BÁO CÁO THỰC HÀNH

**Môn học: Bảo mật Web và ứng dụng**

**Lab 4: Pentesting Android Applications**

*GVHD: Ngô Đức Hoàng Sơn*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT132.O12.ATCL.2- Nhóm 4

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Đỗ Thị Yến Ly | 21520337 | [21520337@gm.uit.edu.vn](mailto:21520337@gm.uit.edu.vn) |
| 2 | Lê Hoàng Oanh | 21521253 | 21521253@gm.uit.edu.vn |
| 3 | Nguyễn Đại Bảo Duy | 21520772 | [21520772@gm.uit.edu.vn](mailto:21520772@gm.uit.edu.vn) |

1. **NỘI DUNG THỰC HIỆN:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | **Yêu cầu 1** | 100% |
| 2 | **Yêu cầu 2** | 100% |
| 3 | **Yêu cầu 3** | 100% |
| 4 | **Yêu cầu 4** | 100% |
| 5 | **Yêu cầu 5** | 100% |
| 6 | **Yêu cầu 6** | 100% |
| 7 | **Yêu cầu 7** | 100% |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

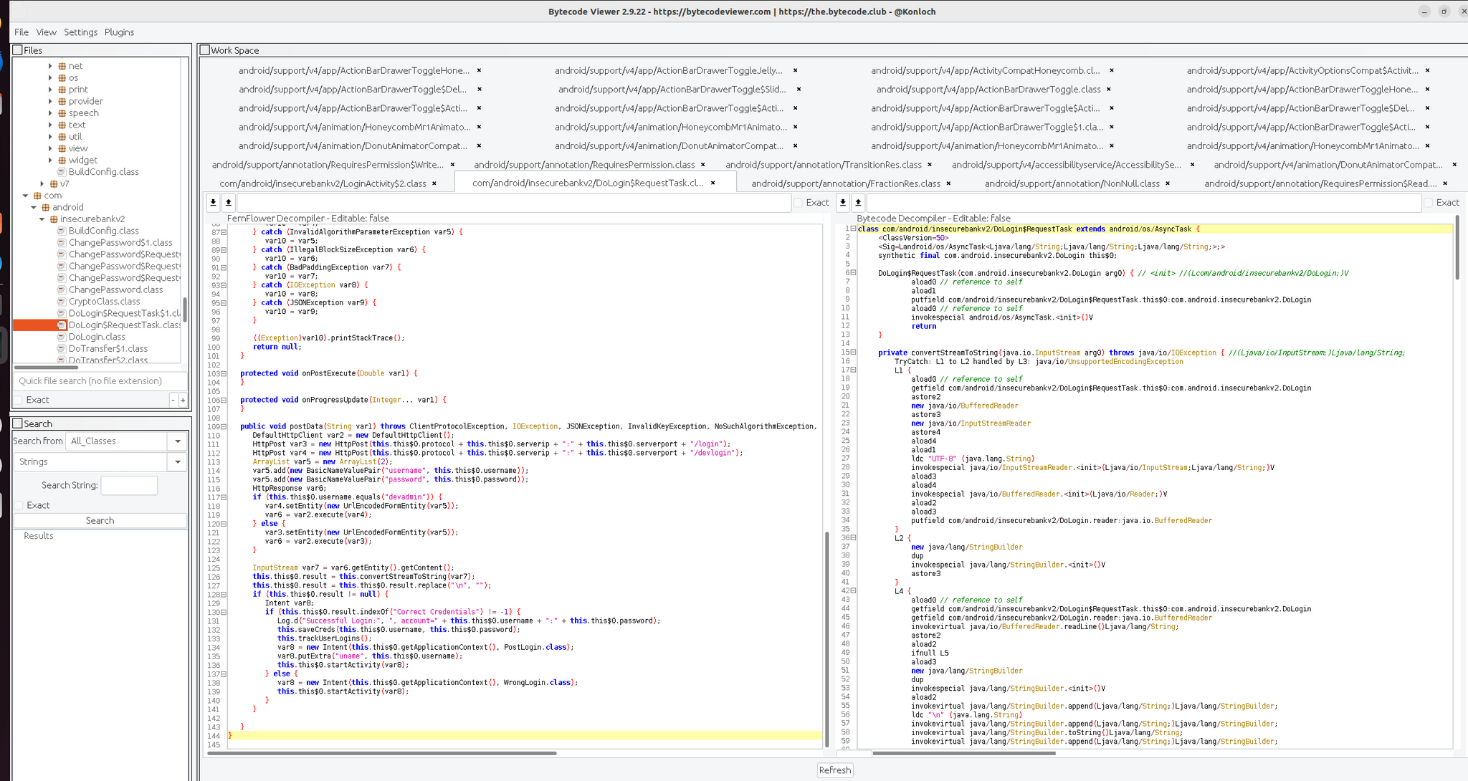
**Yêu cầu 1. Phân tích và chỉ ra điểm bất thường của đoạn code trên?**

