

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

**BÁO CÁO BÀI TẬP 3: TÌM HIỂU CÔNG CỤ KIỂM THỬ**

**Môn: Kiểm thử xâm nhập**

Giảng Viên : Đinh Trường Duy

Nhóm BTL: Nhóm 07

**Sinh viên thực hiện:**

Vũ Ngọc Phương B20DCAT142

Ninh Chí Hướng B20DCAT094

Hoàng Trung Kiên B20DCAT098

Nguyễn Văn Khang B20DCAT102

Nguyễn Trần Minh B20DCAT126

Lê Đình Quân B20DCAT146

**Hà Nội – 2024**

**Mục lục**

[I. Tìm hiểu công cụ Công cụ MobSF. 3](#_Toc166275022)

[1. Giới thiệu. 3](#_Toc166275023)

[**2.** Chức năng chính của MobSF. 3](#_Toc166275024)

[3. Ưu nhược điểm của MobSF. 4](#_Toc166275025)

[II. Cài đặt sử dụng công cụ MobSF. 5](#_Toc166275026)

[1. Cài đặt 5](#_Toc166275027)

[2. Kết luận và đánh giá chung mức độ bảo mật của ứng dụng: 10](#_Toc166275028)

[3. Biện pháp khắc phục. 10](#_Toc166275029)

# I. Tìm hiểu công cụ Công cụ MobSF.

## 1. Giới thiệu.

Mobile Security Framework (MobSF) là nền tảng nghiên cứu bảo mật dành cho các ứng dụng di động trên Android, iOS và Windows Mobile. MobSF có thể được sử dụng cho nhiều trường hợp sử dụng khác nhau như bảo mật ứng dụng di động, kiểm tra thâm nhập, phân tích phần mềm độc hại và phân tích quyền riêng tư. Trình phân tích tĩnh hỗ trợ các tệp nhị phân ứng dụng di động phổ biến như APK, IPA, APPX và mã nguồn. Trong khi đó, Trình phân tích động hỗ trợ cả ứng dụng Android và iOS, đồng thời cung cấp nền tảng để kiểm tra thiết bị tương tác, dữ liệu thời gian chạy và phân tích lưu lượng mạng. MobSF tích hợp liền mạch với quy trình DevSecOps hoặc CI/CD của bạn, được hỗ trợ bởi các API REST và công cụ CLI, giúp nâng cao quy trình làm việc bảo mật của bạn một cách dễ dàng.

## **2.** Chức năng chính của MobSF.

* MobSF có thể thực hiện nhiều loại phân tích khác nhau và chức năng, bao gồm:
* **Phân tích tĩnh:** Phân tích mã nguồn ứng dụng để tìm kiếm các lỗ hổng bảo mật tiềm ẩn.
* **Phân tích động:** Thực thi ứng dụng trên thiết bị thực hoặc giả lập để giám sát hành vi của nó và xác định các mối đe dọa tiềm ẩn.
* **Phân tích phần mềm độc hại:** Xác định xem ứng dụng có chứa phần mềm độc hại hay không.
* **Kiểm tra API web:** Phân tích các API web được sử dụng bởi ứng dụng để tìm kiếm các lỗ hổng bảo mật.
* **Báo cáo chi tiết:** MobSF tạo ra các báo cáo chi tiết về kết quả phân tích, giúp bạn dễ dàng xác định và sửa chữa các lỗ hổng bảo mật.
* **Tích hợp với các công cụ khác:** MobSF có thể tích hợp với các công cụ khác, chẳng hạn như Burp Suite và ZAP, để cung cấp cho bạn một cái nhìn toàn diện hơn về bảo mật ứng dụng của mình.

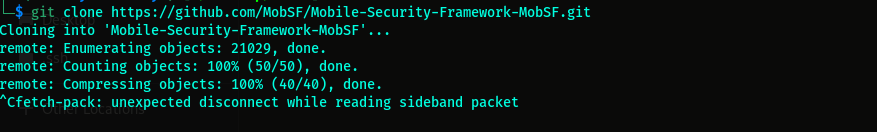
## 3. Ưu nhược điểm của MobSF.

