SafeGuard Solutions
Security Assessment Findings Report

Business Confidential

Date: June 01st, 2024
Report Prepared By: SafeGuard Solutions
Version 1.0

Table of Contents

Pernyataan Kerahasiaan

Dokumen ini adalah properti eksklusif dari SafeGuard Solutions. Dokumen ini mengandung informasi properti dan rahasia. Penggandaan, redistribusi, atau penggunaan, baik secara keseluruhan maupun sebagian, dalam bentuk apapun, memerlukan persetujuan dari SafeGuard Solutions.

SafeGuard Solutions dapat membagikan dokumen ini kepada pihak auditor berdasarkan perjanjian kerahasiaan untuk menunjukkan kepatuhan kebutuhan uji penetrasi.

Penafian

Uji penetrasi dianggap sebagai gambaran pada suatu waktu. Temuan dan rekomendasi mencerminkan informasi yang dikumpulkan selama penilaian dan bukan perubahan atau modifikasi yang dilakukan di luar periode tersebut.

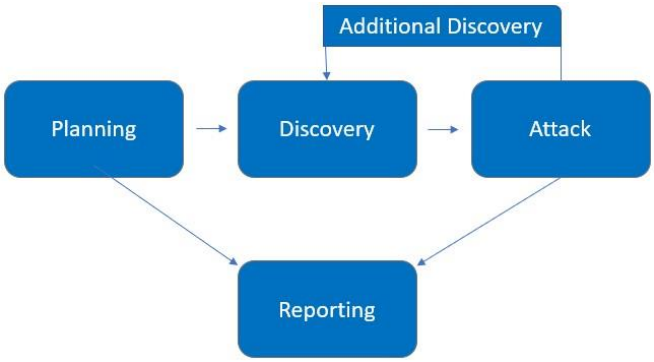
Keterlibatan yang terbatas waktu tidak memungkinkan untuk evaluasi penuh dari semua kontrol keamanan. SafeGuard Solutions memprioritaskan penilaian untuk mengidentifikasi kontrol keamanan yang paling lemah yang akan dieksploitasi oleh penyerang. SafeGuard Solutions merekomendasikan untuk melakukan penilaian serupa secara tahunan oleh penilai internal atau pihak ketiga untuk memastikan kesuksesan berkelanjutan dari kontrol-kontrol tersebut.

Ikhtisar Penilaian

Mulai dari 30 Mei 2024 hingga 1 Juni 2024, SafeGuard Solutions melibatkan tim keamanan untuk mengevaluasi posisi keamanan infrastrukturnya. Semua pengujian yang dilakukan didasarkan pada Panduan Teknis terbaik untuk Pengujian dan Penilaian Keamanan Informasi, Panduan Pengujian OWASP (v4), dan kerangka pengujian yang disesuaikan.

Fase-fase kegiatan uji penetrasi meliputi hal-hal berikut:

- Perencanaan – Tujuan pelanggan dikumpulkan dan aturan keterlibatan diperoleh.
- Discovery – Melakukan pemindaian dan enumerasi untuk mengidentifikasi kerentanan potensial, area yang lemah, dan eksploitasi.
- Serangan – Mengonfirmasi kerentanan potensial melalui eksploitasi dan melakukan discovery tambahan saat akses baru diperoleh.
- Pelaporan – Mendokumentasikan semua kerentanan dan eksploitasi yang ditemukan, percobaan gagal, serta kekuatan dan kelemahan perusahaan.



Kompoenen Penilaiaan

Uji Penetrasi Eksternal

Uji penetrasi eksternal mensimulasikan peran seorang penyerang yang berusaha untuk mendapatkan akses ke jaringan internal tanpa sumber daya internal atau pengetahuan internal. Seorang dari tim SafeGuard Solutions berusaha untuk mengumpulkan informasi sensitif melalui intelijen sumber terbuka (OSINT), termasuk informasi username/email, kata sandi yang rentan dan dapat dimanfaatkan untuk mendapatkan akses jaringan internal.

Penemuan Tingkat Keparahan

Tabel berikut menentukan tingkat keparahan dan rentang skor CVSS yang digunakan dalam dokumen ini untuk menilai kerentanan dan dampak risiko.

