



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

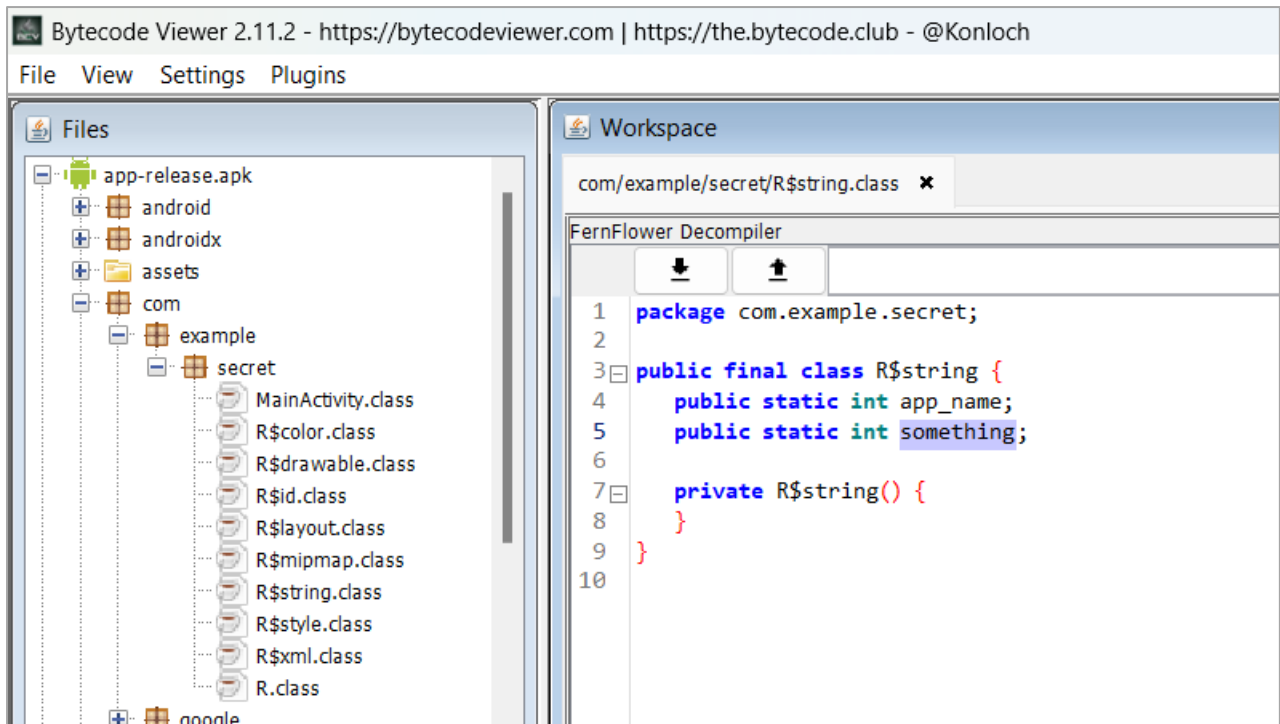
2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Crack M3	100%
2	FlappyBird	100%

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

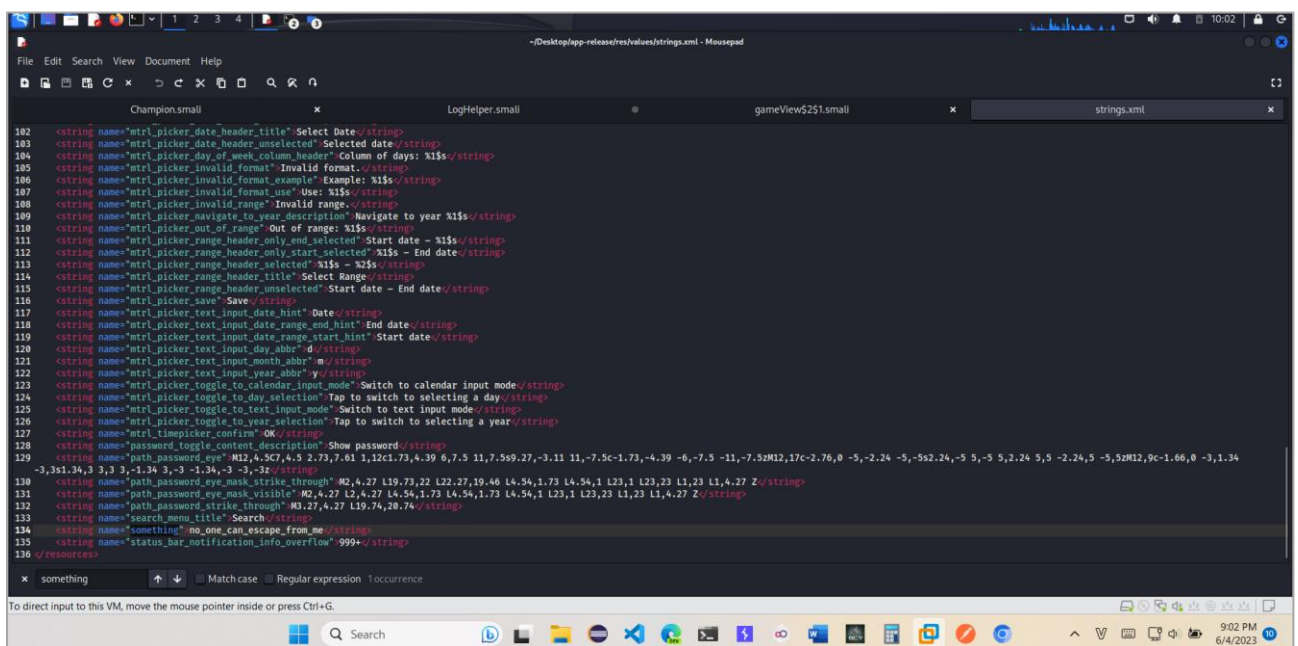
¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

