BÁO CÁO THỰC HÀNH

**Môn học: Bảo mật web và ứng dụng**

**Lab 6: Basic Android Secure Programming**

*GVHD: Ngô Khánh Khoa*

1. **THÔNG TIN CHUNG:**

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

Lớp: NT213.O21.ATTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Hà Thị Thu Hiền | 21522056 | 21522056@gm.uit.edu.vn |
| 2 | Phạm Ngọc Thơ | 21522641 | 21522641@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Tất cả các bài tập | 100% |

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

BÁO CÁO CHI TIẾT

1. **C.1 HelloWorld**

A screenshot of a computer

Description automatically generated

A screen shot of a cell phone

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **C.2 Tạo HTTP Request**

* Mục tiêu truy vấn đến server;
* Có thể tạo một Project mới;
* Ta sẽ code trên 2 tập tin MainActivity.java và AndroidManifest.xml
* Permission là gì? (https://developer.android.com/guide/topics/permissions/overview)
* Android sẽ không cho ta tương tác tới các thành phần hệ thống (Camera, Internet, Disk…), nếu muốn phải request permisson.
* Để gửi HTTP Request cần phải định nghĩa trong AndroidManifest.xml “2” permissons sau:

A screenshot of a computer program

Description automatically generated

A screen shot of a computer

Description automatically generated

A computer screen shot of a blue screen

Description automatically generated

A computer screen shot of a blue screen

Description automatically generated

A screen shot of a computer code

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a web sitemap

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **C.3 Android Activity**

* Activity là gì? (<https://developer.android.com/reference/android/app/Activity>)
* Là một hành động user có thể thực hiện.
* Bên trong một Activity có nhiều hàm callback như onCreate(), onStart()…
* Vòng đời của Activity như sau:

A diagram of activity

Description automatically generated

A screenshot of a computer

Description automatically generated

**A screenshot of a computer program

Description automatically generated**

**A screen shot of a computer

Description automatically generated**

* Thử với tất cả các phương thức callback của vòng đời activity xem như thế nào.

**A screenshot of a computer program

Description automatically generated**

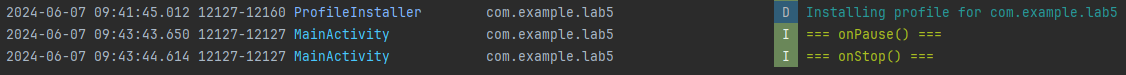
**A screen shot of a computer

Description automatically generated**

* Click vào home.

**A screen shot of a cell phone

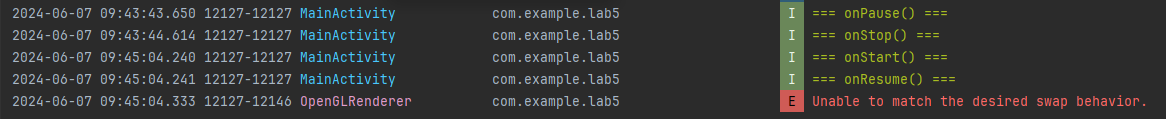
Description automatically generated**

****

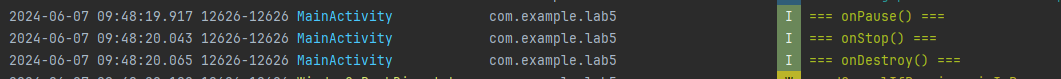
* Bấm vào overview, chọn lại app hello word đã tạo.

**A screenshot of a cell phone

Description automatically generated**

****

* Khi tắt app.

****

* **Các callback đều được gọi khi thực hiện đúng với bảng ban đầu.**

A screenshot of a computer

Description automatically generated

1. **C.4 Intent & Intent Filter**

* Intent & Intent Filter? (https://developer.android.com/guide/components/intents-filters)
* Hiểu nôm na là lời nhắn, các thành phần trong Android sử dụng lời nhắn để gọi nhau.
* Có 2 loại Intent là Explicit và Implicit
* **Explicit Intent:** dùng để gọi nội bộ ứng dụng, thường là activity A gọi activity B.

Intent i = new Intent(FirstActivity.class, SeacondActivity.class);

startActivity(i)

A couple of cell phones with text

Description automatically generated

* **Implicit Intent:** thường không cần tên của target. Implicit được sử dụng để gọi các thành phần của app khác.

