Security Assessment Finding Report

Jay’s Bank Application Penetration Testing

Date: June 05th, 2024

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. Praktikan prioritized the assessment to identify the weakest security controls an attacker would exploit. Praktikan recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Assessment Overview

From May 5th, 2019 to May 6th, 2024, Parkitkan engaged Praktikan to evaluate the security posture of its infrastructure compared to module best practices that included an external penetration test. All testing performed is based on the Module 4-6 customized testing frameworks.

Phases of penetration testing activities include the following:
· Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
· Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
· Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.

Contact Information

Name	Title	Contact Information
Technology Information - ITS		
Dwiyasa Nakula	Praktikan EH	5027221001

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

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	Detail
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.	http://167.172.75.216

Scope Exclusions

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.

Client Allowances

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).

Executive Summary

Praktikan evaluated DC's external security posture through an external network penetration test from May 5th, 2024 to May 7th, 2024. By leveraging a series of recon methods, Praktikan found low to Medium level vulnerabilities that access to the target IP. It is highly recommended that DC address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

Attack Summary

The following table describes how TCMS gained internal network access, step by step:

Step	Action	Recommendation
1	** <script>alert(10)</script> ** Melakukan operasi XSS untuk mendapatkan akses halaman *dashboard*	Untuk mengatasi injeksi SQL dan XSS dengan mudah, gunakan kerangka kerja aman atau ORM (Laravel, Django, Sequelize, dll.) yang secara otomatis menggunakan kueri berparameter untuk mencegah injeksi SQL. Selain itu, gunakan perpustakaan sanitasi seperti DOMPurify untuk memeriksa dan membersihkan input pengguna secara ketat guna mencegah XSS. Kerangka kerja modern ini memiliki mekanisme bawaan untuk mengatasi sebagian besar masalah keamanan. Oleh karena itu, risiko serangan dapat dikurangi secara signifikan dengan memastikan bahwa masukan divalidasi dan dibersihkan sebelum diproses atau ditampilkan kepada pengguna.sss
2	auth token salah satu user dapat digunakan device lain untuk login menggunakan dengan credential tersebut dan membuka peluang untuk MITM attack untuk privilege escalation	masukan auth token untuk menjadi cookie

Security Strengths

input sudah dibersihkan

Security Weaknesses

XSS, dan auth token.

External Penetration Test Findings

Auth token – http://167.172.75.216 (low)

Description:	Auth token
Impact:	low
System:	http://167.172.75.216
References:	??