Đầu tiên chạy chương trình phân tích code, ta thấy nó hiện một số lỗ hổng như USE\_CREDENTIALS,…

**A screenshot of a computer

Description automatically generated**

Tiếp theo, ta dùng ByteCode Viewer để xem code

****

Có một số điểm bất thường trong đoạn mã này:

* Sử dụng DefaultHttpClient: DefaultHttpClient đã bị loại bỏ từ API 23 và cao hơn.
* Sử dụng HTTP trong thời đại hiện tại: Mặc dù HTTP vẫn có thể hoạt động, nhưng nó không được khuyến khích sử dụng trong các ứng dụng mới. HTTPS là một tiêu chuẩn an toàn hơn. Sử dụng HttpsURLConnection hoặc OkHttpClient với HTTPS.
* Sử dụng BasicNameValuePair: Class BasicNameValuePair đã bị loại bỏ trong phiên bản Android mới nhất. Thay vào đó, bạn nên sử dụng NameValuePair từ gói org.apache.http.message.
* Xử lý response bằng cách convert InputStream thành String bằng cách thủ công: Điều này không hiệu quả và có thể dễ gây ra vấn đề về hiệu suất. Thay vào đó, bạn nên sử dụng EntityUtils.toString() để chuyển đổi response thành String.
* So sánh chuỗi bằng cách sử dụng indexOf: Điều này có thể không đủ chính xác và không linh hoạt. Thay vào đó, bạn nên sử dụng phương thức contains() hoặc equals().
* Sử dụng Intent để chuyển hướng giữa các Activity: Đoạn mã này đang sử dụng Intent để chuyển hướng giữa các Activity, điều này có thể dẫn đến vấn đề về quản lý bộ nhớ và hiệu suất. Sử dụng các phương thức khác như startActivityForResult hoặc Navigation Component để quản lý quá trình chuyển hướng Activity.
* Lưu trữ mật khẩu trong văn bản thô: Mật khẩu được lưu trữ dưới dạng văn bản thô trong mã nguồn, điều này không an toàn. Thay vào đó, sử dụng các phương pháp an toàn như SharedPreferences hoặc KeyStore để lưu trữ thông tin nhạy cảm như mật khẩu.
* Không xử lý các ngoại lệ một cách chính xác: Mã không xử lý các ngoại lệ một cách chính xác, ví dụ như không có xử lý cho IOException hoặc các ngoại lệ liên quan đến mã hóa và băm. Điều này có thể dẫn đến crash không mong muốn hoặc lỗ hổng bảo mật.

**Yêu cầu 2. Chỉ ra rằng dữ liệu lưu trữ có an toàn hay không?**

Ta sẽ thực hiện login và connect vào thiết bị sau đó sử dụng shell

Sau khi đã login vào, ta thấy màn hình sau:

A screenshot of a phone

Description automatically generated

Connect shell tới máy android

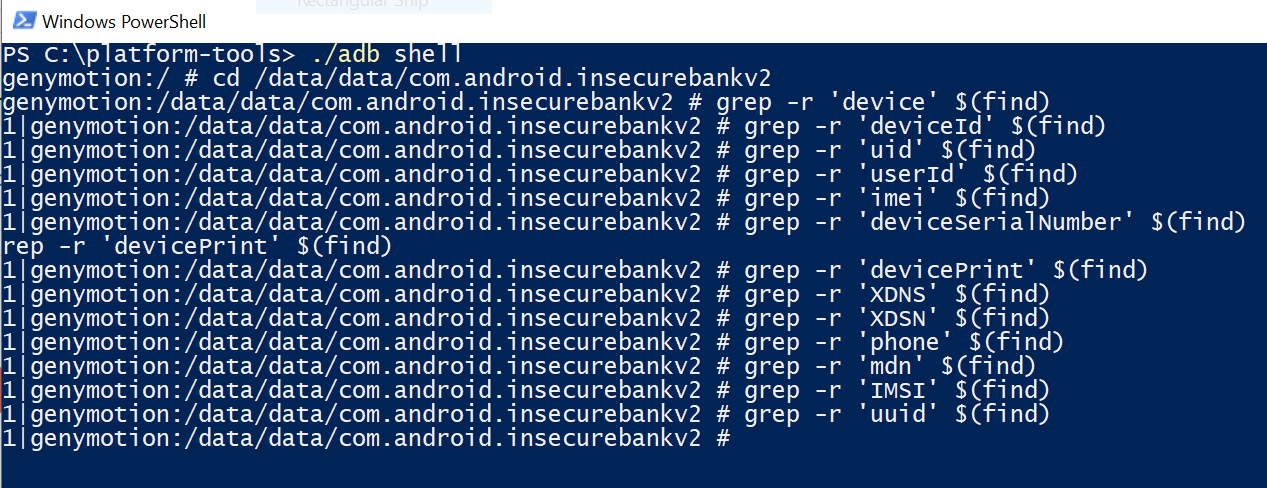
Xem thử trong database thì thấy có thông tin đăng nhập nhạy cảm không được mã hóa => không an toàn

A computer screen with white text

Description automatically generated

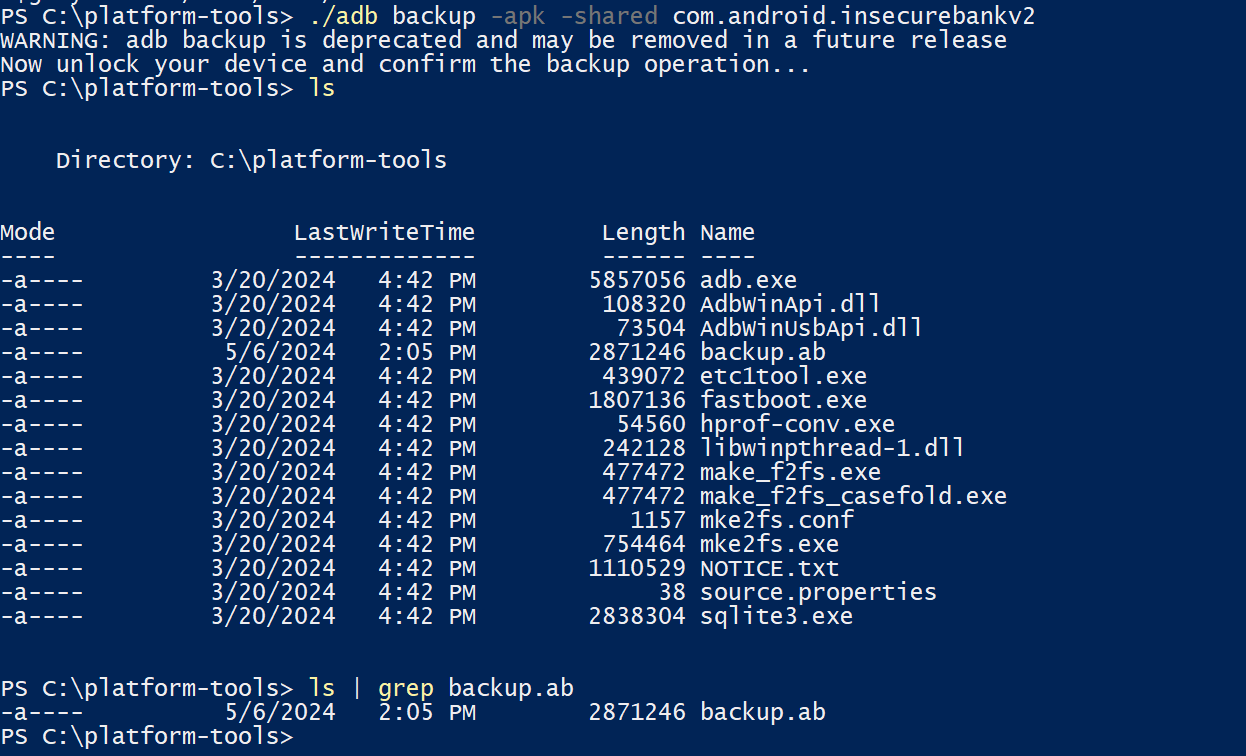
**Yêu cầu 3. Kiểm tra xem thông tin nhạy cảm có lưu lại trên thiết bị hay không? Một số từ khoá: deviceId, userId, imei, deviceSerialNumber, devicePrint, phone, XDSN, mdn, IMSI, uuid…**

