



BÁO CÁO BÀI TẬP

Môn học: Bảo mật Web và Ứng dụng

Kỳ báo cáo: Lab 5

Tên chủ đề: Ôn tập

GV: Ngô Khánh Khoa

Ngày báo cáo: 23/05/2023

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.N21.ANTT.1

STT	Họ và tên	MSSV	Email
1	Lê Vĩnh Hiếu	20521320	20521320@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá	Người đóng góp
1	Kịch bản 01: Báo cáo lỗi hổng tìm thấy. Sử dụng format theo mẫu sau	100%	
2	Kịch bản 02: Báo cáo lỗi hổng tìm thấy. Sử dụng format theo mẫu sau	100%	
3	Kịch bản 03: Báo cáo lỗi hổng tìm thấy. Sử dụng format theo mẫu sau	100%	
4	Kịch bản 04: Báo cáo lỗi hổng tìm thấy. Sử dụng format theo mẫu sau	100%	
5	Kịch bản 05: Báo cáo lỗi hổng tìm thấy. Sử dụng format theo mẫu sau	100%	

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

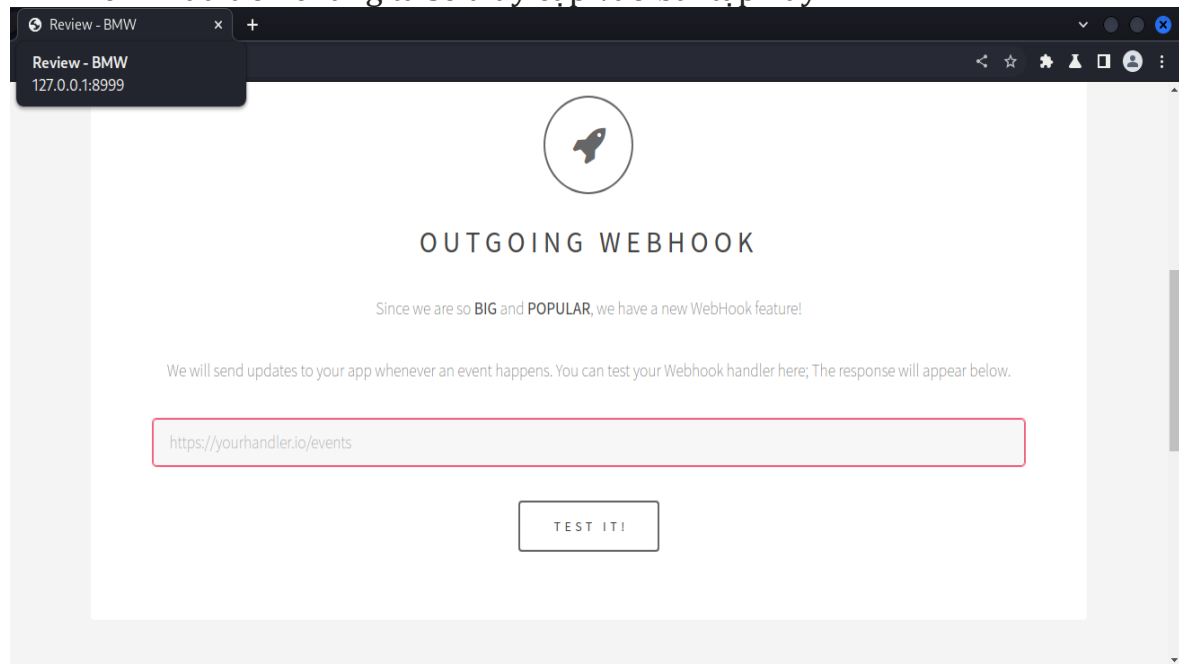
¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Kịch bản 01: Báo cáo lỗ hổng tìm thấy. Sử dụng format theo mẫu sau:

