

Jay's Bank Application Penetration Testing Findings Report

Asadel Naufaleo (5027221009)

Date:
May
31th,
2024

Pernyataan Kerahasiaan

Dokumen ini dibuat oleh Asadel Naufaleo sebagai penguji *pentest* dari Mahasiswa Teknologi Informasi ITS sebagai bagian dari asesmen *Ethical Hacking*. Dokumen ini berisi laporan kerentanan serta celah keamanan dari system *Jay's Bank* dengan izin dan sepengetahuan dari pihak yang terlibat serta mengandung informasi-informasi tertutup dari pihak yang bersedia untuk dijalankan tes ini.

Disclaimer

Penetration Test ini dilakukan dengan *consent* penuh dari pihak yang bersangkutan yaitu *Jay's Bank*. Segala penemuan yang ditemukan oleh penguji telah dimuat dalam dokumen ini sebagai perjanjian awal mengenai kerahasiaan dan sebagai tanda kepatuhan terhadap *MOU* antara kedua pihak.

Contact Information

Nama: Asadel Naufaleo

No.Telp: 5027221009

Email: a.naufaleo@gmail.com

Status: Mahasiswa Teknologi Informasi ITS

Assesment Overview

Tujuan utama dari praktikum ini adalah untuk mengidentifikasi kerentanan dalam infrastruktur Jay's Bank dengan menggunakan prinsip-prinsip Ethical Hacking. Dengan mensimulasikan serangan dunia nyata, penilaian bertujuan untuk mengungkap kelemahan yang dapat dimanfaatkan oleh pihak jahat untuk mengkompromi keamanan dan integritas sistem Jay's Bank.

Fase aktivitas *Penetration Testing* termasuk sebagai berikut:

- Planning – Merencanakan dan mengumpulkan informasi mengenai target.
- Discovery – Melakukan *scanning* dan *enumeration* untuk mendeteksi kemungkinan kerentanan serta celah keamanan pada *website*.
- Attack – Melakukan eksploitasi pada sisi lemah dan celah keamanan yang ada.
- Reporting – Mendokumentasikan semua penemuan kerentanan, hasil eksploitasi, serta semua yang berkaitan dengan informasi *penetration test* yang dilakukan.

Assesment Components

Blackbox Penetration Test

Blackbox Penetration Test adalah tipe *pentest* dimana penguji hanya diberikan informasi yang minim mengenai target atau website yang akan diuji. Pada kasus ini, penguji hanya mendapatkan informasi awal berupa link dari website tersebut. Penguji tidak diberikan info lain selain dari informasi tersebut, sehingga pengujian ini lebih mensimulasikan kondisi yang realistis dimana penyerang dari luar tidak memiliki informasi apapun.

Severity Rating

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.

Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Scope

Assessment	Details
Blackbox Penetration Test	<ul style="list-style-type: none"> 167.172.75.216/

Client Allowances

Pihak yang diuji (*Jay's Bank*) tidak memberikan Batasan mengenai pengujian yang dilakukan, sehingga penguji dapat melakukan metode-metode apapun.

Executive Summary

Penguji telah mengevaluasi kewanaran system *website* Jay's Bank melalui *Penetration Testing* efektif dari tanggal 29 May 2024 sampai 1 Juni 2024. Pada bagian-bagian berikut telah disajikan berbagai ringkasan mengenai penemuan kerentanan, keberhasilan dan kegagalan eksploitasi, juga kelebihan dan kekurangan dari system.

Scoping and Time Limitations

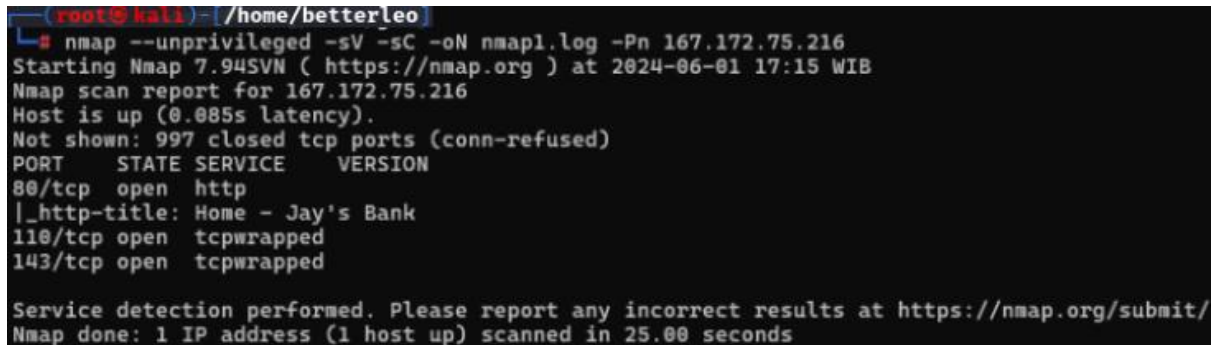
Larangan Tidak diperbolehkan untuk melakukan serangan yang dapat merusak data atau infrastruktur aplikasi. Tidak diperbolehkan untuk mengeksploitasi kerentanan yang dapat memberikan akses ke server (contoh: RCE, privilege escalation). Hindari serangan DoS/DDoS yang dapat mengganggu ketersediaan layanan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