Không thấy thông tin nhạy cảm nào được lưu lại



**Yêu cầu 4. Theo bạn thư mục sao lưu chứa thông tin nào cần mã hoá, chỉ ra.**

Tiếp tục quá trình ta sẽ thực hiện việc sao lưu thông tin, tạo nén và giải nén



A computer screen shot of a computer

Description automatically generated

Sau khi hoàn thành ta sẽ có file backup trên, thực hiện kiểm tra thì ta thấy có được một số thông tin được mã hoá

A computer screen with white text

Description automatically generated

Những thông tin database nên được mã hóa

A computer screen with white text

Description automatically generated

**Yêu cầu 5. Viết chương trình giải mã đoạn dữ liệu mã hoá (python3 chẳng hạn…)**

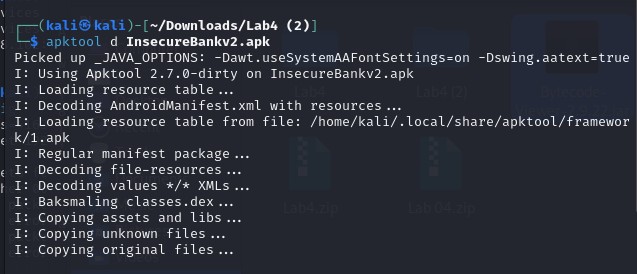
Ta thấy mã hoá đang sử dụng là AES CBC, với key là “This is the super secret key 123” và iv.

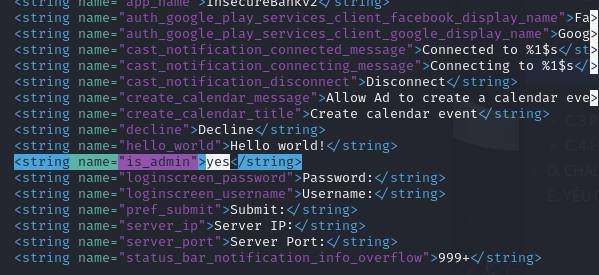
Ta thực hiện code python để giải mã thì ta có kết quả như sau:

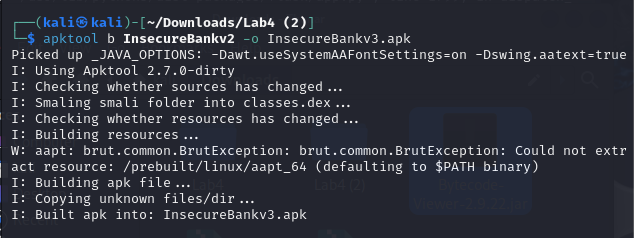


Ta thấy được thông tin bị mã hoá là mật khẩu của tài khoản Dinesh.

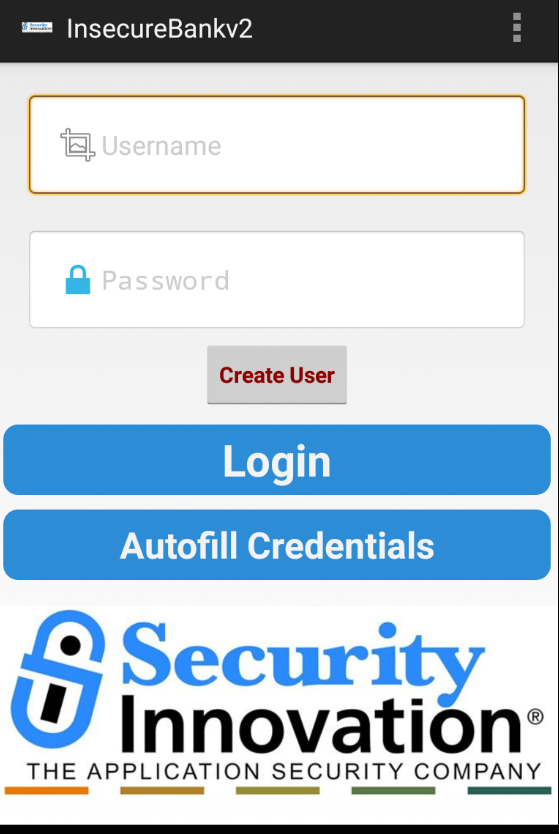
**Yêu cầu 6. Sinh viên điều chỉnh mã nguồn ứng dụng sao cho luôn hiển thị trạng thái “Rooted Device!!” với bất kỳ trạng thái nào của thiết bị.**