* Ưu điểm của MobSF:
* **Miễn phí và mã nguồn mở:** MobSF là một công cụ miễn phí và mã nguồn mở, có nghĩa là bất kỳ ai cũng có thể sử dụng và sửa đổi nó. Điều này khiến nó trở thành một lựa chọn hấp dẫn cho các cá nhân và tổ chức có ngân sách hạn hẹp.
* **Dễ sử dụng:** MobSF có giao diện web trực quan giúp người dùng dễ dàng sử dụng và hiểu kết quả phân tích.
* **Hỗ trợ nhiều nền tảng:** MobSF hỗ trợ các hệ điều hành di động phổ biến như Android, iOS và Windows Phone.
* **Tính năng phong phú:** MobSF cung cấp nhiều tính năng khác nhau, bao gồm phân tích tĩnh, phân tích động, phân tích phần mềm độc hại và kiểm tra API web.
* **Có thể mở rộng:** MobSF có thể mở rộng với các plugin tùy chỉnh, cho phép người dùng thêm các chức năng mới vào công cụ.
* **Cộng đồng lớn:** MobSF có một cộng đồng người dùng lớn và tích cực, những người có thể cung cấp hỗ trợ và hướng dẫn.
* **Cập nhật thường xuyên:** MobSF được cập nhật thường xuyên với các tính năng và bản sửa lỗi mới.
* Nhược điểm của MobSF:
* **Có thể phức tạp đối với người mới bắt đầu:** Mặc dù MobSF có giao diện web trực quan, nhưng nó vẫn có thể phức tạp đối với người mới bắt đầu sử dụng công cụ phân tích bảo mật di động.
* **Yêu cầu kiến thức về bảo mật di động:** Để sử dụng MobSF hiệu quả, người dùng cần có kiến thức cơ bản về bảo mật di động.
* **Có thể mất thời gian để phân tích ứng dụng lớn:** Phân tích các ứng dụng di động lớn có thể mất nhiều thời gian, đặc biệt là khi sử dụng phân tích động.
* **Có thể tạo ra nhiều cảnh báo sai:** MobSF có thể tạo ra nhiều cảnh báo sai, khiến người dùng khó xác định các lỗ hổng thực sự.
* **Yêu cầu cài đặt:** MobSF cần được cài đặt trên máy tính cục bộ, điều này có thể không phù hợp với tất cả người dùng.

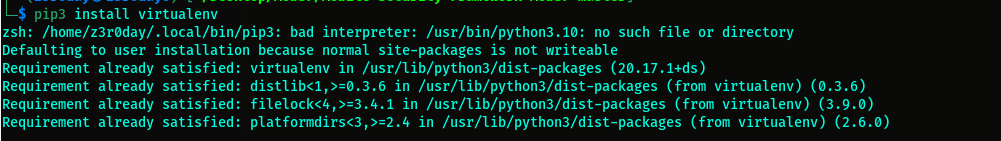
# II. Cài đặt sử dụng công cụ MobSF.

