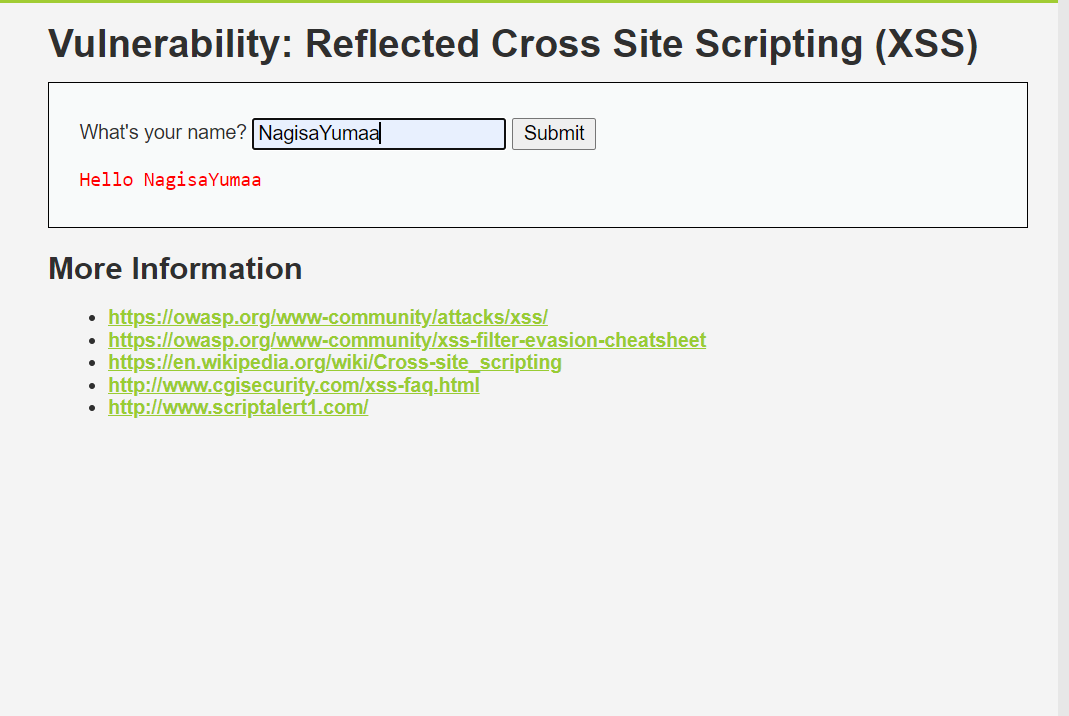
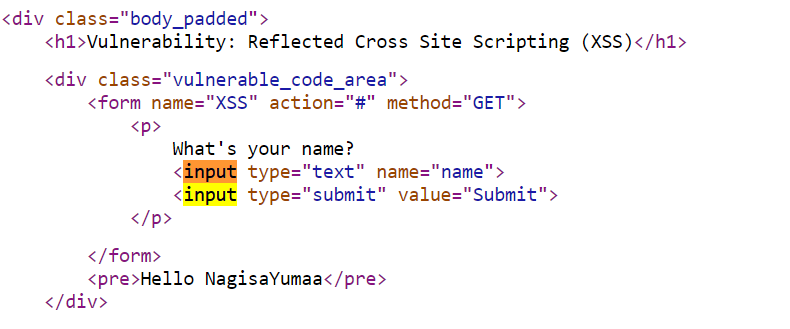
Xss DVWA :> mình bị xóa mất bài cũ nên giải thích ít thôi nhé

