Jay's Bank Application

Security Assessment Findings Report

Business Confidential

Date: May 25th, 2024
Project: 38-5027
Version 1.0

Table of Contents

Pernyataan Kerahasiaan

Dokumen ini adalah milik eksklusif Jay's Bank dan SafeGuard Solutions. Dokumen ini berisi informasi yang bersifat kepemilikan dan rahasia. Duplikasi, distribusi ulang, atau penggunaan, secara keseluruhan atau sebagian, dalam bentuk apa pun, memerlukan persetujuan dari Jay's Bank dan SafeGuard Solutions.

Disclaimer

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

Keterlibatan yang dibatasi waktu tidak memungkinkan untuk evaluasi penuh terhadap semua kontrol keamanan. SafeGuard Solutions memprioritaskan penilaian untuk mengidentifikasi kontrol keamanan terlemah yang akan dieksploitasi oleh penyerang. SafeGuard Solutions merekomendasikan untuk melakukan penilaian serupa setiap tahun oleh penilai internal atau pihak ketiga untuk memastikan keberhasilan kontrol yang berkelanjutan.

Informasi Kontak

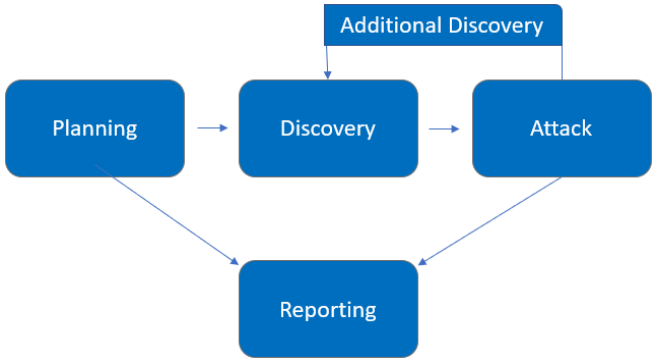
Name	Title	Contact Information
Jay's Bank		
Admin Ethical Hacking	VP	089xxxxxxxx zbjxxxxx@gmail.com
SafeGuard Solutions		
Zulfa Hafizh K	Teknisi	089yyyyyyyyy zulxxxxxxxxx@gmail.com

Overview Penilaian

Dari tanggal 5 Mei 2024 hingga 8 Mei 2024, Jay's Bank melibatkan SafeGuard Solutions untuk mengevaluasi aplikasi mockup bank yang masih dalam tahap development dibandingkan dengan praktik terbaik industri saat ini yang mencakup uji penetrasi eksternal

Fase kegiatan pengujian penetrasi meliputi hal-hal berikut:

- Perencanaan - Tujuan pelanggan dikumpulkan dan aturan main diperoleh.
- Penemuan - Melakukan pemindaian dan enumerasi untuk mengidentifikasi potensi kerentanan, area yang lemah, dan eksploitasi.
- Serangan - Mengonfirmasi kerentanan potensial melalui eksploitasi dan melakukan penemuan tambahan setelah mendapatkan akses baru.
- Pelaporan - Mendokumentasikan semua kerentanan dan eksploitasi yang ditemukan, percobaan yang gagal, serta kekuatan dan kelemahan perusahaan.



Komponen Penilaian

Uji Penetrasi Eksternal

Uji penetrasi eksternal meniru peran penyerang yang mencoba mendapatkan akses ke jaringan internal tanpa sumber daya internal atau pengetahuan orang dalam. Seorang teknisi SafeGuard Solutions berusaha mengumpulkan informasi sensitif yang bisa dimanfaatkan untuk melawan sistem eksternal untuk mendapatkan akses jaringan internal. Teknisi juga melakukan pemindaian dan pencacahan untuk mengidentifikasi potensi kerentanan dengan harapan dapat dieksploitasi.

