Jay’s Bank Application

Security Assessment Findings Report

Imam Nurhadi - 5027221046

Date: June 1, 2024

SCOPE

Assesment	Details
Internal Penetration Test	167.172.75.216
Mekanisme	Akun pengguna dan autentikasi
Area	Web API
Interaksi	Databse dan Data handling

Client Allowances

- Anda diizinkan untuk mencari dan mengidentifikasi kerentanan dalam aplikasi Jay’s Bank.
- Fokus pada kerentanan aplikasi seperti SQL injection, XSS, dan authentication/authorization issues.
- Apabila memungkinkan, kerentanan yang ditemukan dapat di-exploit untuk mengakses akun pengguna lain, tetapi hanya sebatas aplikasi (tidak ke server).
- Tidak diperbolehkan untuk melakukan serangan yang dapat merusak data atau infrastruktur aplikasi.
- Tidak diperbolehkan untuk mengeksploitasi kerentanan yang dapat memberikan akses ke server (contoh: RCE, privilege escalation).
- Hindari serangan DoS/DDoS yang dapat mengganggu ketersediaan layanan aplikasi.

SUMMARY

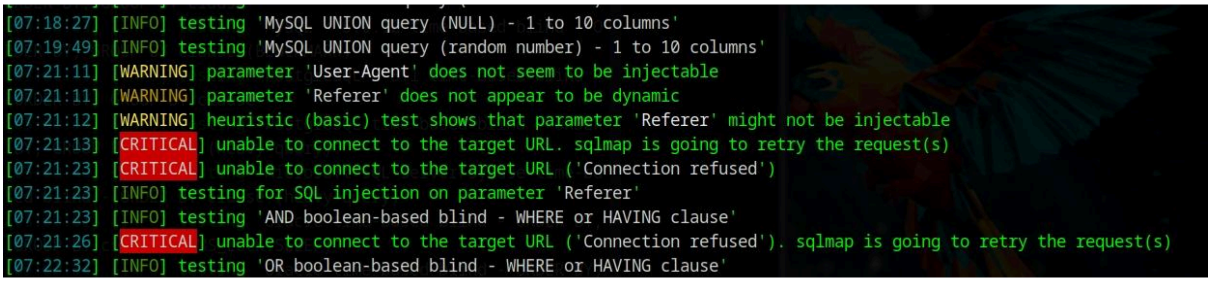
- Scoping atau pentesting dilakukan hingga tanggal 1 Juni 2024 pukul 19.00.
- Beberapa tools yang digunakan dalam reconnaisance antara lain nmap, dirb, dan sqlmap
- Pada IP **167.172.75.216** ditemukan 3 port yaitu: 80, 110, dan 143
- Pada web ditemukan directory diantara lain: login, register, logout, profile, dashboard

Technical Findings

Description:	Tidak ada celah yang bisa dilakukan SQL *injection* berdasarkan hasil *command run* sqlmap -u

	"http://167.172.75.216/login" --level=5 --risk=3 --delay=1
Impact:	None
System:	**167.172.75.216**
References:	