Exploitation Proof of Concept

Login user

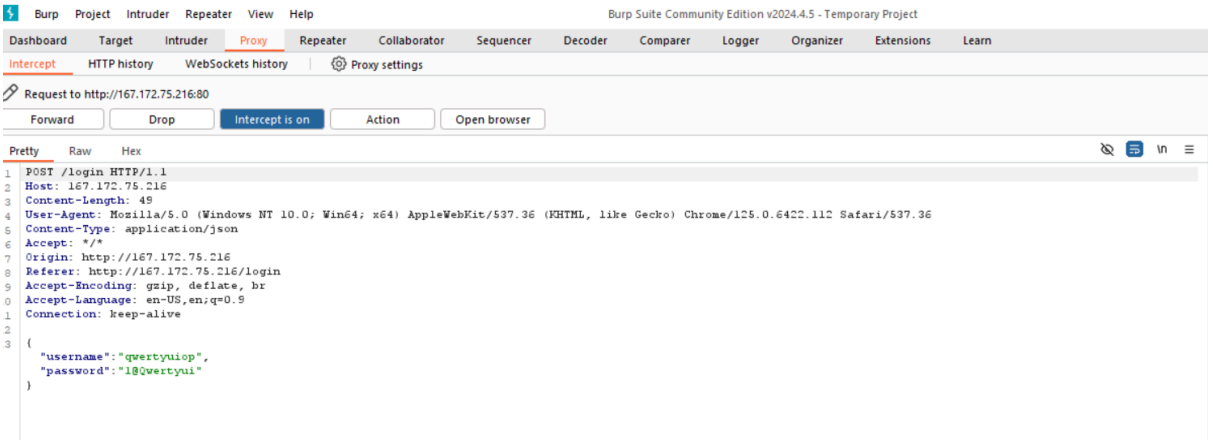

Figure 1: login menggunakan account user 1

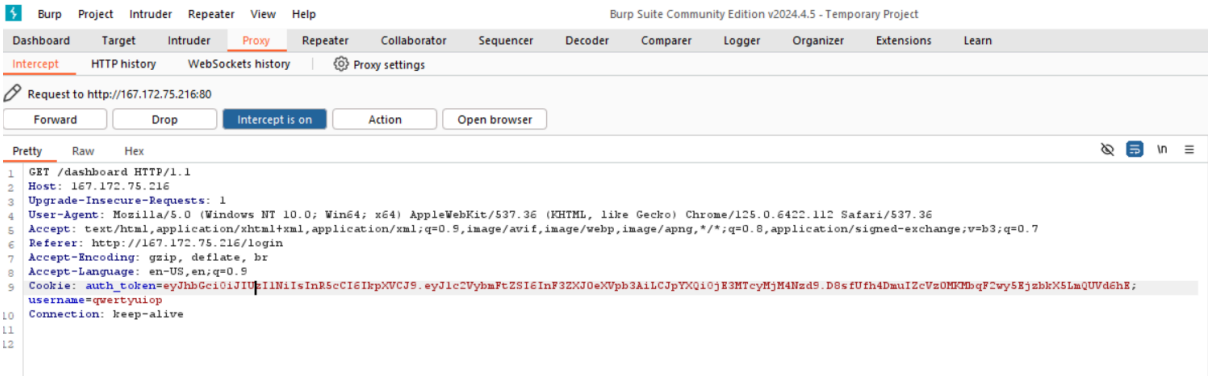

Figure 2: dapatkan auth_token

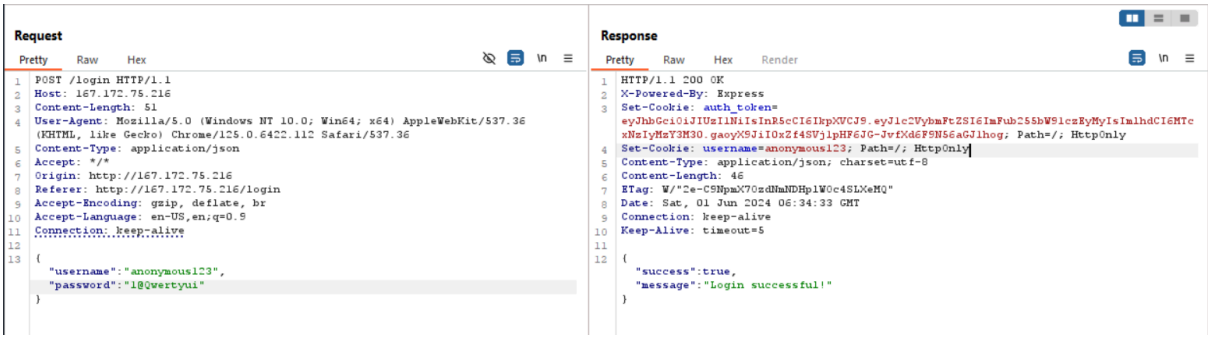

Figure 3: dapatkan auth_token user lain

Figure 4: gantikan auth_token pada intruder

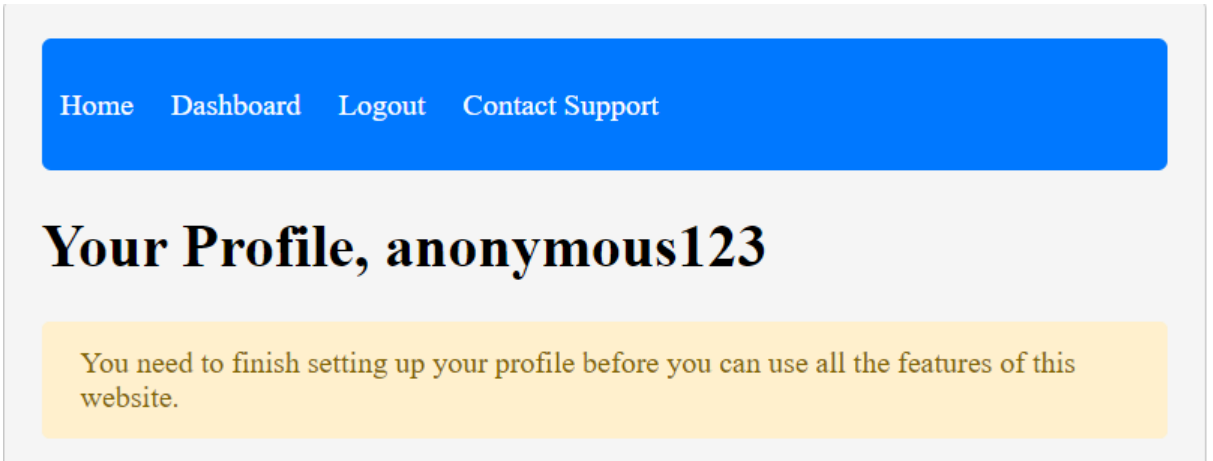

Figure 4: Berhasil login sebagai user lain

Praktikan leveraged the valid celah ini untuk log melalui gain access ke directory tersebut. Dan mendapatkan backup.sql user

WordPress Username Enumeration – http://167.172.75.216 (Low)

