Laporan Pengerjaan Lab Praktikum
Ethical hacking

Nama : Gilang Raya Kurniawan
NRP : 5027221045

Daftar Isi

Disclaimer

Pengerjaan Praktikum 2 kali ini dilaksanakan dalam periode selama tiga hari, dimulai dari tanggal 28 Mei 2024 hingga 1 Juni 2024. Pengerjaan praktikum bertujuan untuk menemukan kerentanan IP web yang di berikan dengan menggunakan prinsip prinsip ethical hacking

Contact Information

Name	Title	Contact Information
Peserta		
Gilang Raya Kurniawan	Mahasiswa Teknologi Informasi Angkatan 2022	Email: gilangraya869@gmail.com

Mengidentifikasi Tingkat Kerentanan

0	0	0	0	0
Critical	High	Moderate	Low	Informational

Penemuan	keparahan	Rekomendasi
Internal Penetration Test		
-	-	-

Context

Anda adalah seorang ahli keamanan yang ditugaskan oleh perusahaan konsultan keamanan SafeGuard Solutions untuk melakukan penetration testing terhadap aplikasi mockup bank yang masih dalam tahap development, yang disebut Jay's Bank. Tujuan dari praktikum ini adalah untuk menemukan kerentanan yang mungkin ada dalam aplikasi dan melaporkannya untuk perbaikan sebelum aplikasi diluncurkan ke publik.

Scope

1. IP Address Aplikasi: 167.172.75.216
2. Semua fungsi aplikasi.
3. Mekanisme akun pengguna dan autentikasi.
4. Antarmuka web dan API.
5. Interaksi database dan proses penanganan data.

Tujuan dan Batasan

1. Anda diizinkan untuk mencari dan mengidentifikasi kerentanan dalam aplikasi Jay's Bank.
2. Fokus pada kerentanan aplikasi seperti SQL injection, XSS, dan authentication/authorization issues.
3. Apabila memungkinkan, kerentanan yang ditemukan dapat di-exploit untuk mengakses akun pengguna lain, tetapi hanya sebatas aplikasi (tidak ke server).

Larangan

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.

Metodologi

1. Gunakan metode non-destruktif dalam testing.
2. Selalu lakukan verifikasi dan validasi atas temuan kerentanan sebelum melaporkannya.
3. Simpan catatan rinci tentang semua langkah yang diambil selama testing.

Rangkuman Kerentanan & Rapor

1. Cara pertama
Coba cek IP address dengan melakukan memasukan command nmap ke terminal kali, nmap --unprivileged -sV -sC -oN nmap1.log -Pn 167.172.75.216

```
┌──(root㉿GRK66-TUF)-[/home/grk]
└─# nmap --unprivileged -sV -sC -oN nmap1.log -Pn 167.172.75.216
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-01 17:15 WIB
Nmap scan report for 167.172.75.216
Host is up (0.085s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE    VERSION
80/tcp  open  http
|_http-title: Home - Jay's Bank
110/tcp open  tcpwrapped
143/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.00 seconds
```

Ternyata tidak ditemukan kerentanan apapun

Cek dengan Nuclei nuclei -u 167.172.75.216 -o grk.txt

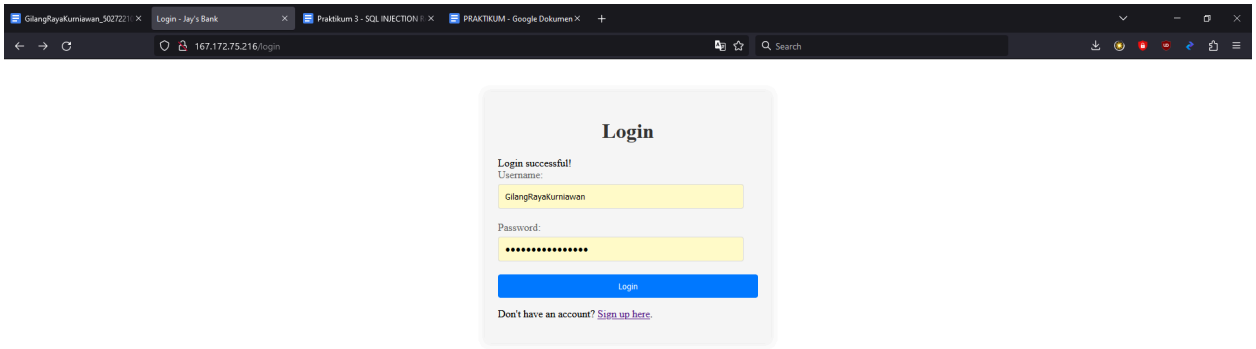
```
┌──(root㉿GRK66-TUF)-[/home/grk]
└─# nuclei -u 167.172.75.216 -o grk.txt

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.2.4

                projectdiscovery.io

[INF] Current nuclei version: v3.2.4 (outdated)
[INF] Current nuclei-templates version: v9.8.7 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 62
[INF] Templates loaded for current scan: 8022
[INF] Executing 8022 signed templates from projectdiscovery/nuclei-templates
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1510 (Reduced 1432 Requests)
[INF] Skipped 167.172.75.216 from target list as found unresponsive 30 times
[INF] No results found. Better luck next time!
```

