

MSSV: 22521329	BÁO CÁO BÀI TẬP THỰC HÀNH TUẦN 5
Họ và tên: Nguyễn Cao Thắng	
Lớp: IE108.O21.CNVN.1	

Bài tập 1.1. A01:2021-Broken Access Control

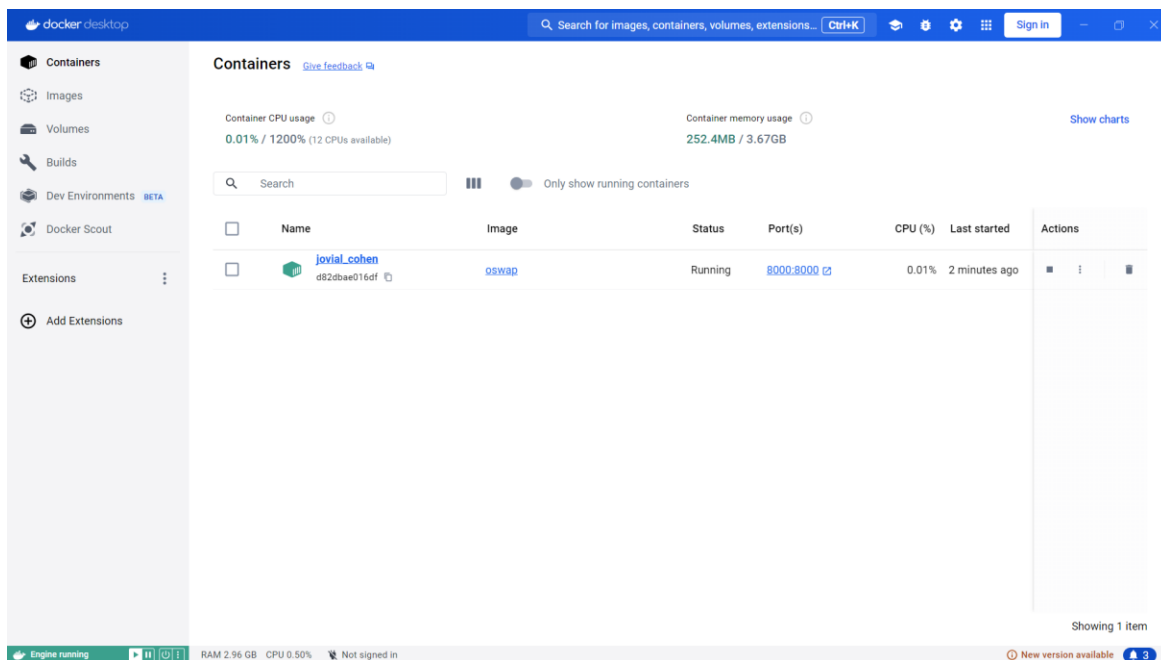
1.1.1. Thực hiện lại bài tấn công trên bằng chức năng Intercept

Chạy môi trường bài thực hành:

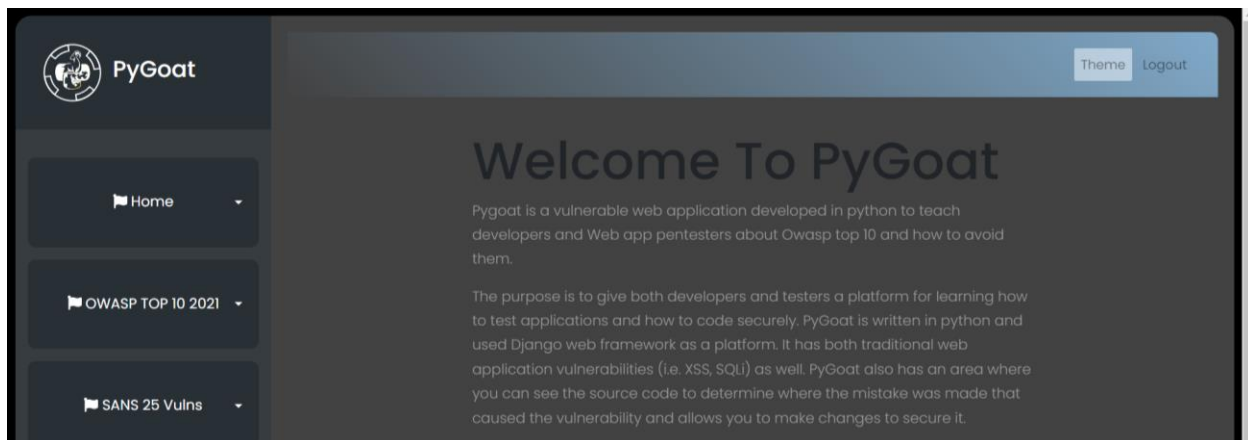
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