Báo cáo Bảo mật Web và Ứng dụng
HOC KỲ II – NĂM HỌC 2022-2023



Hình 2: Vào lớp R\$string.class

Tìm tới “something”:



→ 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;

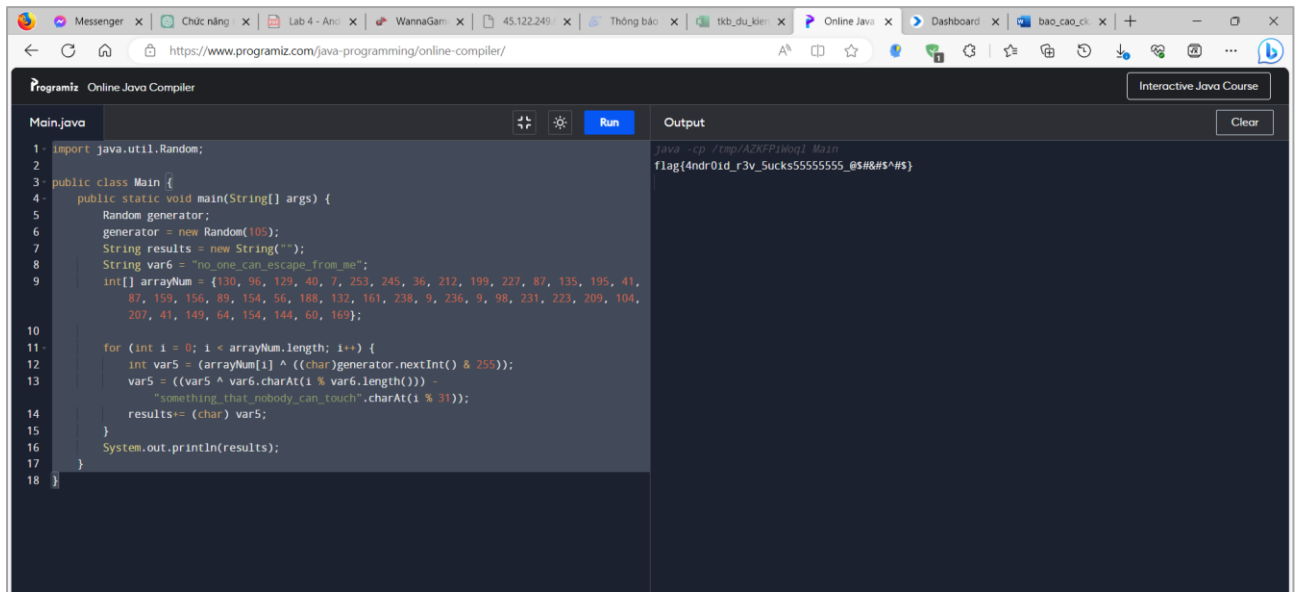
        }

        System.out.println(results);