Keparahan	CVSS V3 Score Range	Definisi
Critical	9.0-10.0	Pemanfaatan mudah dilakukan dan biasanya mengakibatkan kompromi tingkat sistem. Disarankan untuk membentuk rencana tindakan dan memperbarui segera.
High	7.0-8.9	Pemanfaatan lebih sulit namun dapat menyebabkan hak istimewa yang ditingkatkan dan potensial kehilangan data atau waktu henti. Disarankan untuk membentuk rencana tindakan dan memperbarui sesegera mungkin.
Moderate	4.0-6.9	Kerentanan ada tetapi tidak dapat dieksploitasi atau memerlukan langkah tambahan seperti rekayasa sosial. Disarankan untuk membentuk rencana tindakan dan memperbarui setelah masalah prioritas tinggi telah diselesaikan.
Low	0.1-3.9	Kerentanan tidak dapat dieksploitasi tetapi akan mengurangi permukaan serangan organisasi. Disarankan untuk membentuk rencana tindakan dan memperbarui selama jendela pemeliharaan berikutnya.
Informational	N/A	Tidak ada kerentanan yang ada. Informasi tambahan disediakan mengenai item yang diperhatikan selama pengujian, kontrol yang kuat, dan dokumentasi tambahan.

Jangkauan

Assessment	Details
External Penetration Test	167.172.75.216

Pengecualiaan Lingkup

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).

Tunjangan Klien

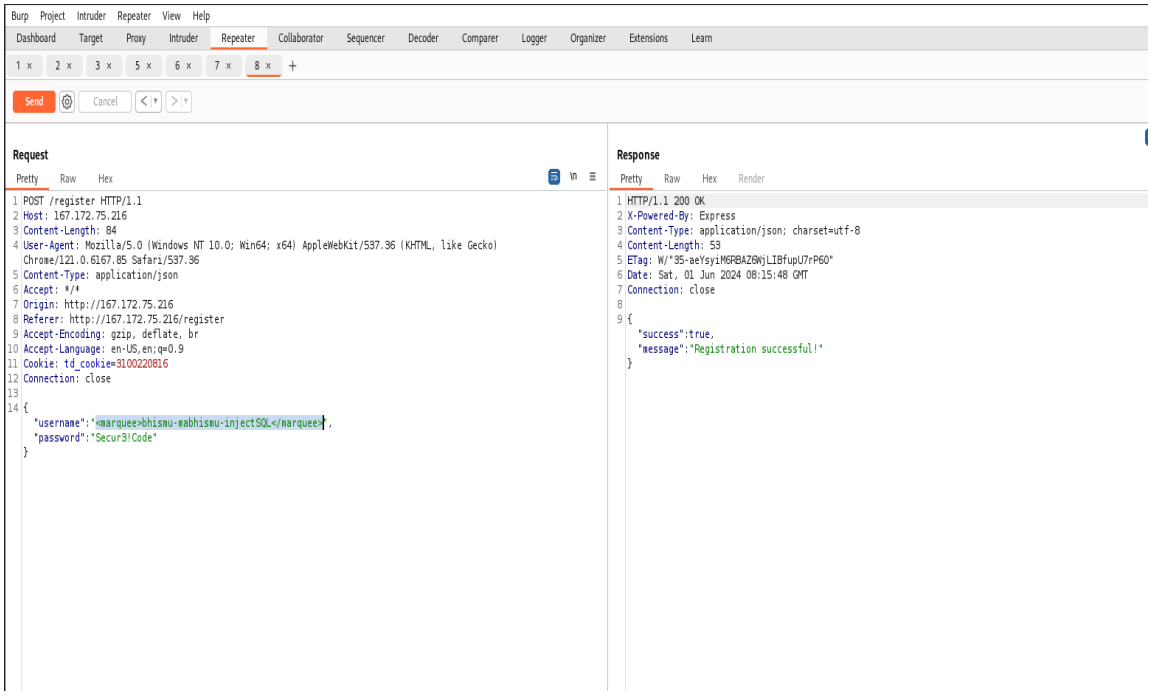
Jay's Bank tidak memberikan tunjangan apa pun untuk membantu pengujian.