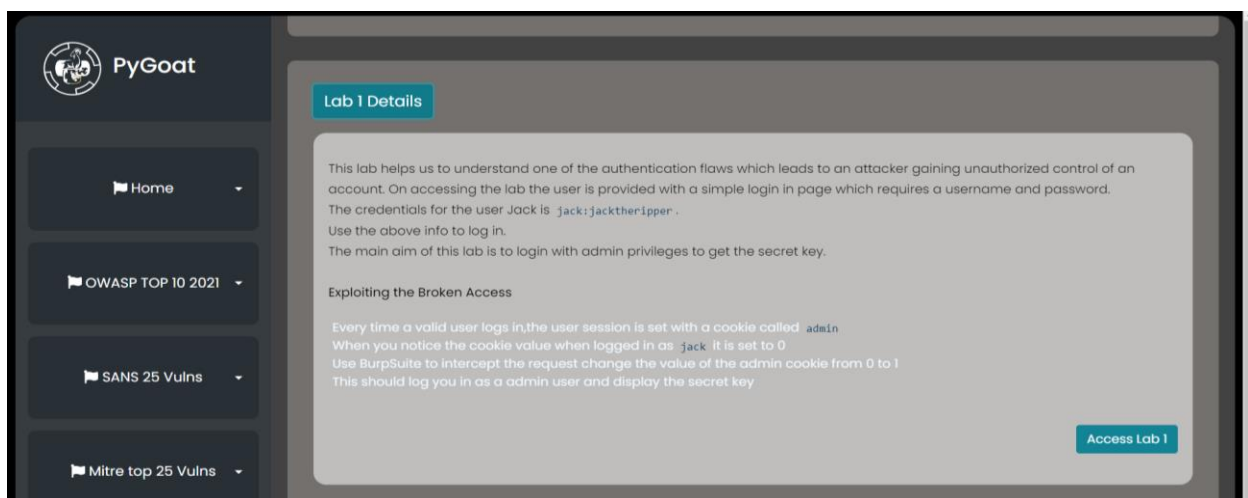
PS C:\Users\Public\Documents> docker load -i owap.tar
Loaded image: oswap:latest
PS C:\Users\Public\Documents> docker images
REPOSITORY    TAG       IMAGE ID       CREATED        SIZE
oswap         latest    f9ceab6f5d37   15 months ago  1.14GB
PS C:\Users\Public\Documents> docker run --rm -p 8000:8000 oswap
[2024-06-06 05:57:41 +0000] [1] [INFO] Starting gunicorn 20.1.0
[2024-06-06 05:57:41 +0000] [1] [INFO] Listening at: http://0.0.0.0:8000 (1)
[2024-06-06 05:57:41 +0000] [1] [INFO] Using worker: sync
[2024-06-06 05:57:41 +0000] [7] [INFO] Booting worker with pid: 7
[2024-06-06 05:57:41 +0000] [8] [INFO] Booting worker with pid: 8
[2024-06-06 05:57:41 +0000] [9] [INFO] Booting worker with pid: 9
[2024-06-06 05:57:41 +0000] [10] [INFO] Booting worker with pid: 10
[2024-06-06 05:57:41 +0000] [11] [INFO] Booting worker with pid: 11
[2024-06-06 05:57:41 +0000] [12] [INFO] Booting worker with pid: 12
```



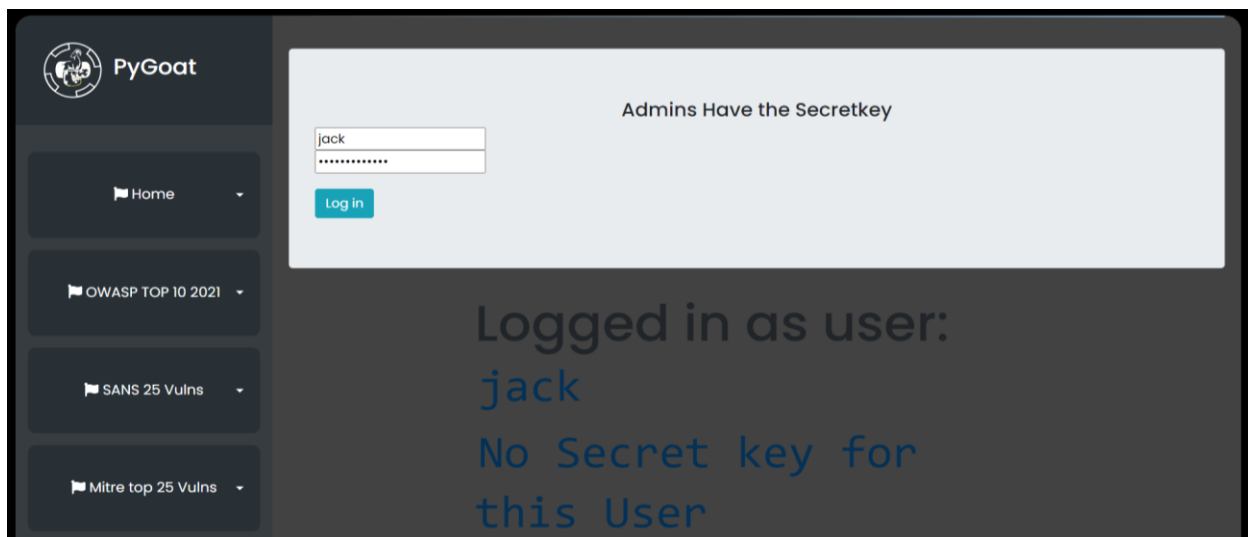
Đăng nhập thành công tài khoản vào PyGoat:



Thực hiện Lab 1:



Đăng nhập với username jack và mật khẩu jacktheripper:



Kiểm tra lịch sử câu truy vấn:

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response...
127	http://localhost:8000	GET	/broken_access_control			200	33873	HTML		Broken Access Control			127.0.0.1		13:04:15.6 J...	8080	23
133	http://localhost:8000	GET	/static/Lab/icons/pygoat-mini.svg			304	160	svg					127.0.0.1		13:04:15.6 J...	8080	2
134	http://localhost:8000	GET	/static/Lab/ssrf.js			304	159	script	js				127.0.0.1		13:04:15.6 J...	8080	4
135	http://localhost:8000	GET	/static/Lab/ssrf.js			304	159	script	js				127.0.0.1		13:04:15.6 J...	8080	4
136	http://localhost:8000	GET	/broken_access_lab_1			200	27432	HTML		Broken Access Control.			127.0.0.1		13:04:15.6 J...	8080	30
142	http://localhost:8000	GET	/static/Lab/icons/pygoat-mini.svg			304	160	svg					127.0.0.1		13:04:46.6 J...	8080	1
143	http://localhost:8000	GET	/static/Lab/ssrf.js			304	159	script	js				127.0.0.1		13:04:46.6 J...	8080	1
144	http://localhost:8000	GET	/static/Lab/ssrf.js			304	159	script	js				127.0.0.1		13:04:46.6 J...	8080	3
145	http://localhost:8000	POST	/broken_access_lab_1			200	27582	HTML		Broken Access Control.			127.0.0.1	admin=0	13:05:07.6 J...	8080	60
150	http://localhost:8000	GET	/static/Lab/ssrf.js			304	159	script	js				127.0.0.1		13:05:08.6 J...	8080	7
152	http://localhost:8000	GET	/static/Lab/ssrf.js			304	159	script	js				127.0.0.1		13:05:08.6 J...	8080	7
153	http://localhost:8000	GET	/static/Lab/icons/pygoat-mini.svg			304	160	svg					127.0.0.1		13:05:08.6 J...	8080	2

The selected request (145) is a POST to /broken_access_lab_1 with status 200 and content type text/html. The response is shown in the right pane, indicating a successful login with the message "Admins Have the Secretkey".

Sửa đổi gói tin GET bằng cách bật Intercept:

The selected request is a GET to /broken_access_lab_1 with status 200 and content type text/html. The response is shown in the right pane, indicating a successful login with the message "Admins Have the Secretkey".

Kết quả sau khi Foward gói tin được sửa đổi:

Burp Suite Community Edition v2024.3.1.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start respon...
299	http://localhost:8000	GET	/static/lab/vss.js			304	159	script	js				127.0.0.1		13:30:54 6 J...	8080	6
300	http://localhost:8000	GET	/static/lab/srf.js			304	159	script	js				127.0.0.1		13:30:54 6 J...	8080	2
301	http://localhost:8000	GET	/static/lab/icons/pygoat-mini.svg			304	160	svg					127.0.0.1		13:30:54 6 J...	8080	2
303	http://localhost:8000	GET	/broken_access_lab_1			200	27432	HTML		Broken Access Control.			127.0.0.1		13:31:01 6 J...	8080	95
309	http://localhost:8000	GET	/static/lab/srf.js			304	159	script	js				127.0.0.1		13:31:02 6 J...	8080	4
310	http://localhost:8000	GET	/static/lab/vss.js			304	159	script	js				127.0.0.1		13:31:02 6 J...	8080	6
311	http://localhost:8000	GET	/static/lab/icons/pygoat-mini.svg			304	160	svg					127.0.0.1		13:31:02 6 J...	8080	3
312	http://localhost:8000	GET	/broken_access_lab_1		✓	200	27432	HTML		Broken Access Control.			127.0.0.1		13:31:21 6 J...	8080	16
317	http://localhost:8000	GET	/static/lab/srf.js			304	159	script	js				127.0.0.1		13:31:27 6 J...	8080	2
319	http://localhost:8000	GET	/static/lab/vss.js			304	159	script	js				127.0.0.1		13:31:27 6 J...	8080	2
320	http://localhost:8000	GET	/static/lab/icons/pygoat-mini.svg			304	160	svg					127.0.0.1		13:31:28 6 J...	8080	1

Original request

