Jay's Bank Application
Penetration Testing

Business Confidential

Table of Contents

Table of Contents 2
Confidentiality Statement 3
Disclaimer 3
Contact Information 3
Assessment Overview 4
Assessment Components 4
External Penetration Test 4
Finding Severity Ratings 5
Scope 6
Scope Exclusions 6
Client Allowances 6
Executive Summary 7
Attack Summary 7
Security Strengths 8
SIEM alerts of vulnerability scans 8
Security Weaknesses 8
Missing Multi-Factor Authentication 8
Weak Password Policy 8
Unrestricted Logon Attempts 8
Vulnerabilities by Impact 9
External Penetration Test Findings 10
Insufficient Lockout Policy – Outlook Web App (Critical) 10
Additional Reports and Scans (Informational) 13

Confidentiality Statement

Dokumen ini merupakan dokumen confidential yang dibuat oleh pentester dan berisi hasil report dari proses percobaan External Penetration Test.

Disclaimer

Penetration Test ini sudah memperoleh izin dari pihak perusahaan untuk mencoba dan mencari kerentanan yang dimiliki oleh website.

Contact Information

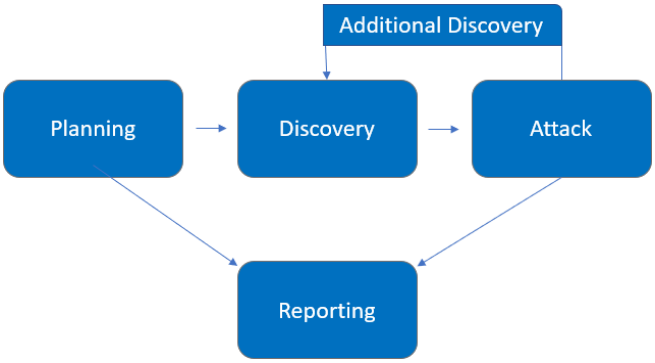
Name	Title	Contact Information
Demo Company		
Aslab	VP, Information Security (CISO)	Office: (555) 555-5555 Email: john.smith@demo.com
Aslab	IT Manager	Office: (555) 555-5555 Email: jim.smith@demo.com
Aslab	Network Engineer	Office: (555) 555-5555 Email: joe.smith@demo.com
Pentest Rawr		
Wikri Cahya	Mahasiswa	Nrp: 5027221020 Email:wikrinew@gmail.com

Assessment Overview

Penetration test dilakukan pada tanggal 28 Mei 2024-1 Juni 2024

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
Scanning Vulnerability Test	167.172.75.216

Scope 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).

Client 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.

Executive Summary

Sesuai dengan notes diatas, pentester melakukan uji coba keamanan website fortify tech untuk mencari akses kerentanan terhadap websitenya.as

Scanning Summary

Tabel ini menjelaskan bagaimana scanning menggunakan wasp untuk keamanan website di 167.172.75.216 menggunakan OWasp Zap

No	Scanning	Description
1	Alert Counts By Site and Risk	Menunjukkan jumlah peringatan yang dihasilkan untuk setiap situs yang satu atau lebih peringatan telah dibuat, berdasarkan tingkat risiko masing-masing peringatan. Peringatan dengan tingkat keyakinan "False Positive" telah dikecualikan dari perhitungan ini. (Angka dalam tanda kurung adalah jumlah peringatan yang dihasilkan untuk situs tersebut pada tingkat risiko tersebut atau di atasnya.)
2	Alert Counts by Alert type	Menunjukkan jumlah peringatan dari setiap jenis peringatan, bersama dengan tingkat risiko jenis peringatan tersebut. (Persen dalam tanda kurung mewakili setiap hitungan sebagai persentase, dibulatkan ke satu tempat desimal, dari total jumlah peringatan yang disertakan dalam laporan ini.)

3	Alert Counts by Alert Type	Menunjukkan jumlah peringatan untuk setiap tingkat risiko dan tingkat keyakinan yang disertakan dalam laporan. (Persen dalam tanda kurung mewakili jumlah sebagai persentase dari total jumlah peringatan yang disertakan dalam laporan, dibulatkan ke satu tempat desimal.)

Security Strengths

Dari hasil scan owasp, terdapat berbagai macam kelemahan di keamanannya, selain itu website tersebut juga mudah untuk register dan login secara paksa menggunakan burpsuite. Da

Security Weaknesses

Header Lost

Temuan tentang kehilangan beberapa header keamanan HTTP, seperti Strict-Transport-Security (HSTS), Content-Security-Policy (CSP), dan X-Frame-Options, menunjukkan kekurangan dalam implementasi kontrol keamanan pada server web. Tanpa header ini, risiko serangan seperti man-in-the-middle (MITM) dan clickjacking meningkat karena kurangnya mekanisme perlindungan yang diterapkan oleh browser.

