Jay's Bank
Security Assessment Findings Report

Business Confidential

Date: May 28th, 2019
Project: 897-19
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Demo Company (DC) and TCM Security (TCMS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both DC and TCMS.

TCMS may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

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. TCMS prioritized the assessment to identify the weakest security controls an attacker would exploit. TCMS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

Name	Title	Contact Information
Demo Company		
Jay's Bank	Praktikum 3	WhatsApp: 08x-xxx-xxx-xxx Email: michaelxxxxxxxxxxxx@gmail.com

Assessment Overview

Pada kesempatan kali ini, praktikan diminta untuk melakukan Penetration Testing pada website yang telah disedikan oleh asisten laboratorium mata kuliah Ethical Hacking.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- 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.
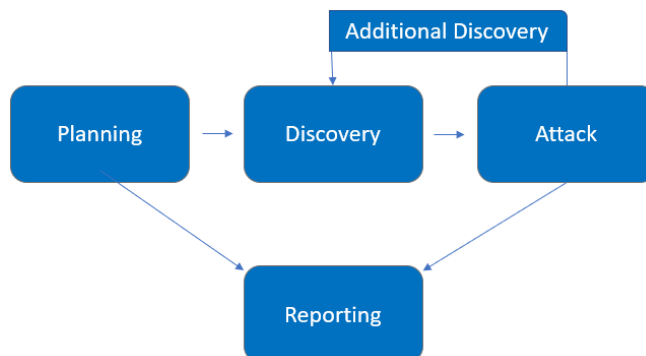
Assessment Components

External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A TCMS engineer attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

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	Details
External Penetration Test	167.172.75.216

- Full scope information provided in "**Demo Company-867-19 Full Findings.xslx**"

Scope Exclusions

Per client request, TCMS did not perform any Denial of Service attacks during testing.

Client Allowances

DC did not provide any allowances to assist the testing.

Executive Summary

Anda adalah seorang ahli keamanan yang ditugaskan oleh perusahaan konsultan keamanan CyberShield untuk melakukan penetration testing terhadap infrastruktur perusahaan FortifyTech. FortifyTech adalah startup perusahaan teknologi dan mereka telah menyewa layanan CyberShield untuk mengevaluasi keamanan sistem mereka.

Temukan kerentanan pada perusahaan FortifyTech dengan menerapkan prinsip Ethical Hacking dan buatlah laporan pada setiap kerentanan yang telah anda temukan, dengan begitu celah kerentanan tersebut dengan cepat bisa diproses oleh mereka.

Attack Summary

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

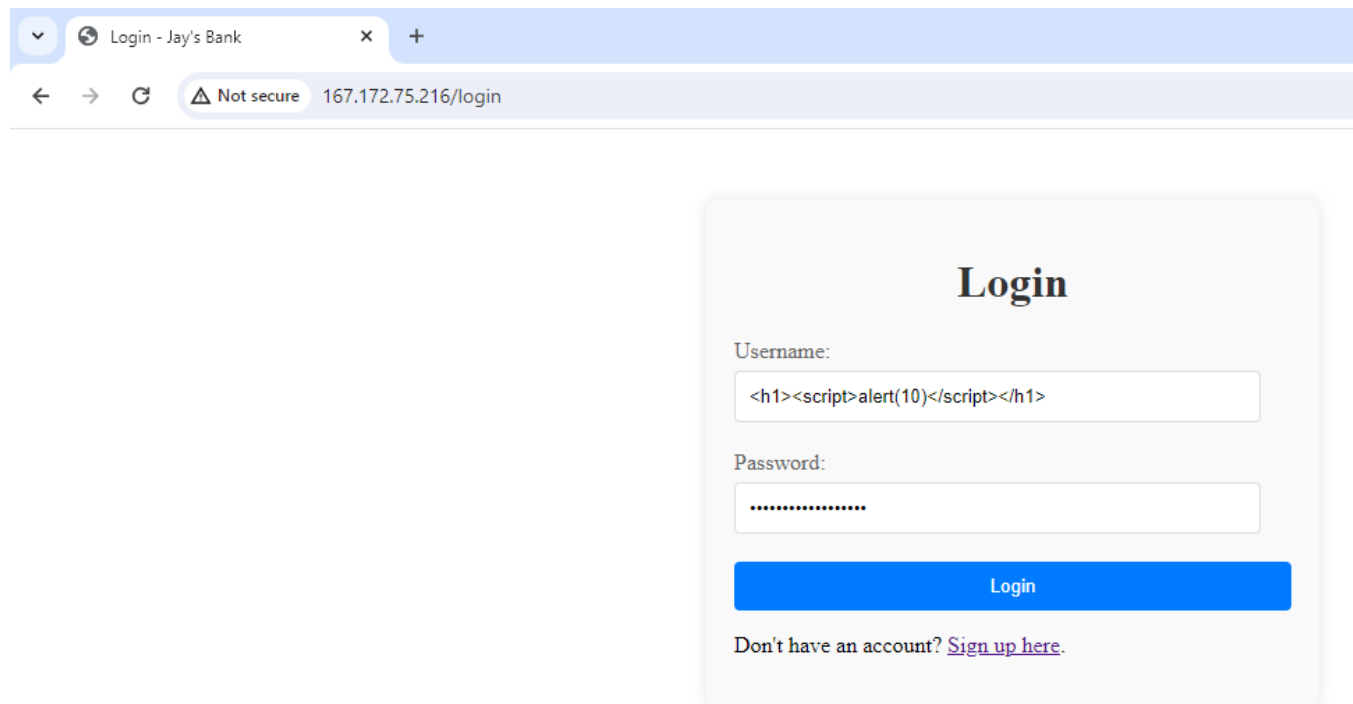| Step	Action	Recommendation
1	** <script>alert(10)</script> ** Melakukan operasi XSS untuk mendapatkan akses halaman *dashboard*	-
2	Melakukan proses **Injection** menggunakan Burpsuite	-