```

1 GET /broken_access_lab_1 HTTP/1.1
2 Host: localhost:8000
3 Cache-Control: max-age=0
4 sec-ch-ua: "Not-A-Brand";v="99", "Chromium";v="124"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.110 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: en-US,en;q=0.9
16 Cookie: csrf-token=spqULng3waw5yFCqa2OWP1gLCBhSg9ybRgRPfwiIIDCaK0W4pbjMdt8S5h6u; sessionid=c1405b6rqg1204bhi54f4h1c60s56nn; admin=0
17 Connection: close

```

Response

```

1 HTTP/1.1 200 OK
2 Server: gunicorn
3 Date: Thu, 06 Jun 2024 06:31:26 GMT
4 Connection: close
5 Content-Type: text/html; charset=utf-8
6 X-Frame-Options: DENY
7 Content-Length: 27135
8 Vary: Cookie
9 X-Content-Type-Options: nosniff
10 Referrer-Policy: same-origin
11 Cross-Origin-Opener-Policy: same-origin
12 <!DOCTYPE html>
13 <html lang="en">
14 <head>
15 <meta charset="utf-8" />
16 <meta name="viewport" content="width=device-width, initial-scale=1.0" />
17 <meta http-equiv="X-UA-Compatible" content="IE=edge" />
18 <title>
19   Broken Access Control.
20 </title>
21 <!-- Bootstrap CSS CDN -->
22 <link
23   rel="stylesheet"
24   href="

```

Inspector

Request attributes 2


Request cookies 3

Request headers 16

Response headers 10

Event log (1) All issues

Memory: 141.5MB


PyGoat
