Jay's Bank
Security Assessment Findings Report

Business Confidential

Date: May 8th, 2024
Project: DC-001
Version 1.0

Table of Contents

Confidentiality Statement

Dokumen ini merupakan milik eksklusif Jay's Bank. Dokumen ini berisi informasi hak milik dan bersifat rahasia. Duplikasi, redistribusi, atau penggunaan, seluruhnya atau sebagian, dalam bentuk apa pun, memerlukan izin dari Jay's Bank.

Jay's Bank dapat membagikan dokumen ini dengan auditor berdasarkan perjanjian kerahasiaan untuk menunjukkan kepatuhan persyaratan uji penetrasi.

Disclaimer

Pentester memprioritaskan penilaian ini untuk mengidentifikasi kontrol keamanan terlemah yang dapat dieksploitasi oleh penyerang. Pentester merekomendasikan dilakukannya penilaian serupa setiap tahun oleh penilai internal atau pihak ketiga untuk memastikan keberhasilan pengendalian yang berkelanjutan.

Contact Information

Name	Title	Contact Information
Fortify Tech		
Bintang Ryan	Pentester	Email : bintangryn@gmail.com

Assessment Overview

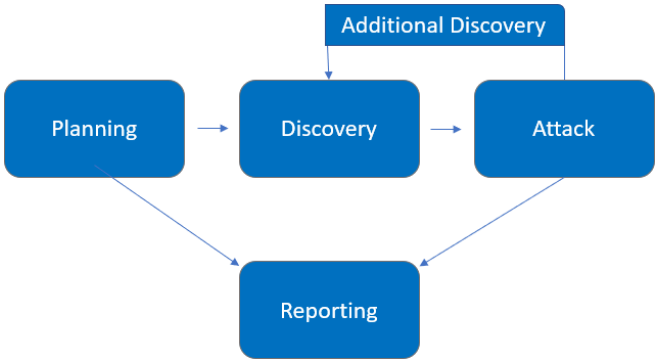
Evaluasi keamanan infrastruktur Jay's Bank oleh Pentester dilakukan sejak 7 Mei 2024 hingga 8 Mei 2024, Jays Bank melibatkan Pentester untuk melakukan praktik terbaik saat ini yang mencakup uji penetrasi jaringan internal. Semua pengujian yang dilakukan didasarkan pada Panduan Teknis NIST SP 800-115 untuk Pengujian dan Penilaian Keamanan Informasi, Panduan Pengujian OWASP (v4), dan kerangka pengujian yang disesuaikan.

Tahapan kegiatan pengujian penetrasi antara lain sebagai berikut:

• Planning – Melakukan perencanaan Pentest terhadap Jays Bank.

• Discovery – Melakukan pemindaian dan enumerasi terhadap IP 167.172.75.216 untuk mengidentifikasi potensi kerentanan, area lemah, dan eksploitasi.

• Attack – Melakukan eksploitasi kerentantan yang ada pada infrastruktur Jays Bank
• Reporting – Mendokumentasikan semua kerentanan dan eksploitasi yang ditemukan, upaya yang gagal, serta kekuatan dan kelemahan perusahaan.



Assessment Components

Internal Penetration Test

Tes penetrasi internal mengemulasi peran penyerang dari dalam jaringan. Pentester akan memindai jaringan untuk mengidentifikasi potensi kerentanan host dan melakukan serangan jaringan internal yang umum dan tingkat lanjut. Pentester akan berusaha mendapatkan akses ke host melalui pergerakan lateral, melakukan penyusupan ke akun pengguna dan admin domain, dan mengumpulkan data sensitive atau pun segala bentuk Informasi penting yang dimiliki olleh Jays Bank.

