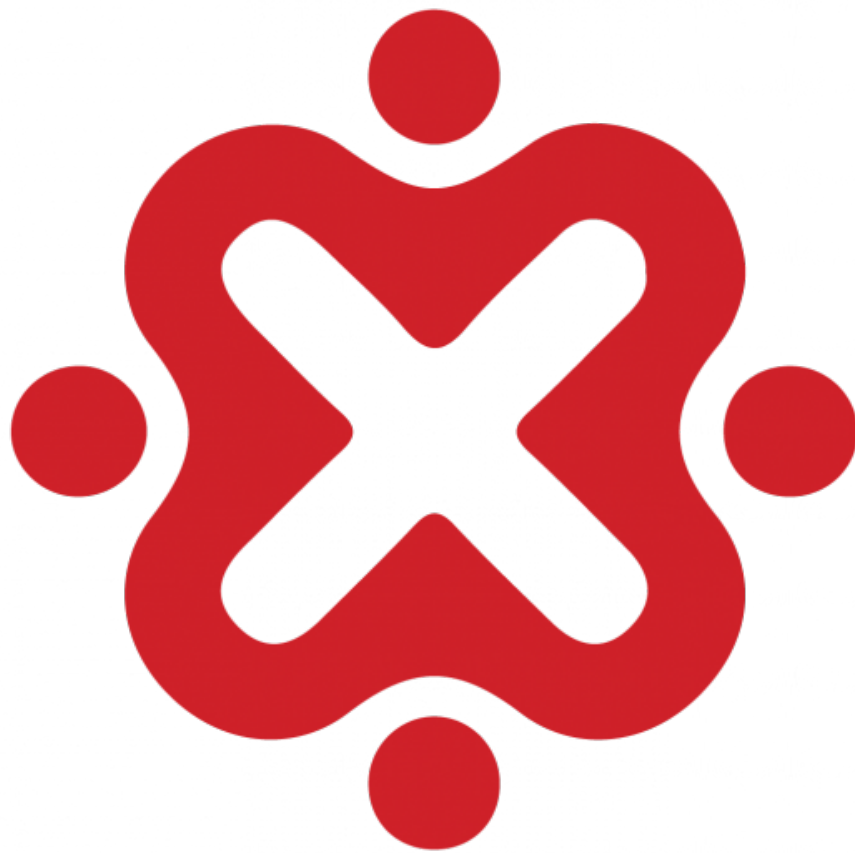


Praktikum

Pengujian Penetrasi pada Laboratorium

InsecureBankv2



ID-Networkers
Indonesian IT Expert Factory



Dokumentasi Praktikum Pengujian Penetrasi

1. Informasi Umum

- **Nama Peserta:** Himawan Imtikhan Azmi
- **Tanggal Praktikum:** 23 – 29 Juni 2025
- **Nama Praktikum:** Pengujian Penetrasi pada Lab. InsecureBankv2
- **Target Sistem:** Laboratorium InsecureBankv2 berbasis Mesin Virtual
- **IP/URL Target:** 10.0.2.6 (Android x86) dan 10.0.2.15 (Kali Linux - AndroLabServer)

2. Tujuan Praktikum

Untuk menguji pengetahuan dan keterampilan dalam mengidentifikasi dan mengurangi kerentanan keamanan umum aplikasi *mobile* dalam lingkungan hukum (atau lingkungan kelas yang terkendali).

3. Tools dan Bahan

- Tools utama: MobSF (Aplikasi berbasis web).
- VM/Lab environment: Android-x86 7.1-R5 Nougat berisi Lab. InsecureBankv2 (Target) dan Kali Linux 2025.2 (Penyerang)

4. Metodologi Pengujian

Metodologi pengujian yang digunakan dalam praktikum ini menggunakan standar dan kerangka kerja uji penetrasi OWASP *Mobile Security Testing Guide (MSTG)* yang meliputi enam tahap yaitu:

- a. *Persiapan:* Meliputi perencanaan dan persiapan lingkungan pengujian.
- b. *Static Analysis:* Meliputi analisis file APK (*Android Package Kit*) secara manual dengan alat seperti MobSF atau jadx.
- c. *Dynamic Analysis:* Meliputi analisis aplikasi yang dijalankan secara langsung di perangkat dan mengamati perilakunya.
- d. *API Testing*
- e. *Reverse Engineering & Tampering*
- f. *Pelaporan & Penilaian Tingkat Kerentanan (Scoring)*