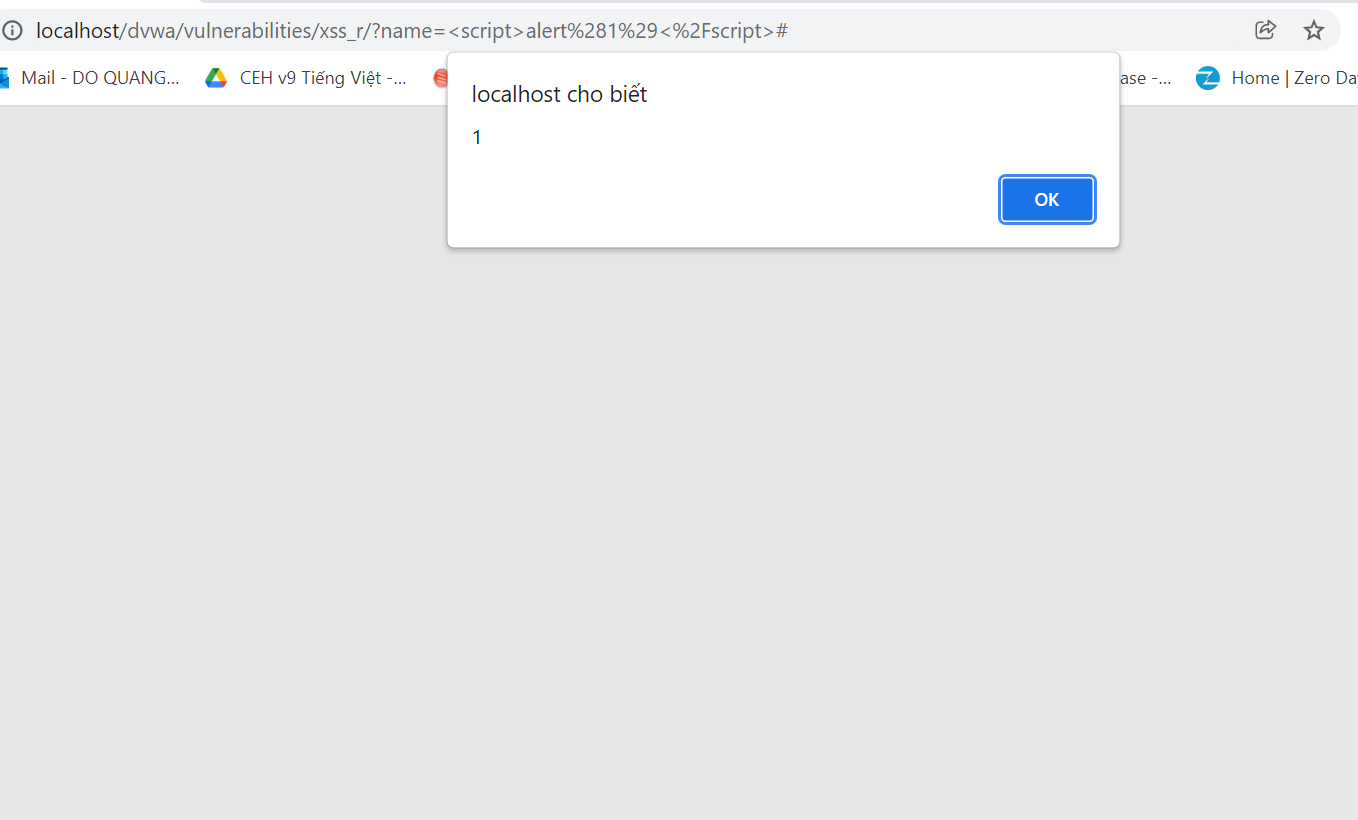
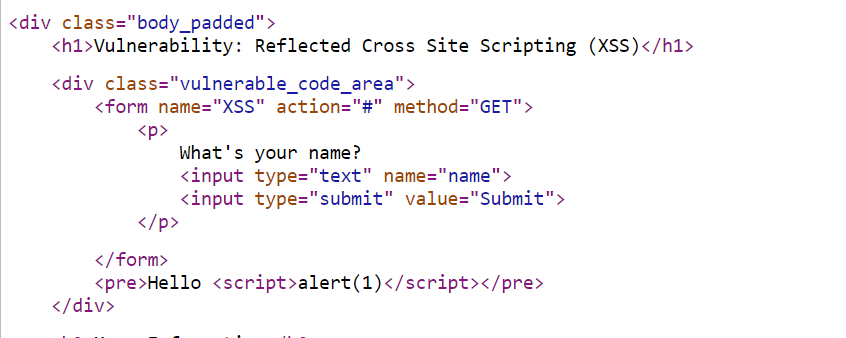
* Low
* **XSS Refected :**



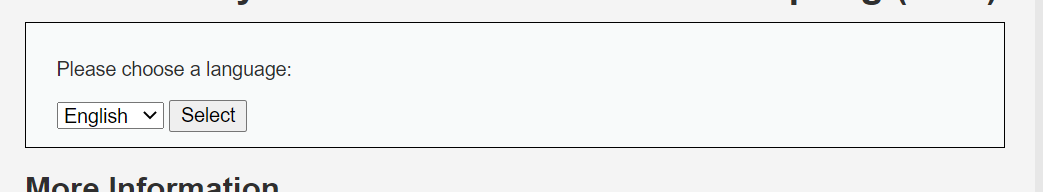
Đây là đoạn mã nguồn này :

* **Thấy đoạn input này không lọc bất cứ điều gì :>**
* Vậy điều gì xảy ra nếu ta chèn câu script đơn giản như này :

