

Laporan Praktikum Modul 3

Ethical Hacking 2024



Ahmad Fauzan Daniswara

5027221057

Date : 01 Juni 2024

Table of Contents

Table of Content.....	1
Confidentially Statement.....	2
Contact Information.....	2
Assesment Overview.....	3
Assesment Components.....	3-4
Executive Summary.....	5
Langkah - langkah.....	5

Confidentially Statement

Pengerjaan Praktikum 3 kali ini dilaksanakan dalam periode selama lima hari, dimulai dari tanggal 28 Mei 2024 hingga 1 Juni 2024. Pengerjaan praktikum bertujuan untuk melakukan penetration testing pada web Jay's Bank dan menemukan vulnerability dari web tersebut dan dilaporkan kepada development sebelum web tersebut dirilis ke publik.

Contact Information

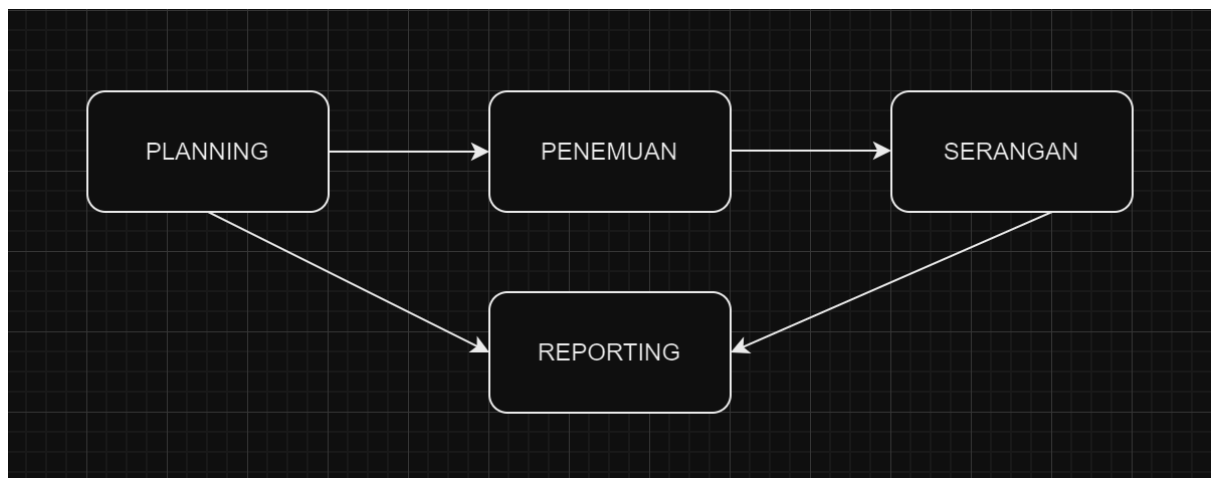
Nama	Judul	Information Contact
Praktikan		
Ahmad Fauzan Daniswara	Pentester	ahmaddaniswara2003@gmail.com

Assesment Overview

Dari tanggal 28 Mei 2024 hingga 1 Juni 2024, praktikan diminta oleh untuk melakukan pentest pada web Jay's Bank yang masih dalam tahap pengembangan sebelum dirilis . Semua pengujian yang dilakukan didasarkan pada Panduan modul praktikum ethical hacking untuk melakukan pentesting.

Tahapan kegiatan pengujian penetrasi antara lain sebagai berikut:

- Perencanaan/Planning – Menyiapkan tools untuk melakukan pentesting pada IP address Jay's Bank.
- Penemuan – Lakukan pemindaian dan enumerasi untuk mengidentifikasi potensi kerentanan, area lemah, dan eksploitasi.
- Serangan – Konfirmasikan potensi kerentanan melalui eksploitasi dan lakukan penemuan tambahan pada akses baru.
- Pelaporan/Reporting – Dokumentasikan semua kerentanan dan eksploitasi yang ditemukan, upaya yang gagal, serta kekuatan dan kelemahan perusahaan.



Assesment Component

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.

Pelaporan

Buat laporan yang mendetail tentang setiap kerentanan yang ditemukan, termasuk deskripsi, langkah reproduksi, dampak potensial, dan rekomendasi perbaikan.