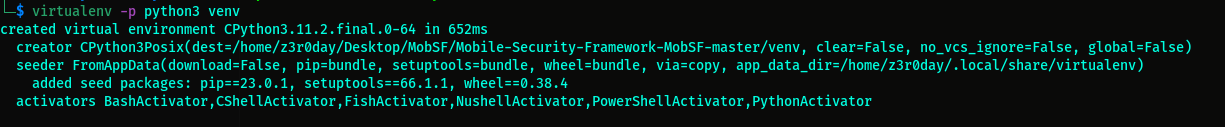
## 1. Cài đặt

* Tải về: <https://github.com/MobSF/Mobile-Security-Framework-MobSF>

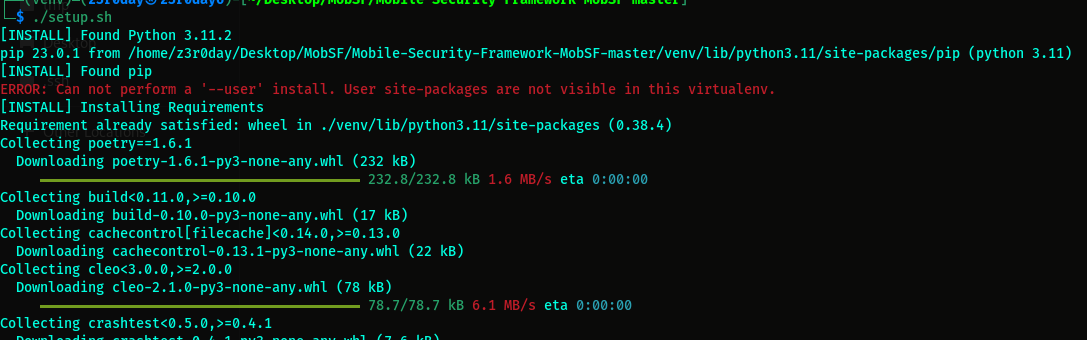


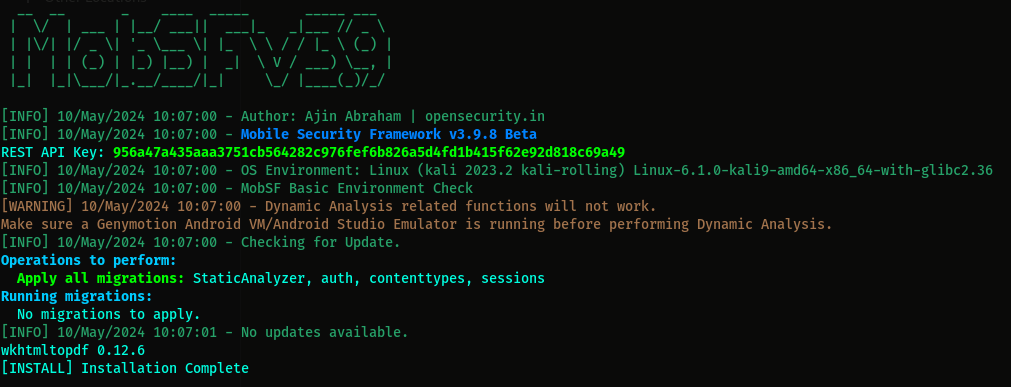
* Cài đặt môi trường ảo cho công cụ



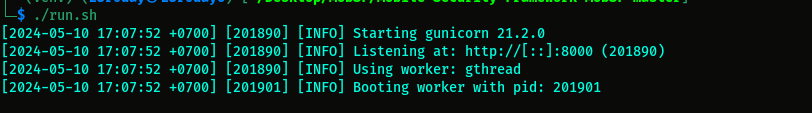