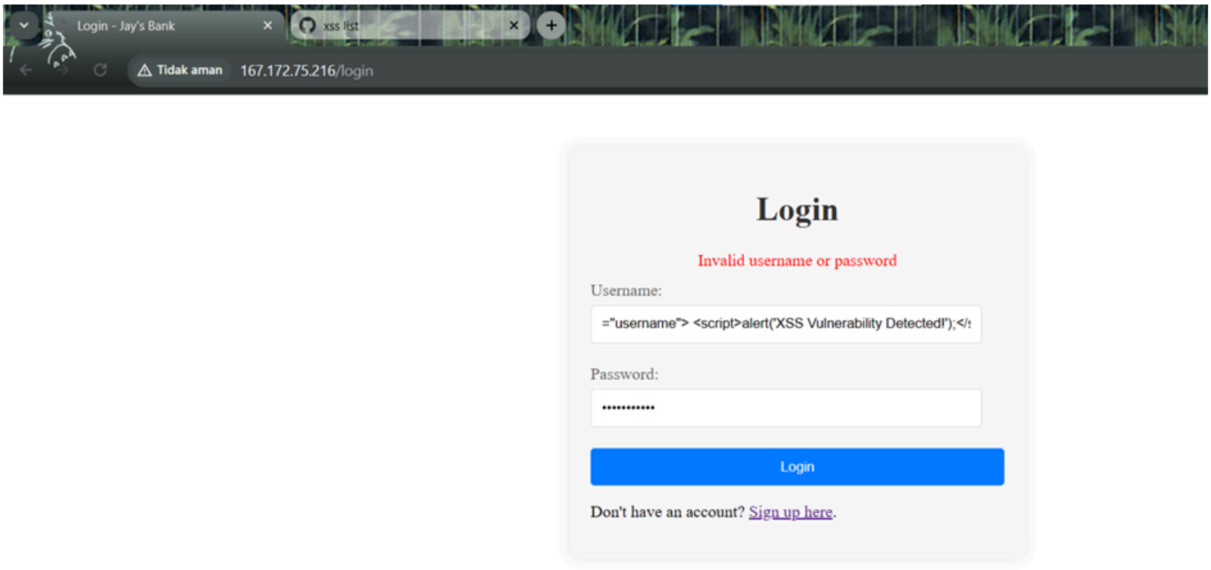
Evidence:



```
[07:18:27] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[07:19:49] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[07:21:11] [WARNING] parameter 'User-Agent' does not seem to be injectable
[07:21:11] [WARNING] parameter 'Referer' does not appear to be dynamic
[07:21:12] [WARNING] heuristic (basic) test shows that parameter 'Referer' might not be injectable
[07:21:13] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[07:21:23] [CRITICAL] unable to connect to the target URL ('Connection refused')
[07:21:23] [INFO] testing for SQL injection on parameter 'Referer'
[07:21:23] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[07:21:26] [CRITICAL] unable to connect to the target URL ('Connection refused'). sqlmap is going to retry the request(s)
[07:22:32] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
```

Description:	Tidak dapat memasukkan script alert terhadap beberapa kolom input untuk memanfaatkan XSS.
Impact:	None
System:	**167.172.75.216**
References:	Modul 10

Evidence:



Login

Invalid username or password

Username:

="username"> <script>alert('XSS Vulnerability Detected!');</:

Password:

