**LAB 11: INSECURE DIRECT OBJECT REFERENCES**

**B1:** Mở phần mềm Burp Suite lên, chuyển sang tab Proxy 🡪 HTTP history 🡪 Open browser.

A screenshot of a computer

Description automatically generated

**B2:** Copy và paste link sau vào browser để thực hiện lab11 (nhớ bấm access lab).

<https://portswigger.net/web-security/access-control/lab-insecure-direct-object-references>

**B3:** Không cần login vào mà hãy bấm vào mục live chat luôn.

A screenshot of a computer

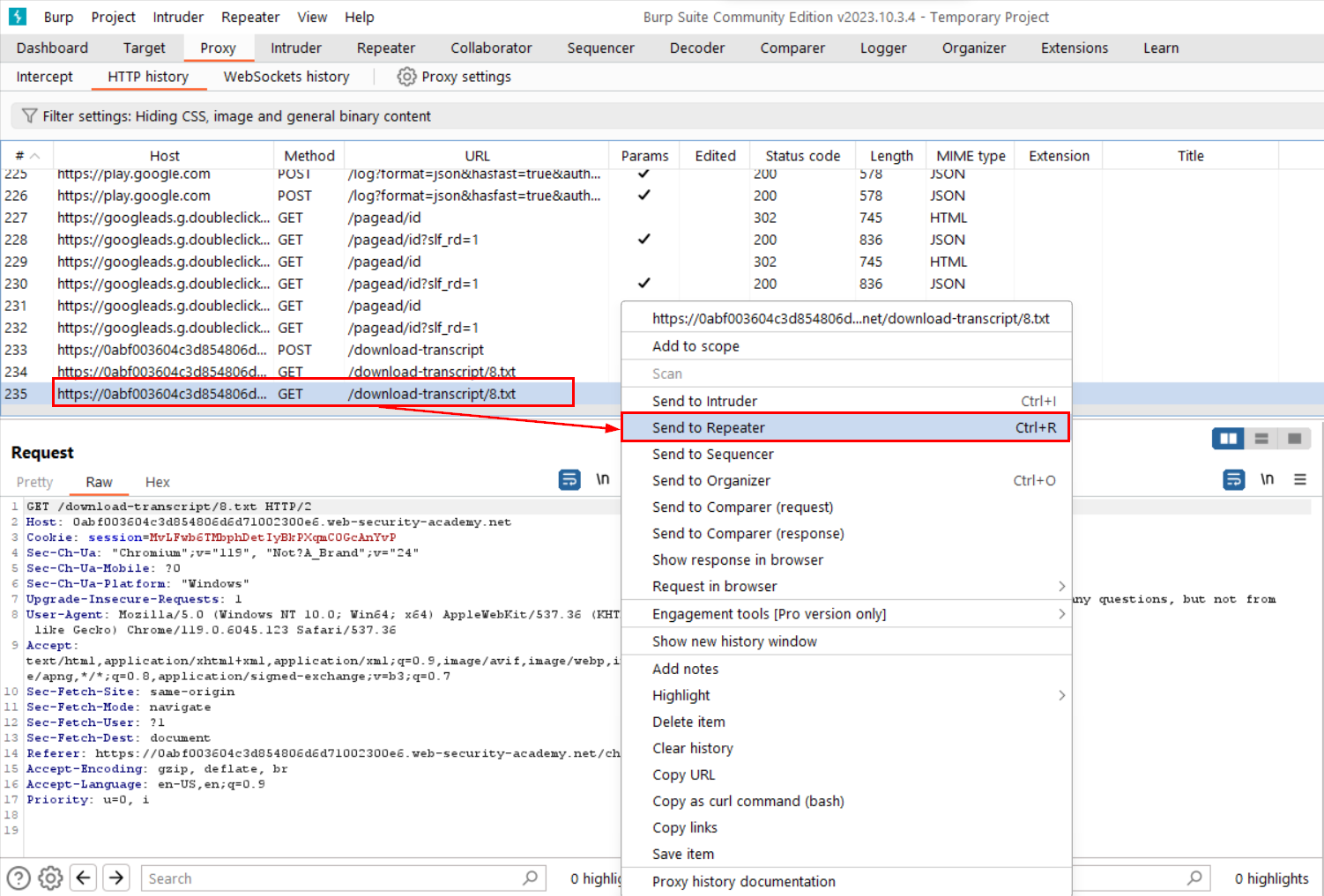
Description automatically generated

**B4:** Bấm View transcript để tải về một file .txt

A screenshot of a computer

Description automatically generated