Security Strengths

Tidak Bisa Command Injection

Tidak bisa menggunakan **Command Injection** untuk melakukan *listing username* maupun *password*

Security Weaknesses

XSS

User dapat melakukan aksi XSS pada *website* tersebut untuk mendapatkan ke halaman *dashboard*
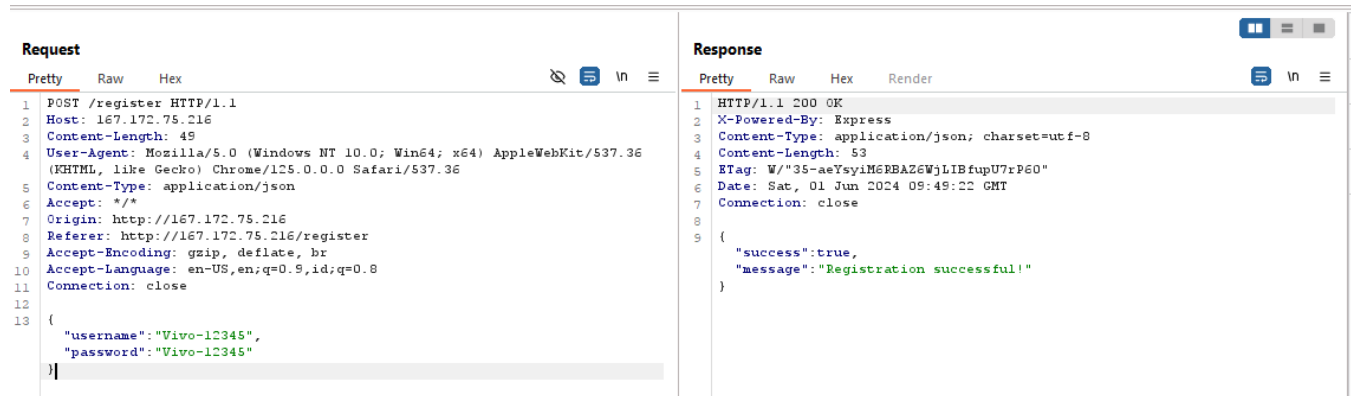

Gambar 1. XSS

Injection
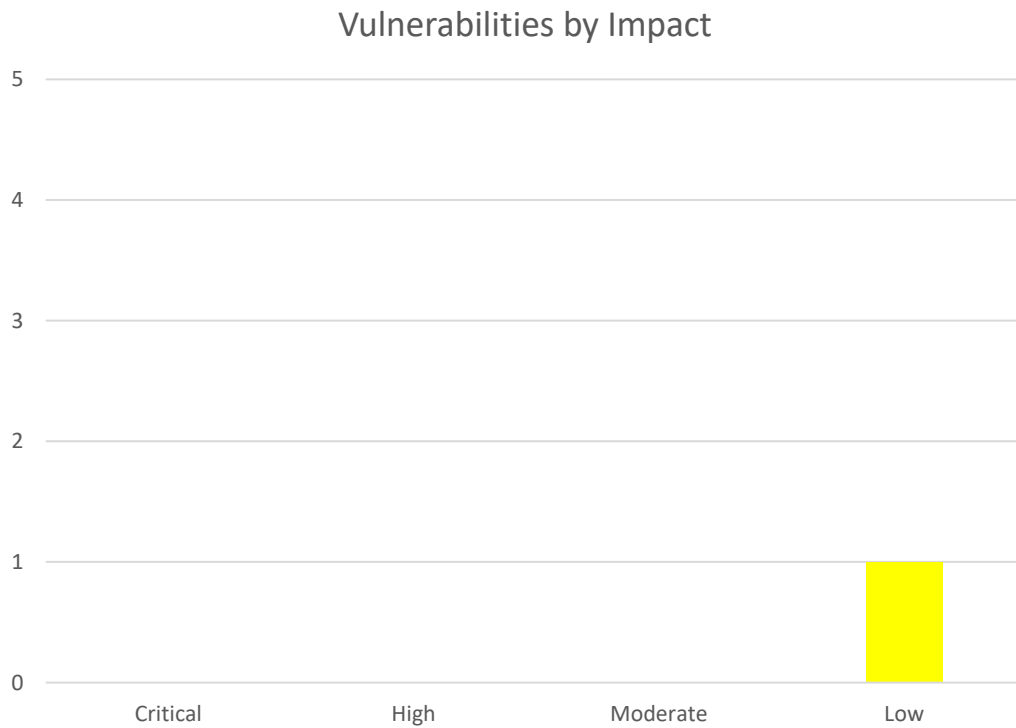
Melakukan proses Injection untuk melakukan proses login