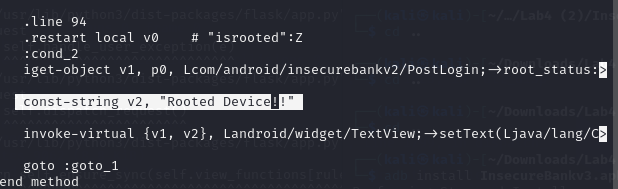


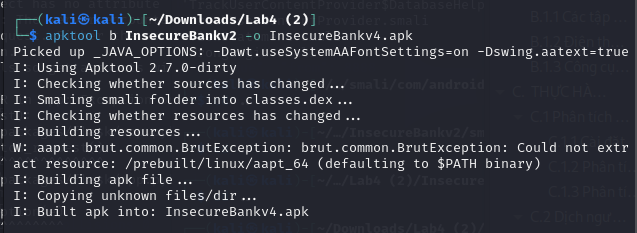


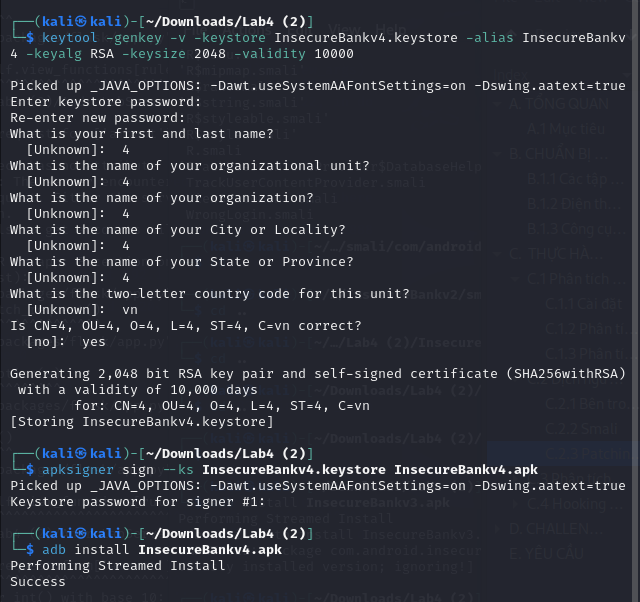


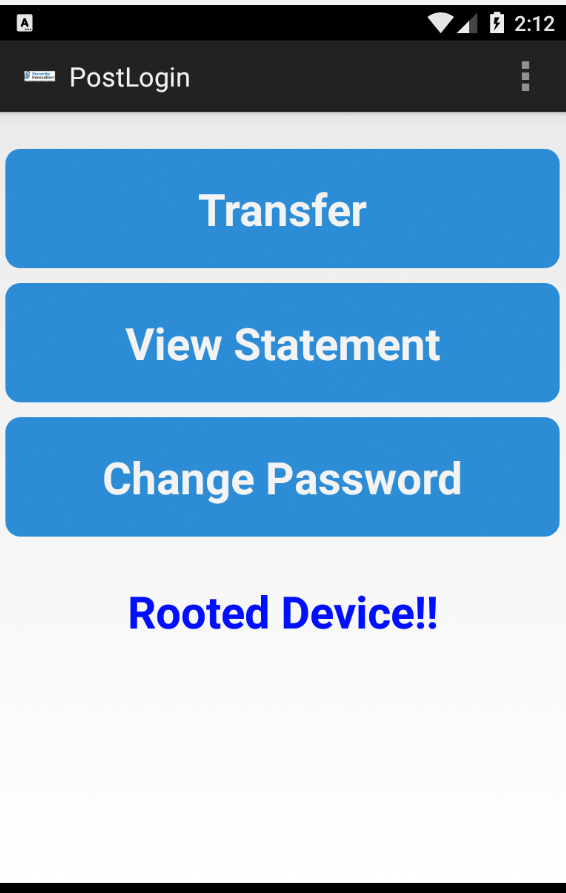












**Yêu cầu 7. Hoàn thiện đoạn code trên và demo.**