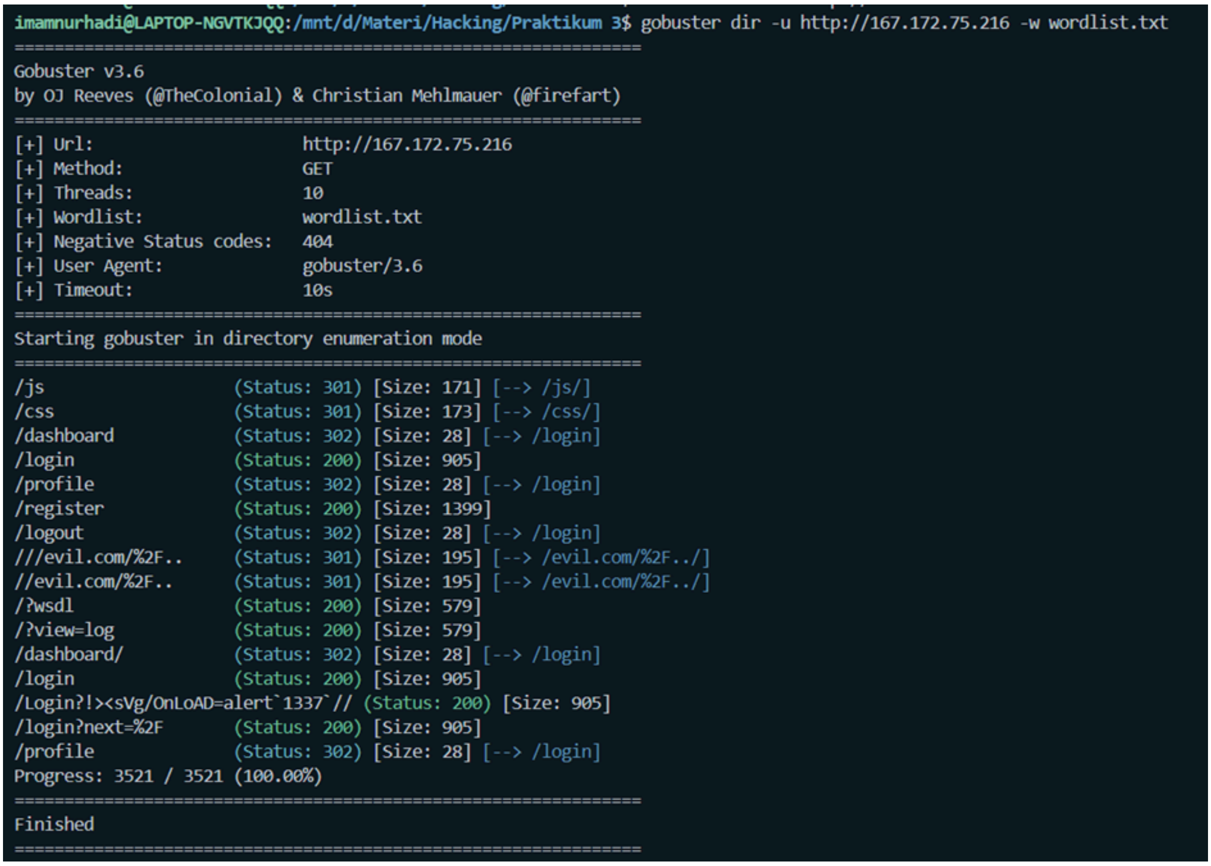
•••••••••••

Login

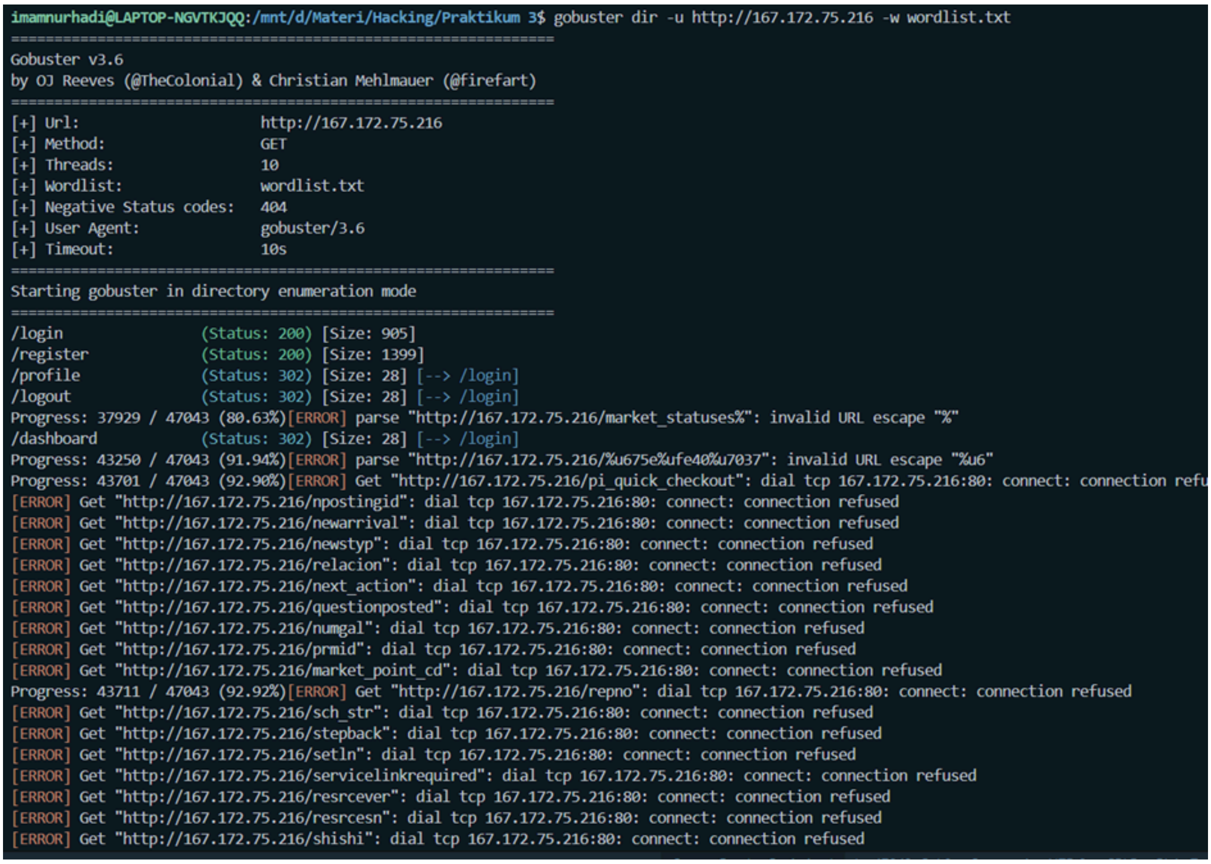
Don't have an account? Sign up here.