Gambar 2. Injection

Vulnerabilities by Impact
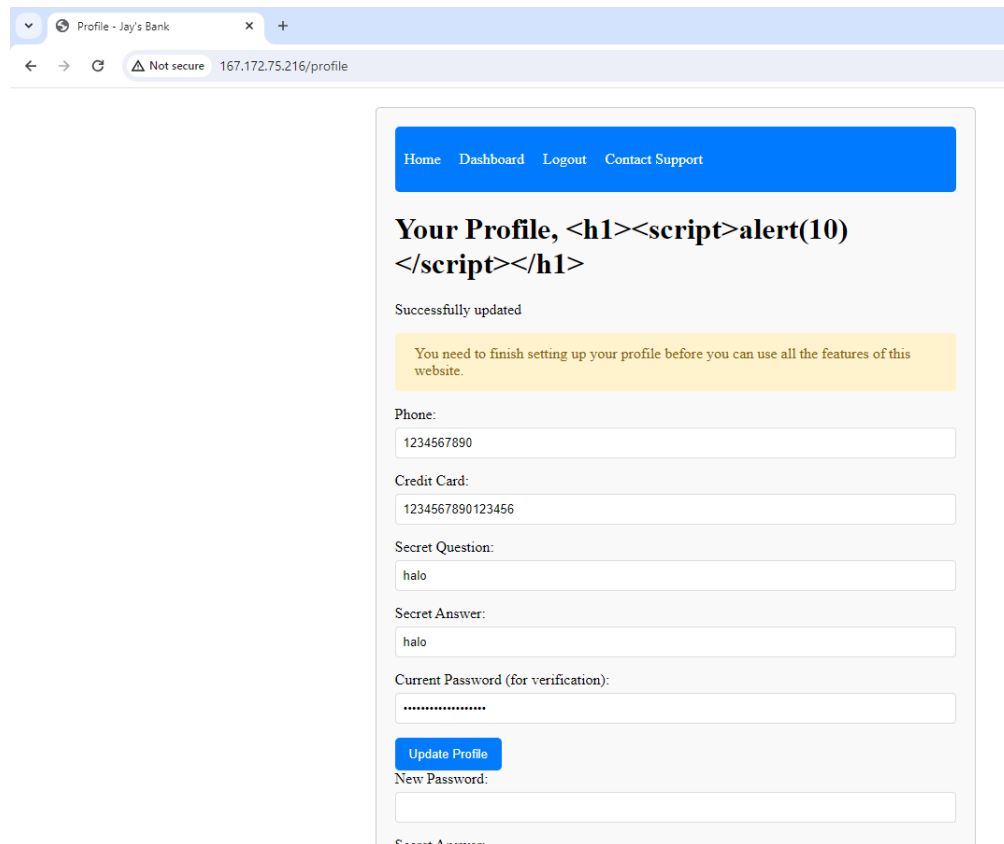
The following chart illustrates the vulnerabilities found by impact:

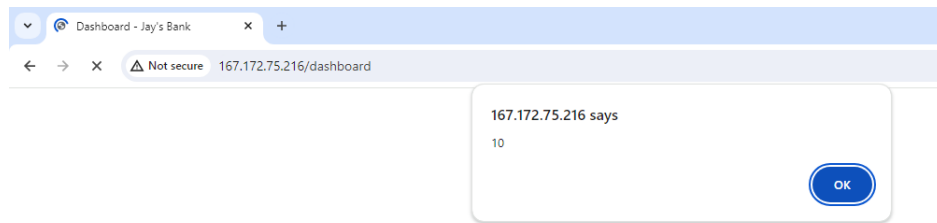# External Penetration Test Findings

Unlimited Login Attempts

Description:	Pihak luar dapat melakukan aksi XSS dan Injection
Impact:	Low
System:	http://167.172.75.216/
References:	

Exploitation Proof of Concept

Lampiran bukti login

Gambar 3. Hasil XSS

Gambar 4. Berhasil Masuk ke Dashboard

Remediation

Who:	IT Team
Vector:	Remote
Action:	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