Theme Logout

Home

OWASP TOP 10 2021

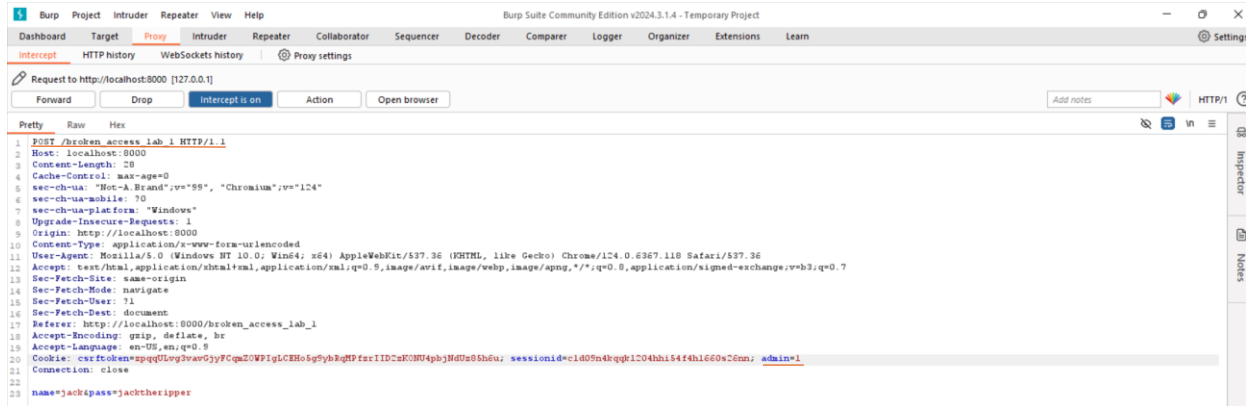
SANS 25 Vulns

Mitre top 25 Vulns

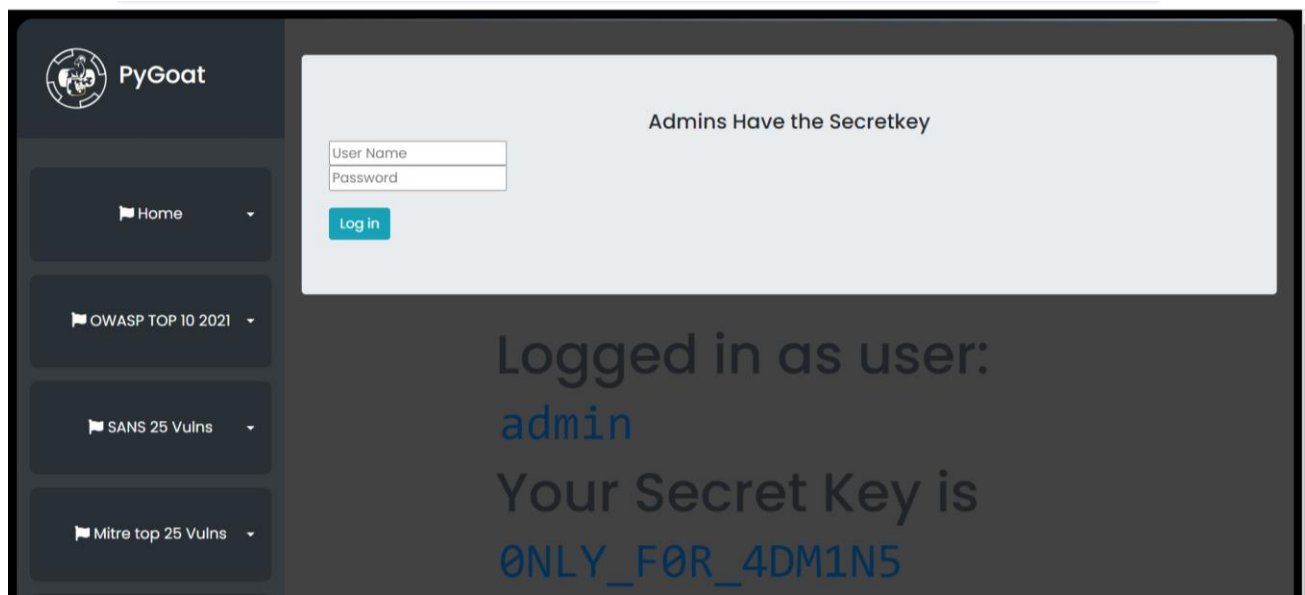
Admins Have the Secretkey

Please Provide Credentials

Thực hiện sửa đổi và Foward gói tin POST:



Kết quả Secret Key thu được sau khi gói tin POST đã chỉnh sửa được Forward



1.1.2. Thực hiện tấn công theo Lab 2 Details của mục này

Inspector		
Request attributes	2	▼
Request query parameters	0	▼
Request body parameters	2	▼
Request cookies	2	▼
Request headers	20	^
Name	Value	
Host	localhost:8000	>
Content-Length	28	>
Cache-Control	max-age=0	>
sec-ch-ua	"Not-A.Brand";v...	>
sec-ch-ua-mobile	?0	>
sec-ch-ua-platfo...	"Windows"	>
Upgrade-Insecur...	1	>
Origin	http://localhost:...	>
Content-Type	application/x-w...	>
User-Agent	pyqoat_admin	>
Accept	text/html,applic...	>
Sec-Fetch-Site	same-origin	>
Sec-Fetch-Mode	navigate	>
Sec-Fetch-User	?1	>
Sec-Fetch-Dest	document	>
Referer	http://localhost:...	>
Accept-Encoding	gzip, deflate, br	>
Accept-Language	en-US,en;q=0.9	>
Cookie	csrftoken=Thx9V...	>
Connection	close	>

Can you log in as an admin and get the secretkey?

Log in

Logged in as user:

admin

Your Secret Key is:

ONLY_FØR_4DM1N5

Admin Status is:

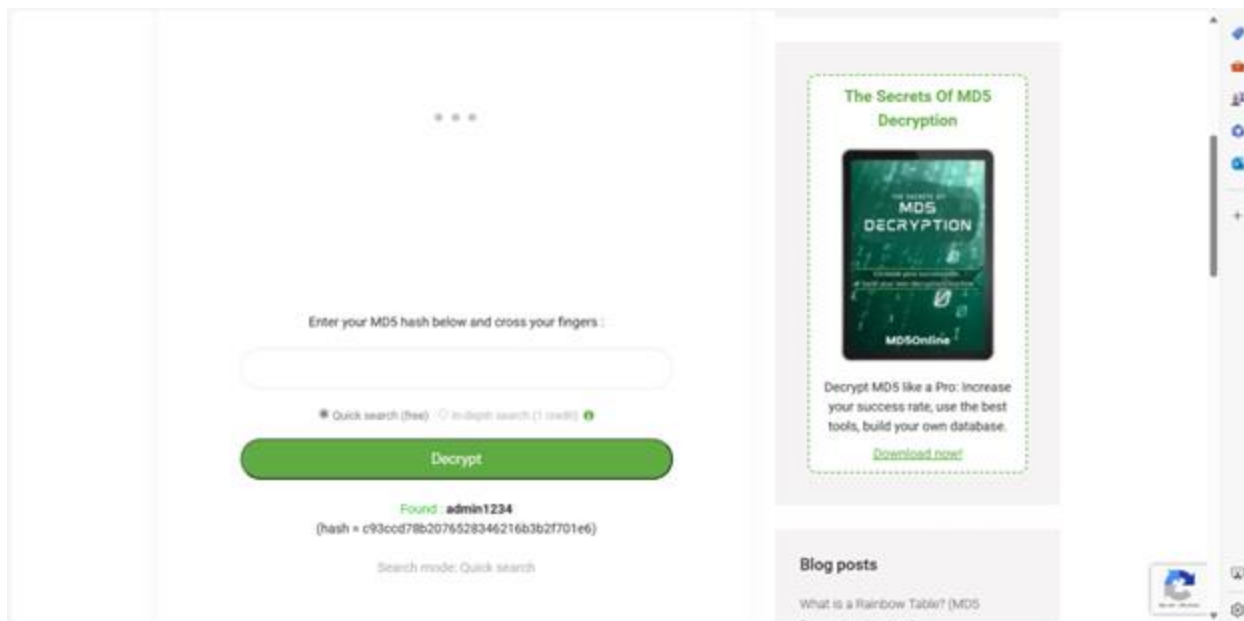