    }

}
```

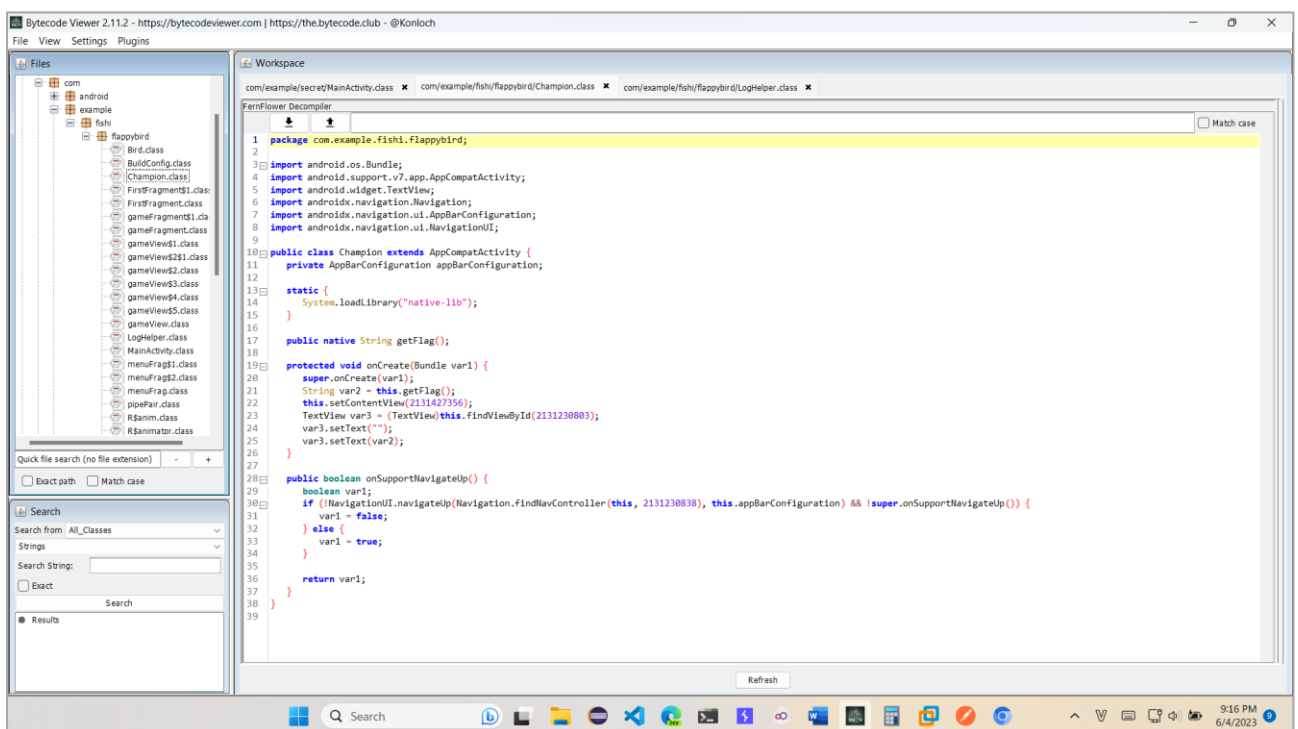
Chuỗi nhận được là: **flag{4ndr0id_r3v_5ucks55555555_@ \$#&# \$^# \$}**



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:



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



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...

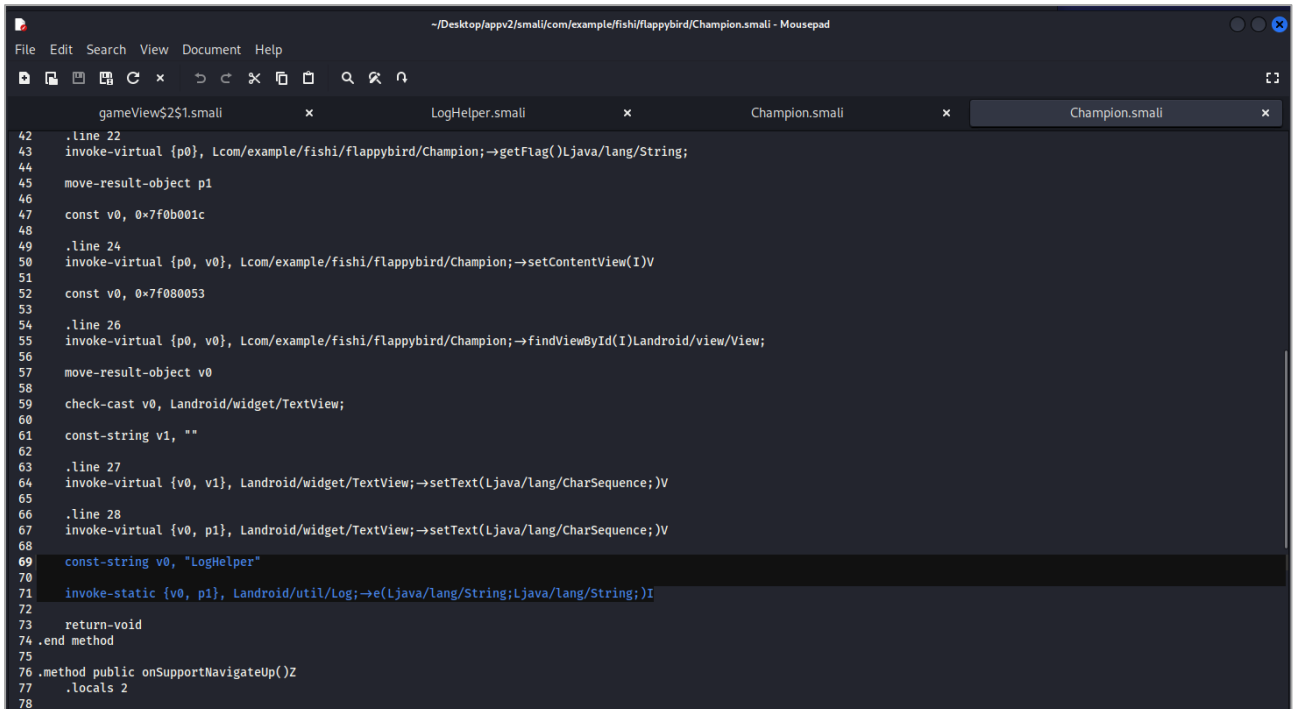
(kali@kali)-[~/Desktop]
$ apktool b app-release_chall.apk -o apprelease.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.7.0-dirty
brut.directory.PathNotExist: apktool.yml

(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 (defaulting 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/APKTOOL15869712436238587305.tmp, -0, resources.arsc, -0, META-INF/android.arch.core_runtime.version, -0, META-INF/android.arch.lifecycle_livedata_core.version, -0, META-INF/android.arch.lifecycle_livedata.version, -0, META-INF/android.arch.lifecycle_runtime.version, -0, META-INF/android.arch.lifecycle_viewmodel.version, -0, META-INF/android.arch.navigation_navigation-common.version, -0, META-INF/android.arch.navigation_navigation-fragment.version, -0, META-INF/android.arch.navigation_navigation-runtime.version, -0, META-INF/android.arch.navigation_navigation-ui.version, -0, META-INF/android.support.design_material.version, -0, META-INF/androidx.appcompat_appcompat.version, -0, META-INF/androidx.asynclayoutinflater_asynclayoutinflater.version, -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/androidx.customview_customview.version, -0, META-INF/androidx.documentfile_documentfile.version, -0, META-INF/androidx.drawerlayout_drawerlayout.version, -0, META-INF/androidx.fragment_fragment.version, -0, META-INF/androidx.interpolator_interpolator.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_localbroadcastmanager.version, -0, META-INF/androidx.print_print.version, -0, META-INF/androidx.recyclerview_recyclerview.version, -0, META-INF/androidx.slidingpanelayout_slidingpanelayout.version, -0, META-INF/androidx.swiperefreshlayout_swiperefreshlayout.
```

Hình 4: Build lỗi

Vậy nên cần sử dụng lệnh trước đó đã đề 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:

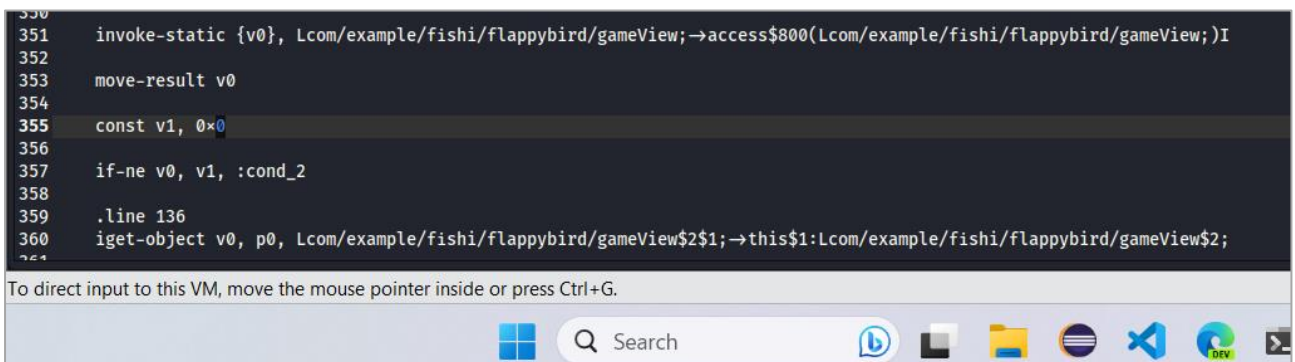


```

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 .line 24
47 invoke-virtual {p0, v0}, Lcom/example/fishi/flappybird/Champion;→setContentView(I)V
48 const v0, 0x7f080053
49 .line 26
50 invoke-virtual {p0, v0}, Lcom/example/fishi/flappybird/Champion;→findViewById(I)Landroid/view/View;
51 move-result-object v0
52 check-cast v0, Landroid/widget/TextView;
53 const-string v1, ""
54 .line 27
55 invoke-virtual {v0, v1}, Landroid/widget/TextView;→setText(Ljava/lang/CharSequence;)V
56 .line 28
57 invoke-virtual {v0, p1}, Landroid/widget/TextView;→setText(Ljava/lang/CharSequence;)V
58 const-string v0, "LogHelper"
59 invoke-static {v0, p1}, Landroid/util/Log;→e(Ljava/lang/String;Ljava/lang/String;)I
60 return-void
61 .end method
62 .method public onSupportNavigateUp()Z
63 .locals 2

```

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 move-result v0
353 const v1, 0x0
354 if-ne v0, v1, :cond_2
355 .line 136
356 iget-object v0, p0, Lcom/example/fishi/flappybird/gameView$2$1;→this$1:Lcom/example/fishi/flappybird/gameView$2;

```

Đổi 999999999 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? View$2$1; → this$1:Lcom/example/fishi/flappybird/gameView$2;
[Unknown]:
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
```

Hình 6: Ký cho tệp apk

Chạy app và:

```
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_compos
mposition_v2 ANDROID_EMU_async_unmap_buffer ANDROID_EMU_sync_buffer_data GL_OES_EGL_image_ex
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 c
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;
        }

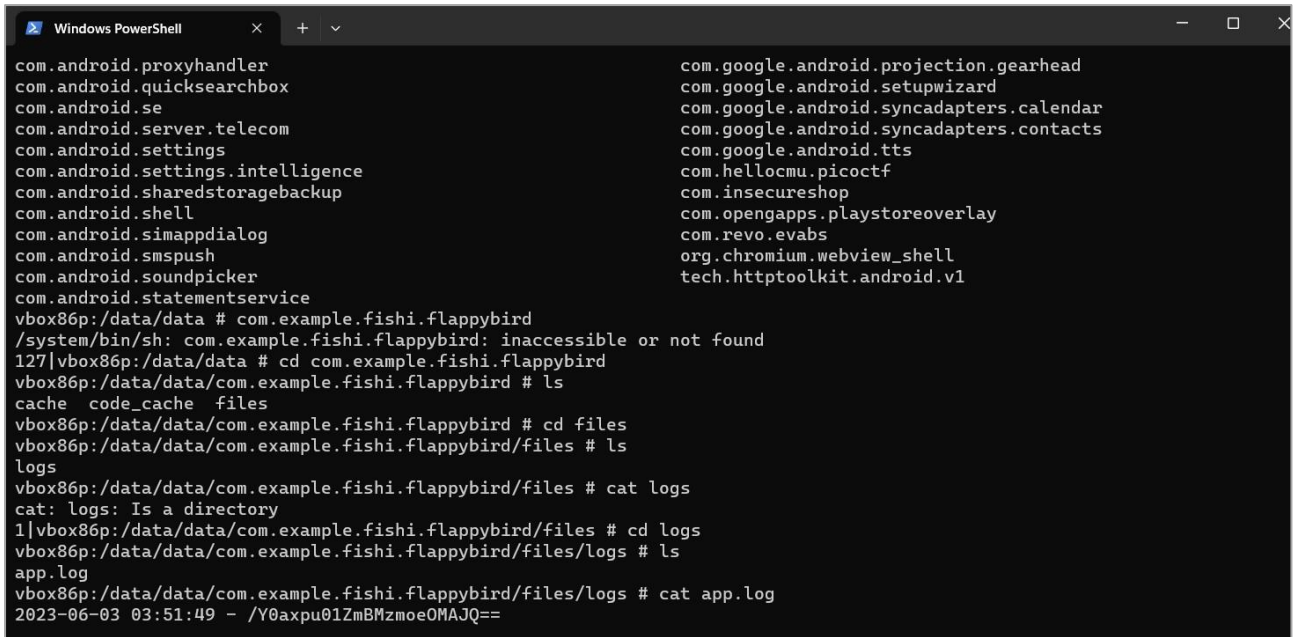
        StringBuilder var7 = new StringBuilder();
```

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.

