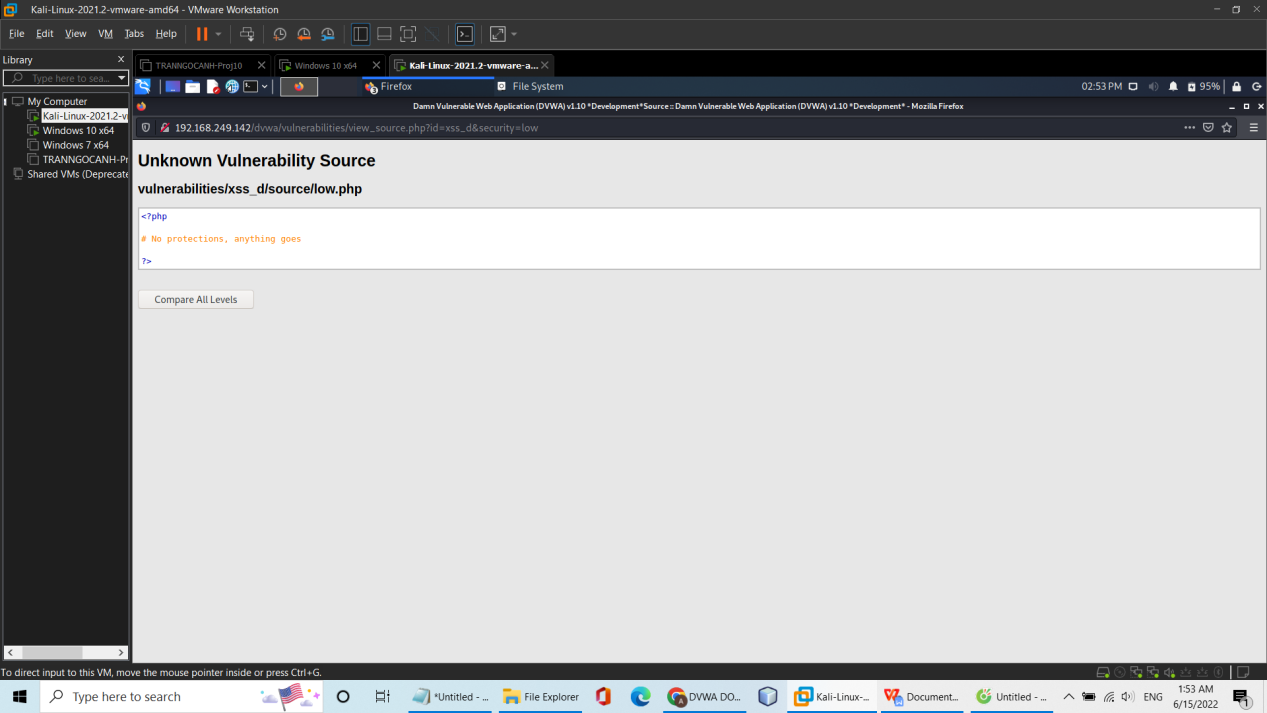
|  |  |
| --- | --- |
| Class | IAW301 |
| Name | Trần Ngọc Anh |
| IC No. | HE151461 |
| Date & Time | 15/6/2022 |