admin

1.1.3. Trả lời câu hỏi: Làm thế nào để khắc phục/vá lỗ hổng này?

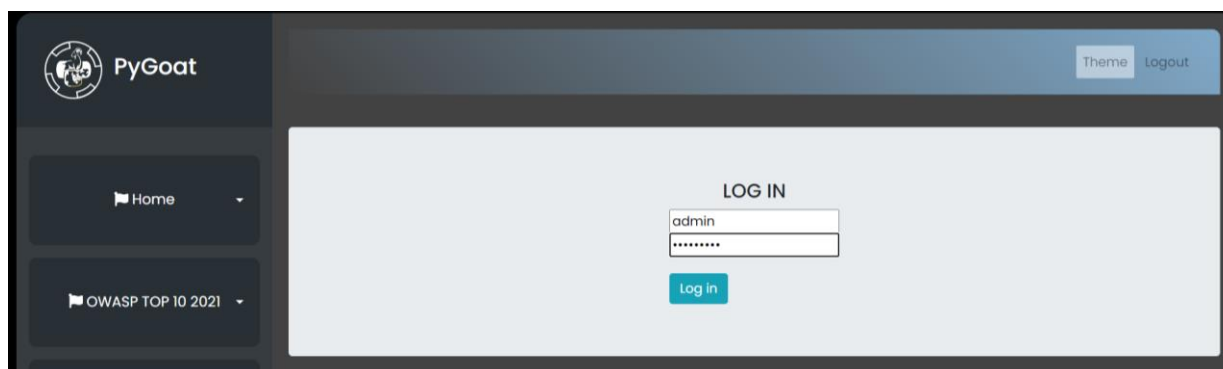
- Giới hạn quyền truy cập API và controller để giảm thiểu thiệt hại.
- Thực hiện các cơ chế kiểm soát quyền truy cập và thực hiện nó trên toàn ứng dụng.
- JWT tokens nên vô hiệu hóa trên server khi đăng xuất.
- Nên cài đặt các rule ở Model để quản lý các thao tác với database.

Bài tập 1.2. A02:2021 – Cryptographic Failures

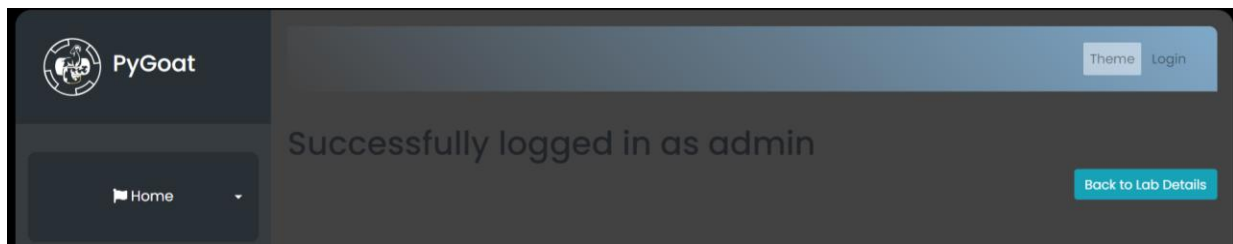
Thực hiện giải mã đoạn mã MD5:



Đăng nhập theo mật khẩu được giải mã:



Kết quả:

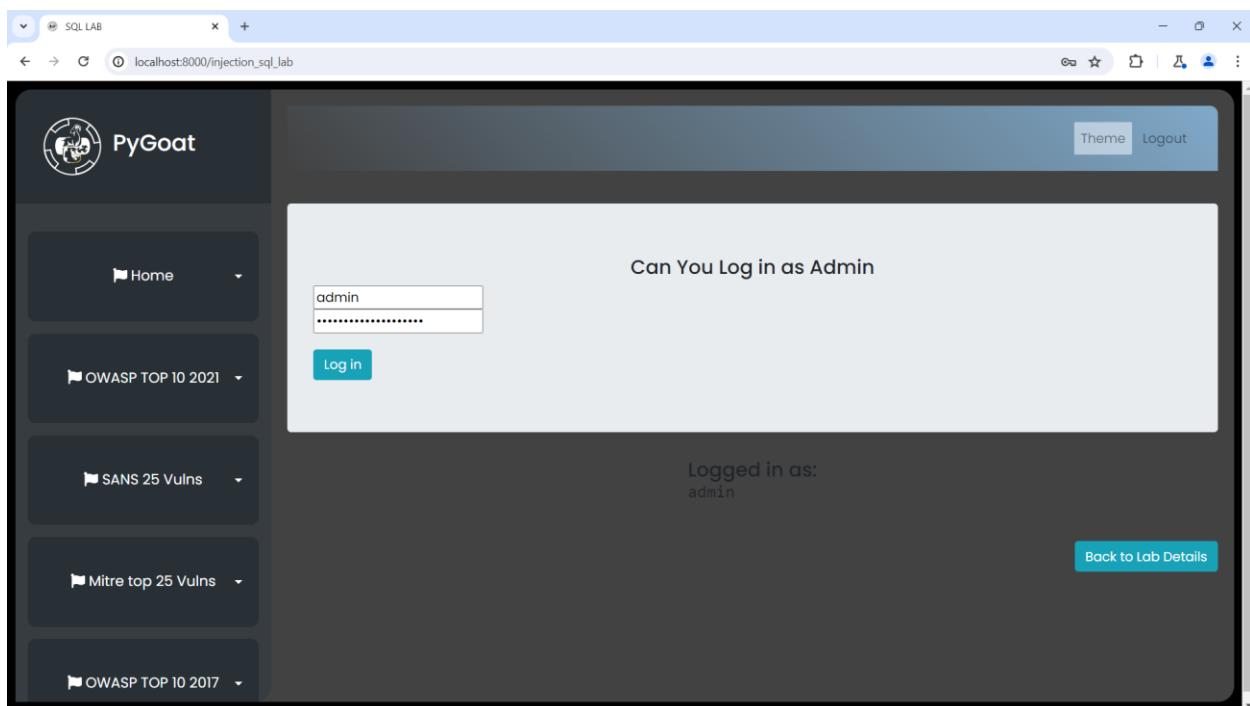


Bài tập 1.3. A03-A10:2021

A03 SQL injection

Mật khẩu của admin là `anything' OR '1' = '1`

Kết quả sau khi đăng nhập:



A05 Security Misconfiguration

Add thêm header x-host có giá trị `admin.localhost:8000`

Name	Value	
Host	localhost:8000	>
sec-ch-ua	"Not-A.Brand";v...	>
sec-ch-ua-mobile	?0	>
sec-ch-ua-platfo...	"Windows"	>
Upgrade-Insecur...	1	>
User-Agent	Mozilla/5.0 (Win...	>
Accept	text/html,applic...	>
Sec-Fetch-Site	same-origin	>
Sec-Fetch-Mode	navigate	>
Sec-Fetch-User	?1	>
Sec-Fetch-Dest	document	>
Referer	http://localhost:...	>
Accept-Encoding	gzip, deflate, br	>
Accept-Language	en-US,en;q=0.9	>
Cookie	csrftoken=Thx9V...	>
