



Lab: Insecure direct object references

This lab stores user chat logs directly on the server's file system, and retrieves them using static URLs.

Solve the lab by finding the password for the user `carlos`, and logging into their account.

 Insecure direct object references
[Back to lab description >>](#)

LAB Not solved 

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


Live chat

System: No chat history on record
CONNECTED: -- Now chatting with Hal Pline --

Your message:

[Send](#) [View transcript](#)

In the Lab Description, it is given that there is a IDOR Vulnerability in the Chat Column, If we click the click view transcript the txt file is downloaded with 2.txt

 Insecure direct object references
[Back to lab description >>](#)

Downloads
2.txt
[Open file](#)
[See more](#)

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

Live chat

CONNECTED: -- Now chatting with Hal Pline --

You: hello

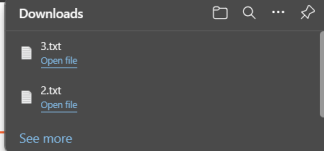
Hal Pline: I'm out of the office at the moment, please leave a message.

Hal Pline: I am the fount of all knowledge, but sorry I don't know that.

Your message:

[Send](#) [View transcript](#)

If we again click view transcript, 3.txt is downloaded we can guess that the number is generated in a incremental order.



Live chat

CONNECTED: -- Now chatting with Hal Pline --

You: hello

Hal Pline: I'm out of the office at the moment, please leave a message.

Hal Pline: I am the fount of all knowledge, but sorry I don't know that.

Hal Pline: Could you spell that please? I think you're making up words again

Your message:

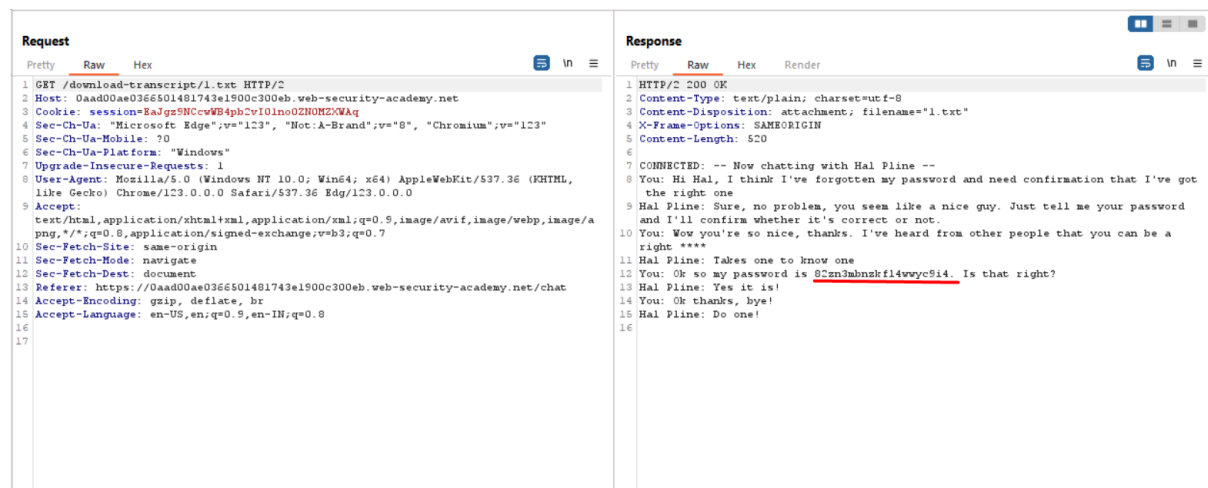
Send

View transcript

But during the first click on the View Transcript, it directly starts from 2.txt instead of 1.txt, using Burpsuite we try to intercept the request of view transcript.



Change the 4.txt to 1.txt and send the request the burp repeater and check the response.



We Obtained the password of the user carlos.



Insecure direct object references

[Back to lab description >>](#)

LAB Solved 

Congratulations, you solved the lab!

Share your skills!   Continue learning >>

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

My Account

Your username is: carlos

Email

Update email