**SCENARIO**

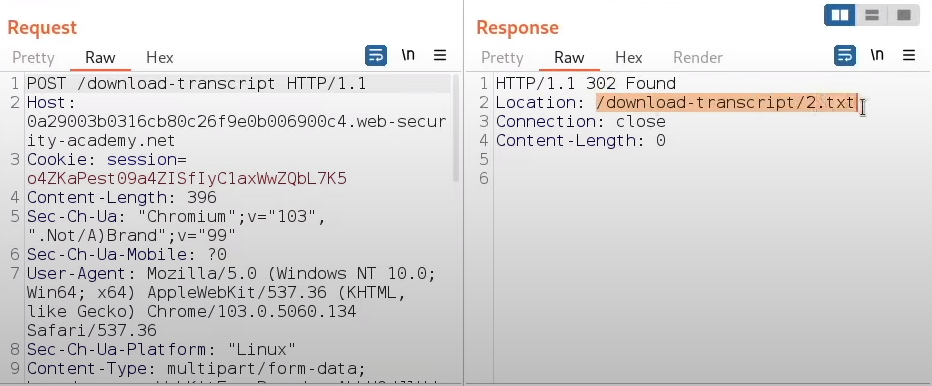
This lab stores user chat logs directly on the server's file system and retrieves them using static URLs. The challenge is to solve the lab by finding the password for the user 'carlos' and logging into their account.

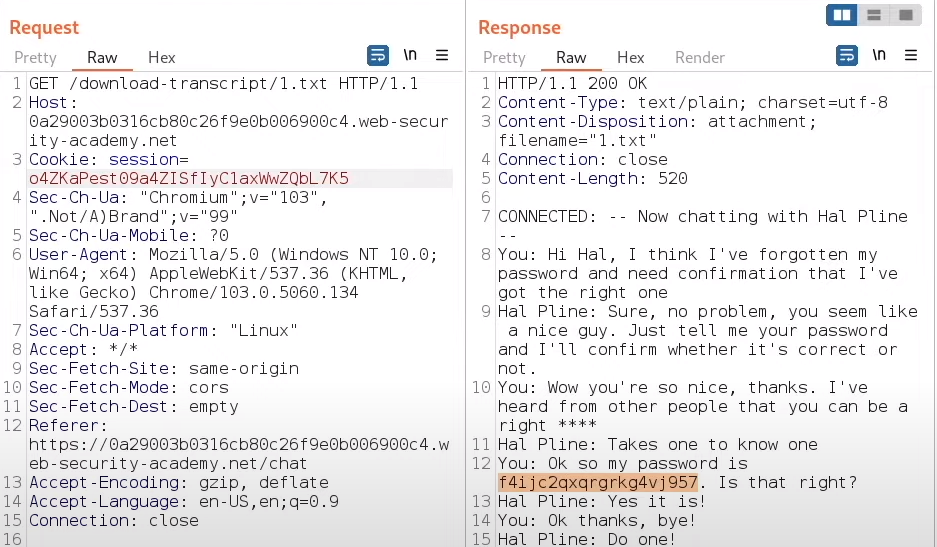
**PROCEDURE**

1. Navigate to the 'Live chat' tab.
2. Send a message and then choose the 'View transcript' option.
3. Examine the URL and take note of how the chat transcripts are stored as text files, with filenames based on incrementing numbers.
4. Modify the filename in the URL to 1.txt and analyze the content. Spot a password mentioned within the chat transcript.
5. Head back to the main lab page and utilize the discovered credentials to log in.
6. Exploit the vulnerability by conversing with a bot. Upon downloading the transcript, notice the filename pattern. By altering the file name in the URL and forwarding the download request using BurpSuite’s Repeater, successfully retrieve the password for the account.

**PAYLOAD**

**PROOF OF CONCEPT**

****

****

**REMEDIATION**

1. **Avoid Static URLs for Sensitive Data:** Instead of using predictable static URLs for sensitive data like chat transcripts, utilize randomized or hashed URLs to ensure they can't be easily guessed or enumerated.
2. **Authentication and Authorization:** Ensure that chat logs are only accessible by authenticated and authorized users. Implement checks to ensure users can only access their own logs.
3. **Rate Limiting and Monitoring:** Implement rate limiting for accessing chat logs to prevent brute-force attempts, and monitor for suspicious patterns of access.