* Cài đặt các thành phần yêu cầu

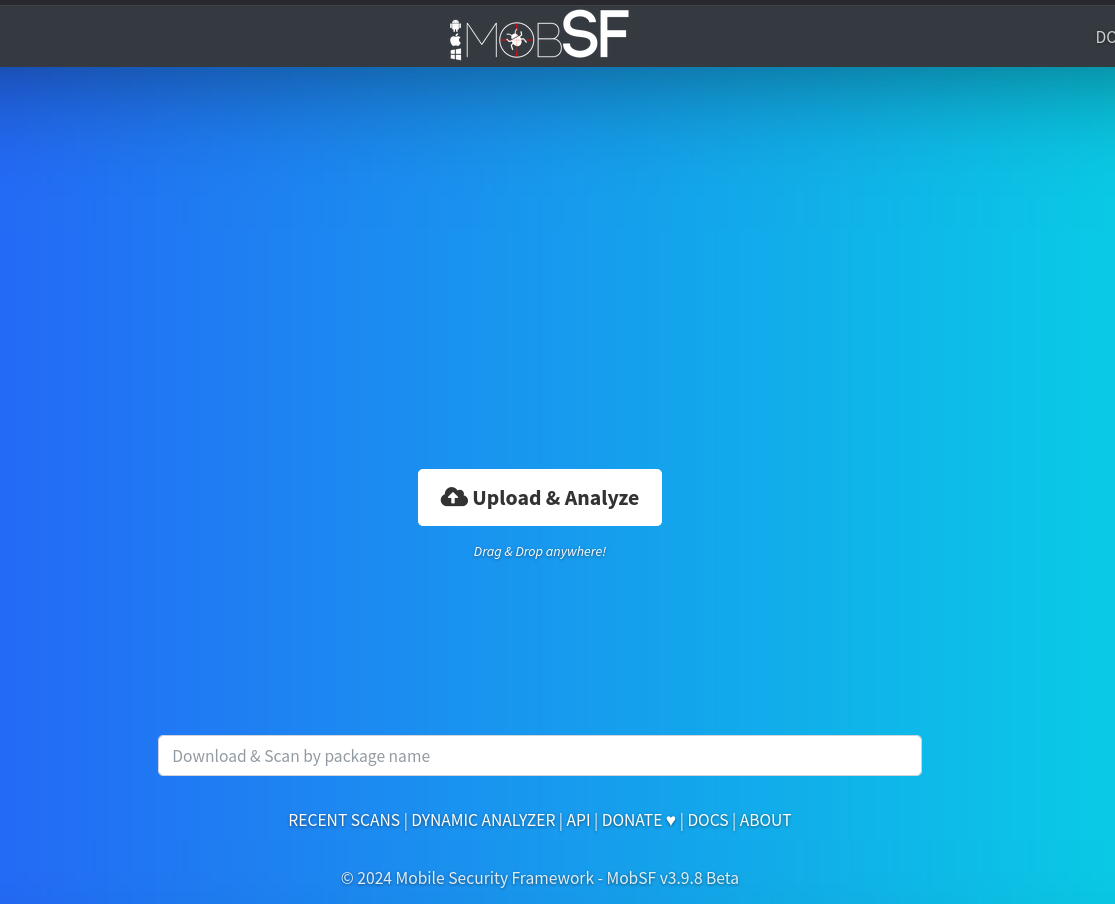




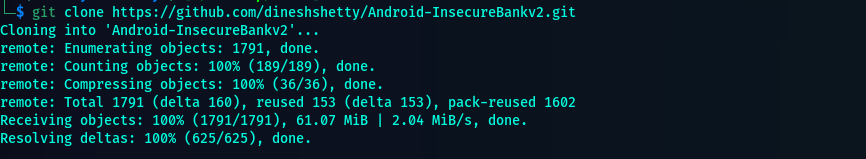
* Chạy công cụ



* Truy cập localhost:8000

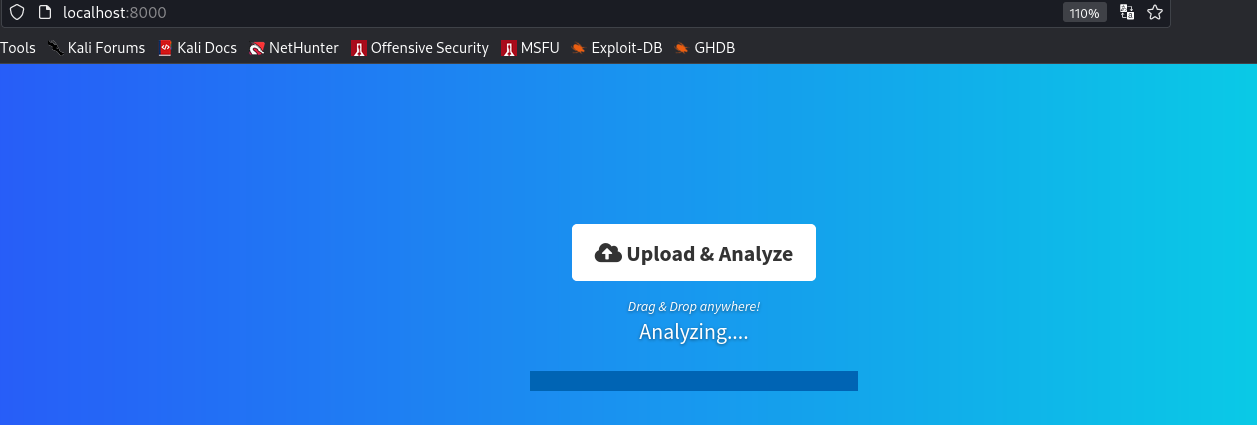


* Tiến hành phân tích:
* File sử dụng để phân tích: <https://github.com/dineshshetty/Android-InsecureBankv2>

