Jay's Bank Application
Security Assessment Findings Report

Business Confidential

Date: June 1st, 2024
Project: 897-19
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Jay's Bank (JB) and SafeGuard Solution (SGS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both JB and SGS.

SSS 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. SGS prioritized the assessment to identify the weakest security controls an attacker would exploit. SGS 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
Jays's Bank Application		
Asisten Lab	VP, Information Security (CISO)	Office: (555) 555-5555 Email: john.smith@demo.com
SafeGuard Solution		
Alma Amira Dewani	Lead Penetration Tester	NRP : 5027221054 Email: almaaamirad@gmail.com

Assessment Overview

From May 20th, 2019 to May 29th, 2019, Jay's Bank engaged SafeGuard Solution to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Tahapan kegiatan pengujian penetrasi antara lain sebagai berikut:

- Perencanaan – Sasaran pelanggan dikumpulkan dan aturan keterlibatan diperoleh.
- Discovery – Melakukan 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 – Mendokumentasikan semua kerentanan dan eksploitasi yang ditemukan, upaya yang gagal, serta kekuatan dan kelemahan perusahaan.

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

Scope Exclusions

- 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.

Client Allowances

- Diizinkan untuk mencari dan mengidentifikasi kerentanan dalam aplikasi Jay's Bank.
- Diizinkan untuk meng-exploit untuk mengakses akun pengguna lain, tetapi hanya sebatas aplikasi (tidak ke server).

Executive Summary

Pentester mengevaluasi postur keamanan eksternal Jay;s Bank melalui uji penetrasi jaringan eksternal dari tanggal 28 Mei 2024 hingga 21 Mei 2024. Dengan memanfaatkan serangkaian serangan, pentester menemukan kerentanan tingkat kritis yang memungkinkan akses jaringan internal penuh ke kantor pusat Jay's Bank. Sangat disarankan agar JB mengatasi kerentanan ini sesegera mungkin karena kerentanan mudah ditemukan melalui pengintaian dasar dan dapat dieksploitasi tanpa banyak usaha.

Security Strengths

SIEM alerts of vulnerability scans

During the assessment, the DC security team alerted TCMS engineers of detected vulnerability scanning against their systems. The team was successfully able to identify the TCMS engineer's attacker IP address within minutes of scanning and was capable of blacklisting TCMS from further scanning actions.

Security Weaknesses

Missing Multi-Factor Authentication

TCMS leveraged multiple attacks against DC login forms using valid credentials harvested through open-source intelligence. Successful logins included employee e-mail accounts through Outlook Web Access and internal access via Active Directory login on the VPN. The use of multi-factor authentication would have prevented full access and required TCMS to utilize additional attack methods to gain internal network access.