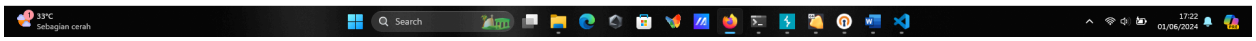
Sama ternyata tidak menemukan kerentanan

2. Cara kedua
Masuk ke website IP tersebut http://167.172.75.216, lalu lakukan register terlebih dahulu, “bisa menggunakan kode seperti di bawah untuk melakukan register”

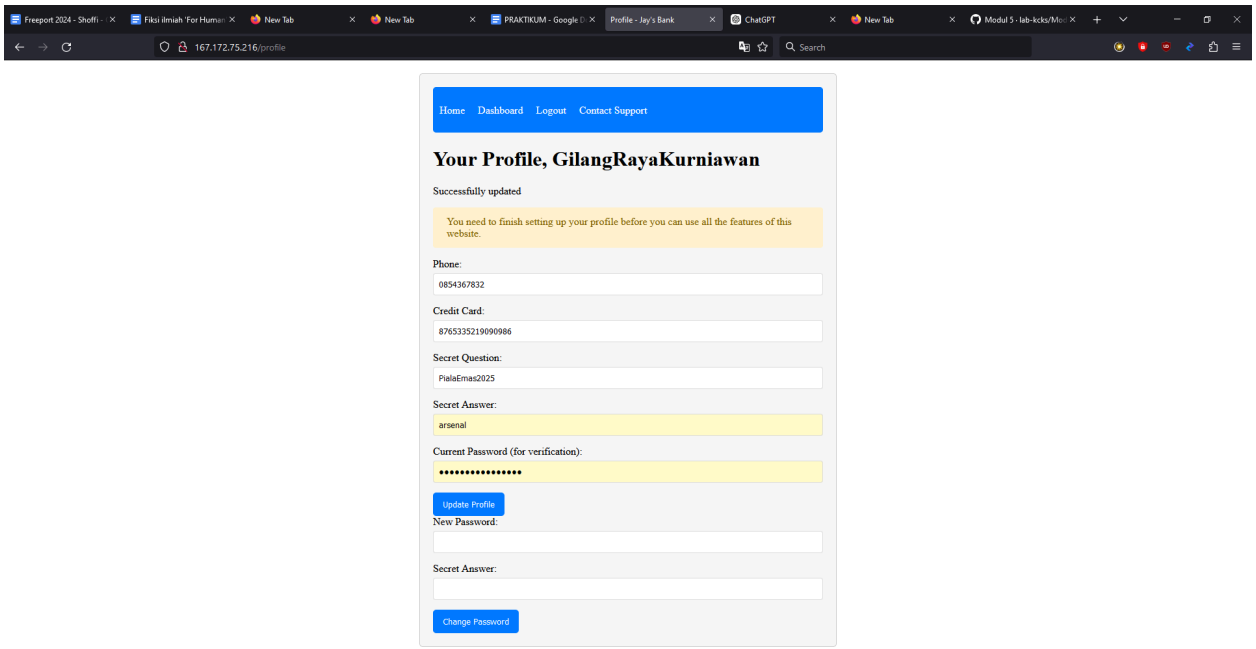
```python
import requests
import json

url = "http://167.172.75.216/register"

data = {
    'username': 'GilangRayaKurniawan',
    'password': 'qwqw1212!@!@QWQW'
}

response = requests.post(url, headers={'Content-Type': 'application/json'}, data=json.dumps(data))

if response.status_code == 200:
    response_data = response.json()
    if response_data.get('success'):
        print("Registration successful!")
    else:
        print(f"Registration failed: {response_data.get('message')}")
else:
    print(f"Registration failed with status code: {response.status_code}")
    print("Response:", response.text)
```