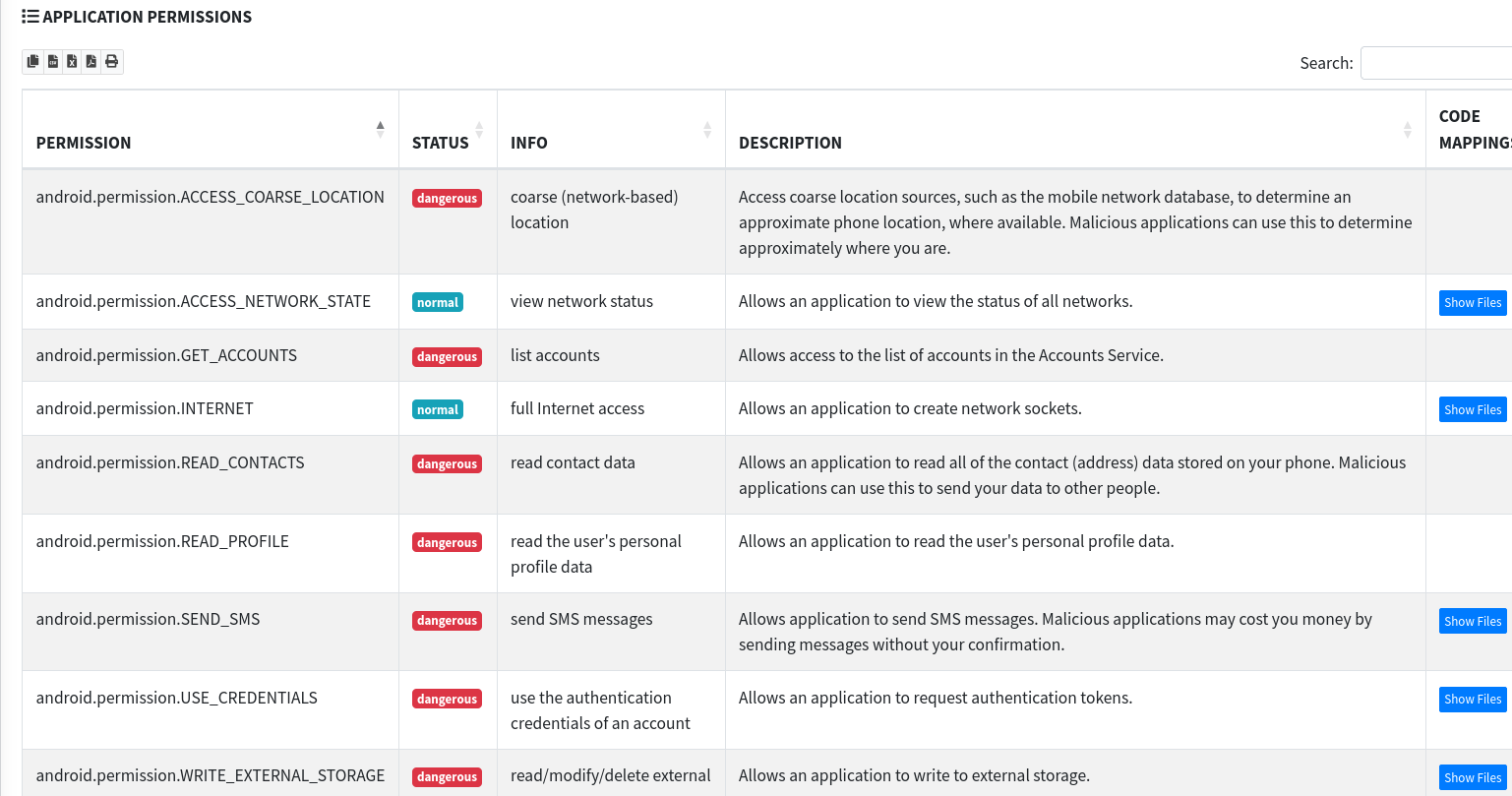




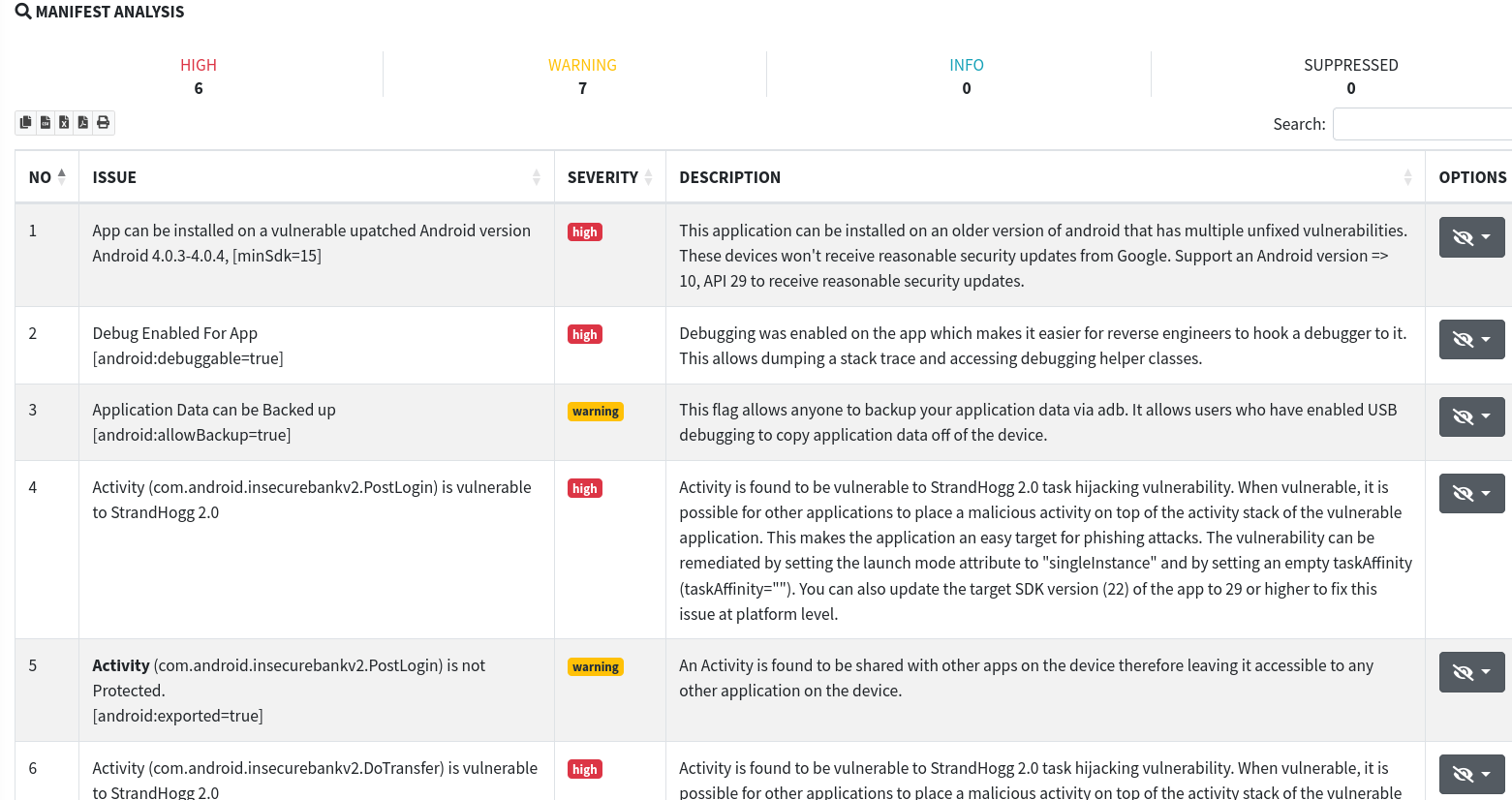
* Upload file apk lên công cụ phân tích mã nguồn:



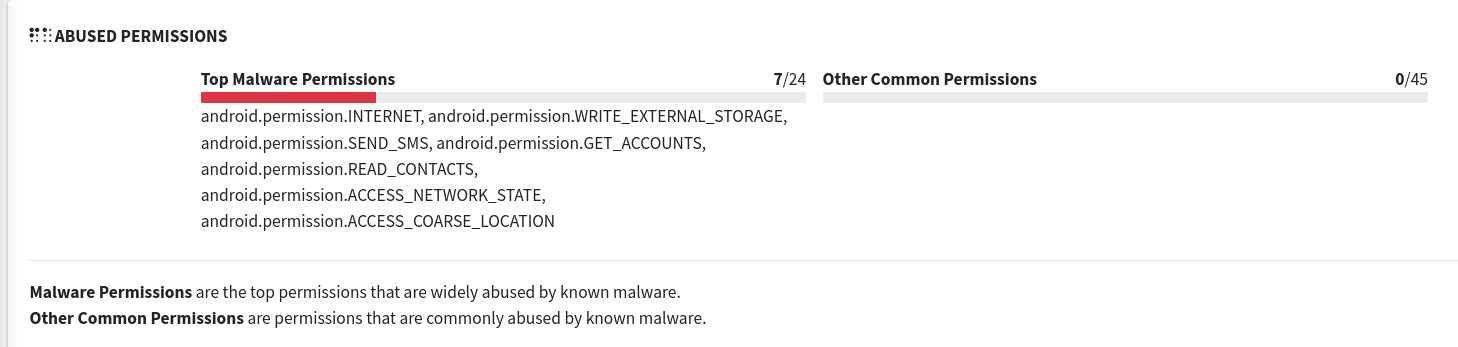
* Kết quả phân tích:
* Các lỗi phân quyền dựa trên cơ sở phân tích mã nguồn:



