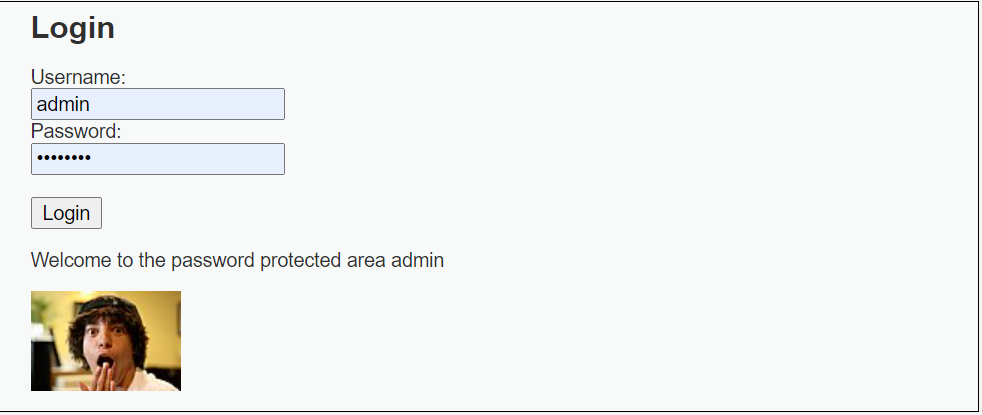
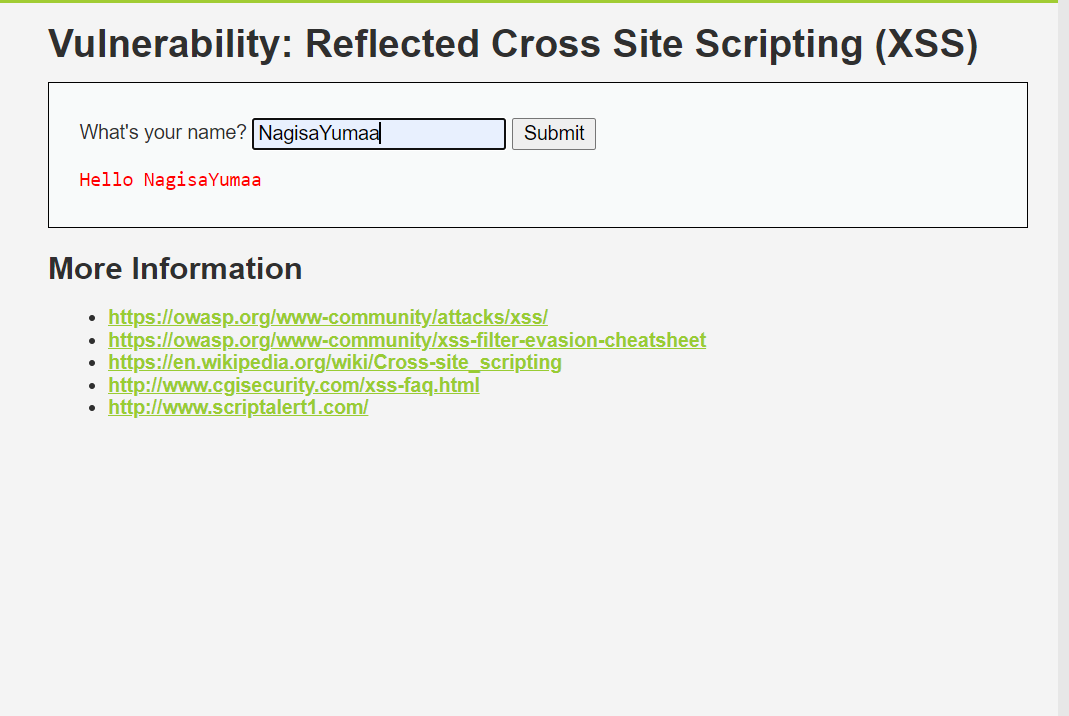
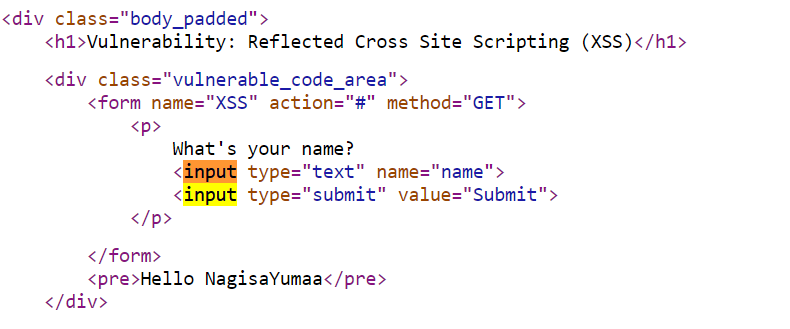
Báo cáo DVWA

