1. To get the flag, use the same payload we used above, but change its JavaScript code to show the cookie instead of showing the url.

Trang chủ

A screenshot of a to-do list

Description automatically generated

Thử chức năng với nhập “test”

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

Ta thấy file script.js sẽ được chạy mỗi khi tải trang

Xem cụ thể nội dung file script.js

A computer code with many black and white text

Description automatically generated

Tham số task từ url được đưa vào Source và  sử dụng hàm innerHTML để ghi biến task vào DOM todo.

Đã kiểm soát đầu vào nhưng đầu ra lại không được khử trùng, do đó trang này có thể dễ bị tấn công DOM XSS.

Ta có payload khai thác :

```bash

<img src="" onerror=alert(document.cookie)>

```

A screenshot of a computer

Description automatically generated

P/s : HTB{pur3ly\_cl13n7\_51d3}