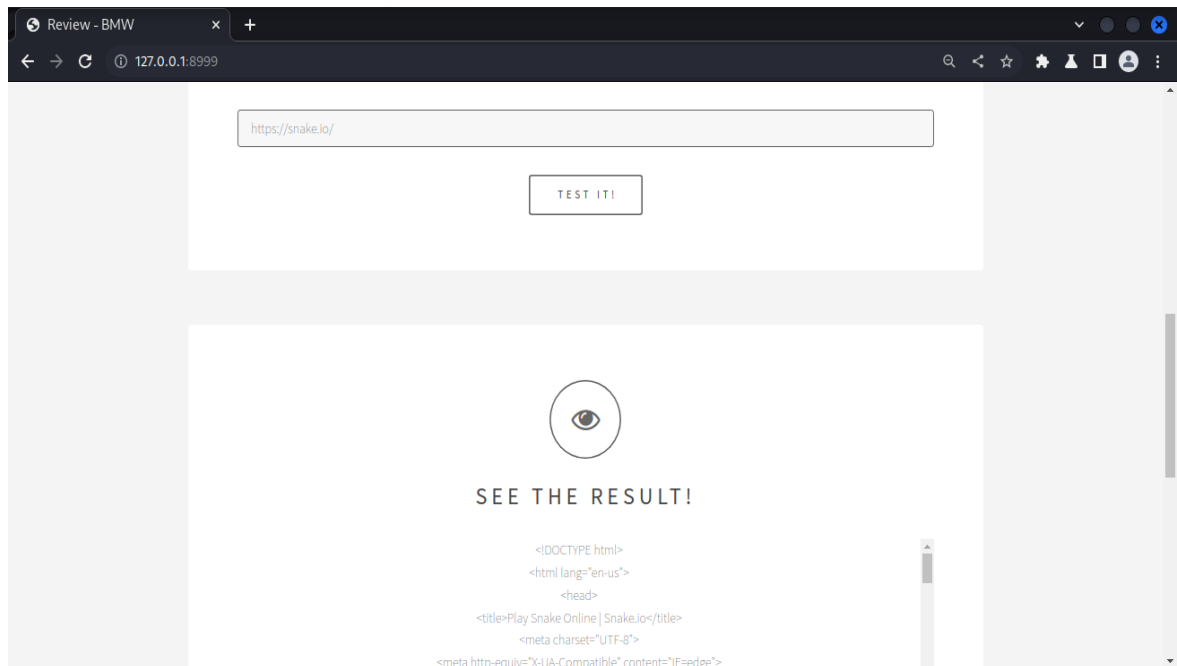
- **Tiêu đề:** Lỗ hổng SSRF là lỗ hổng có khả năng tấn công từ xa và rủi ro thông tin nội bộ. Tài sản bị ảnh hưởng đó là hệ thống máy chủ và dữ liệu quan trọng.
- **Mô tả lỗ hổng:** Lỗ hổng SSRF (Server-Side Request Forgery) là một lỗ hổng bảo mật phổ biến xảy ra trong các ứng dụng web. SSRF xảy ra khi một ứng dụng cho phép kẻ tấn công tạo ra và điều khiển các yêu cầu từ máy chủ nội bộ mà không kiểm tra và xác thực đầy đủ. Điều này có thể cho phép kẻ tấn công đọc hoặc tương tác với các tài nguyên nội bộ mà không được phép, chẳng hạn như các máy chủ cơ sở dữ liệu, các dịch vụ nội bộ, hay các hệ thống quản lý nội bộ.
- **Tóm tắt:** Chúng ta sẽ nhập vào khung text là <file:///etc/passwd> để lấy mật khẩu.
- **Các bước thực hiện:**

+ Bước 1: Đầu tiên chúng ta sẽ truy cập vào bài tập này.