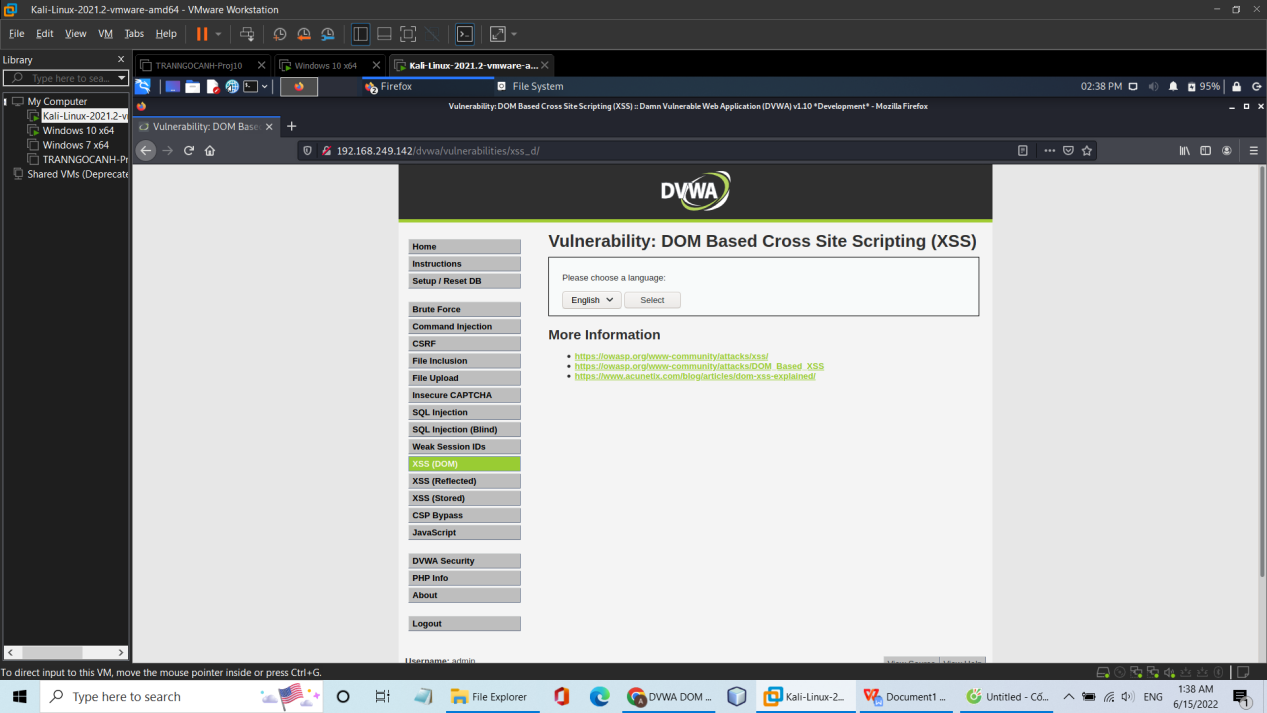
**LAB 17**

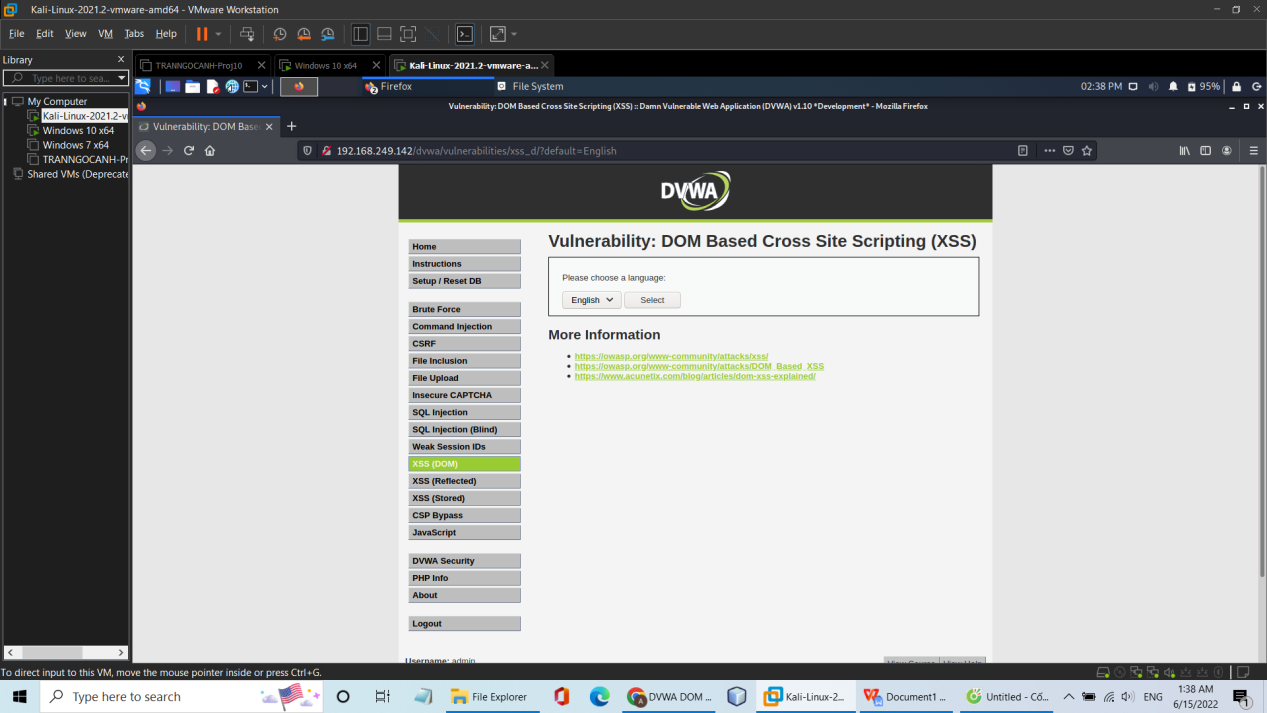
# DOM Based Cross Site Scripting

1. **Low**

- Ở đây chúng ta nhìn thấy không có bất cứ bảo vệ nào ở client-side cũng như server-side.