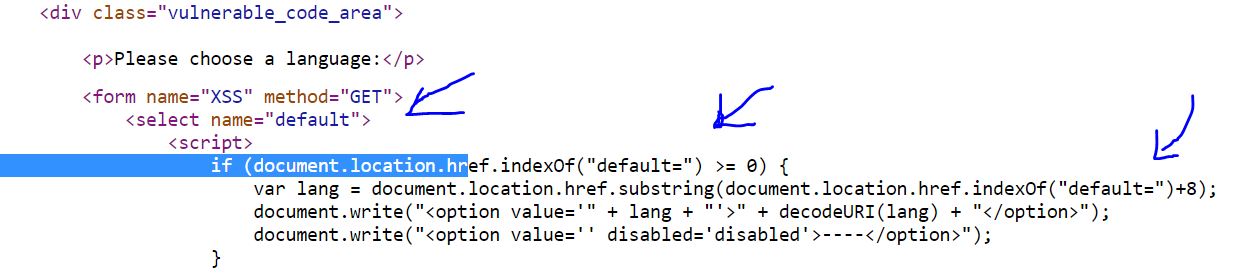
**nagisayumaa <script>alert(1)</script> ?**

* **Nhìn nè :**
* **nhìn lè : đoạn mã nguồn này nó bị thay đổi rùi :>**

bên dưới này nó thành đoạn Js thông báo 1 lun này

* **XSS Dom** :> cái nè thì khó giải thích lúm nhưng nhìn bên dưới nè

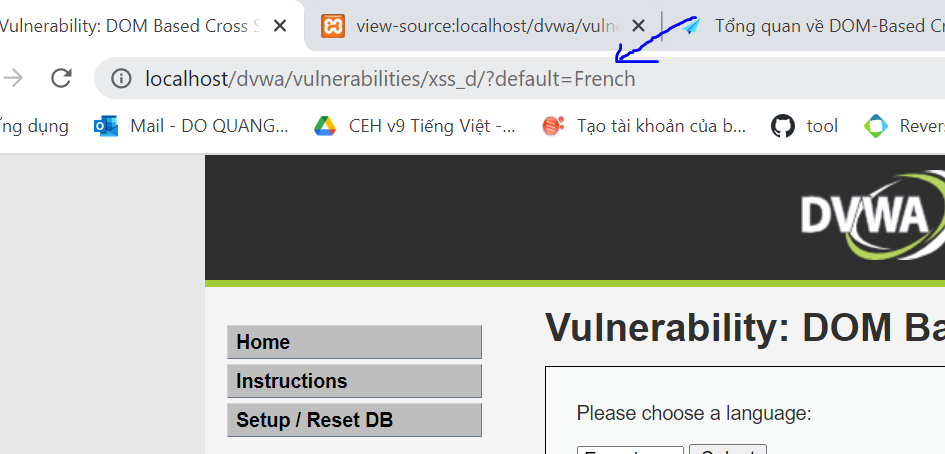
Nhìn thấy nó chỉ là một form bình thường thui đúng khum . Zậy nhìn đoạn mã của nó xem như nào nhé :>



Thấy mấy cái mũi tên màu xanh khum điều gì sẽ xảy ra nếu đoạn này bị chèn Script ?

Nó sẽ như này :> default=”<script>alert(1)</scripts>” --> rùi kết quả sẽ giống bên trên á :>

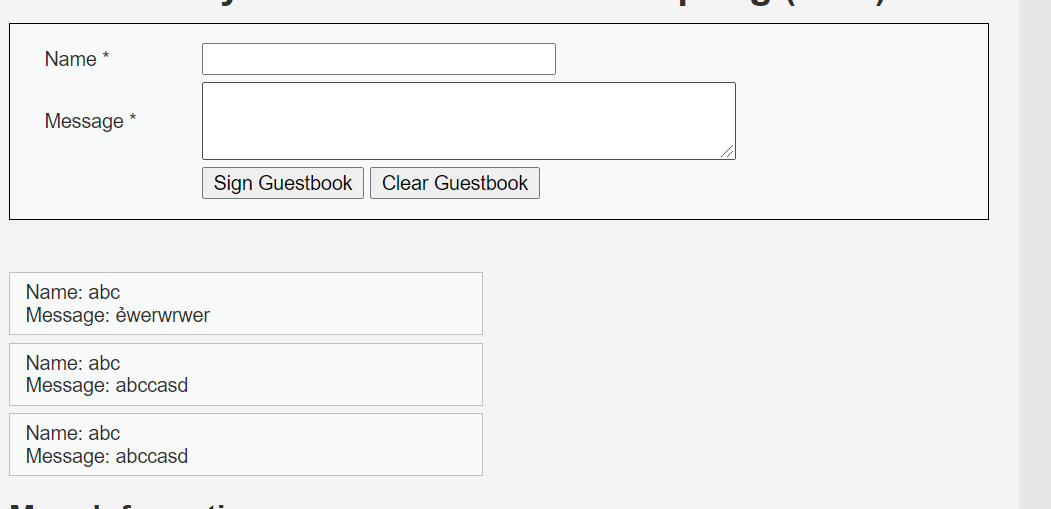
Nhưng nó là form mà thì làm thế nào để thay thì nhìn lè :>