Hình 1. Bài tập 1

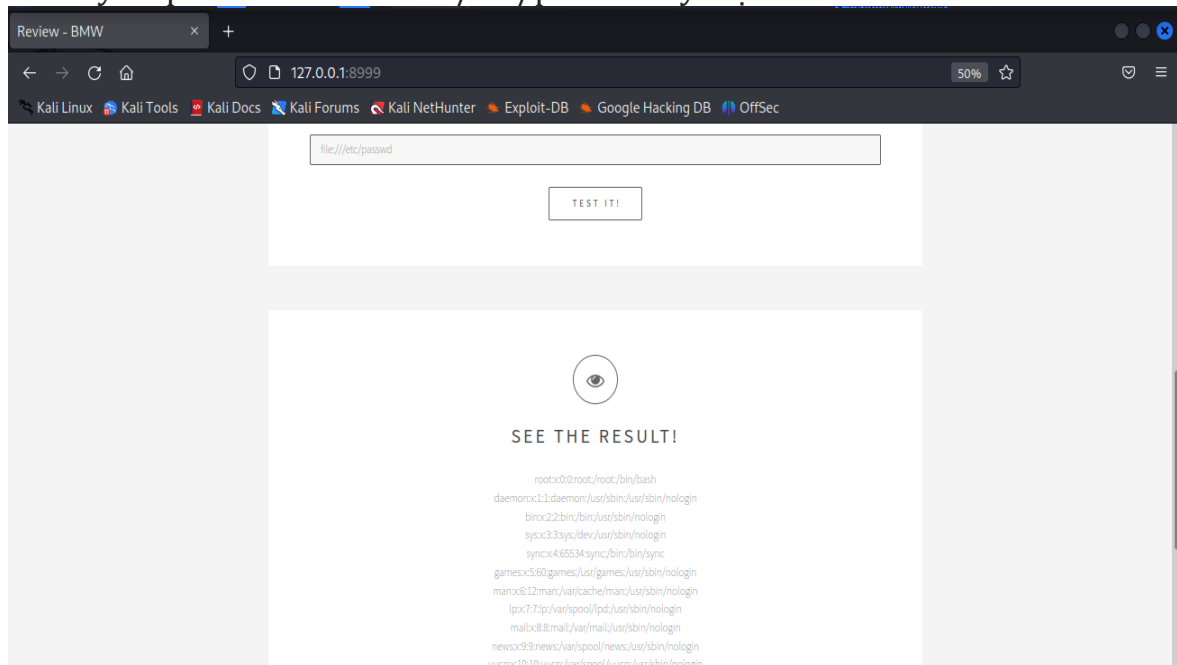
+ Bước 2: Dựa vào giao diện thì chúng ta thấy cần nhập một chuỗi URL vào thanh text rồi bấm nút Test it! để xem kết quả bên dưới là như thế nào thì chúng ta thử nhập đường dẫn của một trang web bất kỳ, đó là đường dẫn tới game snake.io.



Hình 2. Đường dẫn game snake.io

+ Bước 3: Thì chúng ta cũng thấy kết quả sau khi thực hiện ở bước 2 xong thì xuất hiện đoạn code html của trang web snake.io đó và theo những kinh nghiệm thì chúng ta đoán được trang web này có thể bị lỗ hổng SSRF.

+ Bước 4: Bởi vì đoạn text trên chỉ hỗ trợ URL nên chúng ta không thể điền câu lệnh để có thể khai thác được nên chúng ta vẫn sẽ giữ nguyên chuỗi `://` và thay `https` thành `file` để mở `/etc/passwd` lấy mật khẩu.



Hình 3. Câu lệnh khai thác

+ Bước 5: Khai thác thành công

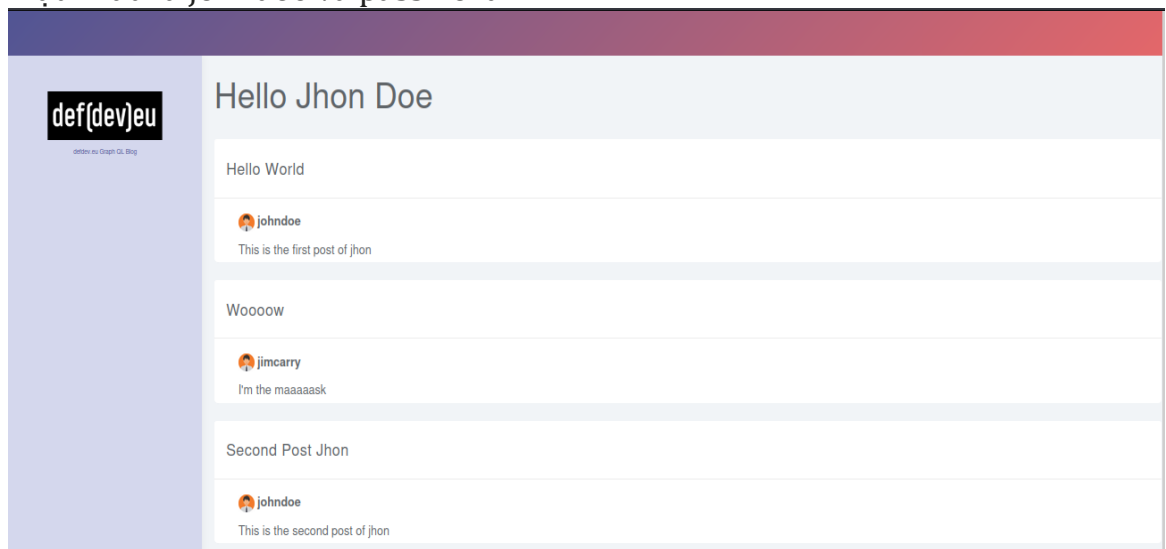
- **Mức độ ảnh hưởng của lỗ hổng:** Mức độ ảnh hưởng của lỗ hổng SSRF có thể rất nghiêm trọng, tùy thuộc vào cách lỗ hổng được khai thác và tầm quan trọng của