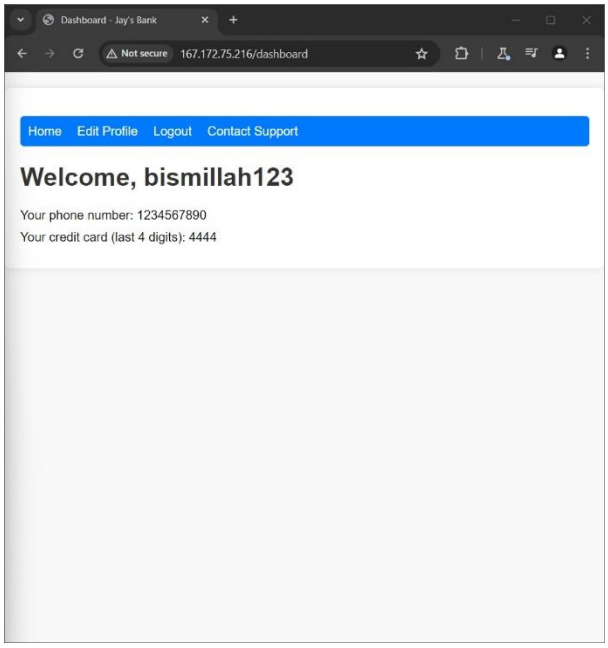
Hilangnya Anti CSRF Token

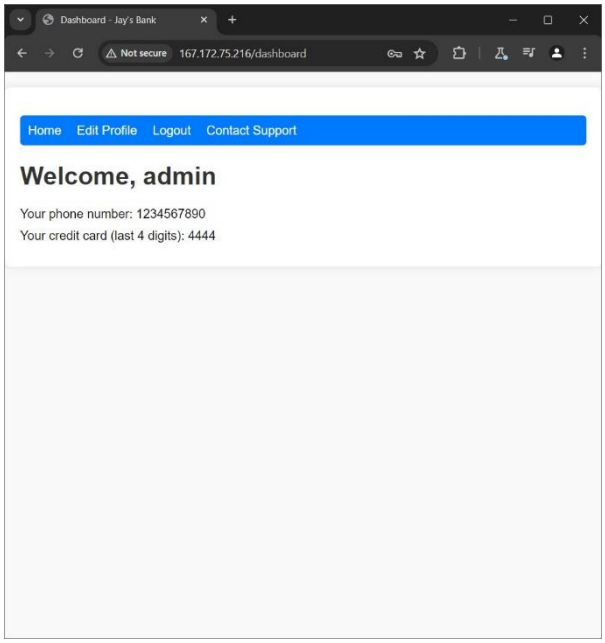
Kehadiran CSRF token biasanya penting dalam mencegah serangan Cross-Site Request Forgery (CSRF) yang memungkinkan penyerang menjalankan tindakan yang tidak diinginkan atas nama pengguna yang sudah di autentikasi. Kehilangan CSRF token pada aplikasi web WordPress meningkatkan risiko serangan CSRF, memungkinkan penyerang

untuk mengeksploitasi perilaku otentikasi pengguna dan melakukan tindakan berbahaya seperti mengubah kata sandi atau posting konten palsu.

XSS Vulnerability

XSS atau cross site scripting adalah serangan keamanan web yang terjadi ketika penyerang menyisipkan kode berbahaya dalam bentuk skrip ke dalam website. Contohnya adalah saat user sedang login dapat diganti username dan atau password dari user tersebut. Hal tersebut dapat dilihat dari gambar di bawah berikut ini:





Rekomendasi Langkah yang Tepat

Remediation

Who:	IT Team
Vector:	Remote

Recommendation	Header Lost 1. Tambahkan header keamanan HTTP yang diperlukan, seperti Strict-Transport-Security (HSTS), Content-Security-Policy (CSP), dan X-Frame-Options melalui konfigurasi server. 2. Gunakan plugin keamanan yang dapat secaraotomatis menambahkan header keamanan ke setiap permintaan HTTP. Anti CSRF Token Lost 1. Pastikan setiap formulir atau tindakan yang sensitif di situs web dilindungi oleh token CSRF. 2. Gunakan plugin keamanan yang secara otomatis menyertakan token CSRF pada setiap permintaan yang memerlukan otentikasi. XSS 1. Gunakan Content security policy 2. Setiap kali menampilkan data yang dimasukkan pengguna di halaman web, enkripsi output tersebut untuk memastikan bahwa karakter berbahaya tidak diinterpretasikan sebagai kode HTML atau JavaScript. 3. Validasi input

Last Page