Finding Severity Ratings

Tabel berikut menjelaskan bagaimana tingkat keparahan dan rentang skor CVSS terkait yang digunakan di seluruh dokumen untuk menilai kerentanan dan dampak risiko.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Eksploitasi langsung yang mengakibatkan kerentanan pada tingkat sistem dan sebaiknya diatasi segera dengan membuat rencana tindakan dan melakukan perbaikan.
High	7.0-8.9	Eksploitasi yang parah yang dapat menyebabkan peningkatan hak istimewa dan potensial kehilangan data atau waktu tidak aktif. Disarankan untuk membuat rencana tindakan dan segera melakukan penambalan.
Moderate	4.0-6.9	Ada kerentanan tetapi tidak dapat dieksploitasi atau memerlukan langkah tambahan seperti rekayasa sosial. Disarankan untuk membuat rencana tindakan dan melakukan penambalan setelah isu-isu yang memiliki prioritas tinggi telah diselesaikan.
Low	0.1-3.9	Kerentanan tidak dapat dieksploitasi tetapi akan mengurangi permukaan serangan organisasi. Disarankan untuk membuat rencana tindakan dan melakukan penambalan selama jendela perawatan berikutnya.
Informational	N/A	Tidak ada kerentanan yang ada. Informasi tambahan disediakan mengenai hal-hal yang diperhatikan selama pengujian, kontrol yang kuat, dan dokumentasi tambahan.

Risk Factors

Risiko didasarkan pada dua factor : Likelihood and Impact

Likelihood

Kemungkinan mengukur potensi kerentanan untuk dieksploitasi. Penilaian diberikan berdasarkan pada kesulitan serangan, alat yang tersedia, tingkat keahlian penyerang, dan lingkungan klien.

Impact

Dampak mengukur efek potensial kerentanan terhadap operasi, termasuk kerahasiaan, integritas, dan ketersediaan sistem dan/atau data klien, kerugian reputasi, dan kerugian keuangan.

Scope

Assessment	Details
Internal Pentest	**167.172.75.216**

Client Allowances

Jays Bank mempersilakan Pentester untuk melakukan hal berikut :

- Akses internal ke jaringan melalui Dropbox dan izin port.

Executive Summary

Pada tanggal 01 Juni 2024, Pentester mengevaluasi postur keamanan internal Jays Bank melalui pengujian penetrasi. Bagian-bagian berikut memberikan gambaran tingkat tinggi tentang kerentanan yang ditemukan, upaya yang berhasil dan gagal, serta kekuatan dan kelemahan.

Testing Summary

Sesuai dengan keterangan pada Assestment Overview, Pentester melakukan serangakaian proses untuk mengevaluasi keamanan infrastruktur Jays Bank. Setelah melakukan serangkaian proses tersebut, Pentester hanya menemukan Informasi umum yang dapat ditemukan oleh siapapun termasuk attacker seperti port yang terbuka, service yang digunakan serta kerentanan yang ada pada infrastruktur Jays Bank.

Tester Notes and Recommendations

Setelah melakukan serangakain proses, Pentester tidak menemukan Informasi yang sensitive karena tidak dapat mengakses ataupun melakukan penyusupan Sebagai admin atau pemilik akses. Pentester hanya menemukan Informasi umum yang dapat ditemukan oleh attacker. Oleh karena itu, tidak ada rekomendasi atau Solusi yang dapat diberikan Pentester kepada Jays Bank terkait keamanan infrastruktur mereka.