Weak Password Policy

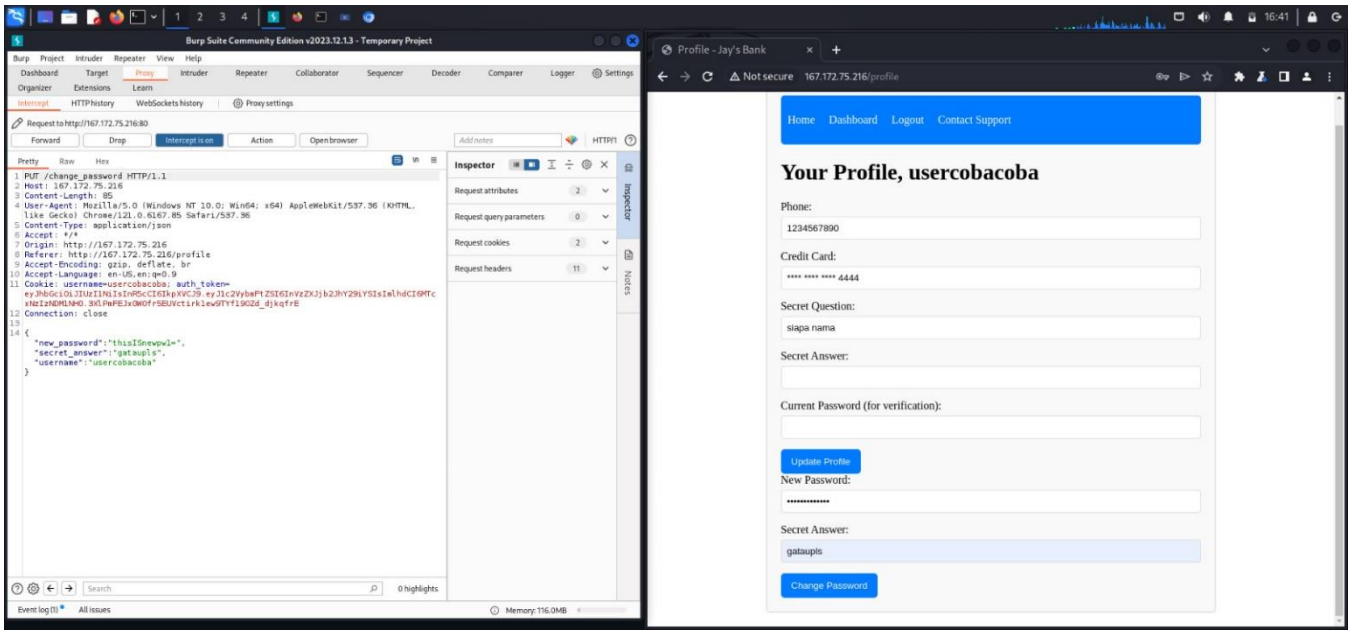
TCMS successfully performed password guessing attacks against DC login forms, providing internal network access. A predictable password format of Summer2018! (season + year + special character) was attempted and successful.