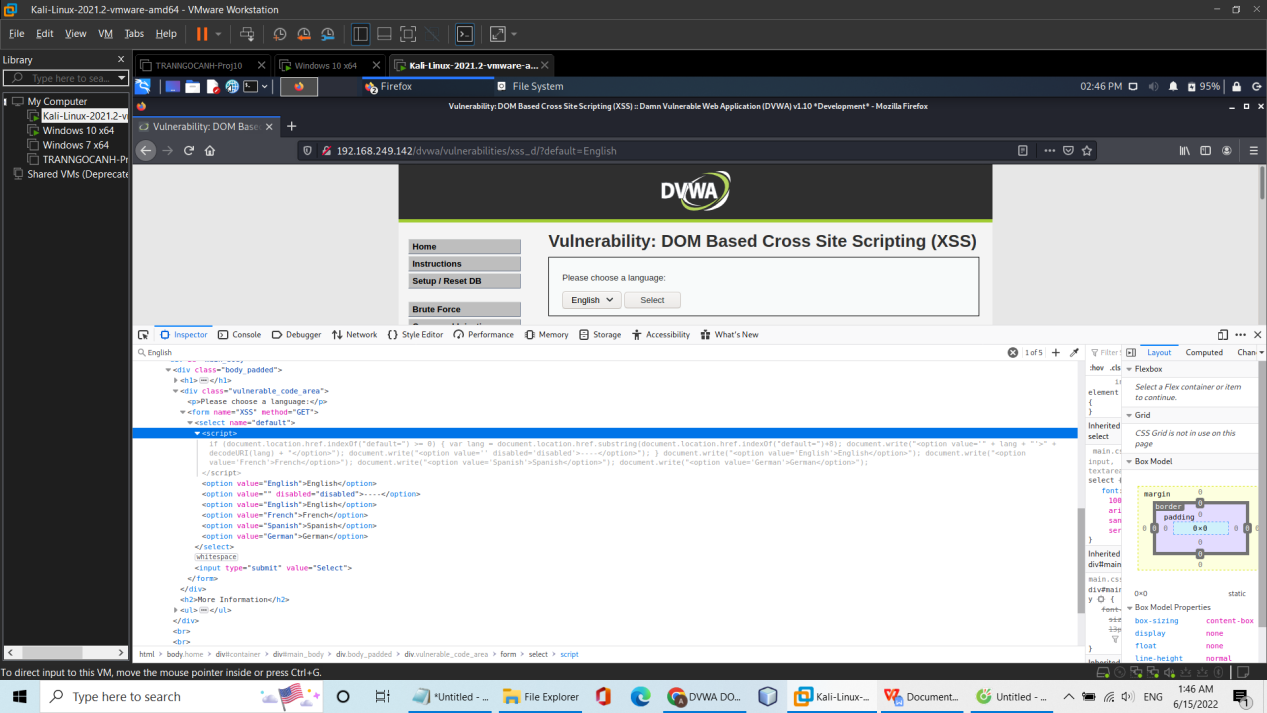




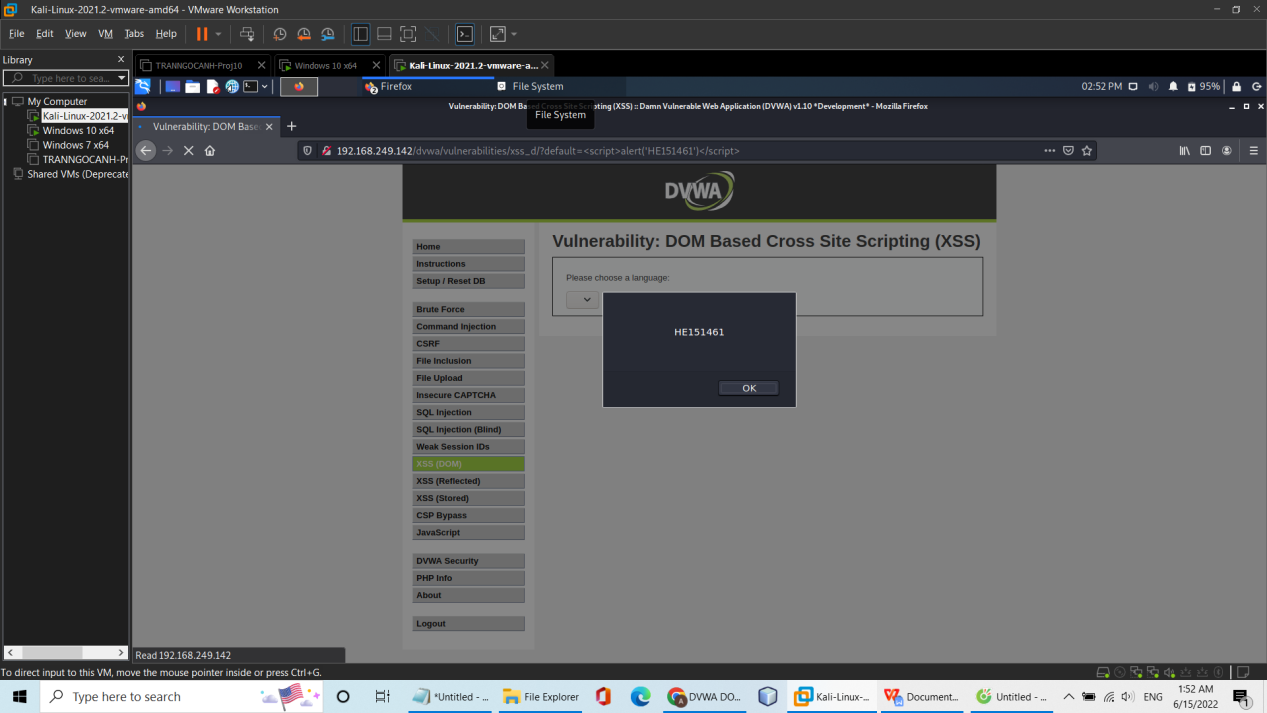


- Hàm document.location.href.substring() dùng để chấp nhận input từ người dùng vào tham số default.

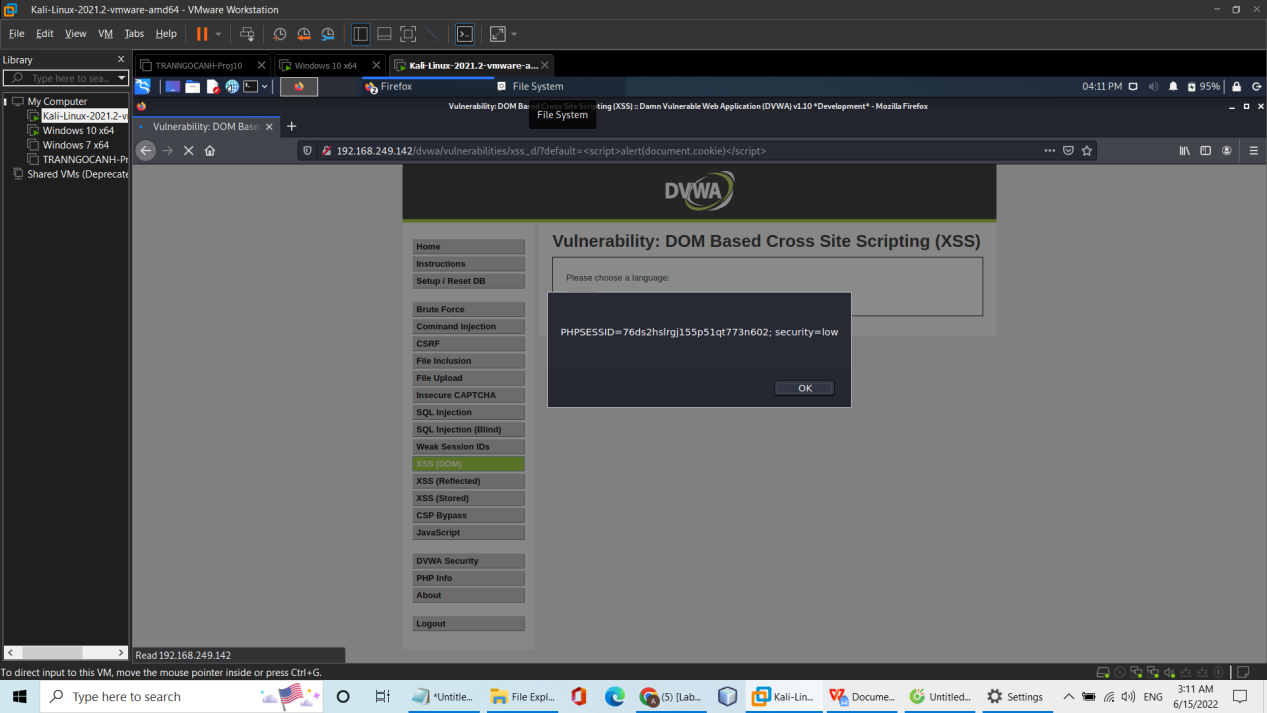
- Hàm document.write() dùng để phản ánh giá trị đã nhập từ nguồn bên trong thẻ <option> … </option>. Điều đó có nghĩa là khi chúng ta nhập bất cứ cái gì vào tham số default sẽ phản ánh lại ở thẻ <option>…</option> bên trong HTML DOM.



- Ta thử bằng script <script>alert('HE151461')</script> để hiển thị ra mã số sinh viên để chứng minh có lỗi DOM-XSS.