Nếu thay ở trên này thì sao :> thử thì kết quả như Refected á : > khum chụp Kq nữa đâu nhé :>

* **XSS Store**

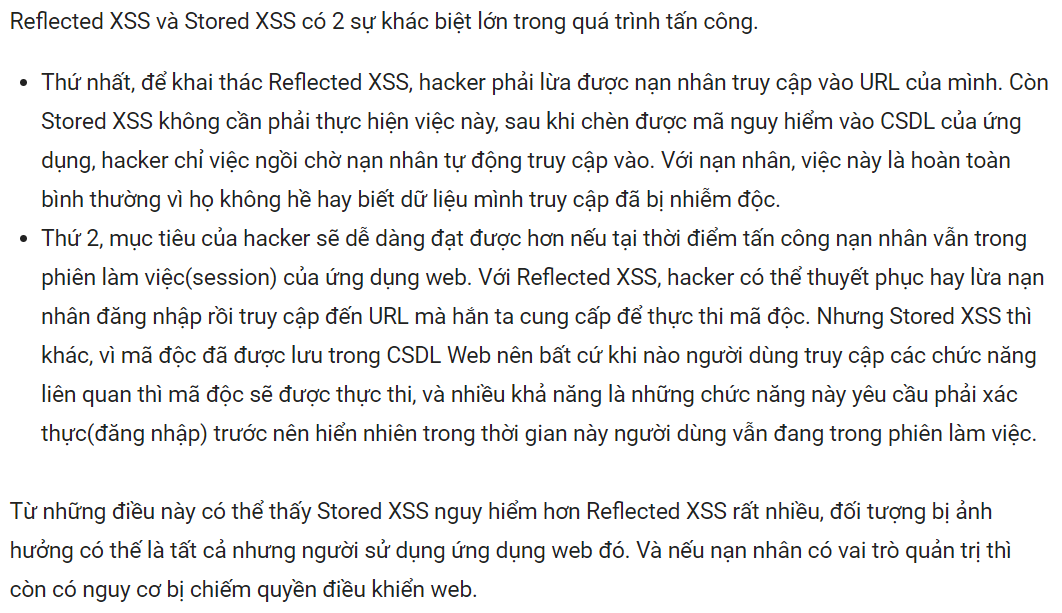
:> tính chất của cái nè thì giống cái trên



Nên up luôn mã nguồn nhớ tương tự lun

s



Lên mạng thì mình đọc đc cái này :> nghe sợ cực

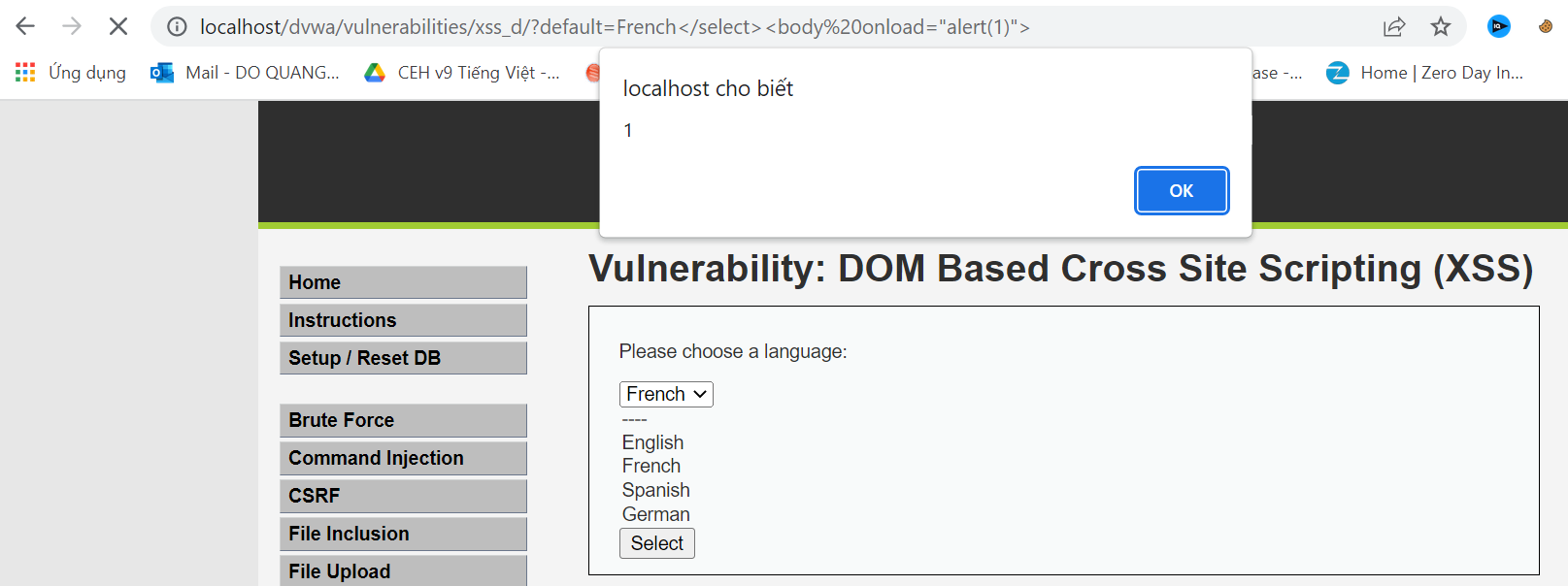
:> đùa tí ở đây tóm tắt cho việc bị xss sẽ như thế nào ấy