Mức Low : không có bảo mật

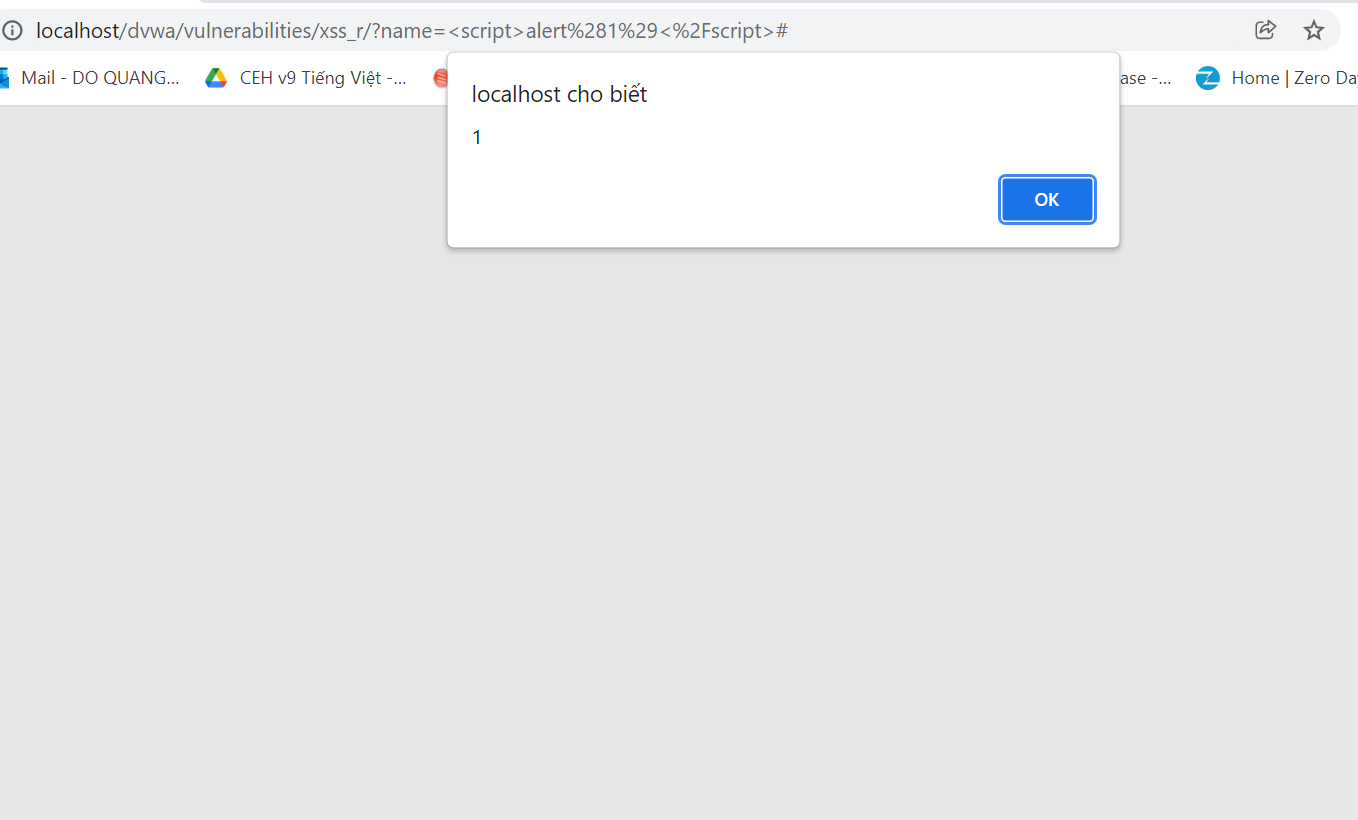
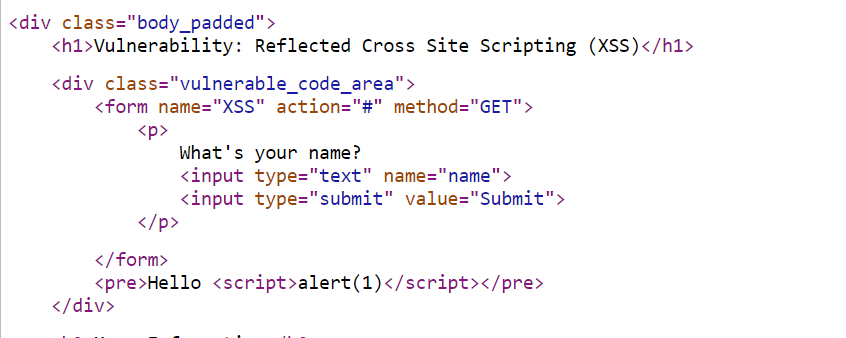
* **Brute force** :
* Password đơn giản :> dễ mò và tất nhiên là password defaut : Password.
* **XSS Refected :**