External Penetration Test Findings

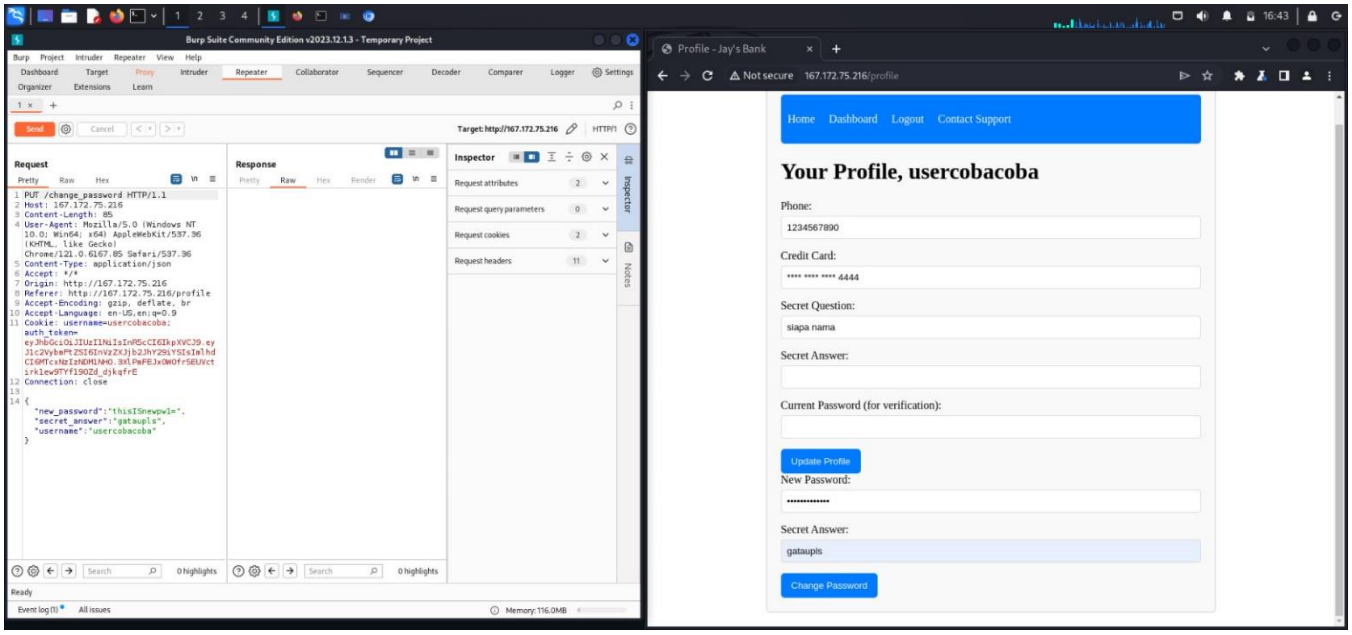
Login as an admin

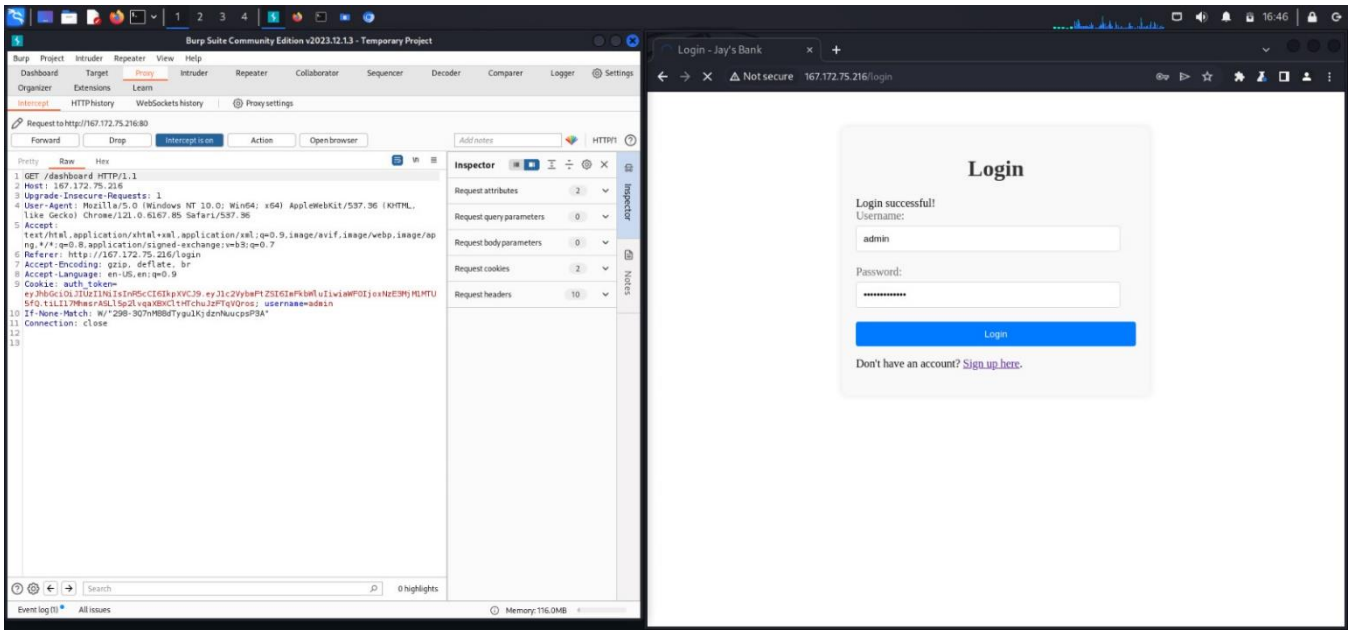
Description:	Pentest berhasil Login sebagai admin dari jay's bank
Impact:	High
System:	167.172.75.216
References:	Burp suite