các hệ thống nội bộ bị tác động. Một số tác động phổ biến của lỗ hổng này đó là tiết lộ thông tin nhạy cảm, tấn công từ chối dịch vụ (DoS), điều hướng yêu cầu tới máy chủ từ xa và tiềm năng cho cuộc tấn công bên trong.

- **Khuyến cáo khắc phục:** Kiểm tra và ràng buộc đầu vào, xác thực và ủy quyền đích, hạn chế quyền truy cập, xử lý lỗi và thông báo cẩn thận, thiết lập các cấu hình bảo mật phù hợp, cập nhật và sử dụng phiên bản phần mềm mới nhất và kiểm tra và kiểm tra thường xuyên.

2. Kịch bản 02: Báo cáo lỗ hổng tìm thấy. Sử dụng format theo mẫu sau:

- **Tiêu đề:** Lỗ hổng Insecure Direct Object References là lỗ hổng tham chiếu đối tượng trực tiếp không an toàn. Tài sản bị ảnh hưởng đó là thông tin cá nhân, dữ liệu nhạy cảm và quyền truy cập và quyền hạn.
- **Mô tả lỗ hổng:** Lỗ hổng Insecure Direct Object References (IDOR) là một lỗ hổng bảo mật trong các ứng dụng web, khiến người dùng có thể truy cập và thay đổi các đối tượng hoặc thông tin mà họ không có quyền truy cập hoặc chỉnh sửa.
- Tóm tắt:
- Các bước thực hiện:
 - + Bước 1: Đầu tiên chúng ta sẽ đăng nhập vào chương trình với tài khoản mật khẩu là johndoe và password1.



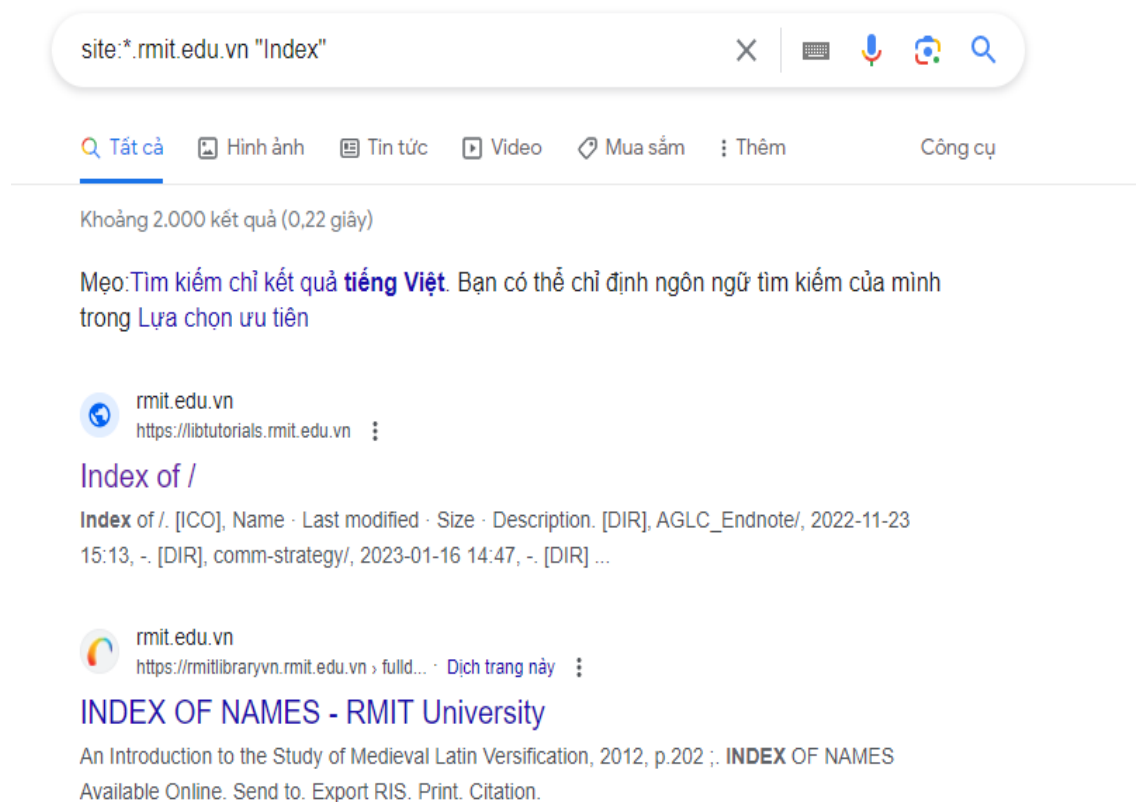
- **Mức độ ảnh hưởng của lỗ hổng:** Mức độ ảnh hưởng của lỗ hổng Insecure Direct Object References (IDOR) có thể rất nghiêm trọng và đa dạng, tùy thuộc vào loại ứng dụng web và dữ liệu mà lỗ hổng này tác động đến. Các mức độ cụ thể là tiết lộ thông tin nhạy cảm, sửa đổi hoặc xóa dữ liệu và truy cập trái phép vào chức năng hoặc tài khoản.
- **Khuyến cáo khắc phục:** Xác thực và kiểm tra quyền truy cập, sử dụng kiểm soát quyền truy cập dựa trên vai trò và sử dụng mã hóa và che giấu đối tượng.