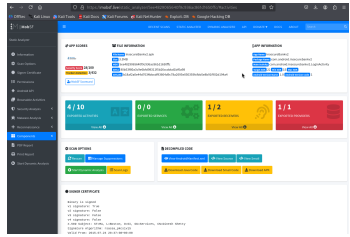
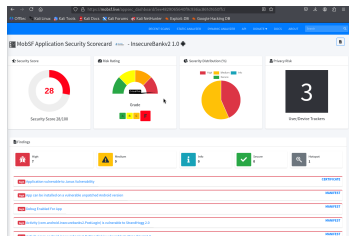


5. Langkah-Langkah Praktikum

Langkah-langkah yang dilakukan dalam pengujian berdasarkan metodologi yang digunakan:

1. Mengakses *server* lab. InsecureBankv2 pada perangkat mesin virtual
2. Mengidentifikasi jenis kerentanan dan menentukan alat uji penetrasi yang sesuai untuk jenis kerentanan.
3. Melakukan uji coba serangan menggunakan alat yang sesuai dengan jenis kerentanan.
4. Menganalisis temuan dan memberikan rekomendasi atau saran sebagai upaya pencegahan.
5. Mendokumentasikan proses praktikum dan menuliskan laporan praktikum.

6. Temuan dan Analisis

No	Jenis Kerentanan	Deskripsi Temuan	Dampak	Bukti (Screenshot/Request)
1	<i>Janus Vulnerability</i> (Kerentanan Janus) [CVE-2017-13156]	Terdapat kerentanan yang dideteksi oleh MobSF sebagai <i>Janus Vulnerability</i> dengan skor tinggi.	Memungkinkan penyerang untuk memodifikasi aplikasi yang tidak terdeteksi.	
2	Kerentanan StrandHogg 2.0	Ditemukan kerentanan pembajakan tugas StrandHogg 2.0 melalui analisis statis MobSF.	Memungkinkan bagi aplikasi lain untuk menempatkan aktivitas berbahaya di atas tumpukan aktivitas aplikasi yang rentan. Hal ini membuat aplikasi menjadi target yang mudah untuk serangan phishing.	



7. Rekomendasi Perbaikan

Upaya yang dapat dilakukan sebagai langkah pencegahan adalah sebagai berikut:

- a) *Janus Vulnerability*
 - 1) Perbarui perangkat Android ke versi perangkat lunak saat ini.
 - 2) Verifikasi bahwa aplikasi yang diunduh dipercaya dan/atau hanya menggunakan V2.
 - 3) Pertimbangkan aplikasi daftar putih pada perangkat perusahaan.
- b) *StrandHogg 2.0 Task Hijacking*

Kerentanan dapat diperbaiki dengan menetapkan atribut mode peluncuran ke *"singleInstance"* dan dengan menetapkan *taskAffinity* kosong (*taskAffinity=""*). Dan memperbarui target versi SDK (22) dari aplikasi ke 29 atau lebih tinggi untuk memperbaiki masalah ini di tingkat *platform*.

8. Evaluasi dan Refleksi

Jawab pertanyaan berikut:

- Apa tantangan utama dalam praktikum ini?

Minimnya pengetahuan praktikan akan jenis kerentanan yang ada pada aplikasi *mobile* menyebabkan lamanya proses pengujian kerentanan. Selain jenis kerentanan, pengetahuan akan alat uji yang sesuai dan cara menggunakannya juga menjadi tantangan dalam laboratorium ini.
- Apakah ada tools/metode yang tidak berjalan sesuai ekspektasi?

Tidak ada, semua berjalan dengan semestinya dan sesuai harapan.
- Apa pelajaran paling penting yang dipelajari dari praktikum ini?

Mengetahui jenis kerentanan aplikasi *mobile* menjadi salah satu hal penting untuk menciptakan ekosistem digital yang aman. Selain itu, mengetahui proses pengujian kerentanan aplikasi *mobile* juga menjadi bagian yang tak kalah penting dalam belajar keamanan siber.