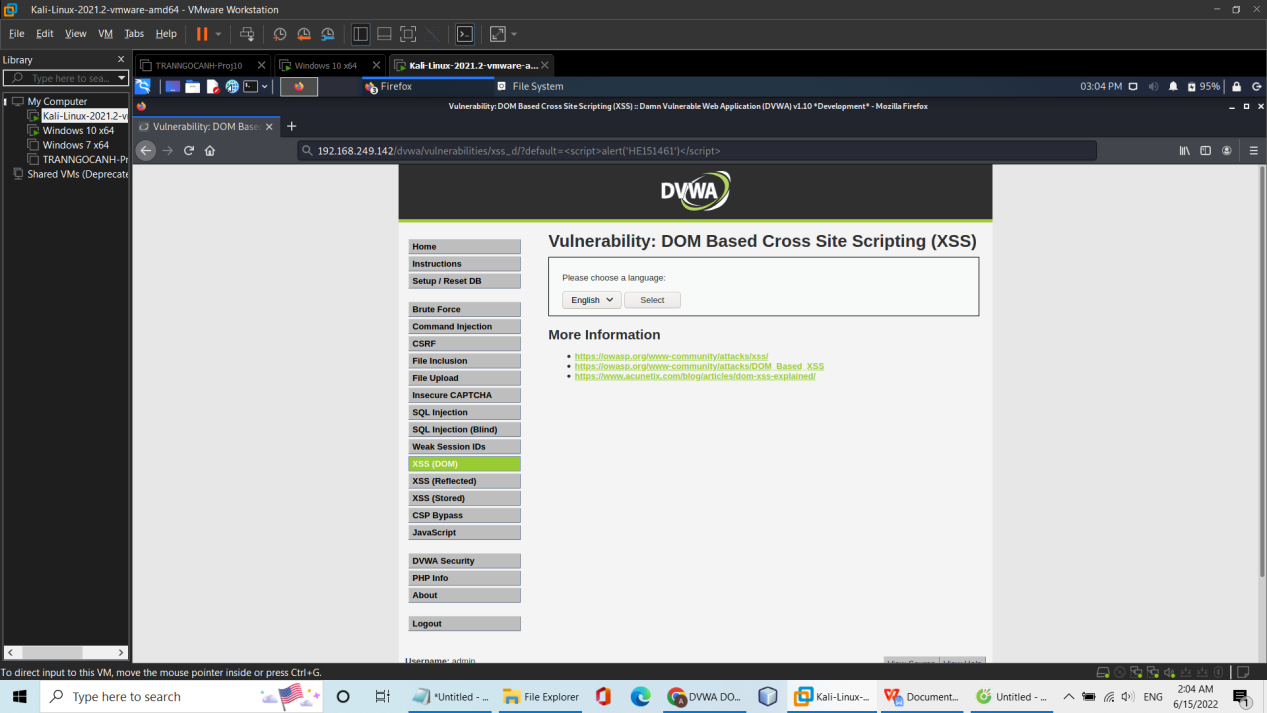


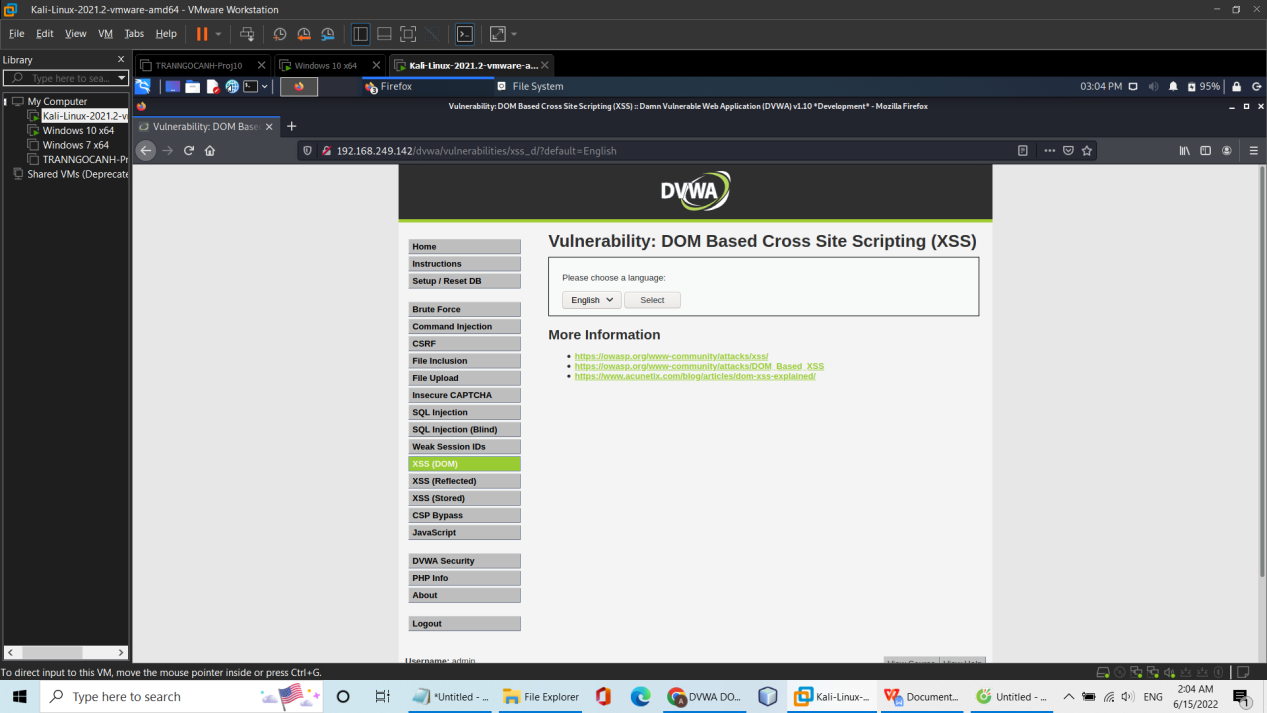
- Sau khi chứng minh được có lỗi chỉ cần lấy được cookie <script>alert(document.cookie)</script> là sẽ hoàn thành mức low.