Description:	Menemukan jalur respon autentikasi web pada ip **167.172.75.216**
Impact:	None
System:	**167.172.75.216**
References:	

Evidence:



```
imamnurhadi@LAPTOP-NGVTKJQQ:/mnt/d/Materi/Hacking/Praktikum 3$ gobuster dir -u http://167.172.75.216 -w wordlist.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://167.172.75.216
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                wordlist.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/js                   (Status: 301) [Size: 171] [--> /js/]
/css                  (Status: 301) [Size: 173] [--> /css/]
/dashboard            (Status: 302) [Size: 28] [--> /login]
/login                (Status: 200) [Size: 905]
/profile              (Status: 302) [Size: 28] [--> /login]
/register             (Status: 200) [Size: 1399]
/logout               (Status: 302) [Size: 28] [--> /login]
///evil.com/%2F..     (Status: 301) [Size: 195] [--> /evil.com/%2F../]
//evil.com/%2F..      (Status: 301) [Size: 195] [--> /evil.com/%2F../]
/?wsdl                (Status: 200) [Size: 579]
/?view=log            (Status: 200) [Size: 579]
/dashboard/           (Status: 302) [Size: 28] [--> /login]
/login                (Status: 200) [Size: 905]
/Login?!><sVg/OnLoAD=alert`1337`// (Status: 200) [Size: 905]
/login?next=%2F       (Status: 200) [Size: 905]
/profile              (Status: 302) [Size: 28] [--> /login]
Progress: 3521 / 3521 (100.00%)
===============================================================
Finished
===============================================================
```



```
imamnurhadi@LAPTOP-NGVTKJQQ:/mnt/d/Materi/Hacking/Praktikum 3$ gobuster dir -u http://167.172.75.216 -w wordlist.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://167.172.75.216
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                wordlist.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/login                (Status: 200) [Size: 905]
/register             (Status: 200) [Size: 1399]
/profile              (Status: 302) [Size: 28] [--> /login]
/logout               (Status: 302) [Size: 28] [--> /login]
Progress: 37929 / 47043 (80.63%)[ERROR] parse "http://167.172.75.216/market_statuses%": invalid URL escape "%"
/dashboard            (Status: 302) [Size: 28] [--> /login]
Progress: 43250 / 47043 (91.94%)[ERROR] parse "http://167.172.75.216/%u675e%ufe40%u7037": invalid URL escape "%u6"
Progress: 43701 / 47043 (92.90%)[ERROR] Get "http://167.172.75.216/pi_quick_checkout": dial tcp 167.172.75.216:80: connect: connection refu
[ERROR] Get "http://167.172.75.216/npostingid": dial tcp 167.172.75.216:80: connect: connection refused
[ERROR] Get "http://167.172.75.216/newarrival": dial tcp 167.172.75.216:80: connect: connection refused
[ERROR] Get "http://167.172.75.216/newstyp": dial tcp 167.172.75.216:80: connect: connection refused
[ERROR] Get "http://167.172.75.216/relacion": dial tcp 167.172.75.216:80: connect: connection refused
[ERROR] Get "http://167.172.75.216/next_action": dial tcp 167.172.75.216:80: connect: connection refused
[ERROR] Get "http://167.172.75.216/questionposted": dial tcp 167.172.75.216:80: connect: connection refused
[ERROR] Get "http://167.172.75.216/numgal": dial tcp 167.172.75.216:80: connect: connection refused
[ERROR] Get "http://167.172.75.216/prmid": dial tcp 167.172.75.216:80: connect: connection refused
[ERROR] Get "http://167.172.75.216/market_point_cd": dial tcp 167.172.75.216:80: connect: connection refused
Progress: 43711 / 47043 (92.92%)[ERROR] Get "http://167.172.75.216/repno": dial tcp 167.172.75.216:80: connect: connection refused
[ERROR] Get "http://167.172.75.216/sch_str": dial tcp 167.172.75.216:80: connect: connection refused
[ERROR] Get "http://167.172.75.216/stepback": dial tcp 167.172.75.216:80: connect: connection refused
[ERROR] Get "http://167.172.75.216/setln": dial tcp 167.172.75.216:80: connect: connection refused
[ERROR] Get "http://167.172.75.216/servicelinkrequired": dial tcp 167.172.75.216:80: connect: connection refused
[ERROR] Get "http://167.172.75.216/resrcever": dial tcp 167.172.75.216:80: connect: connection refused
[ERROR] Get "http://167.172.75.216/resrcesn": dial tcp 167.172.75.216:80: connect: connection refused
[ERROR] Get "http://167.172.75.216/shishi": dial tcp 167.172.75.216:80: connect: connection refused
```