Selalu bertindak secara profesional dan etis dalam setiap langkah penetration testing. Menghormati privasi dan data pengguna lain yang mungkin terlibat dalam testing. Melaporkan temuan secara transparan dan tanpa menyembunyikan informasi apapun.

Konsekuensi Pelanggaran:

Setiap pelanggaran terhadap aturan di atas akan menyebabkan Anda mendapatkan **nilai 0** untuk praktikum ini.

Executive Summary

Berikut adalah IP Address yang digunakan untuk melakukan pentesting :

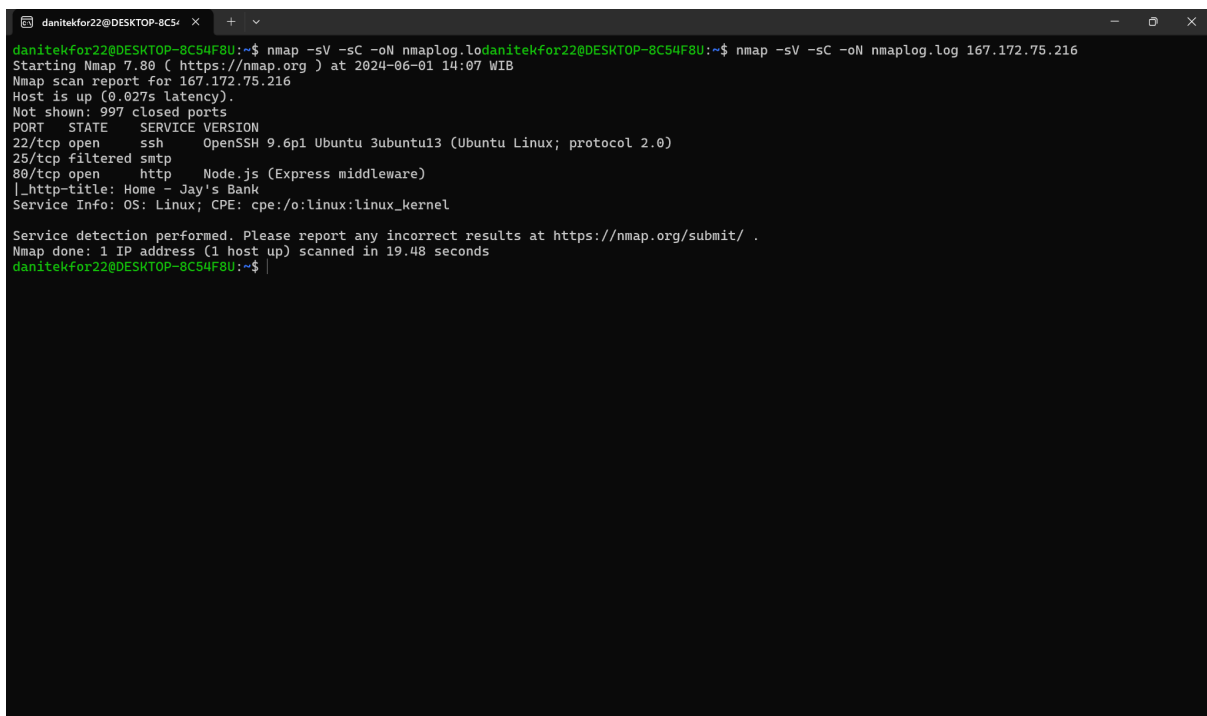
- 167.172.75.216

Percobaan untuk pentesting dimulai dari tanggal 28 Mei hingga 1 Juni 2024 pada IP Address diatas. Terdapat informasi yang bisa didapatkan dari dua IP Address diatas.

Langkah - Langkah

1.Lakukan scanning memakai nmap pada IP address yang dimaksud

`nmap -sV -sC -oN nmaplog.log 167.172.75.216`



```
danitekfor22@DESKTOP-8C54F8U:~$ nmap -sV -sC -oN nmaplog.log
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-01 14:07 WIB
Nmap scan report for 167.172.75.216
Host is up (0.027s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open  http      Node.js (Express middleware)
|_http-title: Home - Jay's Bank
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.48 seconds
danitekfor22@DESKTOP-8C54F8U:~$
```

Dari informasi diatas, ditemukan bahwa :

Port 22 (SSH): Layanan OpenSSH versi 9.6p1 berjalan di server ini. Ini biasanya digunakan untuk akses jarak jauh yang aman ke server.