A diagram of a system

Description automatically generated

* + [1] Activty A tạo 1 intent với 1 lời mời “mời gọi đối tượng” cụ thể thể rồi gọi hàm startActivity()
  + [2] Android System tự tìm ra các app có các đối tượng được định nghĩa trong “intent filter” của app khác.
  + [3] Khi tìm ra được rồi => Hệ thống gọi actvity (Activity B) bằng cách gọi onCreate() method của nó và đem vào Intent.

@Override  
protected void onCreate(Bundle savedInstanceState) {  
 super.onCreate(savedInstanceState);  
 setContentView(R.layout.*activity\_main*);  
 Intent read\_contact=new Intent();  
 read\_contact.setAction(android.content.Intent.*ACTION\_VIEW*);  
 read\_contact.setData(ContactsContract.Contacts.CONTENT\_URI);  
 startActivity(read\_contact);  
}

* + **Intent**: Được tạo với hành động ACTION\_VIEW và dữ liệu là URI của danh bạ (ContactsContract.Contacts.CONTENT\_URI).
  + **Intent Filter**: Hệ thống Android sẽ tìm kiếm các ứng dụng có intent filter phù hợp với hành động ACTION\_VIEW và URI này, sau đó khởi chạy ứng dụng đó để thực hiện hành động.

**Có phải thích gọi là gọi?**

Không phải lúc nào cũng có thể gọi là gọi, vì để một Implicit Intent hoạt động, cần phải có ít nhất một ứng dụng hoặc thành phần đã được đăng ký để xử lý hành động và dữ liệu đó thông qua intent filter. Nếu không có ứng dụng nào phù hợp, hệ thống sẽ không thực hiện hành động và có thể dẫn đến lỗi.

* Hệ điều hành Android sử dụng intent filter để định nghĩa Activities, Services và Broadcast receivers bài được gọi.

A screenshot of a computer

Description automatically generated

1. **C.5 Exploit Activity**

* Tạo một ứng dụng có thể exploit ứng dụng khác.
* Bài trước bypass được login bằng cách gọi trực tiếp vào activity PostLogin bằng lệnh “am” => Nhưng cần phải root máy, mới có terminal để chạy, ví dụ trường hợp không root được máy?

A computer screen shot of a computer program

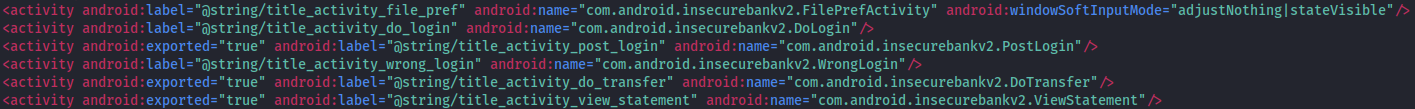
Description automatically generated

* Đọc tập tin AndroidManifest.xml

A screen shot of a computer program

Description automatically generated

* Tìm activity PostLogin?



* ***android:exported="true" ???***
* **Thuộc tính**: android:exported
* **Giá trị**: true hoặc false
  + true: Activity có thể được khởi chạy bởi các thành phần của ứng dụng khác.
  + false: Activity chỉ có thể được khởi chạy bởi các thành phần của cùng một ứng dụng hoặc các ứng dụng có cùng User ID.
* **Ý nghĩa của android:exported="true"**
* **Cho phép ứng dụng khác khởi chạy Activity**: Khi chúng ta đặt thuộc tính android:exported của một Activity là true, chúng ta đang cho phép các ứng dụng khác có thể khởi chạy Activity này. Điều này có nghĩa là các ứng dụng khác có thể gửi một Intent để mở Activity này.
* **Bảo mật và quyền riêng tư**: Việc cho phép ứng dụng khác khởi chạy Activity của chúng ta có thể hữu ích trong một số trường hợp, nhưng cũng có thể gây ra vấn đề về bảo mật và quyền riêng tư nếu không được kiểm soát đúng cách. Do đó, chúng ta cần chắc chắn rằng việc mở Activity này bởi ứng dụng khác không gây ra rủi ro bảo mật.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Trở lại MainActivity.java, ta định nghĩa Button vừa tạo. Sau đó code chức năng cho button.