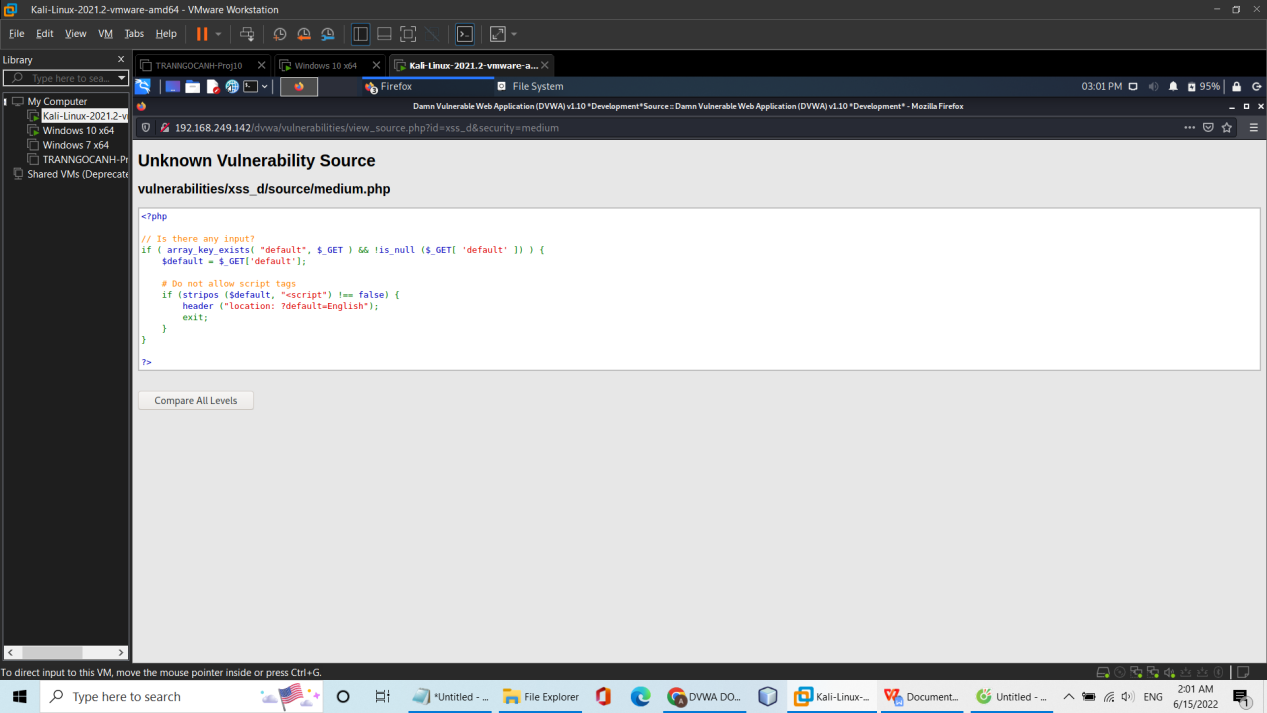
1. **Medium**

- Ở mức medium chúng ta thử như mức low thì không hiển thị được lỗi và trang web đã chuyển hướng về default=English.