Port 80 (HTTP): Layanan HTTP yang dijalankan oleh Node.js dengan middleware Express. Judul halaman utama adalah "Home - Jay's Bank".

Untuk masuk ke webnya, ketikkan <http://167.172.75.216> dan muncul halaman sebagai berikut :



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.](#)

Lalu register dan login dengan cara yang sesuai dan setelah berhasil, akhirnya masuk pada tampilan berikut :

Home Dashboard Logout Contact Support

Your Profile, danitiox12

Invalid phone number

You need to finish setting up your profile before you can use all the features of this website.

Phone:

Credit Card:

Secret Question:

Secret Answer:

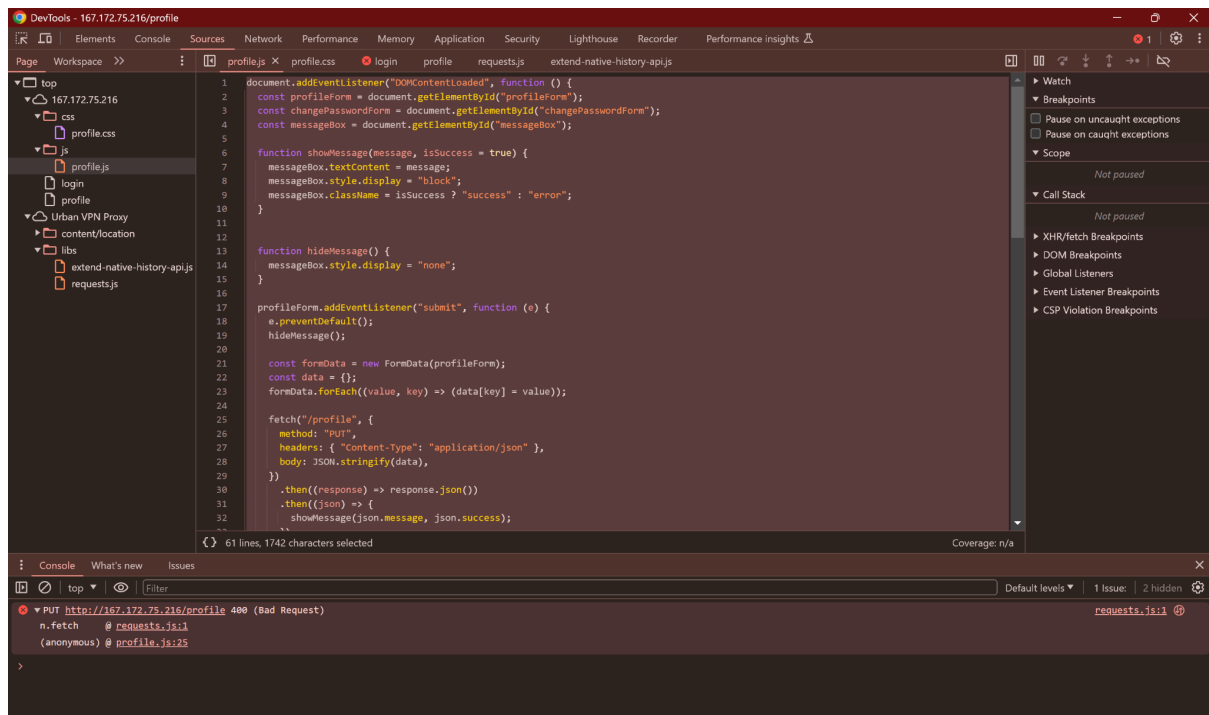
Current Password (for verification):