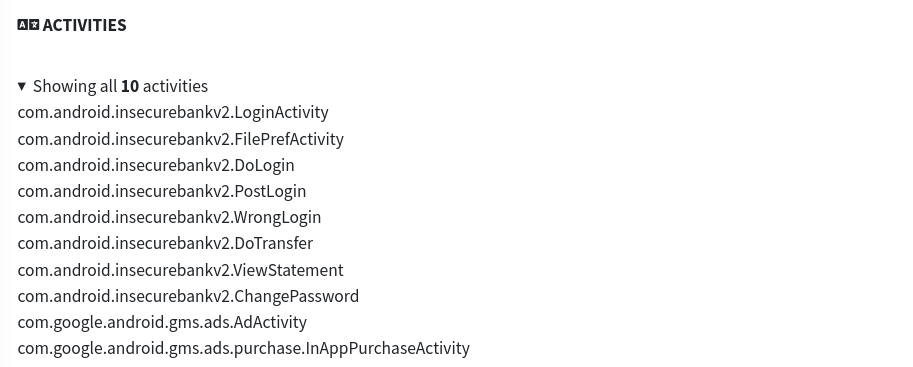
* Các lỗ hổng bảo mật dựa trên phân tích MANIFEST

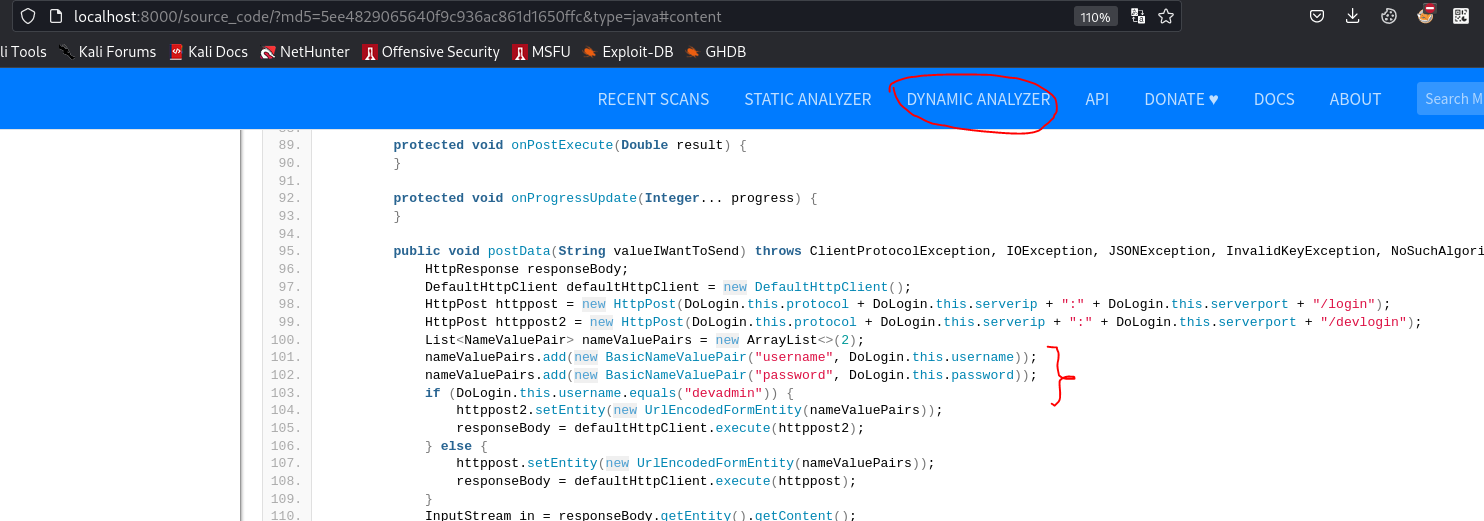
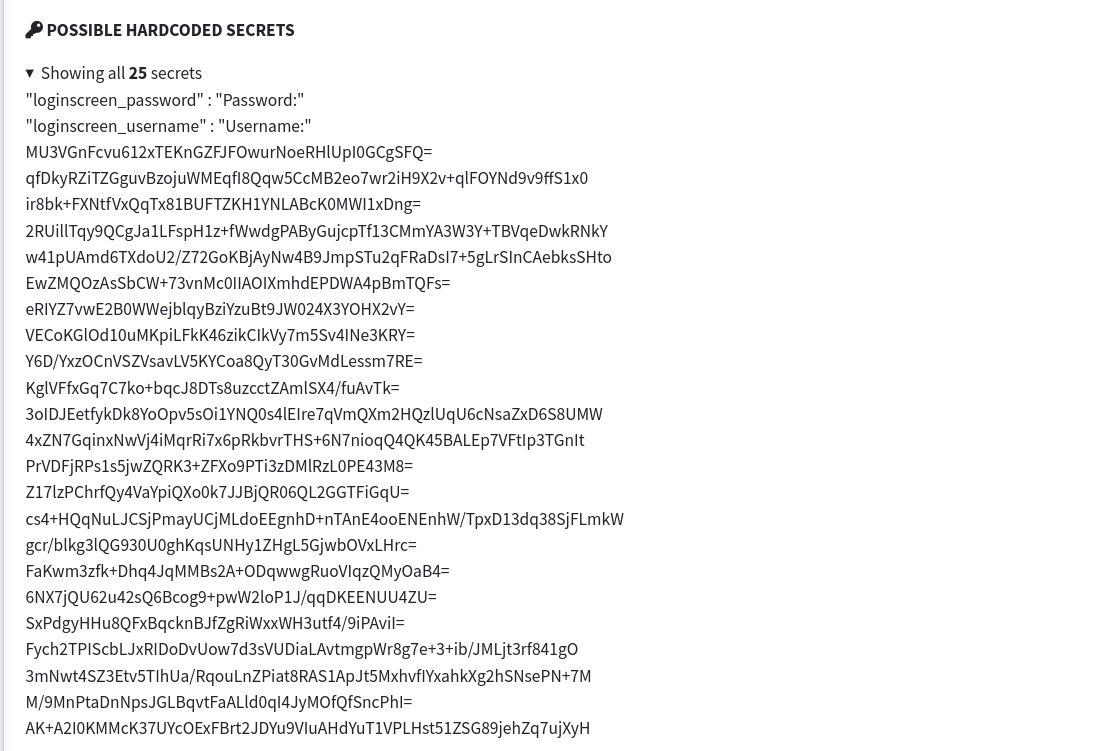