Connection	close	>

Name:

X-Host

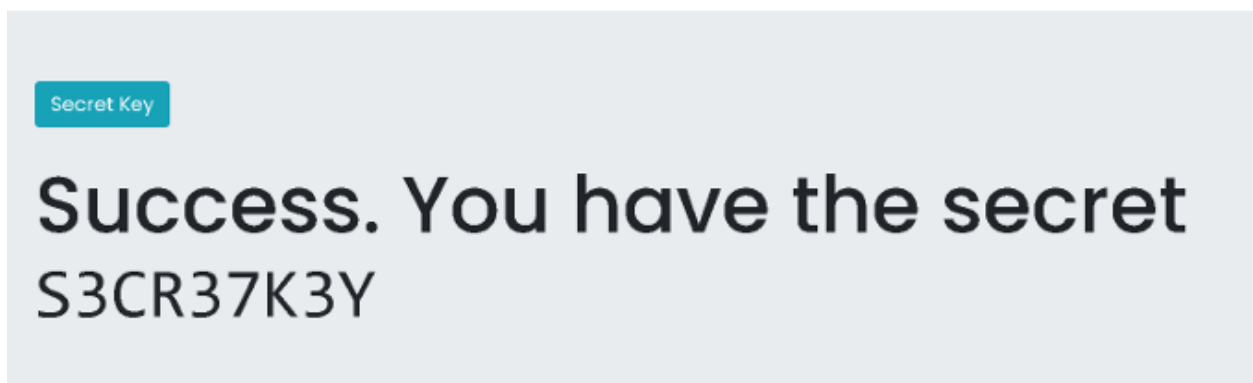
Value:

admin.localhost:8000

Cancel

Add

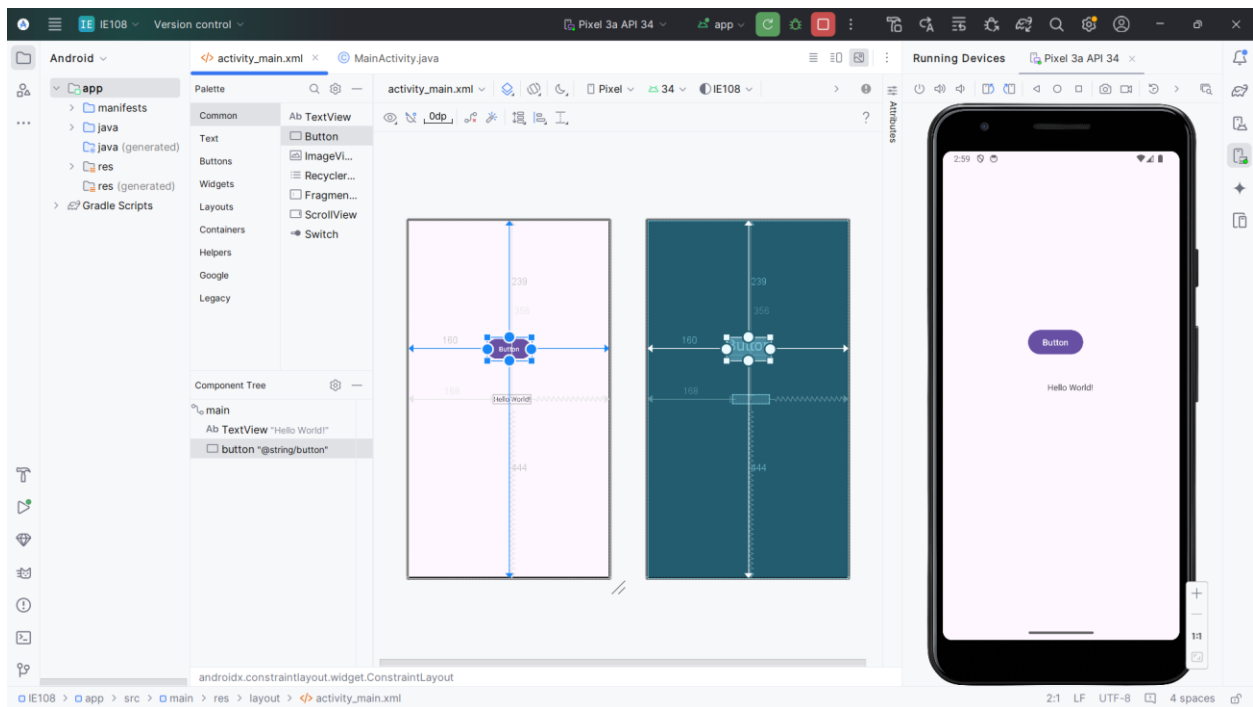
Kết quả:



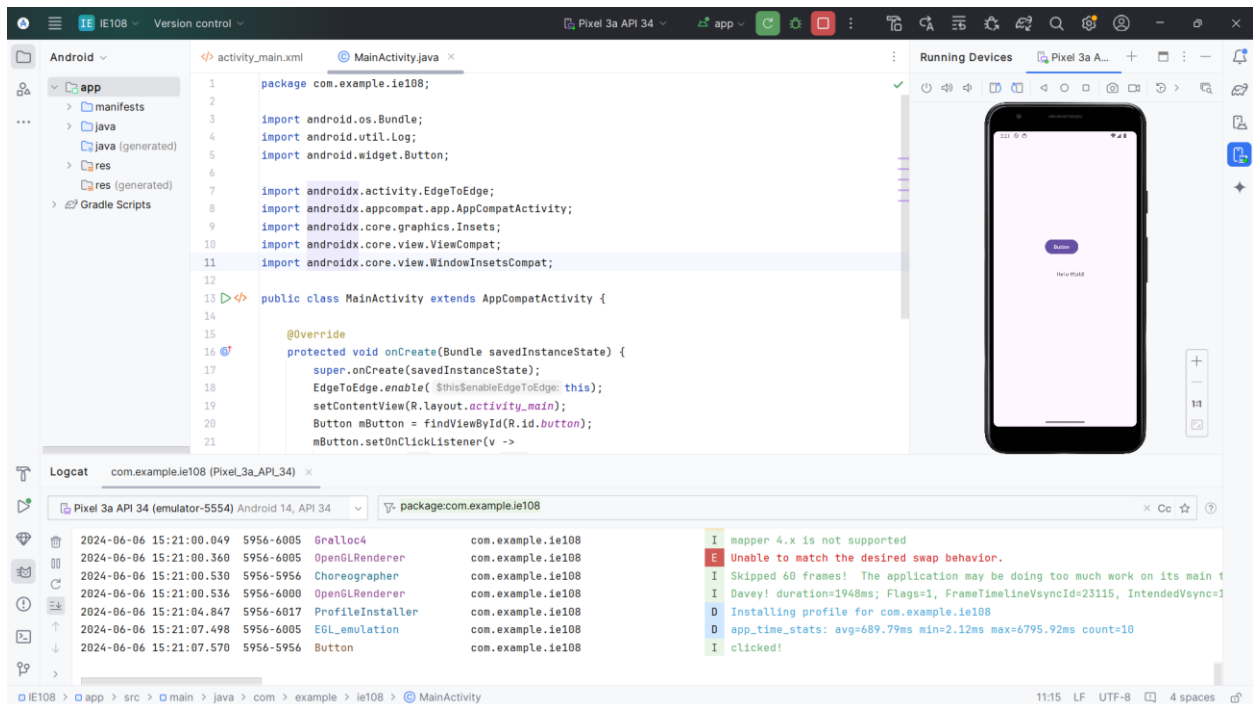
Bài tập 2.1. Lập trình ứng dụng Android cơ bản

Bài tập 2.1.1. Hello World

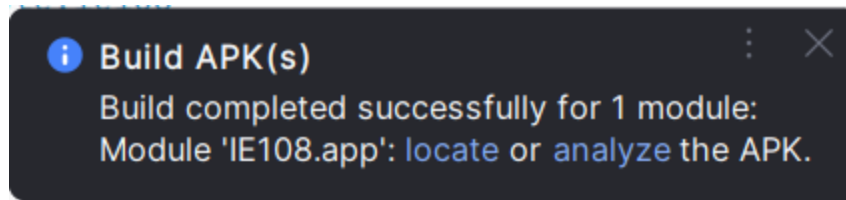
Thêm button vào ứng dụng và thực hiện chạy thử:



Định nghĩa, hiện thực chức năng cho Button và kết quả:

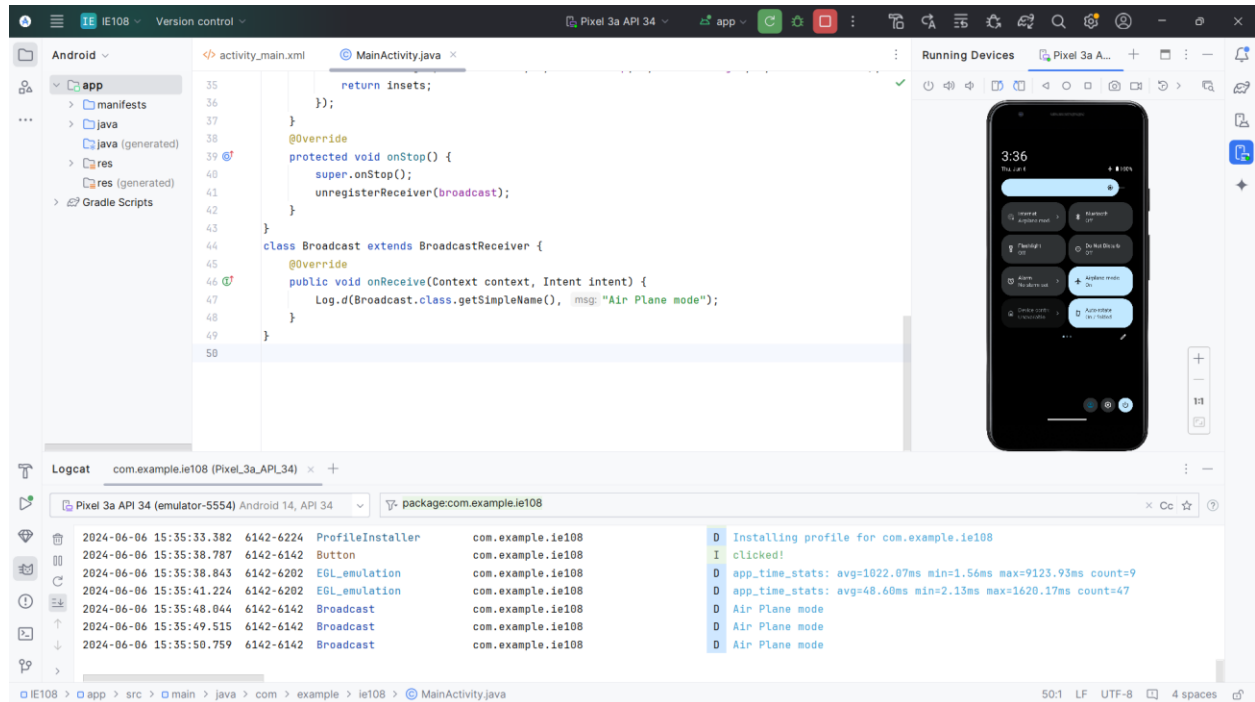


Build ứng dụng thành tệp apk:



Bài tập 2.1.2. Broadcast Receivers

Kết quả sau khi thực hiện thêm Broadcast Receiver cho Airplane Mode:



Bài tập 2.2. Phân tích và khai thác ứng dụng Android

Biên dịch ngược file apk bằng apktool:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Public\Documents> apktool d InsecureBankv2.apk
I: Using Apktool 2.9.3 on InsecureBankv2.apk
I: Loading resource table...
I: Decoding file-resources...
I: Loading resource table from file: C:\Users\aboyw\AppData\Local\apktool\framework\1.apk
I: Decoding values */* XMLs...
I: Decoding AndroidManifest.xml with resources...
I: Regular manifest package...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
Press any key to continue . . .
PS C:\Users\Public\Documents>
```