* Medium :
* XSS Dom: xem nó lọc gì này :> nó bỏ đoạn <script

Vậy thì ta sẽ dùng payload khác nha không đụng đến cái đoạn script nó nhé !!

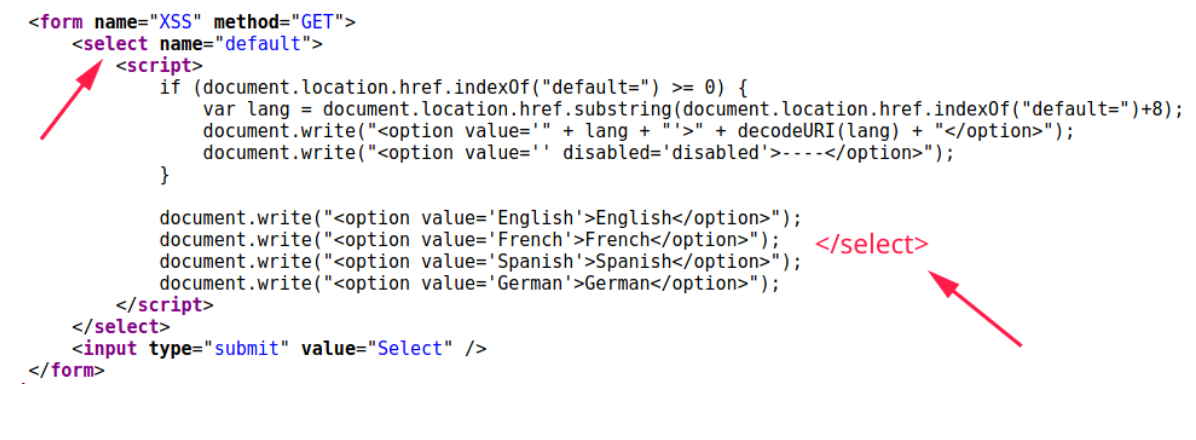
Mình sẽ dùng câu payload này .