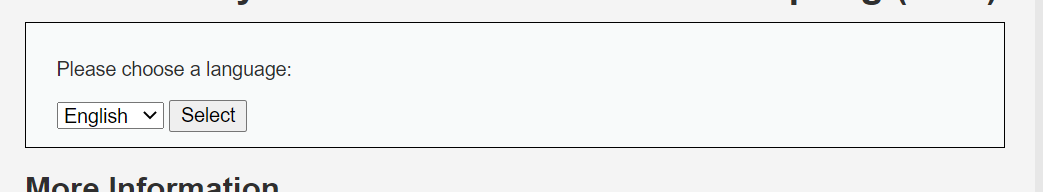
Đây là đoạn mã nguồn này :

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

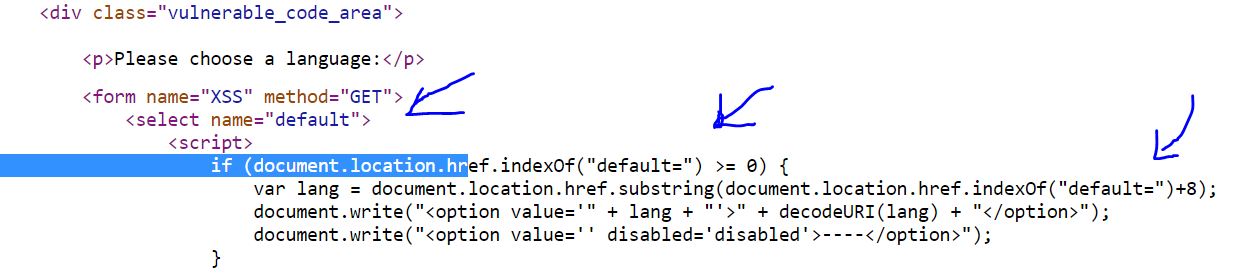
**nagisayumaa <script>alert(1)</script> ?**

* **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

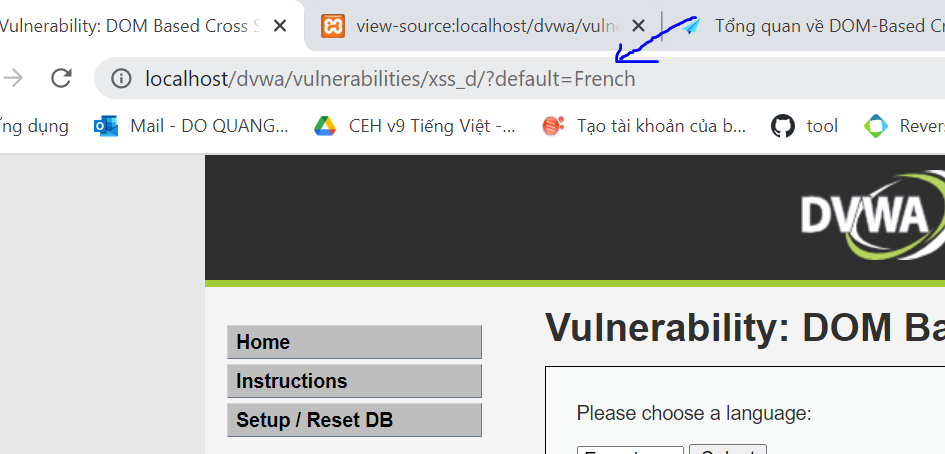
Nhìn thấy nó chỉ là một form bình thường thui đúng khum . Zậy nhìn đoạn mã của nó xem như nào nhé :>