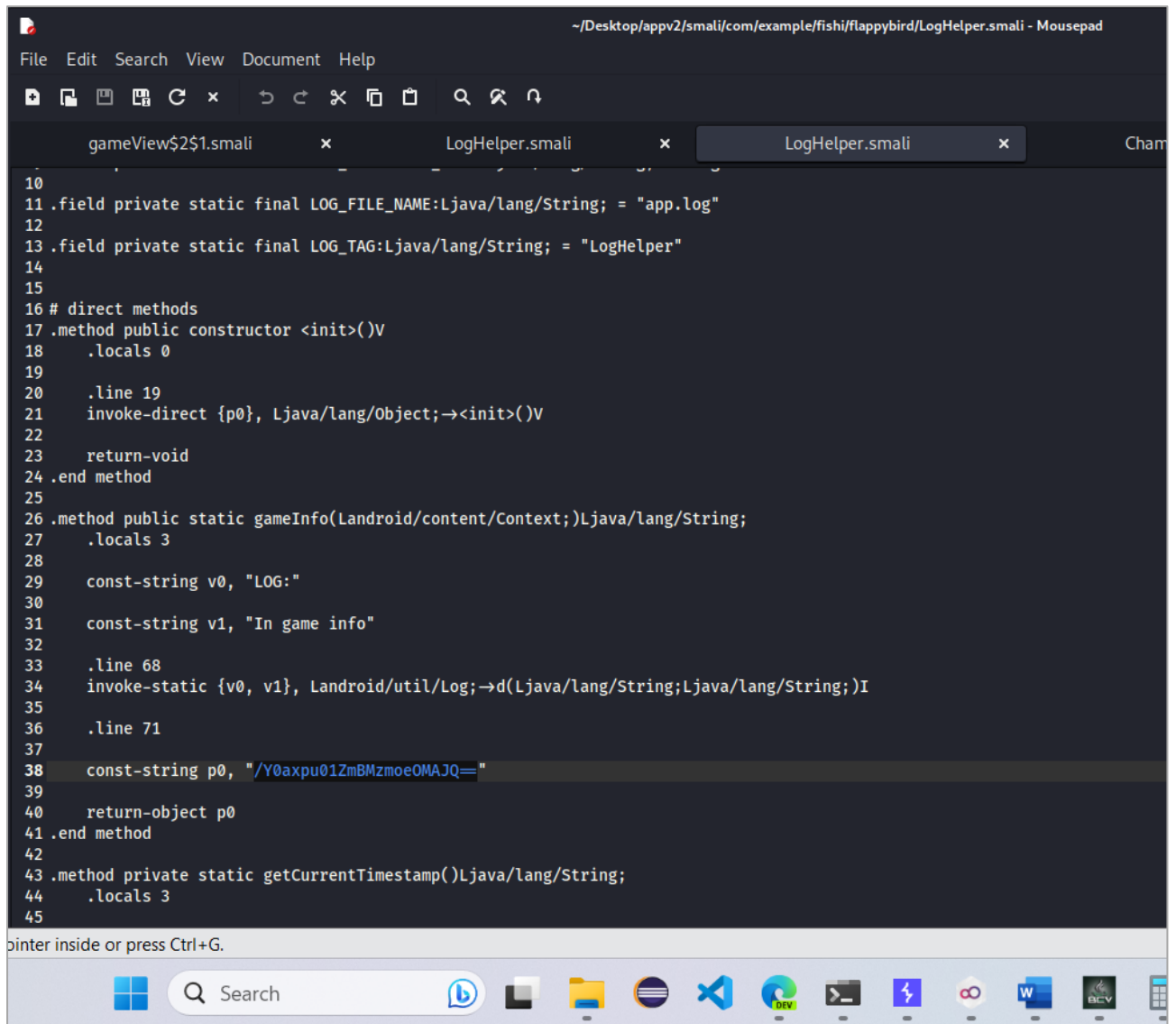
Xem xuống vị trí lưu của log, chúng ta thấy nó được lưu trong log/app.logs, tìm tới vị trí lưu của nó nên chúng ta có thể vào đây và lấy nội dung để hàm gameInfo có thể return thẳng về nó.



```
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.smpush
com.android.soundpicker
com.android.statementservice
com.google.android.projection.gearhead
com.google.android.setupwizard
com.google.android.syncadapters.calendar
com.google.android.syncadapters.contacts
com.google.android.tts
com.helloemu.picocftf
com.insecureshop
com.opengapps.playstoreoverlay
com.revo.evabs
org.chromium.webview_shell
tech.http toolkit.android.v1
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 - /Y0axpu01ZmBMzmoe0MAJQ==
```