abc<body onload="alert("Hacked by NagisaYumaa")>



Payload </ select><body onload=”alert(1)”>

Vậy tại sao lại phải có thêm thẻ select kìa :> thì nhìn nè



=>> mình sẽ đóng cái thẻ đó trước và mở thẻ khác :> đó hay ko :>

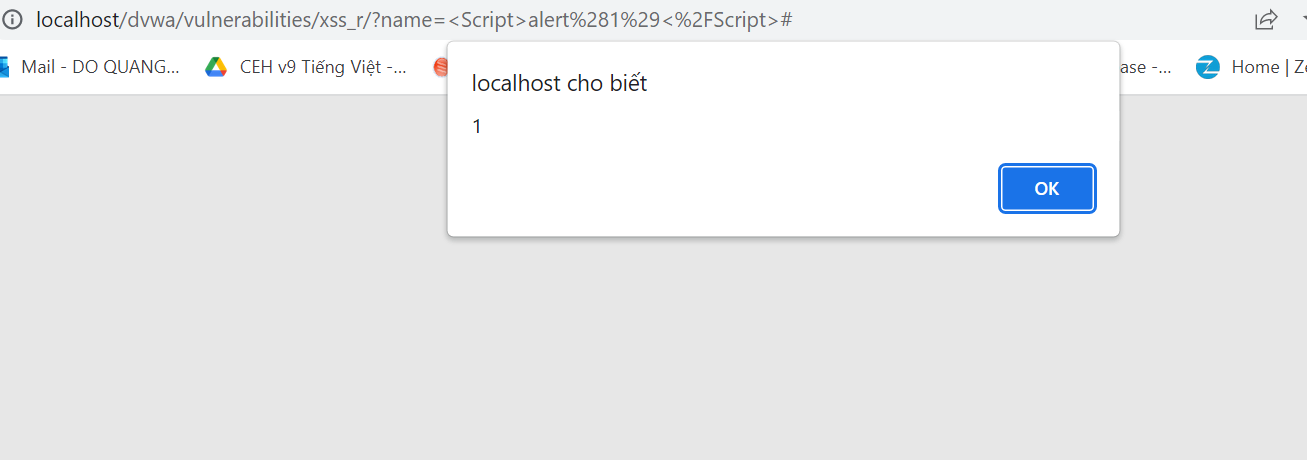
* XSS Reflected: cùng xem nó chặn cái gì nha



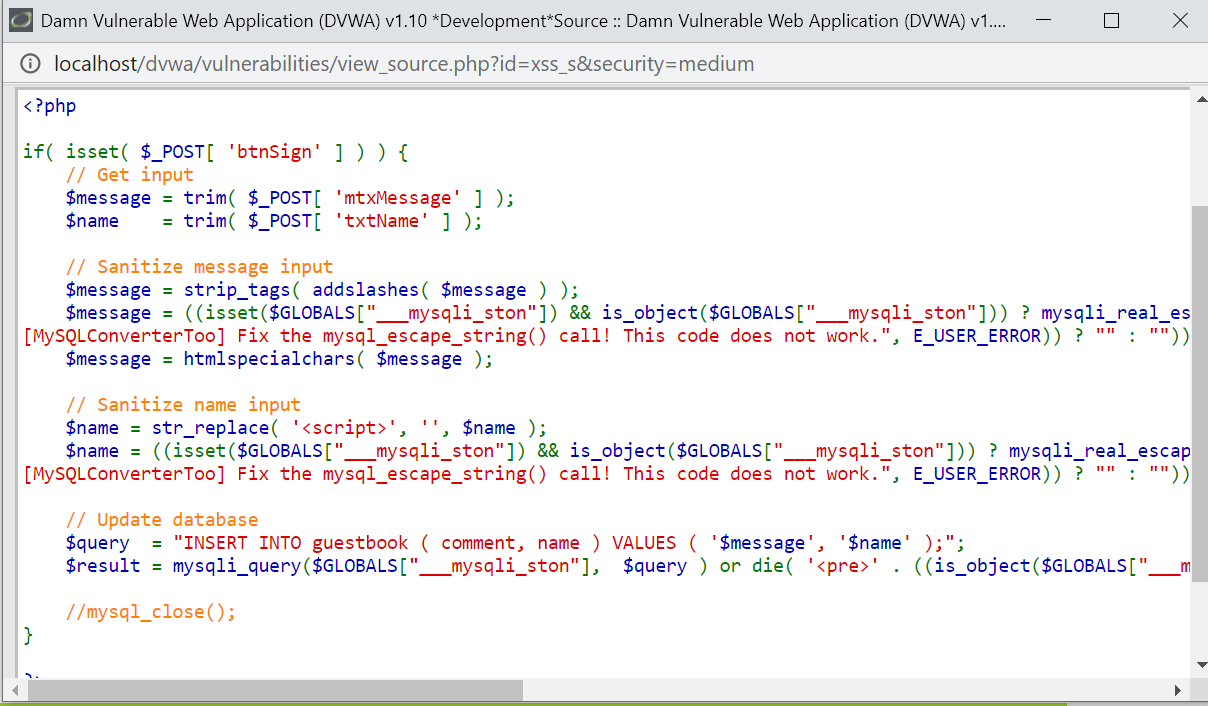
Nó lọc nguyên cái <script> vậy thì mình thử payload cái <Script> xem nó viết hoa nà : >

Xem nà :>

Payload : <Script> alert(1)</Script>



* XSS Stored:



Như đã thấy ở trên á ở cái đoạn message :> có cái strip\_tags nó sẽ loại mấy cái thẻ liên quan đến câu lệnh á