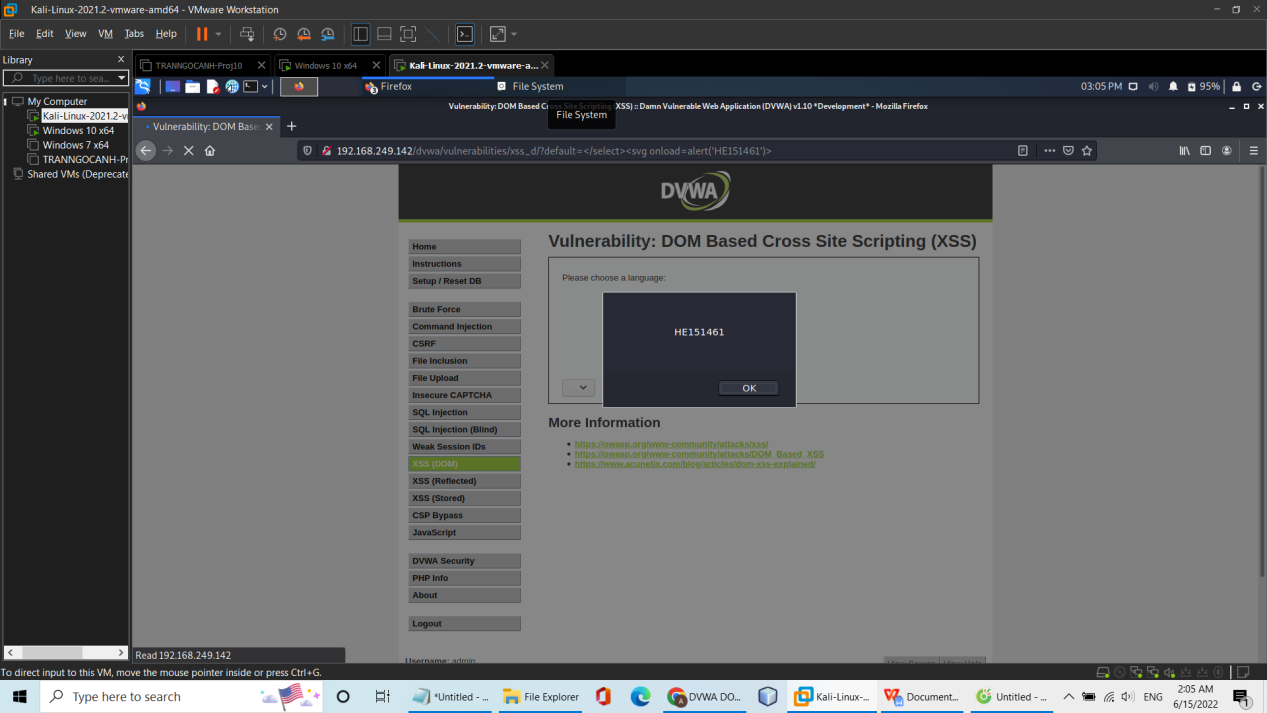


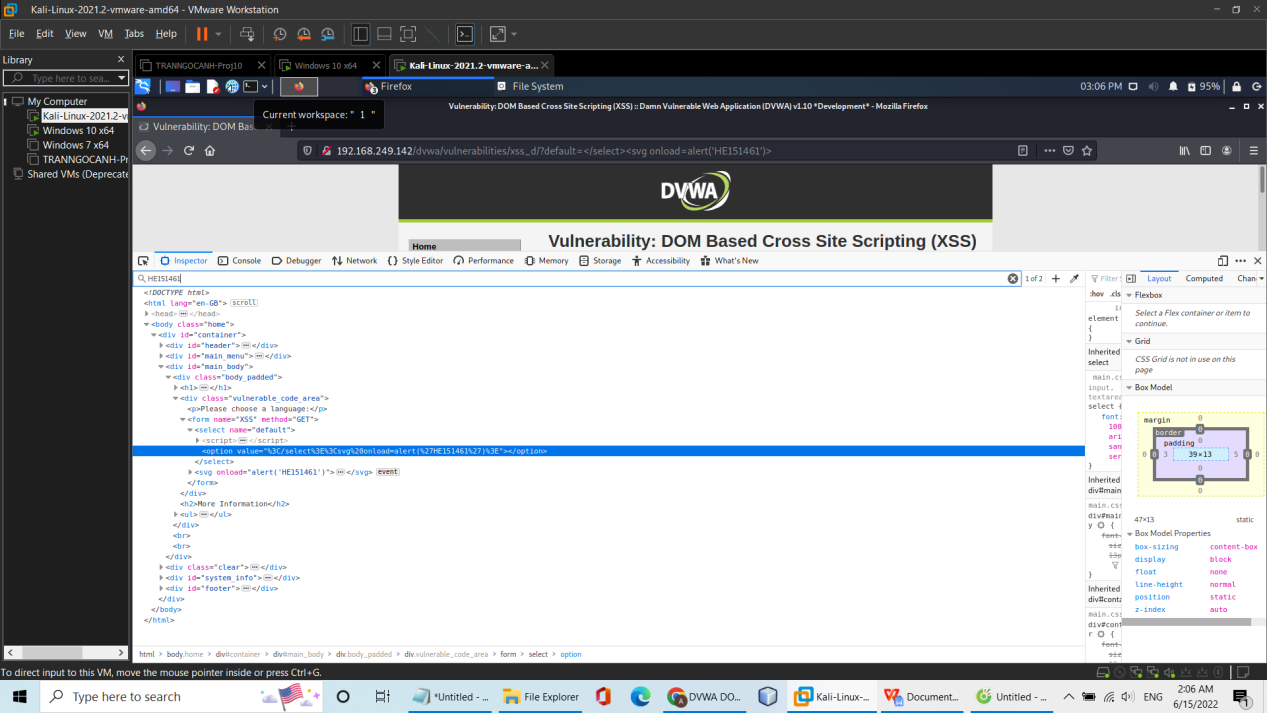


- Chúng ta xem qua source code xem có gì đặc biệt không thì thấy có hàm stripos () dùng để tìm vị trí xuất hiện đầu tiên của một chuỗi bên trong một chuỗi khác. Ở đây thì là tìm xem có “<script” ở trong