Batas waktu telah ditentukan untuk pengujian. *Blackbox Penetration Testing* telah diizinkan untuk dilakukan selama 5 hari.

Testing Summary

Pengujian menggunakan nmap

Tahap pertama yang dikerjakan adalah mengecek IP address menggunakan nmap di terminal kali dengan command '*nmap --unprivileged -sV -sC -oN nmap1.log -Pn 167.172.75.216*'



```
(root@kali)~# 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         Apache/2.4.18
|_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
```

Sayangnya, dari pengujian tersebut tidak ditemukan celah keamanan.

Pengujian dengan Nuclei

Melakukan pengujian dengan command '*nuclei -u 167.172.75.216 -o leo.txt*'

```
(root@kali)-[/home/betterleo]
# nuclei -u 167.172.75.216 -o le.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!
```

Masih sama seperti tadi, tidak ditemukan hal yang signifikan.

Pengujian menggunakan gobuster dir

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

```
(root@kali)-[/home/betterleo]
# gobuster dir -u http://167.172.75.216/ -w /home/leo/gobuster/KaliLists//dirbuster/directory-list-2.3-medium.txt

=====
gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
+ ] Url: http://167.172.75.216/
+ ] Method: GET
+ ] Threads: 10
+ ] Wordlist: /home/grk/gobuster/KaliLists//dirbuster/directory-list-2.3-medium.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]
css (Status: 301) [Size: 173] [-> /css/]
Login (Status: 200) [Size: 905]
js (Status: 301) [Size: 171] [-> /js/]
logout (Status: 302) [Size: 28] [-> /login]
Register (Status: 200) [Size: 1399]
Profile (Status: 302) [Size: 28] [-> /login]
dashboard (Status: 302) [Size: 28] [-> /login]
Logout (Status: 302) [Size: 28] [-> /login]
customer-support (Status: 302) [Size: 28] [-> /login]
Dashboard (Status: 302) [Size: 28] [-> /login]
%C0 (Status: 400) [Size: 1004]
LogIn (Status: 200) [Size: 905]
LOGIN (Status: 200) [Size: 905]
%CF (Status: 400) [Size: 1004]
%CE (Status: 400) [Size: 1004]
```

Dari sinini terlihat beberapa endpoint yang mungkin dapat diakses.

Pengujian menggunakan SQLmap untuk rekon jenis sql

Menggunakan parrot terminal dengan command 'sqlmap -u "http://167.172.75.216/login" --level=5 --risk=3 --delay=1'

Vulnerability Summary & Report Card

Berikut merupakan tabel yang mengilustrasikan kerentanan yang ditemukan berdasarkan dampak dan rekomendsinya.

Blackbox Penetration Test Findings

0	0	0	0	1
Critical	High	Moderate	Low	Informational

Findin g	Severity	Recommendation
<u>Blackbox Penetration Test</u>		
BPT-001: Penemuan endpoint yang dapat diakses	Information al	Mereview aksi dan tahap remediasi

Technical Findings

Blackbox Penetration Test Findings

Finding BPT-001: Penemuan endpoint yang dapat diakses

Description:	Pada link tersebut sesuai dengan gambar yang telah ditampilkan terdapat endpoint yang dapat diakses selanjutnya
Risk:	Mudahnya akses oleh penyerang dengan intensi jahat untuk mendapatkan akses
System:	All
Tools Used:	SQLmap

Other Documentation:

Home Edit Profile Logout Contact Support

Welcome, ciamsoenak

Your phone number: 1234567890

Your credit card (last 4 digits): 0366

Welcome to Jay's Bank

Welcome to my (work in progress) bank. Feel free to look around during our pre-alpha-alpha-alpha stage.

Login Register

Register

Username:

Username must be at least 10 characters long.

Password:

Password must be at least 10 characters long and include at least one digit, one special character, one uppercase letter, and one lowercase letter.

Register

Already have an account? [Login here.](#)

Login

Username:

Password:

Login

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

Your Profile, ciamsoenak

Phone:

Credit Card:

Secret Question:

Secret Answer:

Current Password (for verification):

New Password:

Secret Answer:

Last Page