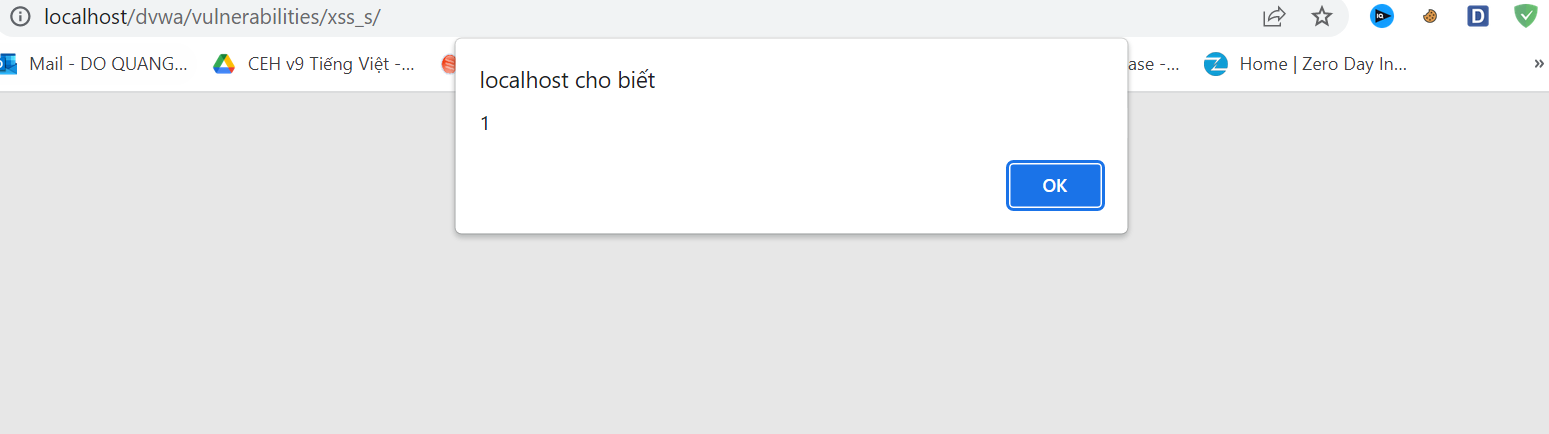
Còn cái $ name thì nó chỉ là str\_replace thôi nên ta sẽ tập chung vào nó

Nhưng sẽ xảy ra vấn đề nữa là tên nó chỉ max là 10 kí tự thôi giờ thì phải làm gì :>

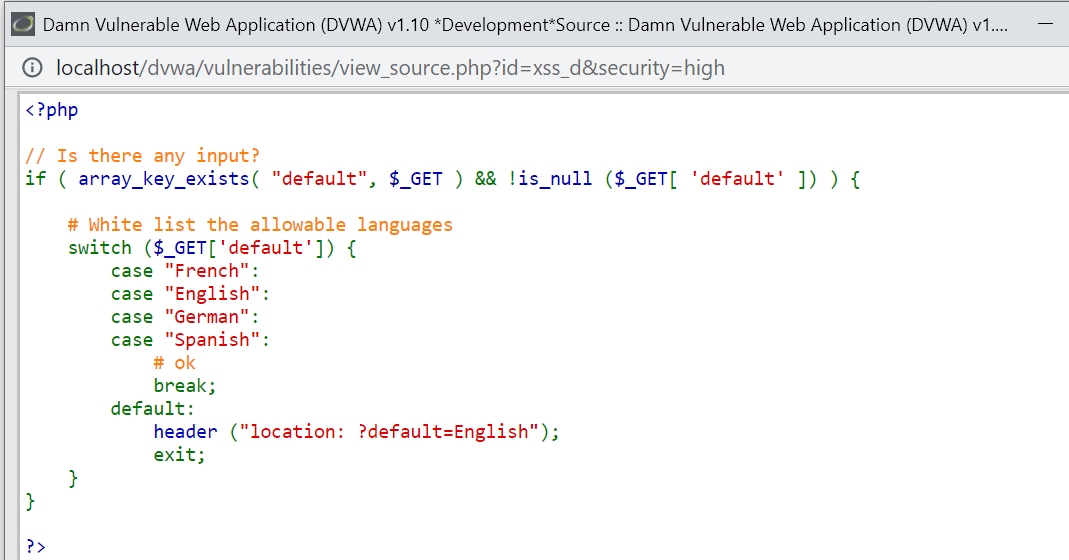
Đúng rồi á Hắc nasa = F12 thôi :> đôi khi meme cũng hay mà đúng không nào



Tang cái mũi tên lên 30 :> rồi chèn câu payload giống phần reflected thử xem như nào nhé :