Update Profile

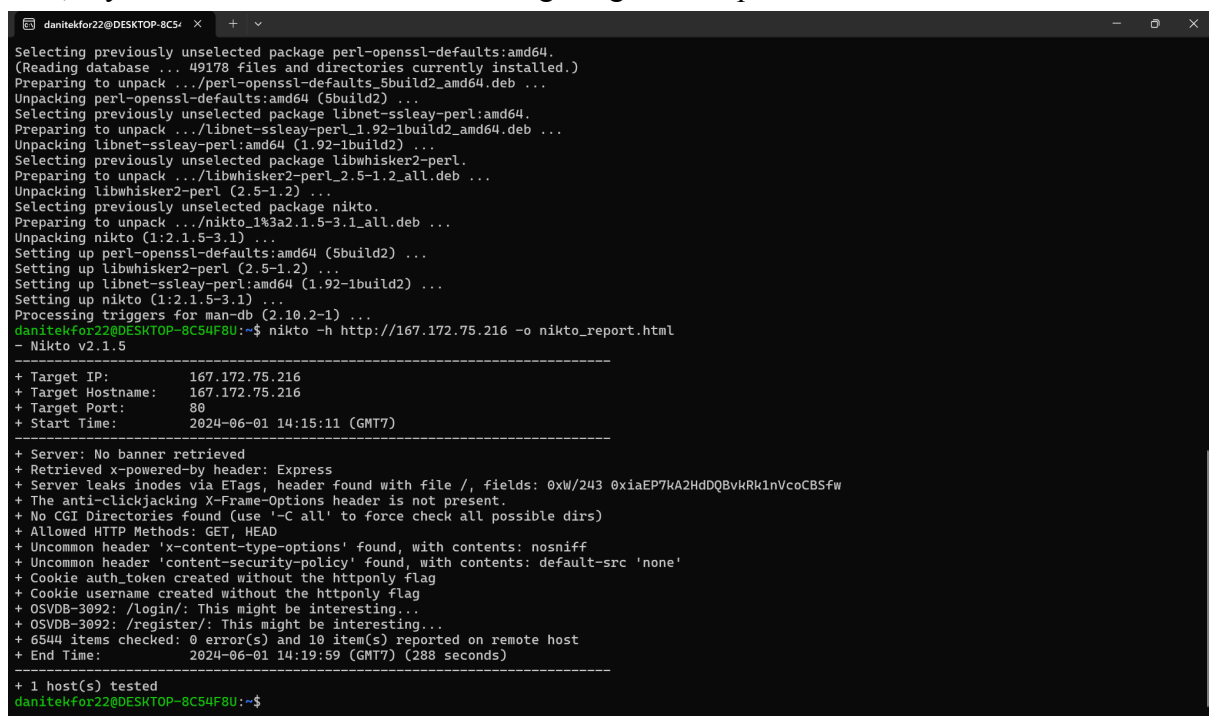
New Password:

Secret Answer:

Kemudian, coba masukkan script yang salah pada keempat kolom diatas dan dari situ bisa melihat isi js dari web tersebut



Lalu, saya coba untuk melakukan scanning dengan nikto pada web tersebut :



Berikut adalah info yang didapatkan pada hasil tersebut dan tingkat keparahannya :

1. Cookies Tanpa HttpOnly

- Cookies auth_token dan username dibuat tanpa flag HttpOnly, yang berarti cookies ini dapat diakses oleh skrip sisi klien (JavaScript), meningkatkan risiko serangan cross-site scripting

(XSS) yang bisa mencuri cookies ini. Tanpa flag HttpOnly, cookies lebih rentan terhadap pencurian melalui serangan XSS, yang bisa mengarah pada pengambilalihan sesi pengguna.

- Tingkat Keparahan : Sedang

2. Uncommon Header

- Server menggunakan header x-content-type-options: nosniff dan content-security-policy: default-src 'none'. Header ini merupakan praktik keamanan yang baik.

- Tingkat Keparahan : Informasional

3. Menarik: /login/ dan /register/

- URL /login/ dan /register/ menunjukkan halaman yang mungkin rentan terhadap serangan brute force atau injection. Jika halaman ini rentan terhadap serangan brute force atau injection, ini bisa memberikan penyerang akses tidak sah ke sistem atau data pengguna.

- Tingkat Keparahan : Tinggi

Berikut adalah solusi yang mungkin bisa diberikan :

1. Tambahkan flag HttpOnly pada cookies auth_token dan username saat dibuat. Ini akan mencegah akses skrip sisi klien ke cookies ini, sehingga mengurangi risiko pencurian cookies melalui serangan XSS.

2. Implementasikan batasan jumlah percobaan login dengan menggunakan mekanisme seperti rate limiting atau captcha setelah sejumlah percobaan login yang gagal.