9. Lampiran



```
Android-x86 7.1-R5 Nougat [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Window 1
3: ip6_vti0@NONE: <NOARP> mtu 1500 qdisc noop state DOWN group default qlen 1
   link/tunnel6 :: brd ::
4: sit0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1
   link/sit 0.0.0.0 brd 0.0.0.0
5: ip6tnl0@NONE: <NOARP> mtu 1452 qdisc noop state DOWN group default qlen 1
   link/tunnel6 :: brd ::
6: wifi_eth: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
   link/ether 08:00:27:16:31:b2 brd ff:ff:ff:ff:ff:ff
   inet6 fe80::a00:27ff:fe16:31b2/64 scope link
       valid_lft forever preferred_lft forever
7: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
   link/ether 08:00:27:16:31:b2 brd ff:ff:ff:ff:ff:ff
   inet 10.0.2.6/24 brd 10.0.2.255 scope global wlan0
       valid_lft forever preferred_lft forever
   inet6 fe80::a00:27ff:fe16:31b2/64 scope link
       valid_lft forever preferred_lft forever
x86_64:/ $
```

Figure 1: IP Address dari Mesin Virtual Android x86 7.1-R5 Nougat

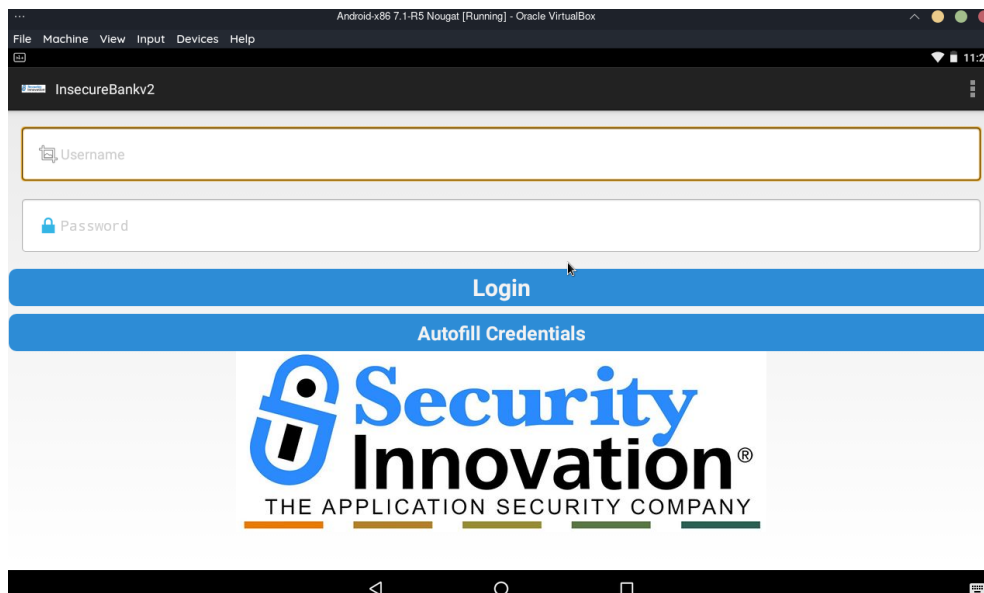


Figure 2: Aplikasi InsecureBankv2 yang dipasang di Mesin Virtual Android x86

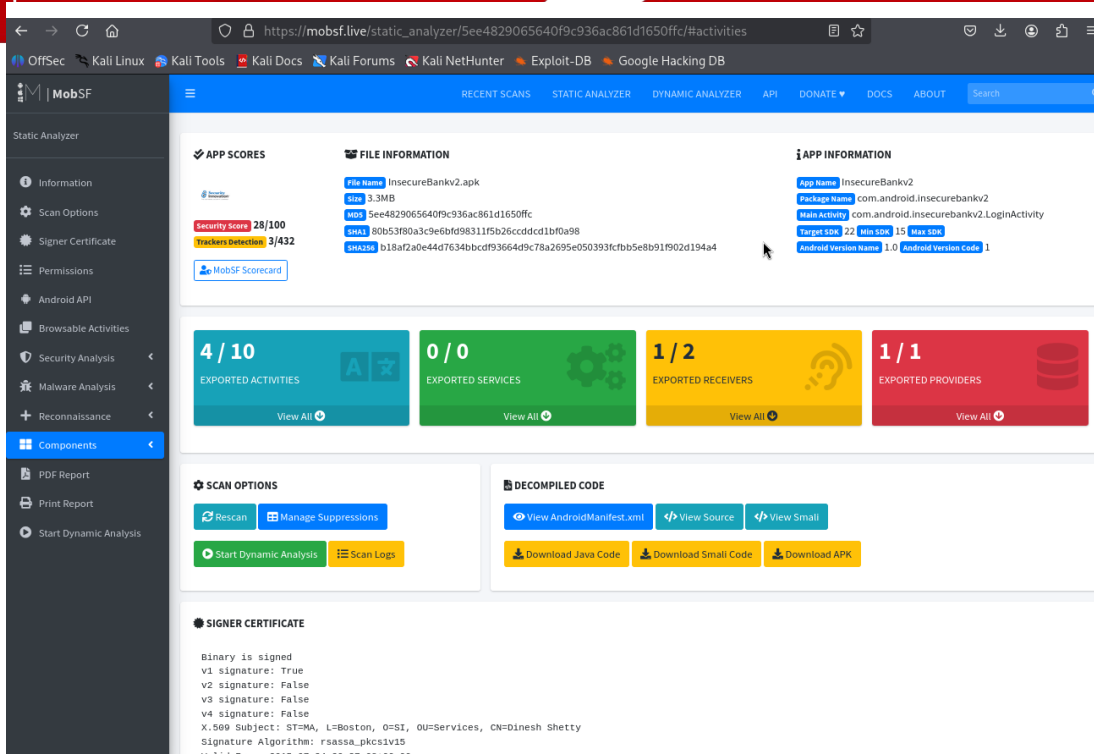


Figure 3: Hasil Analisis Statis oleh MobSF

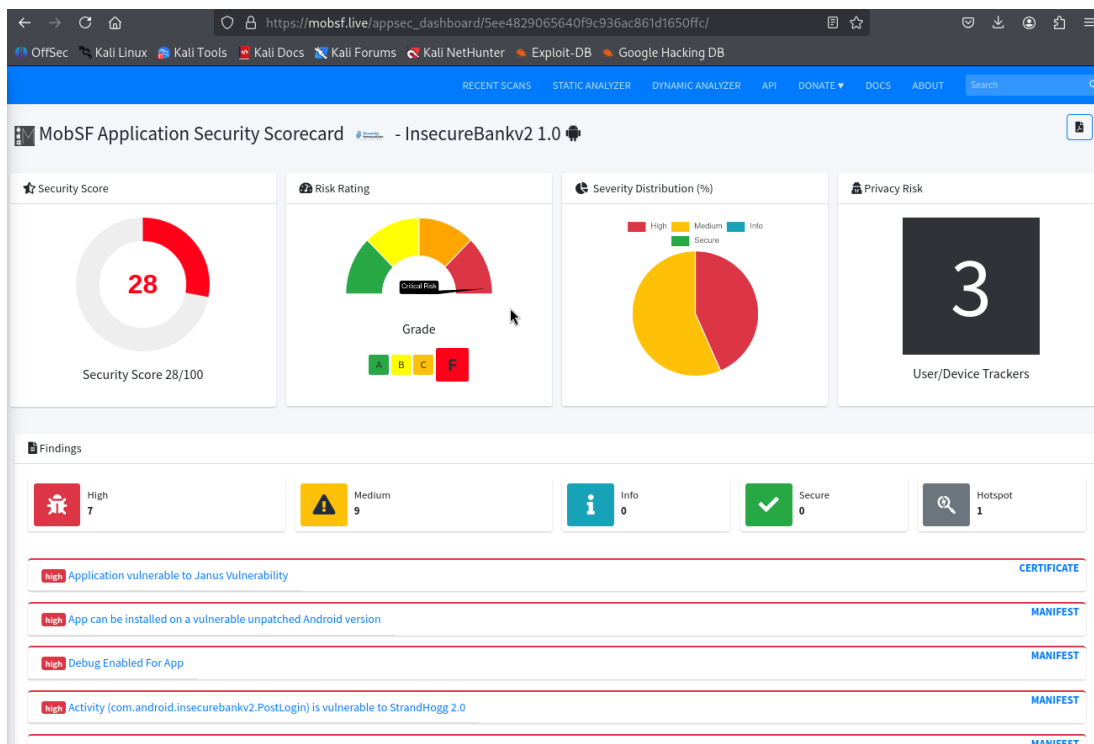


Figure 4: Hasil MobSF AppSec Scorecard



10. Referensi

- <https://github.com/dineshshetty/Android-InsecureBankv2>
- <https://owasp.org/www-project-mobile-app-security/>
- <https://github.com/OWASP/owasp-masvs>
- <https://medium.com/@uaybora/insecurebankv2-analysis-and-poc-360c13723189>
- <https://can-ozkan.medium.com/insecurebankv2-apk-android-walkthrough-34f83d814cfe>
- <https://gist.github.com/ruevaughn/54b254b831f77537199e40cb482d6a25>
- <https://www.cve.org/CVERecord?id=CVE-2017-13156>