3. Kịch bản 03: Báo cáo lỗ hổng tìm thấy. Sử dụng format theo mẫu sau:

- **Tiêu đề:** Lỗ hổng Directory Listing là lỗ hổng liệt kê thư mục. Tài sản bị ảnh hưởng là tập tin và thư mục nhạy cảm, quyền riêng tư của người dùng và cấu trúc hệ thống.

- **Mô tả lỗ hổng:** Lỗ hổng Directory Listing (hay còn gọi là Directory Traversal) là một lỗ hổng bảo mật phát sinh khi một ứng dụng web không kiểm soát hoặc không hạn chế đúng cách quyền truy cập vào các thư mục trên máy chủ web.
- **Tóm tắt:** Sử dụng google hacking để tìm thông tin nhạy cảm
- **Các bước thực hiện:**







Bước 1: Đầu tiên để thực hiện tìm kiếm lỗ hổng này thì chúng ta sẽ sử dụng google hacking là một cách để có thể tìm kiếm những thứ bị ẩn ở một số trang web hay subdomain, tại thanh search google chúng ta sẽ nhập `site:*.rmit.edu.vn "Index"` thì kết quả sẽ xuất hiện một trang web chứa những thông tin nhạy cảm của domain này.



Hình 4. Sử dụng google hacking

+ Bước 2: Khi truy cập vào Index of / của subdomain libtutorials trên thì chúng ta thấy xuất hiện khá nhiều thư mục và rất có thể trong đó chứa các thông tin nhạy cảm và chúng ta đã tìm được lỗ hổng của bài này.