Hình 9: Xem nơi lưu chuỗi được mã hoá cũ

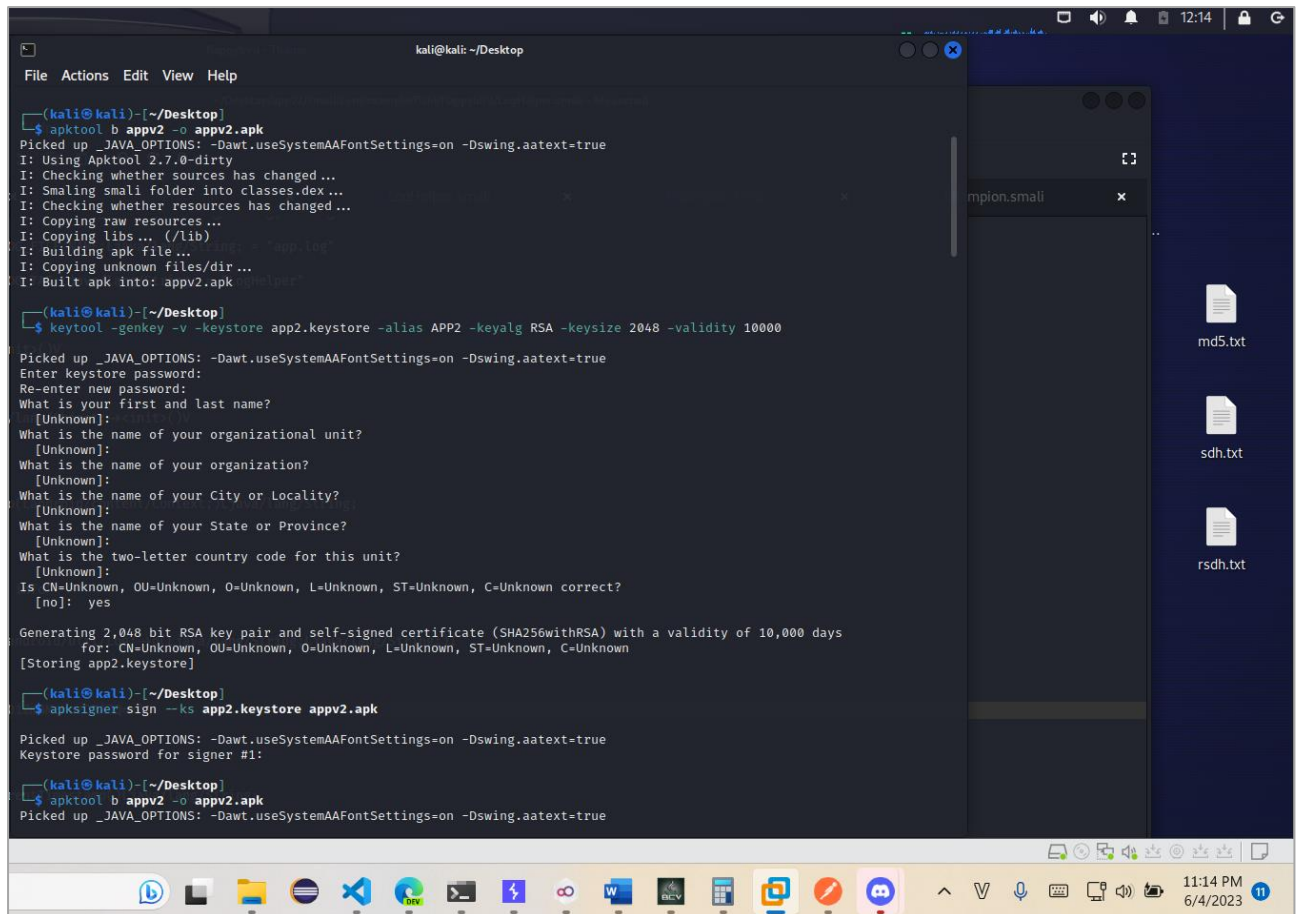
Chúng ta sửa code trong `gameInfo()` return chuỗi này, thực hiện decompile để sửa nội dung app đã được sửa score để gọi tới Champion activity:



```
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>()V
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, "/Y0axpu01ZmBMzmoe0MAJQ=="
39
40     return-object p0
41 .end method
42
43 .method private static getCurrentTimestamp()Ljava/lang/String;
44     .locals 3
45
```