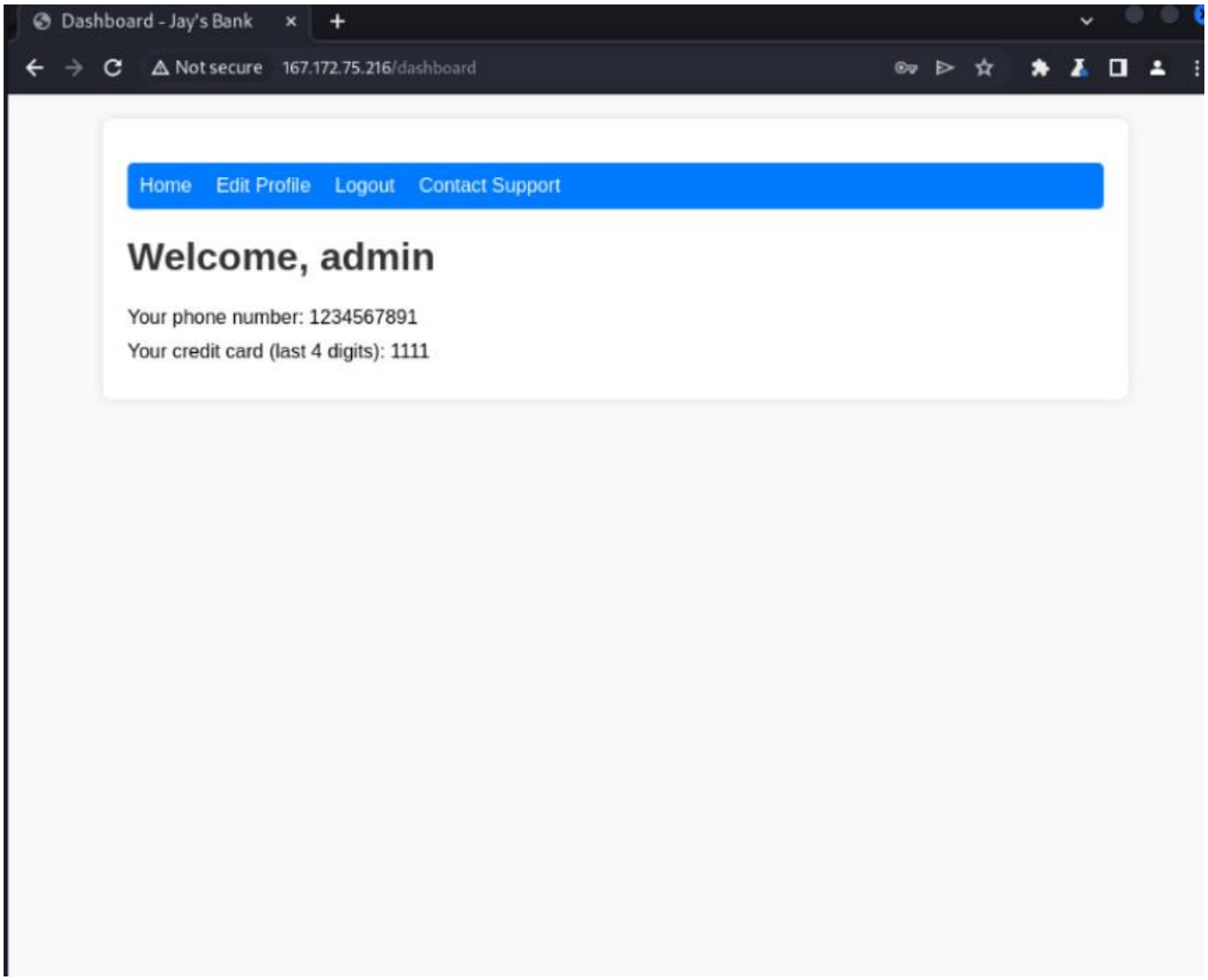
Exploitation Proof of Concept



Pentestor mendaftarkan akun biasa dengan melakukan intercept dengan menggunakan burpsuite.







SQL Injection

Description:	Melakukan sql Injection ke system dengan menggunakan sqlmap
Impact:	Low
System:	167.172.75.216
References:	sqlmap