Index of /

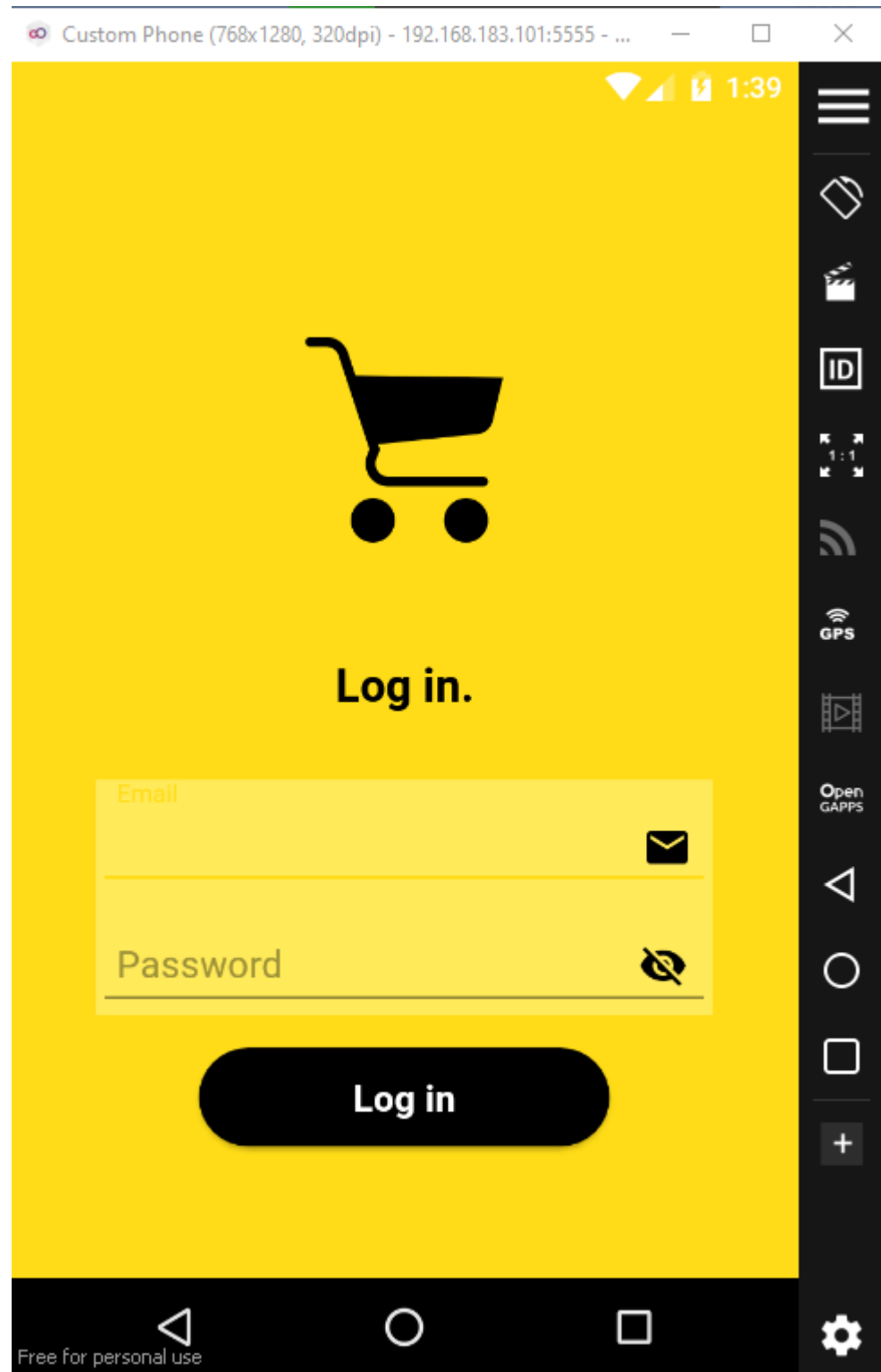
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 AGLC_Endnote/	2022-11-23 15:13	-	
 comm-strategy/	2023-01-16 14:47	-	
 intro-management/	2022-11-23 15:15	-	
 marketing_principles/	2023-03-03 09:48	-	
 research_tutorial/	2021-11-17 14:08	-	
 scd-referencing/	2023-04-18 11:23	-	

Hình 5. Tìm được các thư mục nhạy cảm

- **Mức độ ảnh hưởng của lỗ hổng:** Mức độ ảnh hưởng của lỗ hổng Directory Listing phụ thuộc vào các yếu tố sau đó là loại thông tin lộ ra, quy mô và quyền truy cập của hệ thống, các hành động tiềm năng của kẻ tấn công và ngữ cảnh hệ thống. Từ đó gây ra ảnh hưởng nghiêm trọng tới các tài sản.
- **Khuyến cáo khắc phục:** Cấu hình chính xác máy chủ web, kiểm tra và loại bỏ quyền truy cập không hợp phép, xác thực và kiểm tra đầu vào, sử dụng bảo mật cấp ứng dụng, cập nhật phần mềm và hệ điều hành.

4. Kịch bản 04: Báo cáo lỗ hổng tìm thấy. Sử dụng format theo mẫu sau:

- **Tiêu đề:** Lỗ hổng Application Flow Tampering Vulnerability là lỗ hổng nhiễu loạn luồng ứng dụng. Tài sản bị ảnh hưởng đó là dữ liệu người dùng, quyền truy cập và ủy quyền, tính toàn vẹn của ứng dụng và khả năng hoạt động đúng đắn của ứng dụng.
- **Mô tả lỗ hổng:** Lỗ hổng Application Flow Tampering là một lỗ hổng bảo mật trong ứng dụng, cho phép tấn công can thiệp vào hoặc thay đổi luồng hoạt động dự kiến của ứng dụng một cách trái phép hoặc không mong muốn. Lỗ hổng này có thể xảy ra trong môi trường ứng dụng di động, ứng dụng web, hoặc ứng dụng máy tính.
- **Tóm tắt:** Thực hiện kỹ thuật Activity Hijacking để thay đổi luồng hoạt động.
- **Các bước thực hiện:**
 - + Bước 1: Đầu tiên chúng ta sẽ tải ứng dụng về máy Android và sau đó bật ứng dụng lên.