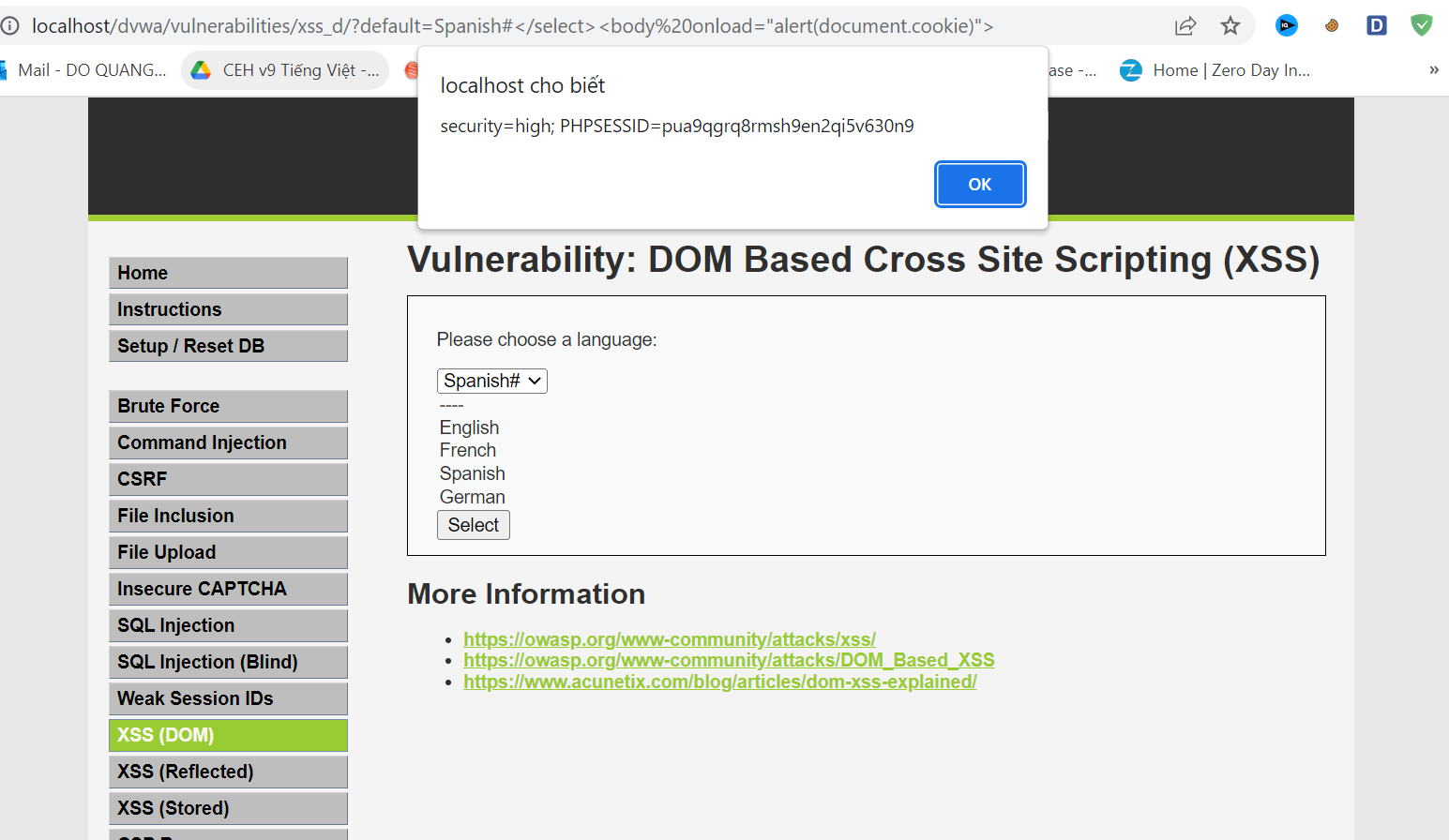
:> kia sẽ là kết quả đó :>

* High:
* XSS Dom:

ở đây á nếu đoạn nhập vào mà không phải là 1 trong 4 lựa chọn thì nó sẽ break về default :> nhưng nếu ta chọn nó và câu lệnh payload thì sao nhỉ ?

cùng xem nhé

English#</select><body onload=”alert(document.cookie)”>



* Thực ra chọn # hay & đều được nhá
* XSS Reflected và Stored: vì cả 2 cùng 1 loại block nên mình sẽ làm 1 cái kia thôi nhé !!

Nó chặn từng chữ 1 trong từ script :> ko trốn được ở đoạn viết hoa nữa :> dùng câu payload khác thôi

Payload :

<body onload =”alert(document.cookie)”>