Đọc tập tin AndroidManifest.xml:

```
Windows PowerShell

PS C:\Users\Public\Documents\InsecureBankv2> more AndroidManifest.xml
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.android.insecurebank
v2" platformBuildVersionCode="22" platformBuildVersionName="5.1.1-1819727">
  <uses-permission android:name="android.permission.INTERNET"/>
  <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
  <uses-permission android:name="android.permission.SEND_SMS"/>
  <uses-permission android:name="android.permission.USE_CREDENTIALS"/>
  <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
  <uses-permission android:name="android.permission.READ_PROFILE"/>
  <uses-permission android:name="android.permission.READ_CONTACTS"/>
  <android:uses-permission android:name="android.permission.READ_PHONE_STATE"/>
  <android:uses-permission android:maxSdkVersion="18" android:name="android.permission.READ_EXTERNAL_STORAGE"/>
  <android:uses-permission android:name="android.permission.READ_CALL_LOG"/>
  <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
  <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
  <uses-feature android:glEsVersion="0x00020000" android:required="true"/>
  <application android:allowBackup="true" android:debuggable="true" android:icon="@mipmap/ic_launcher" android:label="@string/app_name" android:theme="@an
droid:style/Theme.Holo.Light.DarkActionBar">
    <activity android:label="@string/app_name" android:name="com.android.insecurebankv2.LoginActivity">
      <intent-filter>
        <action android:name="android.intent.action.MAIN"/>
        <category android:name="android.intent.category.LAUNCHER"/>
      </intent-filter>
    </activity>
    <activity android:label="@string/title_activity_file_pref" android:name="com.android.insecurebankv2.FilePrefActivity" android:windowSoftInputMode="a
djustNothing|stateVisible">
    </activity>
    <activity android:label="@string/title_activity_do_login" android:name="com.android.insecurebankv2.DoLogin"/>
    <activity android:exported="true" android:label="@string/title_activity_post_login" android:name="com.android.insecurebankv2.PostLogin"/>
  </>
  <activity android:exported="true" android:label="@string/title_activity_do_transfer" android:name="com.android.insecurebankv2.DoTransfer"/>--- More
  <activity android:exported="true" android:label="@string/title_activity_view_statement" android:name="com.android.insecurebankv2.ViewStatement"/>---
  <provider android:authorities="com.android.insecurebankv2.TrackUserContentProvider" android:exported="true" android:name="com.android.insecurebankv2
.TrackUserContentProvider"/>
  <receiver android:exported="true" android:name="com.android.insecurebankv2.MyBroadcastReceiver">
    <intent-filter>
      <action android:name="theBroadcast"/>
    </intent-filter>
  </receiver>
  <activity android:exported="true" android:label="@string/title_activity_change_password" android:name="com.android.insecurebankv2.ChangePassword"/>---
  <activity android:configChanges="keyboard|keyboardHidden|orientation|screenLayout|screenSize|smallestScreenSize|uiMode" android:name="com.google.and
roid.gms.ads.AdActivity" android:theme="@android:style/Theme.Translucent"/>
  <meta-data android:name="com.google.android.gms.wallet.api.enabled" android:value="true"/>
  <intent-filter>
    <action android:name="com.google.android.gms.wallet.ENABLE_WALLET_OPTIMIZATION"/>
  </intent-filter>
</application>
</manifest>
```