Hình 6. Ứng dụng InsecureShop

+ Bước 2: Ứng dụng sẽ bắt chúng ta đăng nhập bằng email và mật khẩu, tiếp theo chúng ta thử decompile file apk của ứng dụng này rồi xem file AndroidManifest.xml xem có gì nào.

```

11      <action android:name="android.intent.action.VIEW"/>
12      <category android:name="android.intent.category.DEFAULT"/>
13    </intent-filter>
14    <intent-filter>
15      <action android:name="android.intent.action.SEND"/>
16      <category android:name="android.intent.category.DEFAULT"/>
17      <data android:mimeType="application/*"/>
18      <data android:mimeType="audio/*"/>
19      <data android:mimeType="image/*"/>
20      <data android:mimeType="text/*"/>
21      <data android:mimeType="video/*"/>
22    </intent-filter>
23    <meta-data android:name="android.servicechooser.chooser_target_service" android:value=".ConversationChooserTargetService"/>
24  </activity>
25  <activity android:exported="true" android:name="com.inseureshop.AboutUsActivity"/>
26  <activity android:name="com.inseureshop.CartListActivity"/>
27  <activity android:name="com.inseureshop.ProductListActivity">
28    <intent-filter>
29      <action android:name="android.intent.action.MAIN"/>
30      <category android:name="android.intent.category.LAUNCHER"/>
31    </intent-filter>
32  </activity>
33  <activity android:name="com.inseureshop.LoginActivity"/>
34  <activity android:name="com.inseureshop.WebViewActivity">
35    <intent-filter>
36      <action android:name="android.intent.action.VIEW"/>
37      <category android:name="android.intent.category.DEFAULT"/>
38      <category android:name="android.intent.category.BROWSABLE"/>
39      <data android:host="com.inseureshop" android:scheme="inseureshop"/>
40    </intent-filter>
41  </activity>
42  <activity android:name="com.inseureshop.WebView2Activity">
43    <intent-filter>
44      <action android:name="com.inseureshop.action.WEBVIEW"/>
45      <category android:name="android.intent.category.DEFAULT"/>