A screen shot of a computer code

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated**A screenshot of a cell phone

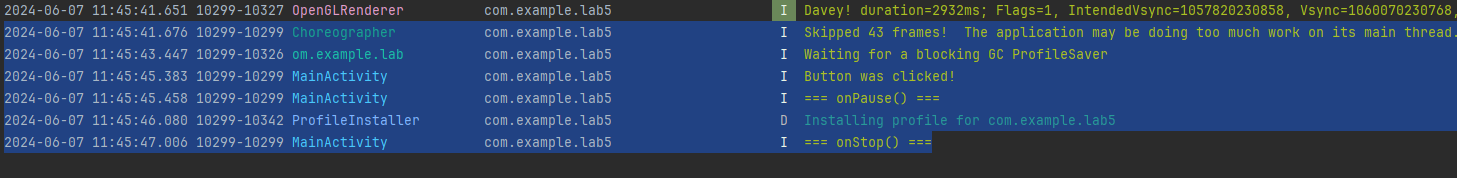
Description automatically generated**

**A screenshot of a computer program

Description automatically generated**

**A screenshot of a computer program

Description automatically generated**

****

1. **C.6 Broadcast Receivers**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

1. **C.7 Exploit Broadcast Receivers**

* Mục tiêu: Tạo được app exploit Broadcast Receivers của app khác.
* Mở tập tin AndroidManifest.xml của InsecureBankv2.apk

A screen shot of a computer program

Description automatically generated

* Đây là đoạn Broadcast Receiver, tên là “theBroadcast”, luồng xử lý sau khi broadcast này nhận được thông tin sẽ thực hiện trong onReceiver() của MyBroadCastRecceiver.
* ChangePassword gửi các parameter đến BroadcastReceivers.

A screenshot of a computer

Description automatically generated

1. **C.9 Xây dựng ứng dụng Android đơn giản**

**A screenshot of a computer

Description automatically generated**

**A screen shot of a cell phone

Description automatically generated**

**A screen shot of a cellphone

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screen shot of a cell phone

Description automatically generated**

1. **C.10 Hiện thực chức năng đăng nhập/đăng ký cho ứng dụng**

**A close up of a text

Description automatically generated**

**A screenshot of a computer program

Description automatically generated**

A screenshot of a computer program

Description automatically generated

A computer screen shot of a program

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated



* Register

A screen shot of a computer

Description automatically generated

* Sau khi register

A screen shot of a phone

Description automatically generated

* Login với tài khoản đã tạo

A screen shot of a phone

Description automatically generated

* Login thành công và password đã được mã hoá

A screen shot of a cell phone

Description automatically generated

****

Để tạo một cơ sở dữ liệu ngoài thiết bị và kết nối đến nó, chúng ta có thể sử dụng MySQL và PHP để tạo API REST. Điều này cho phép ứng dụng Android giao tiếp với cơ sở dữ liệu thông qua mạng. Dưới đây là các bước cơ bản để thực hiện điều này:

1. Thiết lập Cơ sở dữ liệu MySQL

* Tạo CSDL: Tạo một cơ sở dữ liệu MySQL trên máy chủ (có thể là localhost hoặc một máy chủ trực tuyến).
* Tạo Bảng: Tạo bảng để lưu trữ thông tin người dùng, ví dụ như users với các cột id, username, email, encrypted\_password.

2. Viết PHP Scripts

* API Endpoint: Viết các tập tin PHP để xử lý các yêu cầu từ ứng dụng Android. Chúng ta sẽ cần các endpoints cho đăng ký, đăng nhập, và các truy vấn khác.
* Kết nối CSDL: Script PHP sẽ kết nối đến MySQL để lấy hoặc cập nhật thông tin.
* Bảo mật: Đảm bảo rằng các yêu cầu đến API được xác thực (có thể sử dụng token).