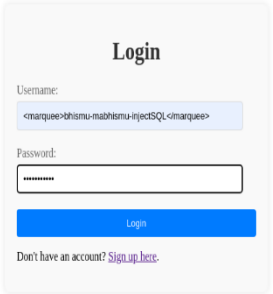
Ringkasan Singkat

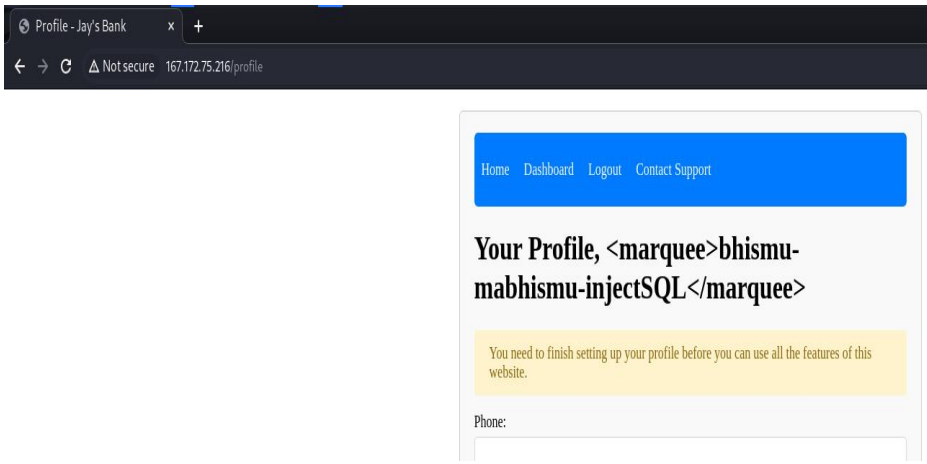
Selama periode penilaian, SafeGuard Solutions melakukan uji penetrasi eksternal pada infrastruktur Jay's Bank. Penilaian bertujuan untuk mengidentifikasi kerentanan dalam lingkup yang disediakan. Temuan yang disajikan dalam laporan ini menguraikan risiko keamanan potensial dan rekomendasi untuk penanganan.

Temuan Uji Penetrasi

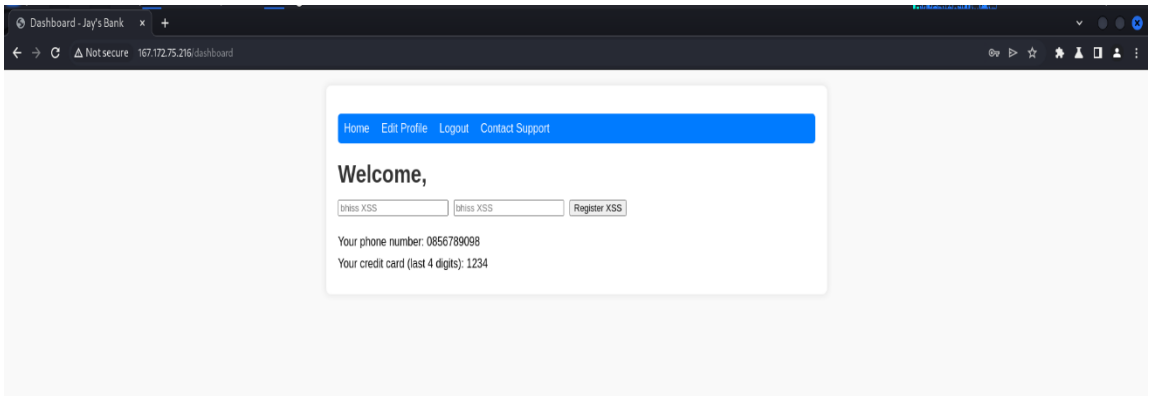
Berdasarkan SQL Injection







Berdasarkan XSS



Kesimpulan:

Pencarian kerentanan mengidentifikasi beberapa kerentanan dalam infrastruktur Jay's Bank, termasuk method yang terbuka dan bisa diulik oleh mereka yang mungkin memiliki niat untuk bobol kerentanan, sehingga dalam SQL Injection bisa terbaca dan menjadikan celah yang perlu diperhatikan, adapun dari input usernamenya seharusnya menggunakan regex username supaya dari pengguna yang menginputkan tidak asal-asalan sehingga tidak terjadi kerentanan dalam XSS, di mana ketika menginputkan nama username seperti element html, maka akan terbaca, untuk keamanan backend cukup bagus, tetapi perlu diperhatikan celah yang ada demi keamanan web Jay’s Bank

Sangat penting bagi Jay's Bank untuk segera mengambil Tindakan yang bertujuan menangani temuan ini guna melindungi infrastrukturnya dari potensi pelanggaran keamanan. SafeGuard Solutions tersedia untuk memberikan bantuan dan panduan lebih lanjut dalam menerapkan langkah-langkah keamanan yang direkomendasikan.