Chuyển file apk sang jar, và đọc bằng jd-gui:

```
C:\WINDOWS\system32\cmd. X + v
dex2jar C:\Users\Public\Documents\InsecureBankv2.apk -> .\InsecureBankv2-dex2jar.jar
```

DoLogin.class - Java Decompiler

File Edit Navigation Search Help

InsecureBankv2-dex2jar.jar

- android.support
- com
 - android.insecurebankv2
 - BuildConfig.class
 - ChangePassword.class
 - CryptoClass.class
 - DoLogin.class
 - DoLogin
 - DoTransfer.class
 - FileRefActivity.class
 - LoginActivity.class
 - MyBroadcastReceiver.class
 - MyWebViewClient.class
 - PostLogin.class
 - R.class
 - TrackerContentProvider.class
 - ViewStatement.class
 - WrongLogin.class
 - google

```
package com.android.insecurebankv2;

import android.app.Activity;
import android.content.ContentValues;
import android.content.Context;
import android.content.Intent;
import android.content.SharedPreferences;
import android.os.AsyncTask;
import android.os.Bundle;
import android.preference.PreferenceManager;
import android.util.Base64;
import android.util.Log;
import android.view.Menu;
import android.view.MenuItem;
import android.widget.Toast;
import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStream;
import java.io.InputStreamReader;
import java.io.UnsupportedEncodingException;
import java.security.InvalidAlgorithmParameterException;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.util.ArrayList;
import javax.crypto.BadPaddingException;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.NoSuchPaddingException;
import org.apache.http.HttpEntity;
import org.apache.http.HttpResponse;
import org.apache.http.client.ClientProtocolException;
import org.apache.http.client.entity.UrlEncodedFormEntity;
import org.apache.http.client.methods.HttpPost;
import org.apache.http.client.methods.HttpUriRequest;
import org.apache.http.impl.client.DefaultHttpClient;
import org.apache.http.message.BasicNameValuePair;
import org.json.JSONException;

public class DoLogin extends Activity {
    public static final String MY_PREFS = "mySharedPreferences";

    String password;

    String protocol = "http://";

    BufferedReader reader;

    String rememberme_password;
```

Kiểm tra mã nguồn các class ChangePassword, My BroadCastReceiver:

```
ChangePassword.class

String protocol = "http://";

BufferedReader reader;

String result;

SharedPreferences serverDetails;

String serverip = "";

String serverport = "";

TextView textView_Username;

String uname;

private void broadcastChangepasswordSMS(String paramString1, String paramString2) {
    if (TextUtils.isEmpty(paramString1.toString().trim())) {
        System.out.println("Phone number Invalid.");
        return;
    }
    Intent intent = new Intent();
    intent.setAction("theBroadcast");
    intent.putExtra("phonenumber", paramString1);
    intent.putExtra("newpass", paramString2);
    sendBroadcast(intent);
}
```

Giá trị str3 là số điện thoại của người dùng bị gửi đi qua một Text Message

```
ChangePassword.class  MyBroadCastReceiver.class

package com.android.insecurebankv2;

import android.content.BroadcastReceiver;
import android.content.Context;
import android.content.Intent;
import android.content.SharedPreferences;
import android.telephony.SmsManager;
import android.util.Base64;

public class MyBroadCastReceiver extends BroadcastReceiver {
    public static final String MYPREFS = "mySharedPreferences";

    String usernameBase64ByteString;

    public void onReceive(Context paramContext, Intent paramIntent) {
        String str2 = paramIntent.getStringExtra("phonenumber");
        String str1 = paramIntent.getStringExtra("newpass");
        if (str2 != null)
            try {
                SharedPreferences sharedPreferences = paramContext.getSharedPreferences("mySharedPreferences", 1);
                this.usernameBase64ByteString = new String(Base64.decode(sharedPreferences.getString("EncryptedUsername", null), 0), "UTF-8");
                String str3 = sharedPreferences.getString("superSecurePassword", null);
                String str4 = (new CryptoClass()).aesDecryptedString(str3);
                str3 = str2.toString();
                str1 = "Updated Password from: " + str4 + " to: " + str1;
                SmsManager smsManager = SmsManager.getDefault();
                System.out.println("For the changepassword - phonenumber: " + str3 + " password is: " + str1);
                smsManager.sendTextMessage(str3, null, str1, null, null);
                return;
            } catch (Exception exception) {
                exception.printStackTrace();
                return;
            }
        System.out.println("Phone number is null");
    }
}
```

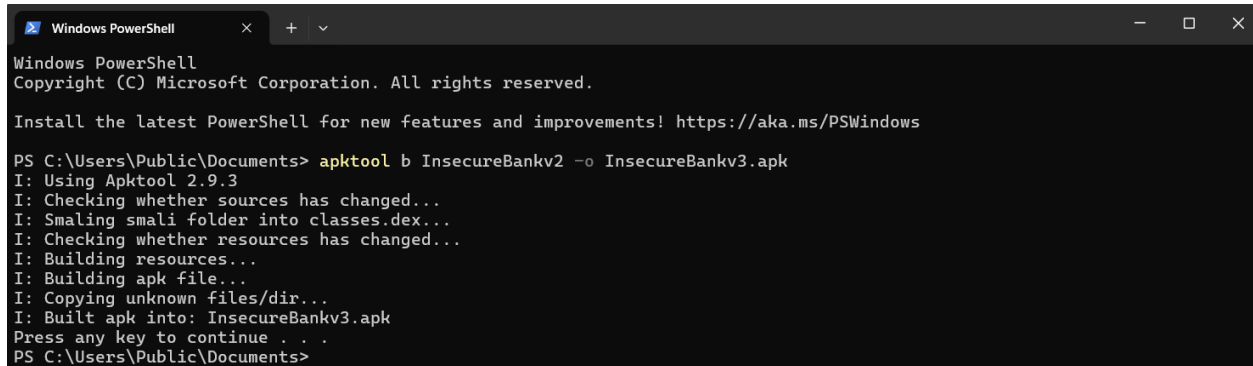
Vá lỗi hỏng bằng cách sửa trường android:exported="false" trong AndroidManifest.xml

```

28 | <provider android:authorities="com.android.insecurebankv2.TrackUserContentProvider" android:exported="true" android:name="com.android.insecurebankv2.TrackUserCont
29 | <receiver android:exported="false" android:name="com.android.insecurebankv2.MyBroadcastReceiver">
30 |   <intent-filter>
31 |     <action android:name="theBroadcast"/>
32 |   </intent-filter>
33 | </receiver>

```

Thực hiện biên dịch lại mã nguồn:



```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Public\Documents> apktool b InsecureBankv2 -o InsecureBankv3.apk
I: Using Apktool 2.9.3
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk into: InsecureBankv3.apk
Press any key to continue . . .
PS C:\Users\Public\Documents>

```

Các quyền mà InsecureBankv2 yêu cầu sử dụng:

1. Quyền truy cập tệp:

```
public static final String FOREGROUND_SERVICE_DATA_SYNC
```

2. Quyền truy cập cuộc gọi:

```
public static final String FOREGROUND_SERVICE_PHONE_CALL
```

3. Quyền truy cập camera:

```
public static final String FOREGROUND_SERVICE_CAMERA
```

4. Quyền truy cập tài khoản:

```
public static final String FOREGROUND_SERVICE_CONNECTED_DEVICE
```

Tóm lại, InsecureBankv2 yêu cầu nhiều quyền truy cập nhạy cảm trên thiết bị của bạn.