Setelah melakukan register lalu login/masuk pada halaman login web

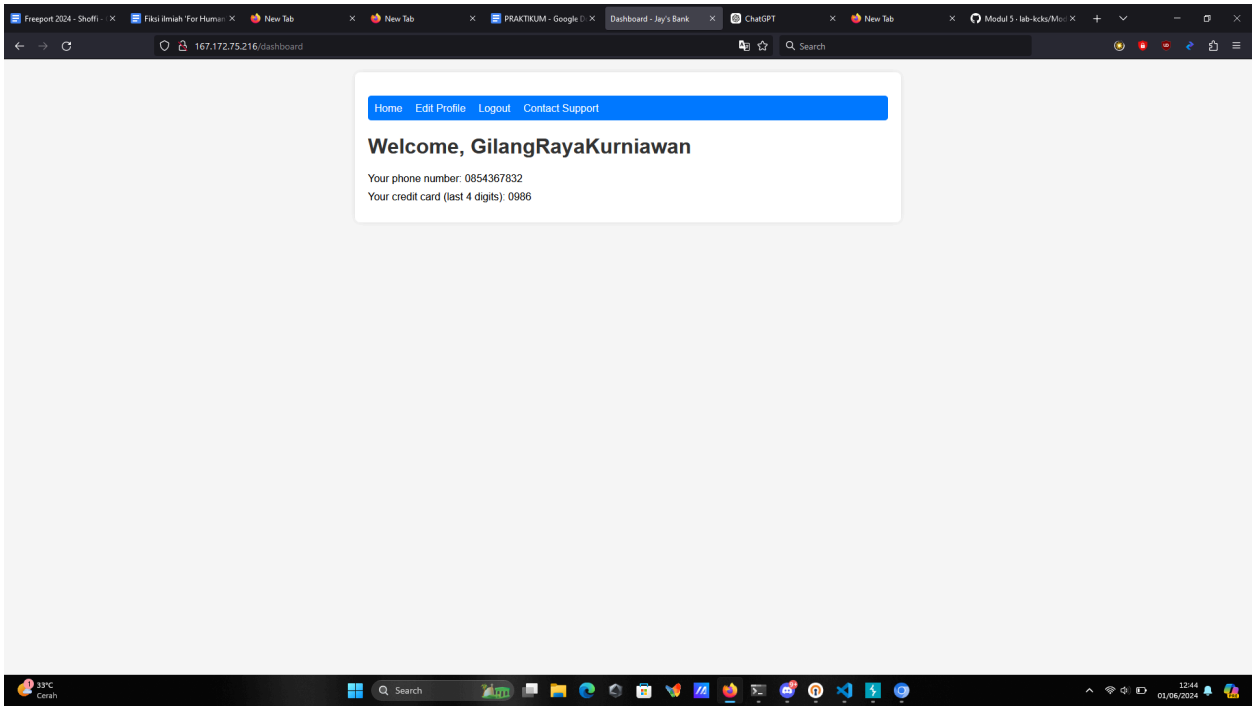




Lalu masuk, saya masukkan data isi tabel tabel sesuai dengan yang anda mau, dengan maksimal jumlah angka nomor telepon 10 dan maksimal nomor kartu kredit 16



