Jay's Bank
Security Assessment Findings Report

Confidentiality Statement

Kami berkomitmen untuk menjaga kerahasiaan seluruh informasi yang kami akses dan temukan selama proses pengujian penetrasi aplikasi Jay's Bank. Hal ini mencakup data sensitif, informasi pengguna, dan temuan kerentanan. Kami tidak akan mengungkapkan informasi apa pun kepada pihak ketiga tanpa izin, kecuali diperlukan untuk tujuan peningkatan keamanan. Kami akan bertindak secara profesional dan etis, menghormati privasi semua pihak yang terlibat dalam proses ini.

Disclaimer

Pengujian penetrasi dilakukan dengan tujuan untuk meningkatkan keamanan aplikasi Jay's Bank. Namun, hasil pengujian ini mungkin tidak mencakup seluruh potensi kerentanan dan tidak menjamin keamanan sepenuhnya. Kami tidak bertanggung jawab atas segala kerusakan atau kerugian yang mungkin timbul akibat penggunaan atau interpretasi informasi dalam laporan ini. Penggunaan informasi dalam laporan hendaknya dilakukan dengan pertimbangan dan tindakan sesuai dengan standar keamanan yang berlaku

Contact Information

Name	Title	Contact Information
Marselinus Krisna	Ethical Hacking A	...@gmail.com

Assessment Overview

Pengerjaan Pentesting ini dilakukan dari tanggal 5 Mei 2024 hingga 8 Mei 2024. Pentesting ini dilakukan guna mengevaluasi keamanan sistem dan jaringan dari ip yang telah diberikan menggunakan teknik penetration testing untuk mengidentifikasi potensi kerentanan dan mendapatkan pemahaman yang komprehensif tentang tingkat keamanan.

Terdapat beberapa fase yang akan dilakukan yaitu :

1. **Planning:** Tahap ini melibatkan pembuatan rencana penilaian yang mencakup penetapan sasaran, tujuan, dan metode yang akan digunakan selama penilaian.
2. **Discovery:** Pada fase ini, dilakukan pencarian dan pengumpulan informasi tentang target yang akan dievaluasi.
3. **Attack:** Tahap ini merupakan implementasi dari serangan terhadap sistem dan jaringan dengan tujuan untuk menguji keamanan dan mencari potensi kerentanan yang dapat dieksploitasi.
4. **Reporting:** Setelah tahap penilaian selesai, hasilnya akan didokumentasikan dalam laporan yang mencakup temuan kerentanan, rekomendasi perbaikan, dan kesimpulan dari penilaian tersebut.

Assessment Components

Fokus pada kerentanan aplikasi seperti SQL injection, XSS, dan authentication/authorization issues

Finding Severity Ratings

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Temuan kritis menggambarkan kerentanan yang memiliki potensi dampak serius terhadap kerahasiaan, integritas, atau ketersediaan sistem. Eksploitasi kerentanan ini dapat mengakibatkan akses penuh ke sistem, kerugian data kritis, atau gangguan layanan yang signifikan.
High	7.0-8.9	Temuan tinggi menunjukkan kerentanan yang memiliki potensi dampak yang signifikan terhadap keamanan sistem. Meskipun tidak seberat temuan kritis, eksploitasi kerentanan ini masih dapat menghasilkan akses yang tidak sah atau pencurian data sensitif.
Moderate	4.0-6.9	Temuan menengah mencakup kerentanan yang memiliki potensi dampak moderat terhadap keamanan sistem. Meskipun mungkin tidak langsung mengancam kerahasiaan atau integritas data, eksploitasi kerentanan ini masih dapat menyebabkan gangguan operasional atau akses tidak sah ke sistem.
Low	0.1-3.9	Temuan rendah menunjukkan kerentanan yang memiliki dampak minimal terhadap keamanan sistem. Eksploitasi kerentanan ini mungkin memerlukan kondisi khusus atau akses yang terbatas, dan dampaknya terhadap operasional sistem terbatas.
Informational	N/A	Saran atau rekomendasi untuk peningkatan keamanan, tetapi tidak memerlukan tindakan perbaikan segera.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Kemungkinan mengukur potensi kerentanan yang dieksploitasi. Peringkat diberikan berdasarkan tingkat kesulitan serangan, alat yang tersedia, tingkat keterampilan penyerang, dan lingkungan klien.