Description:	** <script>alert(10)</script> ** Melakukan operasi XSS untuk mendapatkan akses halaman *dashboard*
Impact:	medium
System:	http://167.172.75.216
References:	

Exploitation Proof of Concept

Membuat user dengan username sebagai script XSS <h1><script>alert(CVE)<script><h1>, password nya bebas 1@Qwertyui.

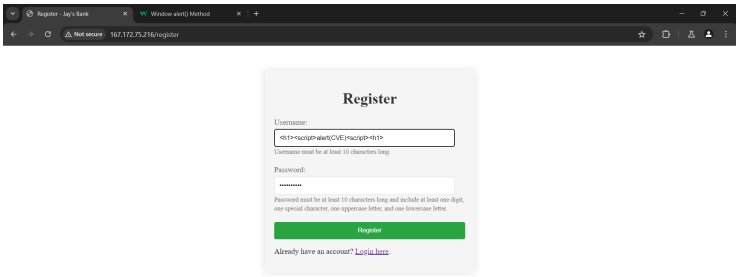

Figure 1: Masukan script XSS ke register

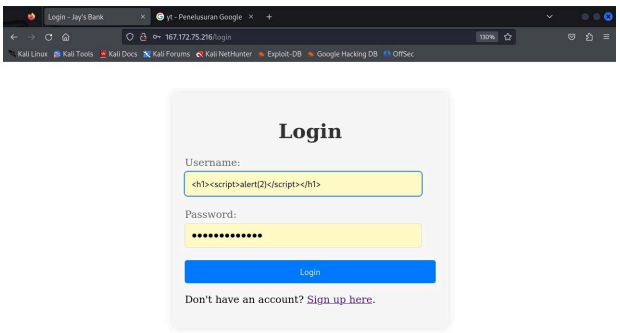

Figure 2: login dengan user tersebut

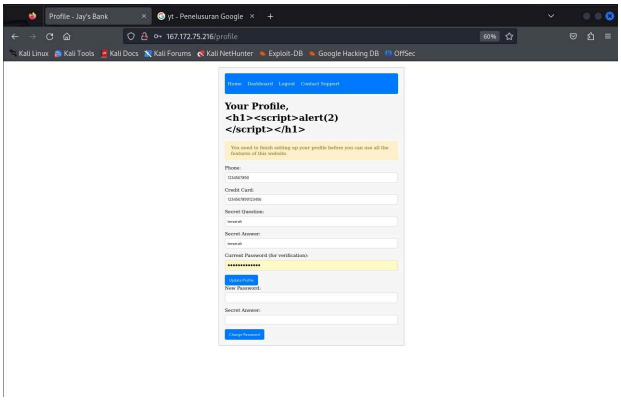

Figure 3: user nya berupa script XSS

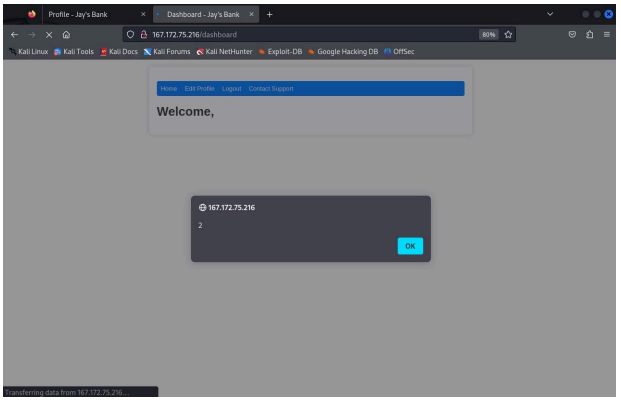

Figure 4: XSS berhasil di execute