Klasifikasi Tingkat Keparahan

Tabel berikut ini mendefinisikan tingkat keparahan dan rentang skor CVSS yang sesuai yang digunakan di seluruh dokumen untuk menilai kerentanan dan dampak risiko.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Eksploitasi sangat mudah dan biasanya menghasilkan kompromi tingkat sistem. Disarankan untuk membuat rencana tindakan dan segera menambalnya.
High	7.0-8.9	Eksploitasi lebih sulit tetapi dapat menyebabkan peningkatan hak istimewa dan berpotensi kehilangan data atau waktu henti. Disarankan untuk membuat rencana tindakan dan menambal sesegera mungkin.
Moderate	4.0-6.9	Kerentanan ada tetapi tidak dapat dieksploitasi atau memerlukan langkah ekstra seperti rekayasa sosial. Disarankan untuk membuat rencana tindakan dan menambal setelah masalah-masalah yang menjadi prioritas utama diselesaikan.
Low	0.1-3.9	Kerentanan tidak dapat dieksploitasi tetapi akan mengurangi permukaan serangan organisasi. Disarankan untuk membuat rencana tindakan dan menambal selama masa pemeliharaan berikutnya.
Informational	N/A	Tidak ada kerentanan. Informasi tambahan disediakan mengenai hal-hal yang diperhatikan selama pengujian, kontrol yang kuat, dan dokumentasi tambahan.

Scope

Assessment	Details
Uji Penetrasi Eksternal	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.

Scope Exclusions

Sesuai permintaan klien, SafeGuard Solutions tidak melakukan serangan hal - hal yang melanggar etika selama pengujian.

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

SafeGuard Solutions mengevaluasi postur keamanan eksternal Jay's Bank melalui uji penetrasi jaringan eksternal dari tanggal 25 Mei 2024 hingga 1 Juni 2024. Dengan memanfaatkan serangkaian serangan, SafeGuard Solutions menemukan beberapa kerentanan tingkat moderat. Disarankan untuk membuat rencana tindakan dan menambal setelah masalah-masalah yang menjadi prioritas utama diselesaikan

Attack Summary

Tabel berikut ini menjelaskan bagaimana SafeGuard Solutions mendapatkan akses jaringan internal, langkah demi langkah:

Step	Action	Recommendation
1	Menggunakan Nmap untuk mengumpulkan informasi terkait service, aplikasi, device, dan lain-lain yang akan kita uji keamanannya	
2	Menggunakan Gobuster dan Dirbuster untuk scanning directory yang terdapat pada suatu web application.	
3	Menggunakan sqlmap untuk validasi kelemahan, hingga otomasi serangan	.

Security Weaknesses

[INFO] URI parameter '#1*' appears to be 'Oracle stacked queries (DBMS_LOCK.SLEEP)' injectable (167.172.75.216)

Parameter URI dengan nama "#1*" tampaknya dapat diinjeksikan menggunakan teknik yang dikenal sebagai "Oracle stacked queries" dengan fungsi DBMS_LOCK.SLEEP.

Temuan Uji Penetrasi Eksternal

URI parameter '#1*' appears to be 'Oracle stacked queries (DBMS_LOCK.SLEEP)' injectable (Low)

Description:	- **Oracle Stacked Queries**: Ini adalah jenis serangan SQL injection yang memanfaatkan fungsionalitas tumpukan kueri yang ditemukan dalam sistem basis data Oracle. Dengan menggunakan teknik ini, penyerang dapat menjalankan beberapa kueri secara bersamaan dalam satu pernyataan SQL. - **DBMS_LOCK.SLEEP**: Ini adalah fungsi dalam basis data Oracle yang dapat digunakan untuk menunda eksekusi kueri untuk jumlah waktu tertentu. Fungsi ini sering digunakan dalam serangan SQL injection untuk menguji keberadaan kerentanan dan menunda respon dari server, memberikan petunjuk tentang apakah serangan berhasil atau tidak.
Impact:	Low
System:	1. 167.172.75.216
References:	

Last Page