* Phân tích các quyền nguy hiểm chung của toàn bộ app:

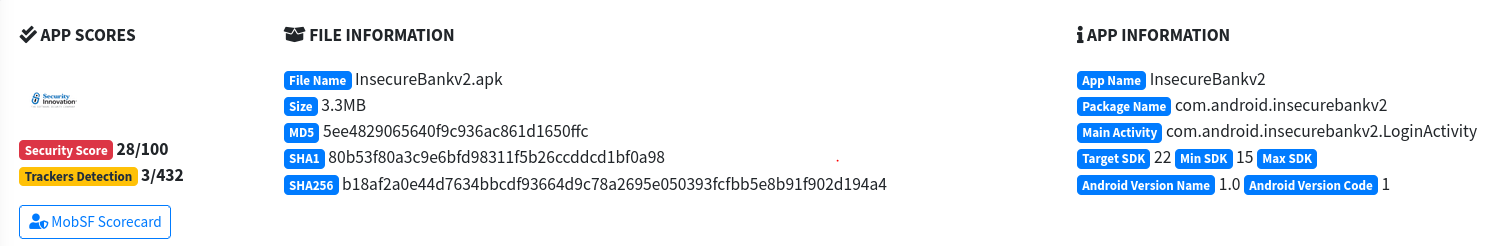


* Liệt kê toàn bộ activity chính có trong ứng dụng:



* Hiển thị đoạn mã có khả năng khai thác cao trong một số các activity chính:  
  
* Phân tích các giá trị khóa, biến được hardcode có giá trị cao:  
  

## 2. Kết luận và đánh giá chung mức độ bảo mật của ứng dụng:



## 3. Biện pháp khắc phục.

* Loại bỏ hoặc thay thế các đoạn hardcode
* Hạn chế quyền truy cập thiết bị của ứng dụng
* Mã hóa các chuỗi tĩnh trong mã nguồn
* Sử dụng các giải pháp bên thứ 3 để hạn chế việc dịch ngược ứng dụng