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 :>

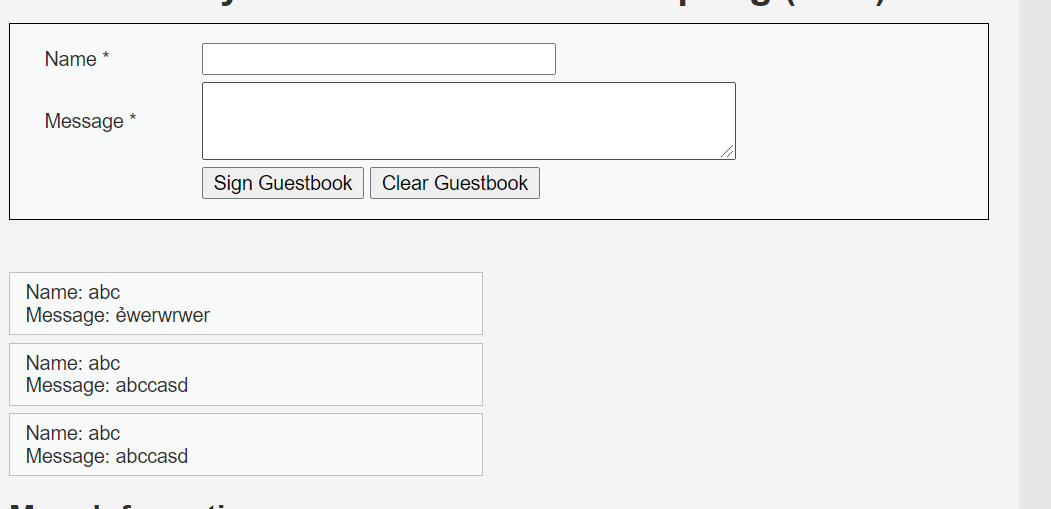
Nhưng nó là form mà thì làm thế nào để thay thì nhìn lè :>



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

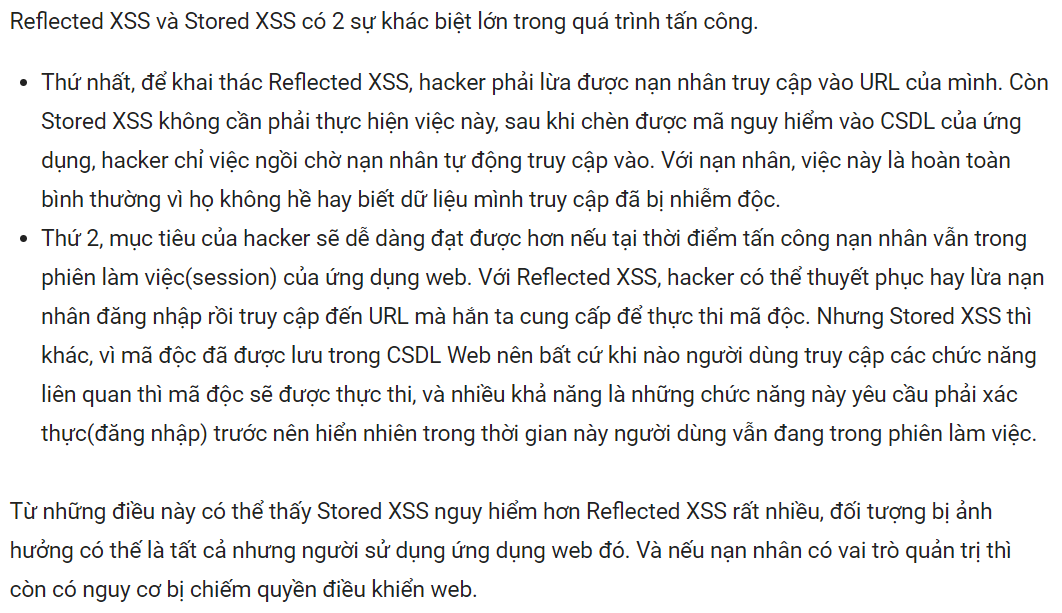
* **XSS Store**

:> tính chất của cái nè thì giống cái trên



Nên up luôn mã nguồn nhớ tương tự lun



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

* **CSRF :** tấn công giả mạo :>

Đa phần nó sẽ chủ yếu hiểu ở việc dùng session cookies để đăng nhập thay thế việc đăng nhập của người dùng . Đến giờ tui vẫn chưa hiểu ý của bài DVWA là gì .

-