**B5:** Vô lại phần mềm Burp Suite, chọn phần URL như sau (của mọi người có thể là 2.txt), chọn Send to Repeater.



**B6:** Chuyển sang tab Repeater, ở phần Inspector, chọn Request attributes.

A screenshot of a computer

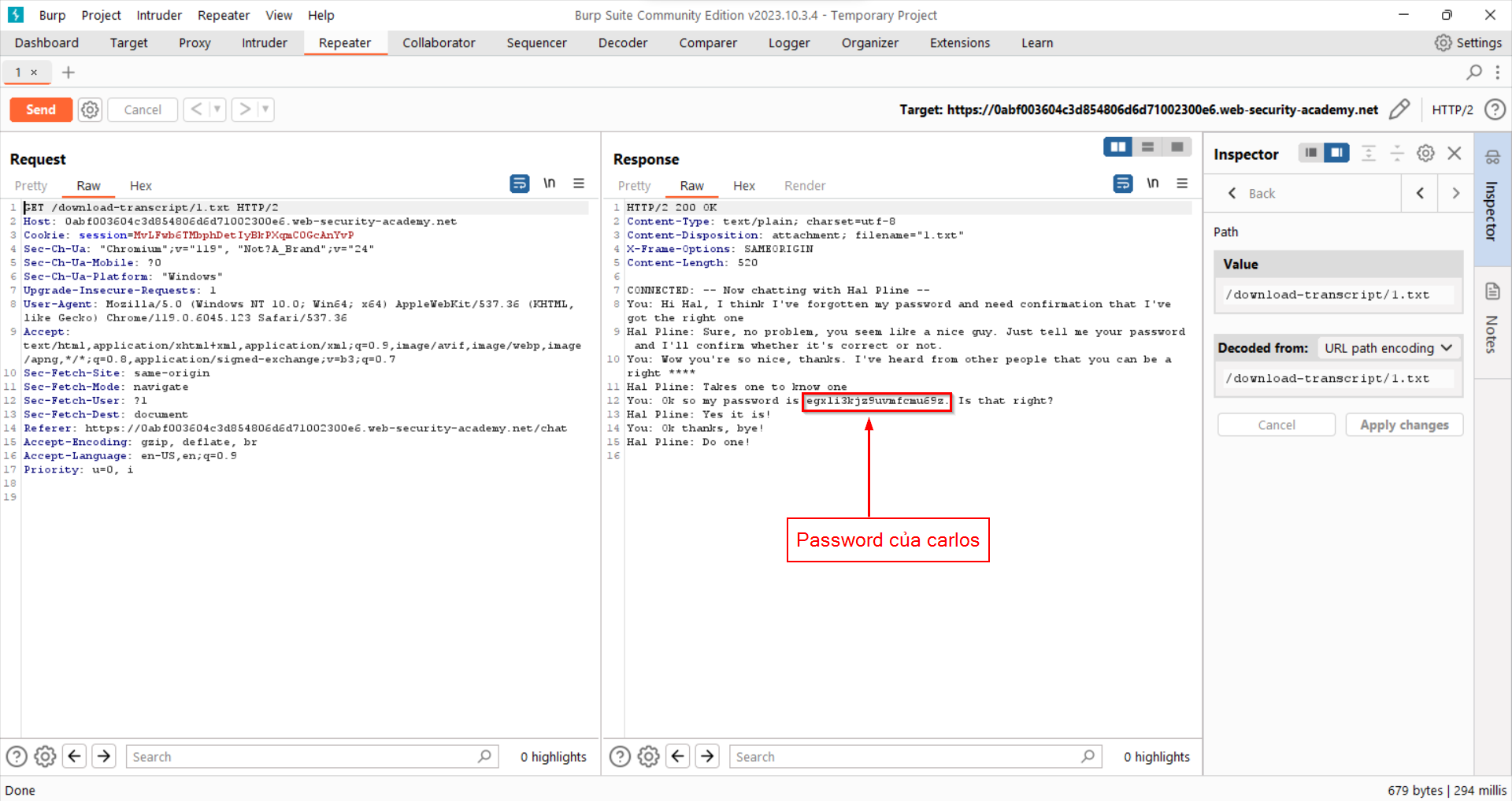
Description automatically generated

**B7:** Tiến hành thay đổi value của Path, đổi thành “download-transcript/1.txt”, rồi nhấn Send.

A screenshot of a computer

Description automatically generated

**B8:** Quan sát phần Response thì ta sẽ thấy được mật khẩu của user carlos, hãy copy mật khẩu này.



**B9:** Vô lại trang lab, chọn My account, login với username là carlos, password là cái mà ta vừa copy khi nãy.

A screenshot of a computer

Description automatically generated

**B10:** Vậy là ta đã hoàn thành lab này.

A screenshot of a computer

Description automatically generated

**-- HẾT --**