Save lalu cek di dashboard, apakah berhasil atau tidak



3. Cara ketiga

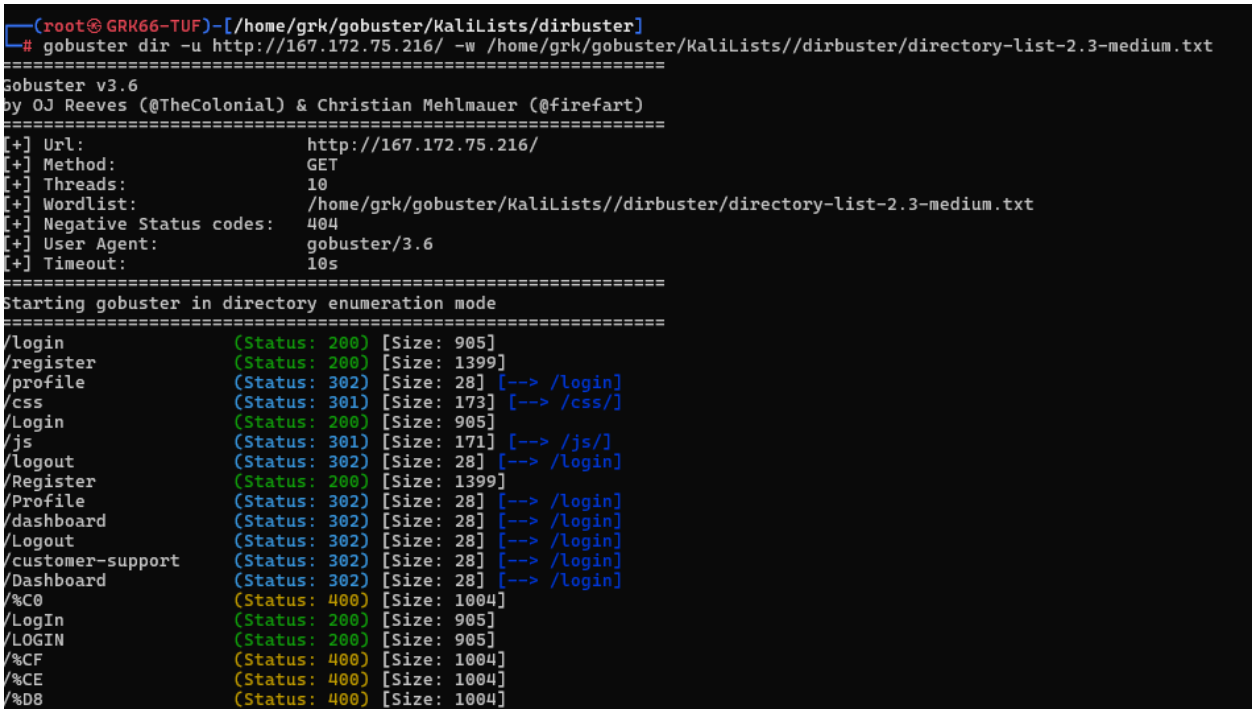
Gunakan SQLmap untuk merekon jenis sql apa saja yang ada pada IP tersebut gunakan command pada terminal parrot sqlmap -u "http://167.172.75.216/login" --level=5 --risk=3 --delay=1, lalu cek (mungkin memerlukan waktu yang lumayan lama karena alat tersebut untuk memetakan database, dan eksploitasi database)

```
┌─[✗]─[parrot@parrot]─[~]
└──╼ $sqlmap -u "http://167.172.75.216/login" --level=5 --risk=3 --delay=1
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.7.2#stable}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 respon
sible for any misuse or damage caused by this program

[*] starting @ 07:25:18 /2024-06-01/

[07:25:18] [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 paramete
rs through option '--data'
do you want to try URI injections in the target URL itself? [Y/n/q] y
[07:25:20] [INFO] testing connection to the target URL
[07:25:21] [INFO] testing if the target URL content is stable
[07:25:22] [INFO] target URL content is stable
```

```
ER BY clause (original value)'
[11:31:55] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY claus
e'
[11:31:57] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY claus
e (original value)'
[11:31:59] [INFO] testing 'Microsoft Access boolean-based blind - ORDER BY, GROU
P BY clause'
[11:32:02] [INFO] testing 'Microsoft Access boolean-based blind - ORDER BY, GROU
P BY clause (original value)'
[11:32:04] [INFO] testing 'SAP MaxDB boolean-based blind - ORDER BY, GROUP BY cl
ause'
[11:32:07] [INFO] testing 'SAP MaxDB boolean-based blind - ORDER BY, GROUP BY cl
ause (original value)'
[11:32:09] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY clause'
[11:32:11] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY clause (origin
al value)'
[11:32:14] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'
[11:33:00] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Stacked queries'
[11:33:31] [INFO] testing 'MySQL < 5.0 boolean-based blind - Stacked queries'
[11:33:31] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'
```

4. Cara ke empat

Menggunakan gobuster dir dengan command, gobuster dir -u http://167.172.75.216/ -w /home/grk/gobuster/KaliLists//dirbuster/directory-list-2.3-medium.txt



Setelah dilakukan recon ternyata ada beberapa endpoint yang mungkin dapat diakses