```

Hình 7. File AndroidManifest.xml

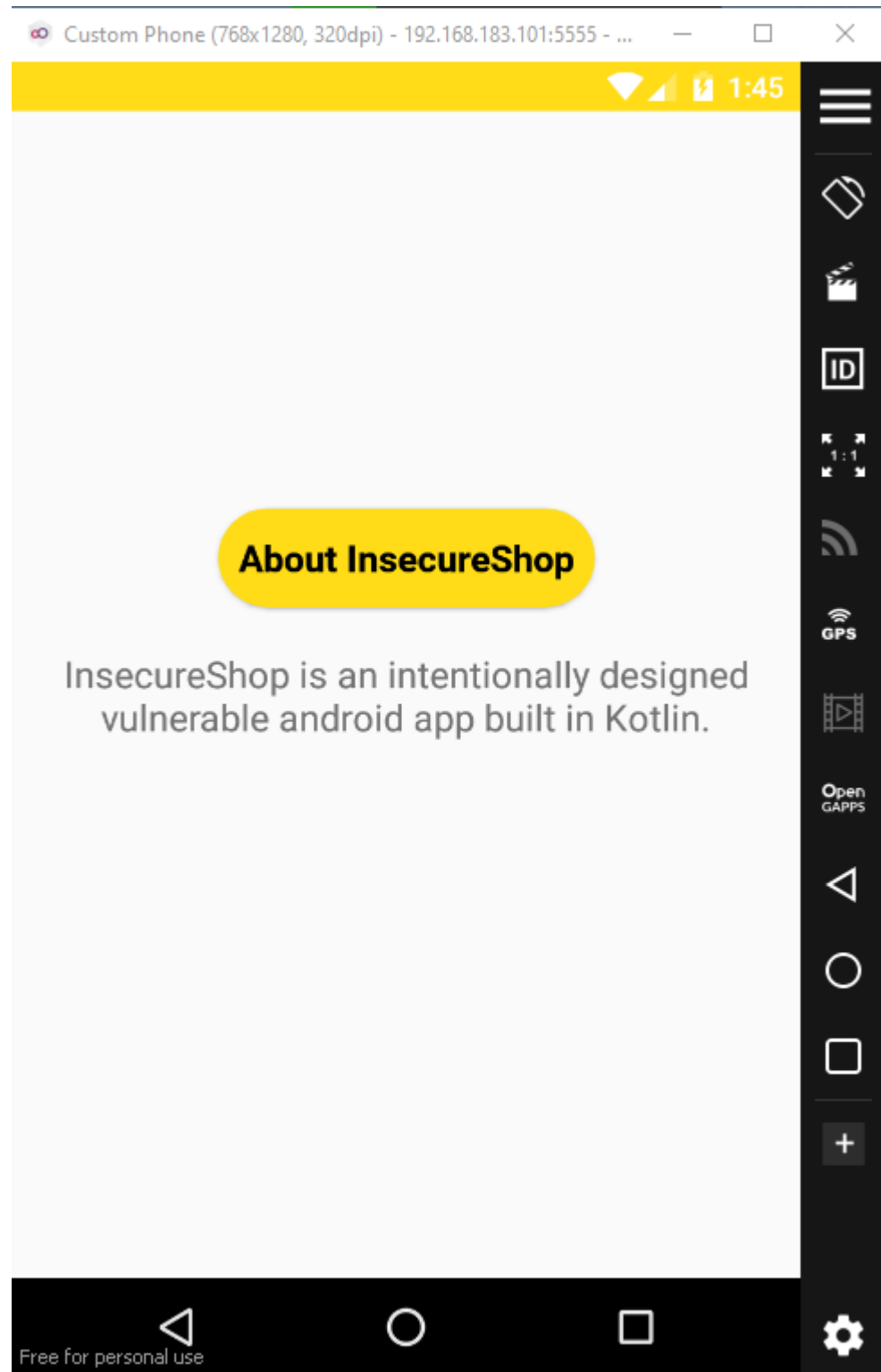
+ Bước 3: Chúng ta thấy rằng có một hoạt động được exported đó là AboutUsActivity. Đây là một hành động ẩn và chúng ta chỉ kích hoạt được nó bởi một ứng dụng khác nên chúng ta thử sử dụng Activity Hijacking là một kỹ thuật thay đổi luồng hoạt động và kích hoạt hành động mà chúng ta muốn, và bây giờ chúng ta sẽ kích hoạt hành động đó.

```

genymotion:/ # am start -n com.inseureshop/.AboutUsActivity
Starting: Intent { cmp=com.inseureshop/.AboutUsActivity }
genymotion:/ #

```

Hình 8. Kỹ thuật Activity Hijacking



Hình 9. Thực hiện hành động thành công

- + Bước 4: Như vậy chúng ta đã kích hoạt hành động đó thành công mà không cần phải đăng nhập email mật khẩu để vào ứng dụng này.
- **Mức độ ảnh hưởng của lỗ hổng:** Mức độ ảnh hưởng của lỗ hổng Application Flow Tampering có thể thay đổi tùy thuộc vào các yếu tố cụ thể của ứng dụng và cách mà lỗ hổng được khai thác. Một số mức độ ảnh hưởng đó là tính toàn vẹn và

quyền riêng tư, hoạt động bất thường và lỗi, đánh cắp thông tin và lừa đảo và tấn công khác vào hệ thống.

- **Khuyến cáo khắc phục:** Xác thực và ủy quyền, kiểm tra dữ liệu đầu vào, mã hóa dữ liệu, xác minh luồng hoạt động, kiểm tra và phân tích bảo mật, cập nhật và bảo trì, giáo dục và đào tạo và theo dõi và giám sát.

5. Kịch bản 05: Báo cáo lỗ hổng tìm thấy. Sử dụng format theo mẫu sau:

- Tiêu đề:
- Mô tả lỗ hổng:
- Tóm tắt:
- Các bước thực hiện:
- Mức độ ảnh hưởng của lỗ hổng:
- Khuyến cáo khắc phục:

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

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo 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 **.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]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).
Ví dụ: [NT101.K11.ANTT]-Session1_Group3.
- 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.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

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

HẾT