Impact

Dampak mengukur dampak potensi kerentanan terhadap operasi, termasuk kerahasiaan, integritas, dan ketersediaan sistem dan/atau data klien, kerusakan reputasi, dan kerugian finansial.

Scope

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

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.

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).

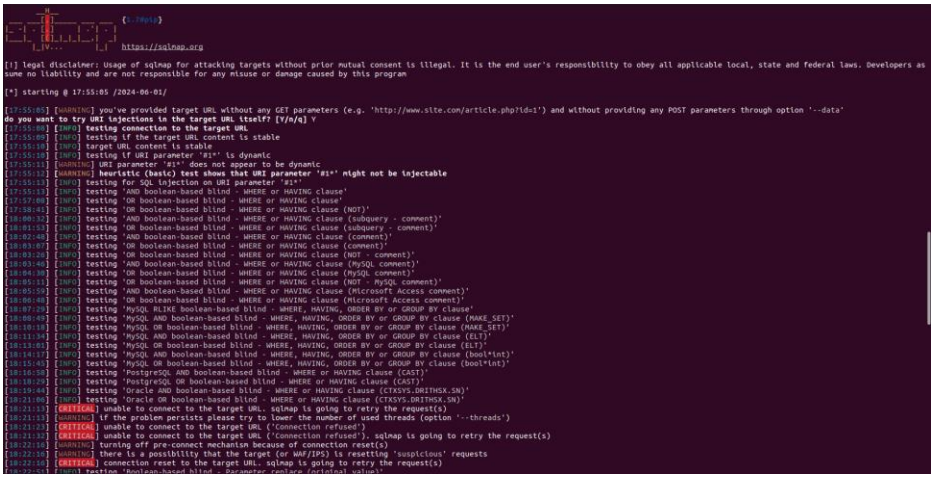
Executive Summary

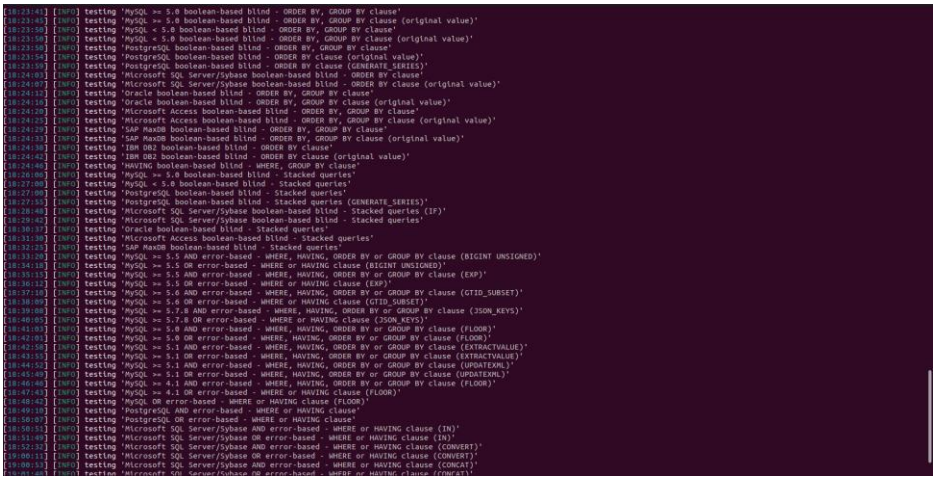
Testing Summary

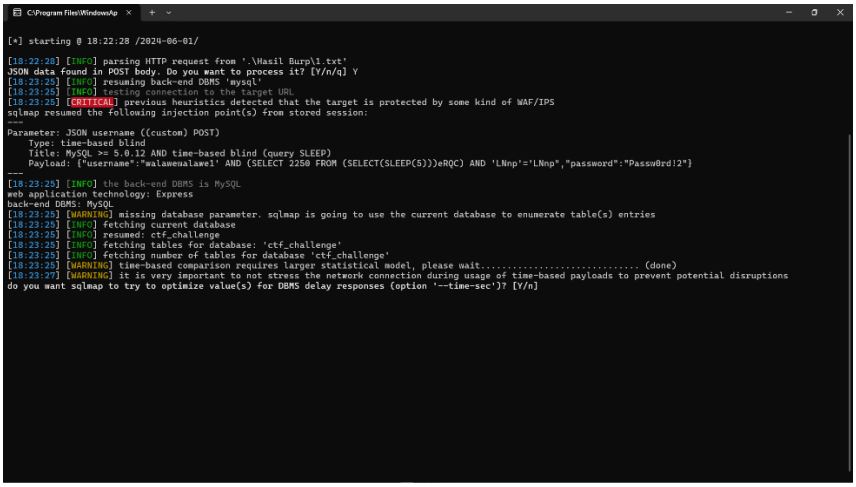
Setelah melakukan serangkaian pengujian keamanan pada 167.172.75.216, terdapat temuan yang cukup signifikan terkait dengan celah keamanan. Beberapa di antaranya termasuk kerentanan SQL Injection, XSS, serta permasalahan terkait dengan autentikasi.

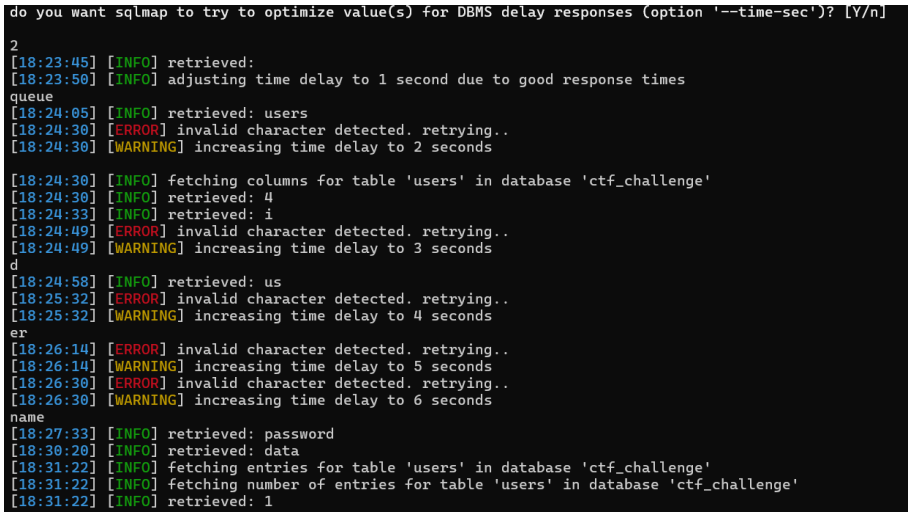
Proses pengujian tersebut telah melibatkan upaya untuk menyusuri dan memahami berbagai potensi risiko yang mungkin terjadi pada aplikasi tersebut. Meski begitu, kendala waktu dan kompleksitas kode yang dihadapi menjadi hambatan dalam mencapai hasil yang optimal.

Banyaknya masalah yang harus diatasi dalam waktu terbatas menjadi tantangan tersendiri. Hasil dari pengujian tersebut tercermin secara jelas dalam gambar yang disajikan di bawah ini, yang menunjukkan sejumlah kendala yang dihadapi serta upaya-upaya yang telah dilakukan dalam mengatasi berbagai masalah keamanan yang ditemui.









Proses eksplorasi dan pengujian masih berlangsung, sebagaimana yang terlihat dalam gambar yang disertakan. Meskipun begitu, belum dapat disimpulkan bahwa percobaan telah selesai dengan keseluruhan tantangan yang dihadapi.

Dalam perjalanan pengujian ini, satu peringatan yang muncul terkait dengan versi server SQL yang digunakan. Peringatan ini menjadi fokus penting untuk ditinjau lebih lanjut guna memastikan keamanan dan kestabilan sistem secara menyeluruh. Dengan demikian, meski proses pengujian masih berlanjut, pemahaman terhadap setiap peringatan dan potensi risiko menjadi langkah krusial dalam memastikan keselamatan aplikasi

Last Page