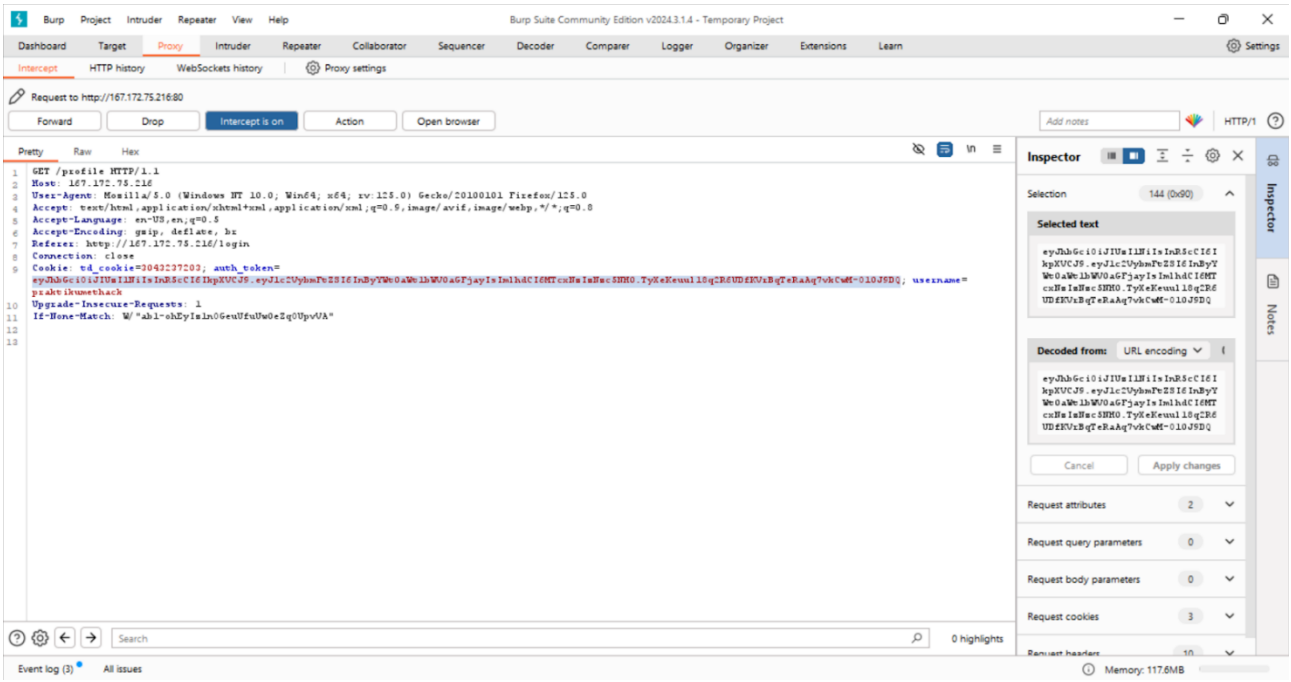
Technical Findings

Internal Penetration Test Findings

Finding IPT-001 : Menggunakan Auth_Token BurpSuite untuk Melakukan Login tanpa password

Description:	Kita dapat memperoleh auth_token untuk sebuah akun dengan menggunakan burpsuite. Kita dapat mengakses akun lain tanpa mengetahui kata sandi jika kita menggunakan auth_token di dalamnya. Auth Token: Dalam aplikasi web, auth_token adalah JSON Web Token (JWT) yang digunakan untuk otorisasi dan otentikasi. Ini adalah bagian dari permintaan HTTP untuk mengautentikasi pengguna dan memberikan akses ke sumber daya yang dilindungi. Server menandatangani token untuk menjamin integritas dan keasliannya. Ini terdiri dari data pengguna yang disandikan, termasuk detail sesi dan nama pengguna. Perilaku yang Terlihat: Kolom auth_token dan nama pengguna dalam permintaan HTTP POST yang disediakan telah menyematkan kode JavaScript (<script>alert(22)</script>), yang menunjukkan bahwa serangan XSS mungkin telah dilakukan. Hal ini menyiratkan bahwa aplikasi
Risk:	XSS : Tinggi - Aplikasi yang memasukkan data yang tidak dipercaya ke dalam halaman web tanpa validasi atau jalan keluar yang memadai dapat rentan terhadap serangan XSS. Hal ini dapat digunakan oleh penyerang untuk menyisipkan skrip berbahaya ke dalam halaman web pengguna lain. Skrip ini memiliki kemampuan untuk mengendalikan sesi pengguna, mengubah halaman web, mengalihkan pengguna ke situs web yang berbahaya, dan melakukan tindakan atas nama pengguna tanpa izin.
System:	All
Tools Used:	Burpsuite, XSS
References:	https://github.com/payloadbox/xss-payload-list