3. Thay đổi Quyền trong Android

* **Internet Permission**: Đảm bảo rằng ứng dụng của có quyền truy cập Internet trong **AndroidManifest.xml**:



* **Network Security Config**: Nếu ta kết nối tới server không sử dụng HTTPS, chúng ta cần phải thêm config để cho phép giao tiếp không mã hóa trong **network\_security\_config.xml**:

A screen shot of a computer code

Description automatically generated

4. Gọi API từ Android

* **HttpClient**: Sử dụng một thư viện như **OkHttp** để thực hiện các yêu cầu HTTP từ Android đến PHP server.
* **Xử lý Response**: Xử lý câu trả lời từ server để thực hiện các tác vụ tiếp theo (chẳng hạn như chuyển đến một màn hình khác sau khi đăng nhập thành công).

**api/login.php**

<?php

include 'db\_config.php';

$username = $\_POST['username'];

$password = $\_POST['password']; // Đã được mã hóa từ client

// Tạo kết nối

$conn = new *mysqli*($servername, $dbusername, $dbpassword, $dbname);

// Kiểm tra kết nối

if ($conn->connect\_error) {

    die("Connection failed: " . $conn->connect\_fatal\_error());

}

$sql = "SELECT \* FROM users WHERE username = '$username' AND encrypted\_password = '$password'";

$result = $conn->query($sql);

if ($result->num\_rows > 0) {

    echo "Login success";

} else {

    echo "Login failed";

}

$conn->close();

?>

A close up of a text

Description automatically generated

**ProGuard** là một công cụ trong Java có thể được sử dụng để tối ưu hóa, làm nhỏ và mã hóa mã bytecode của ứng dụng. Khi sử dụng trong phát triển Android, nó giúp giảm kích thước của file APK và bảo vệ mã nguồn khỏi việc được đọc dễ dàng thông qua các công cụ decompile.

1. **Bước 1: Cài đặt và Cấu hình ProGuard**

Trong Android Studio, ProGuard đã được cấu hình sẵn và chỉ cần được kích hoạt trong file cấu hình **build.gradle** của module ứng dụng:

A screenshot of a computer program

Description automatically generated

* **minifyEnabled true** cho phép làm nhỏ và mã hóa mã.
* **proguardFiles** chỉ định các file cấu hình ProGuard.

1. **Bước 2: Định nghĩa ProGuard Rules**

Bạn cần chỉ định các rules trong file **proguard-rules.pro** để bảo vệ mã nguồn mà không làm hỏng chức năng của ứng dụng. Ví dụ, để giữ cho các phương thức và lớp không bị loại bỏ hoặc đổi tên:

A screenshot of a computer program

Description automatically generated

1. **Bước 3: Build APK**

Để build APK:

A screenshot of a program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **Bước 4: Sử dụng apktool để Giải nén và So Sánh**

A screenshot of a computer program

Description automatically generated

A computer screen with blue folders

Description automatically generated

1. **Trình bày Khác Biệt Trước và Sau khi Sử dụng ProGuard**

* **Kích thước APK**: APK sau khi dùng ProGuard thường nhỏ hơn do bỏ đi các mã và tài nguyên không sử dụng.
* **Mã nguồn**: Mã trong APK được mã hóa khó đọc hơn nhiều, các tên biến và phương thức thường được đổi tên thành các ký tự ngẫu nhiên.
* **Hiệu suất**: Tải ứng dụng có thể nhanh hơn nhờ việc loại bỏ mã không cần thiết.

Sử dụng ProGuard là một bước quan trọng trong quy trình phát hành ứng dụng để vừa đảm bảo hiệu suất vừa bảo vệ mã nguồn khỏi được phân tích ngược dễ dàng.

**Link toàn bộ source code:** [**https://drive.google.com/drive/folders/1UoSn0x43WpsEPQ-5WXsBvqO1r5mZsOkB?usp=sharing**](https://drive.google.com/drive/folders/1UoSn0x43WpsEPQ-5WXsBvqO1r5mZsOkB?usp=sharing)

**…**

***Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này***

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
* Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
* Sinh viên báo cáo kết quả thực hiện và nộp bài.

**Báo cáo:**

* File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
* Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
* Đặt tên theo định dạng: [Mã lớp]-ExeX\_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

*Ví dụ: [*NT101.K11.ANTT*]-Exe01\_Group03.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
* Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài nộp.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**:

* Hoàn thành tốt yêu cầu được giao.
* Có nội dung mở rộng, ứng dụng.

*Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)