastruktur aplikasi.
2. Tidak diperbolehkan untuk mengeksploitasi kerentanan yang dapat memberikan akses ke server (contoh: RCE, privilege escalation).
3. Hindari serangan DoS/DDoS yang dapat mengganggu ketersediaan layanan aplikasi.

Lingkup dan Batasan Waktu

- 167.172.75.216
- Sabtu, 1 Juni 2024 19:00 WIB

Dokumentasi

Saya menggunakan beberapa cara untuk menggunakan kerentanan untuk yang pertama saya menggunakan nmap



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -traceroute 167.172.75.216  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 14:35 EDT  
Traceroute has to be run as root  
QUITTING!  
  
(kali@kali)-[~]  
$ sudo nmap -traceroute 167.172.75.216  
  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 14:35 EDT  
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 32.25% done; ETC: 14:35 (0:00:04 remaining)  
Nmap scan report for 167.172.75.216  
Host is up (0.0028s latency).  
Not shown: 998 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
  
TRACEROUTE (using port 80/tcp)  
HOP RTT      ADDRESS  
1    2.37 ms   10.0.2.2  
2    2.37 ms   167.172.75.216  
  
Nmap done: 1 IP address (1 host up) scanned in 30.88 seconds  
  
(kali@kali)-[~]  
$
```

Untuk nmap disini tidak menemukan kerentanana apapu hanya dapat melihat port apasaja yang open

```
(kali㉿kali)-[~]
$ nikto -h 167.172.75.216
- Nikto v2.5.0

+ Target IP: 167.172.75.216
+ Target Hostname: 167.172.75.216
+ Target Port: 80
+ Start Time: 2024-05-31 12:20:17 (GMT-4)

+ Server: No banner retrieved
+ /: Retrieved x-powered-by header: Express.
+ /: 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-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: GET, HEAD .
+ /login/: Cookie ; Path created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /login/: This might be interesting.
+ /register/: This might be interesting.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8105 requests: 2 error(s) and 8 item(s) reported on remote host
+ End Time: 2024-05-31 12:28:05 (GMT-4) (468 seconds)

+ 1 host(s) tested
```

Untuk berikutnya saya menggunakan nikto dan di sini menemukan beberapa bagian yang mungkin terdapat kerentanan seperti pada bagian /login dan register yang mungkin dapat dilakukan XSS ataupun SQL Injection .

Lalu selanjut nya saya menggunakan SQLMAP

```
(kali㉿kali)-[~]
$ sqlmap -u http://167.172.75.216/profile --delay=1 --threads=10

[!] 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. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 02:28:38 /2024-06-01/

[02:28:39] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/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
[02:28:56] [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
[02:29:00] [INFO] testing if the target URL content is stable
[02:29:01] [WARNING] URI parameter '#1*' does not appear to be dynamic
[02:29:02] [WARNING] heuristic (basic) test shows that URI parameter '#1*' might not be injectable
[02:29:03] [INFO] testing for SQL injection on URI parameter '#1*'
[02:29:03] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[02:29:13] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[02:29:15] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
```

```
kali@kali: ~  
File Actions Edit View Help  
[02:29:00] [INFO] testing if the target URL content is stable  
[02:29:01] [WARNING] URI parameter '#1*' does not appear to be dynamic  
[02:29:02] [WARNING] heuristic (basic) test shows that URI parameter '#1*' might not be injectable  
[02:29:03] [INFO] testing for SQL injection on URI parameter '#1*'  
[02:29:03] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'  
[02:29:13] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'  
[02:29:15] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'  
[02:29:21] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'  
[02:29:26] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'  
[02:29:31] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'  
[02:29:36] [INFO] testing 'Generic inline queries'  
[02:29:37] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'  
[02:29:41] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'  
[02:29:46] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'  
[02:29:50] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'  
[02:29:55] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'  
[02:30:00] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'  
[02:30:05] [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  
[02:31:35] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'  
[02:31:40] [WARNING] URI parameter '#1*' does not seem to be injectable  
[02:31:40] [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'
```

Pada sqlmap ini saya mencoba beberapa url tetapi hasil dari setiap url masih sama yaitu

```
[02:31:40] [WARNING] URI parameter '#1*' does not seem to be injectable  
[02:31:40] [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'  
[02:31:40] [WARNING] HTTP error codes detected during run:  
404 (Not Found) - 71 times, 408 (Request Timeout) - 1 times
```

Dan saya juga mencoba sqlmap -u "http://167.172.75.216/login" --level=5 --risk=3 --delay=1
Tetapi hingga sekaran jam 18.45 masih tidak selesai dalam melakukan scanning

Selanjutnya saya menggunakan burp suite

Request

	Pretty	Raw	Hex
1	PUT /change_password HTTP/1.1		
2	Host: 167.172.75.216		
3	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:126.0) Gecko/20100101 Firefox/126.0		
4	Accept: */*		
5	Accept-Language: en-US,en;q=0.5		
6	Accept-Encoding: gzip, deflate, br		
7	Referer: http://167.172.75.216/profile		
8	Content-Type: application/json		
9	Content-Length: 82		
10	Origin: http://167.172.75.216		
11	Connection: keep-alive		
12	Cookie: auth_token= eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc2VybmFtZSI6IldvbG9sb2xvbG8iLCJpYXQiOi0jE3MTcyMjExNDh9.r605cvlKHHBD9fv_Sqw1lILkUVaNxkn_i3W6Kuu2Tm8; username=Wololololo		
13	Priority: u=1		
14			
15	{ "new_password": "Wolololll@", "secret_answer": "Wolololll@", "username": "Wololololo" }		

Namun mungkin dengan kecerdasan saya yang mini saya tidak dapat melihat kerentanan yang ada terdapat 1 bagian yang membuat saya tertarik yaitu bagian **token** dan juga **username**