Evidence

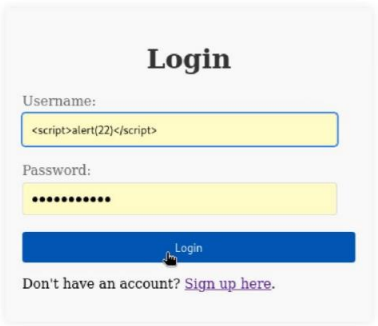


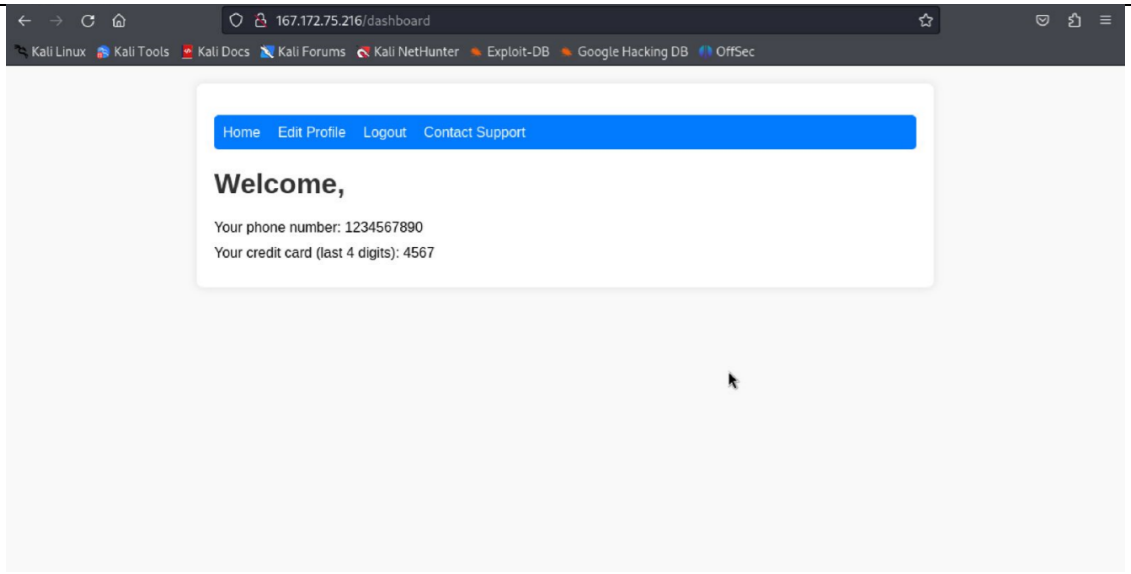
Apabila auth_token tersebut kita pakai pada akun lain, maka kita bisa masuk ke akun praktikumethack tersebut tanpa tahu password

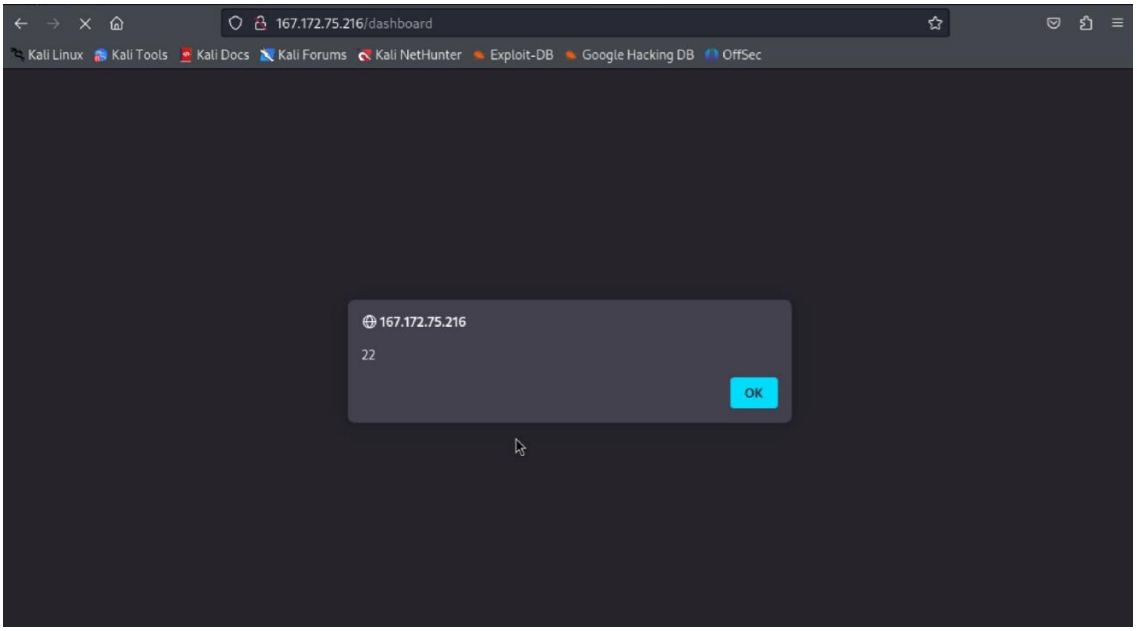
Finding IPT-002 : Script Execution on Notification using XSS