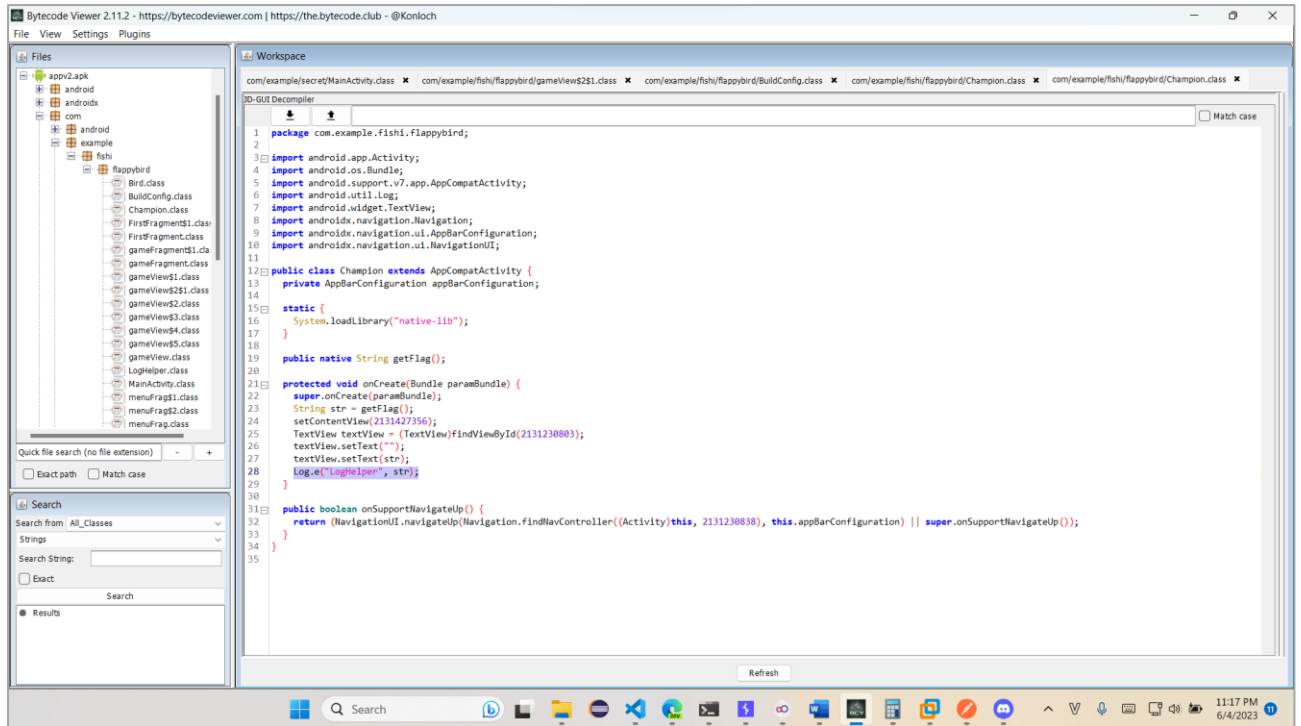
Hình 10: Sửa code

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



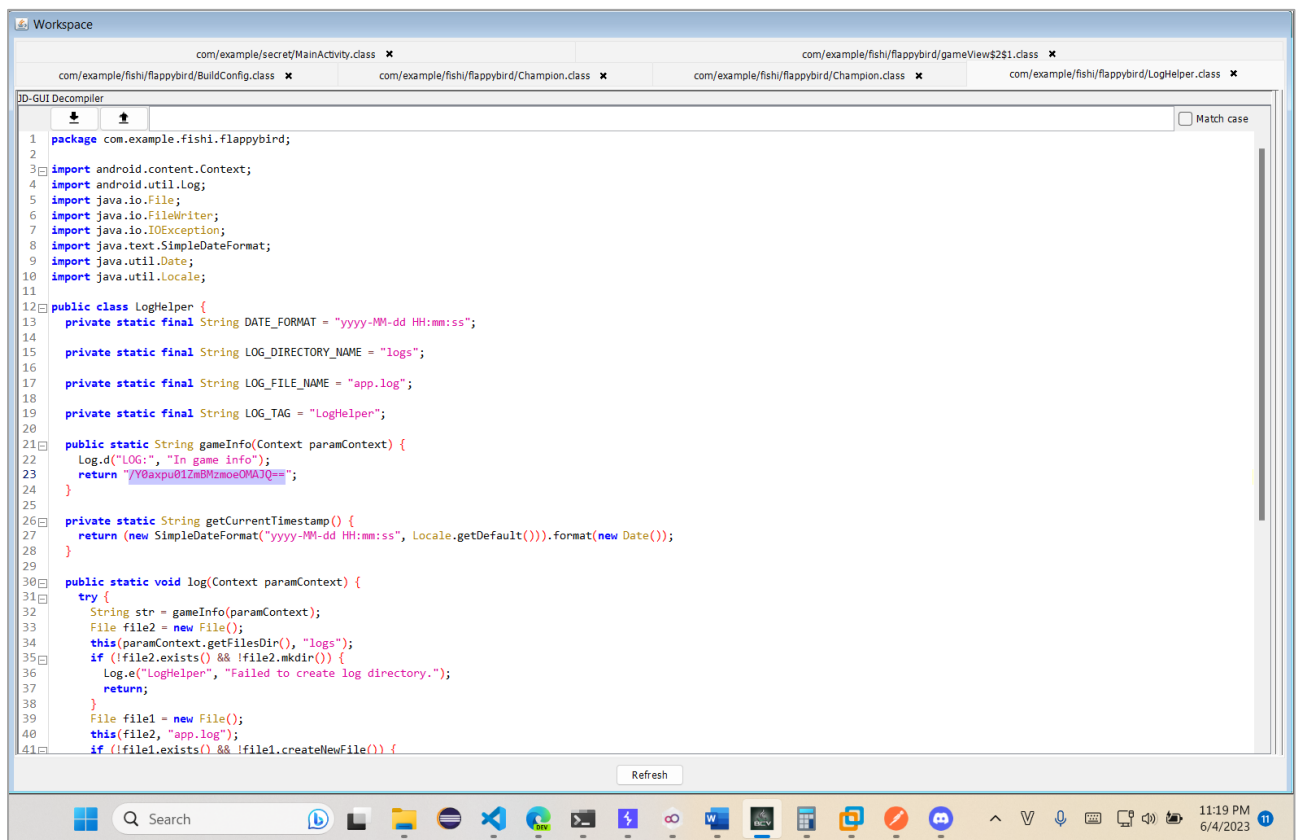
Hình 11: Build và kí

Xem lại nội dung app vừa làm:

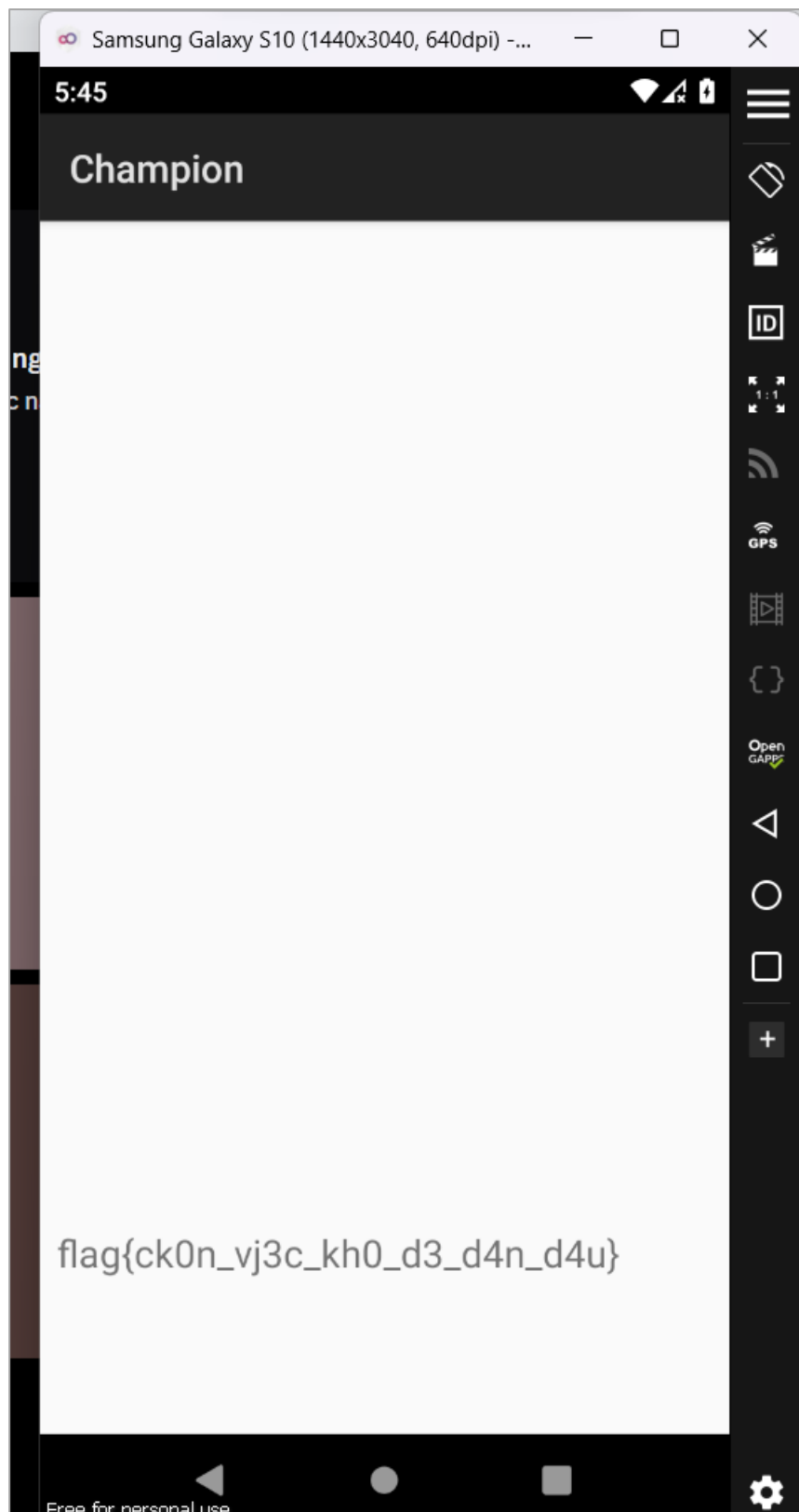


Hình 12: Có thêm log xem flag

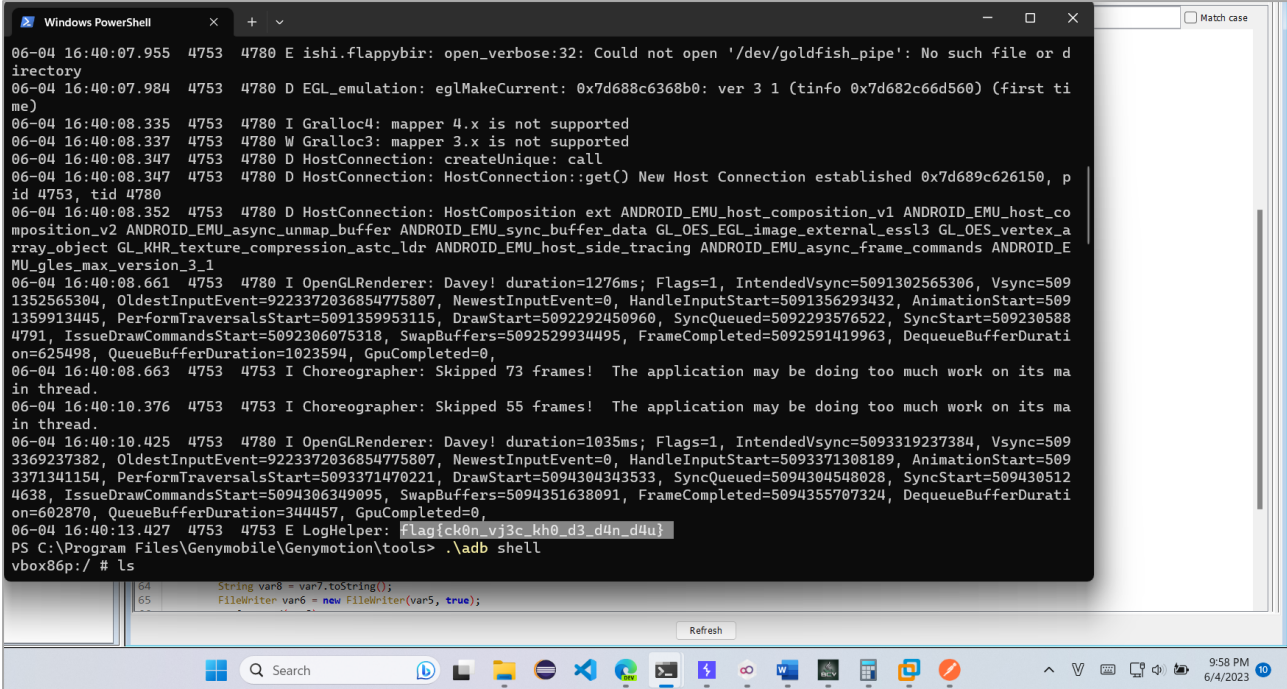
gameInfo() luôn trả về chữ kí cũ:



Hình 13: Kết quả chỉnh sửa trong LogHelper



Hình 14: Khi được 0 điểm thì lập tức nhảy



```
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: eglMakeCurrent: 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_astc_ldr ANDROID_EMU_host_side_tracing ANDROID_EMU_async_frame_commands ANDROID_E
MU_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=5092529934495, FrameCompleted=5092591419963, DequeueBufferDuration=625498, QueueBufferDuration=1023594, GpuCompleted=0,
06-04 16:40:08.663 4753 4753 I Choreographer: Skipped 73 frames! The application may be doing too much work on its main thread.
06-04 16:40:10.376 4753 4753 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 4753 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}