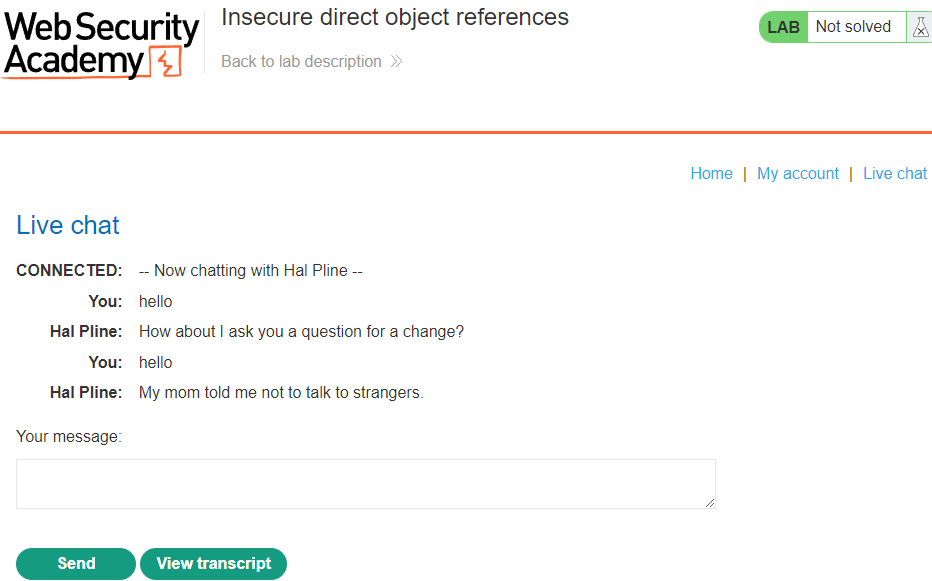
**Lab: Insecure direct object references**

Bài lab này sử dụng tham số trực tiếp trong các URL hoặc dữ liệu yêu cầu để truy cập vào các đối tượng nhạy cảm như tài khoản người dùng. Tuy nhiên, không có cơ chế kiểm tra quyền truy cập hợp lý, dẫn đến việc kẻ tấn công có thể thay đổi tham số này để truy cập vào dữ liệu của người dùng khác.

Mục tiêu của bài lab này là khai thác lỗ hổng Insecure Direct Object References (IDOR) để truy cập vào tài khoản của người dùng carlos. Để hoàn thành bài lab, bạn cần tìm ra URL hoặc tham số yêu cầu có thể bị lợi dụng để xem hoặc sửa đổi dữ liệu của carlos.

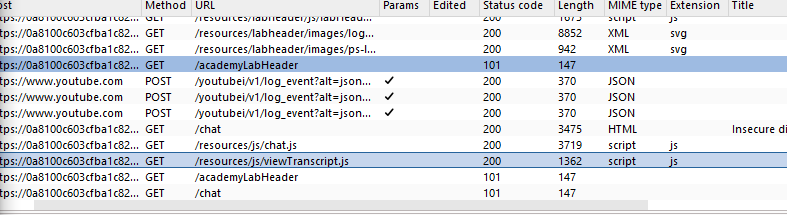
Các bước thực hiện:

Vào live chat, chat bất kỳ



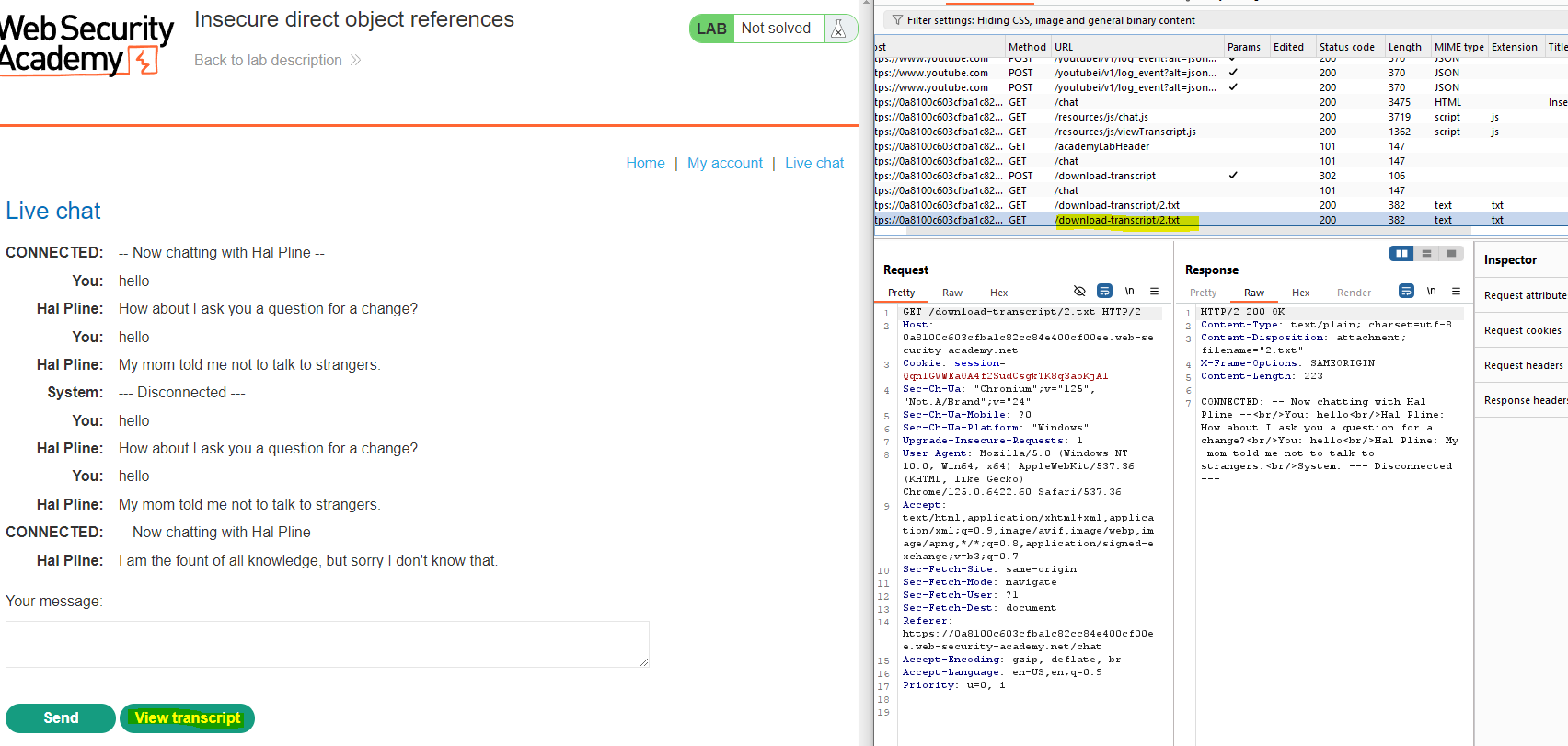
Hình 1. Live chat

Proxy không có mục nào, nên các chat thực hiện trên máy khách



Hình 2. Các đoạn chat không đi qua proxy

Nhấn “view transcript” để test chức năng



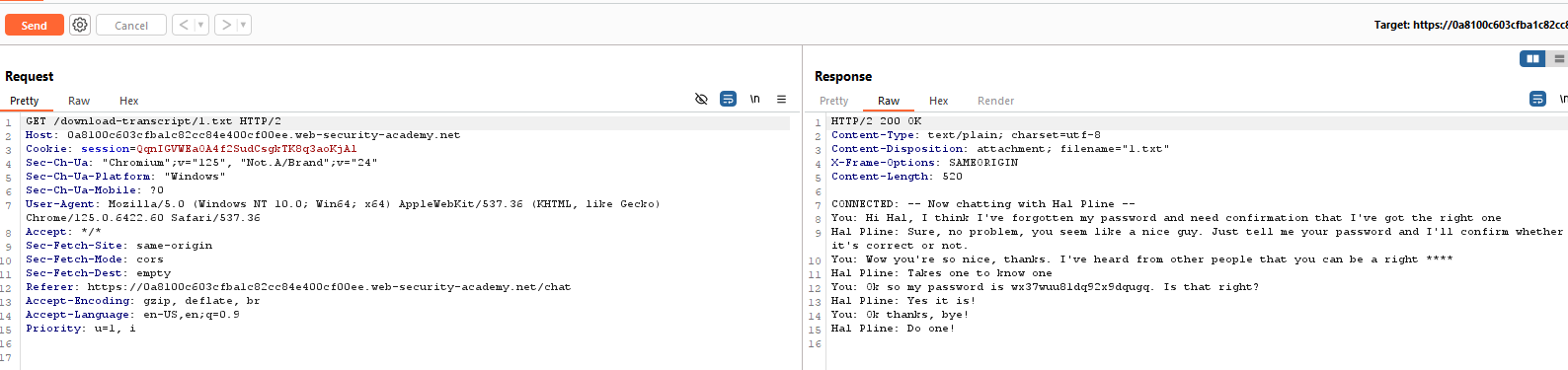
Hình 3. Giao diện sau khi ấn “View Transcript”

Gửi sang Reapeater để xem còn lịch sử đoạn chat nào không



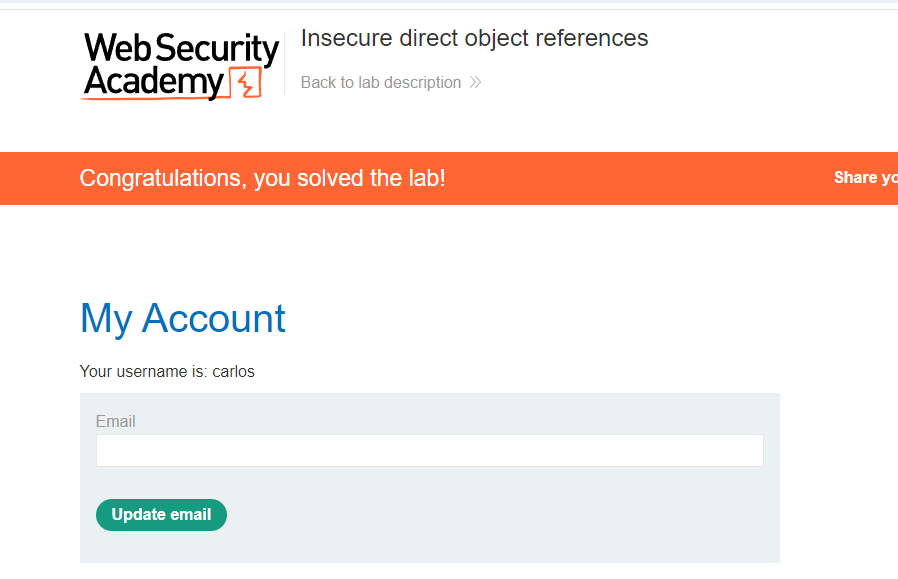
Hình 4. Request /download-transcript/2.txt

Vì thấy 2.txt nên thử 1.txt



Hình 5. Send request GET /download-transcript/1.txt

Tìm được mật khẩu của carlos, tiến hành đăng nhập tài khoản carlos với mật khẩu trên



Hình 6. Đăng nhập thành công tài khoản carlos, bài lab được hoàn thành