Description:	Saat mencoba LOGIN dengan nama pengguna <script>alert(022)</script>, pesan 167.172.75.216 069 muncul. Skrip JavaScript yang berhasil dieksekusi yang disuntikkan ditunjukkan oleh teks pemberitahuan. Hal ini menunjukkan bahwa program ini memiliki kerentanan XSS karena input pengguna tidak dibersihkan secara memadai sebelum ditampilkan kepada pengguna.
Risk:	Tinggi: Penyerang dapat memasukkan skrip berbahaya ke dalam aplikasi dengan menggunakan kerentanan XSS. Ketika pengguna lain menjalankannya, penyerang dapat memanfaatkan sesi pengguna, mengubah tampilan halaman, atau melakukan perbuatan jahat lainnya.
System:	All
Tools Used:	Burpsuite, XSS
References:	https://github.com/payloadbox/xss-payload-list

Evidence



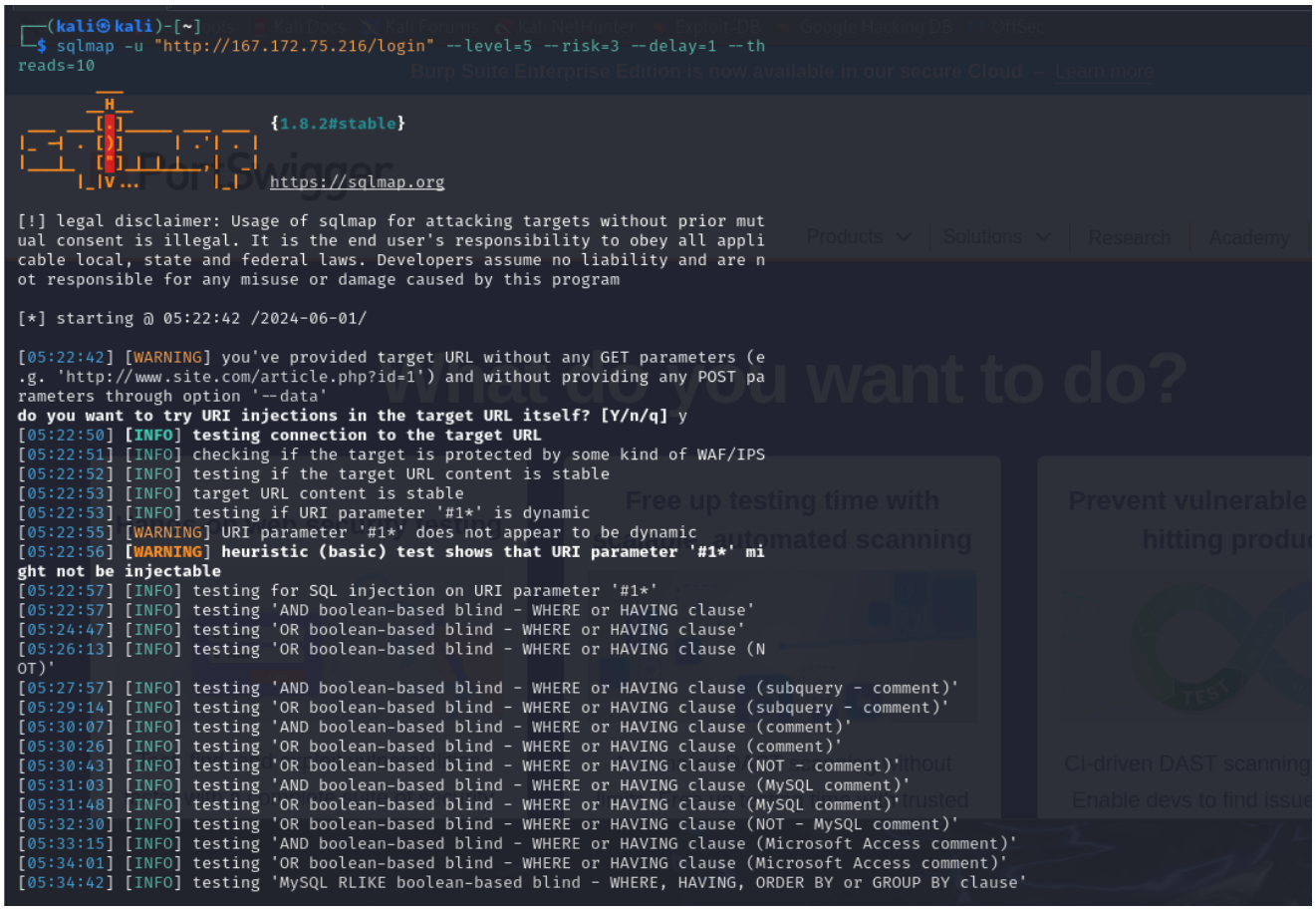


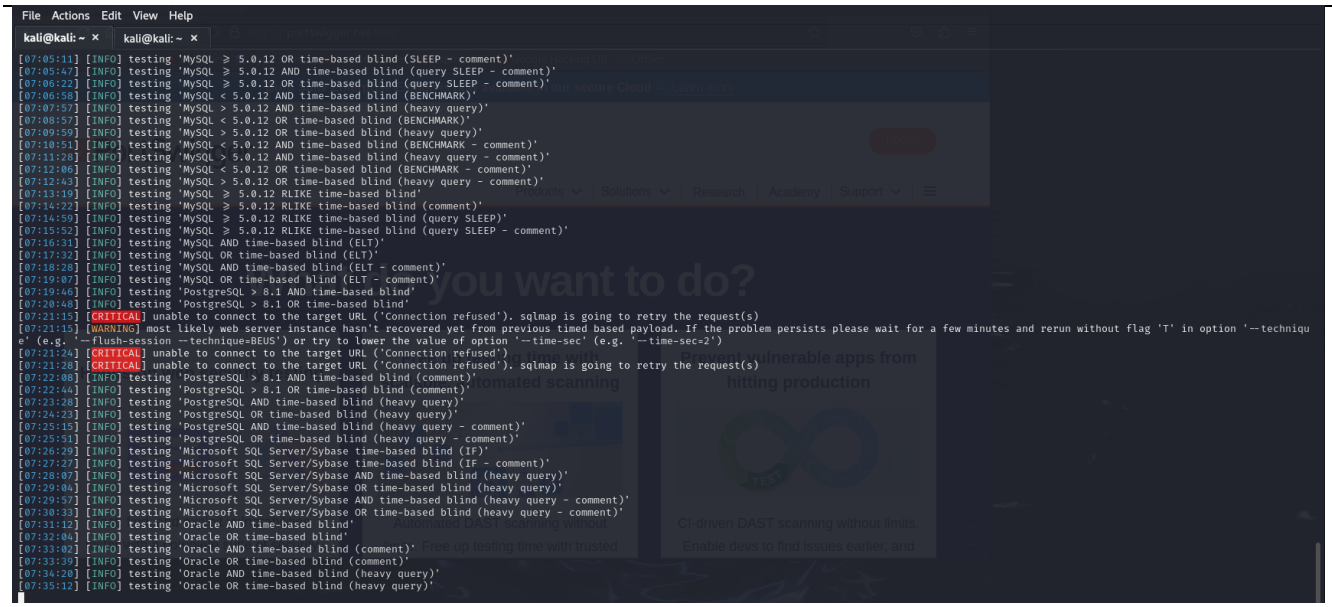


Finding IPT-003 : SQLMap

Description:	SQLMap adalah alat otomatisasi open-source yang digunakan untuk mendeteksi dan mengeksploitasi kerentanan SQL injection pada aplikasi web. SQLMap memiliki kemampuan untuk melakukan berbagai jenis serangan SQL injection, termasuk deteksi, pengambilan data, pengeksekusian perintah pada sistem operasi, dan banyak lagi. Alat ini sangat berguna bagi peneliti keamanan dan penguji penetrasi untuk mengidentifikasi kerentanan dalam aplikasi web.
Risk:	Tinggi: Menggunakan alat seperti SQLMap dengan pengaturan risiko tinggi (--risk=3) dan pengujian mendalam (--level=5) dapat membantu mendeteksi kerentanan serius, namun selalu dilakukan dengan hati-hati dan dalam batas yang diizinkan untuk menghindari kerusakan pada aplikasi web.
System:	All
Tools Used:	SQLMap
References:	

Evidence





Hasil :

Tidak ada informasi penting yang didapatkan dari proses ini.

Last Page