chuỗi input của trường default không , nếu có thì sẽ chuyển hướng trang web về trang mặc định default=English.

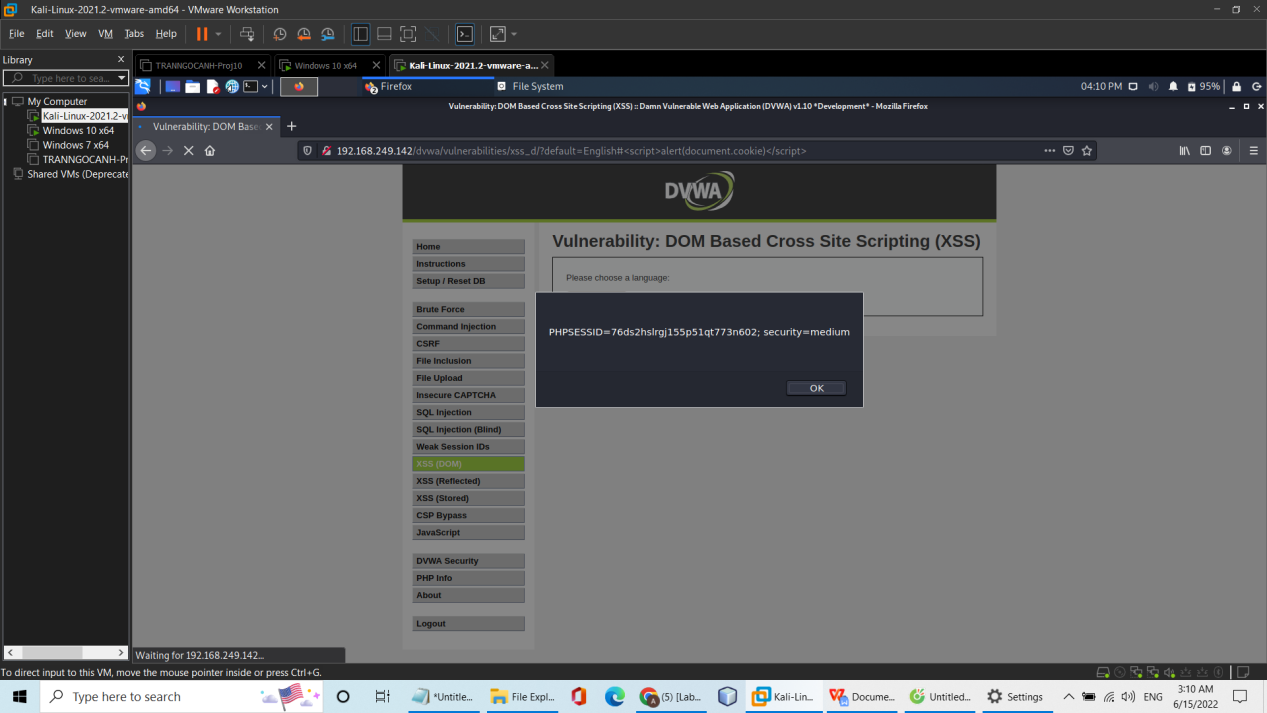


- Vì vậy ta thử payload </select><svg onload=alert('HE151461')> để chứng minh được là có lỗi DOM XSS và hiển thị được mã số sinh viên.



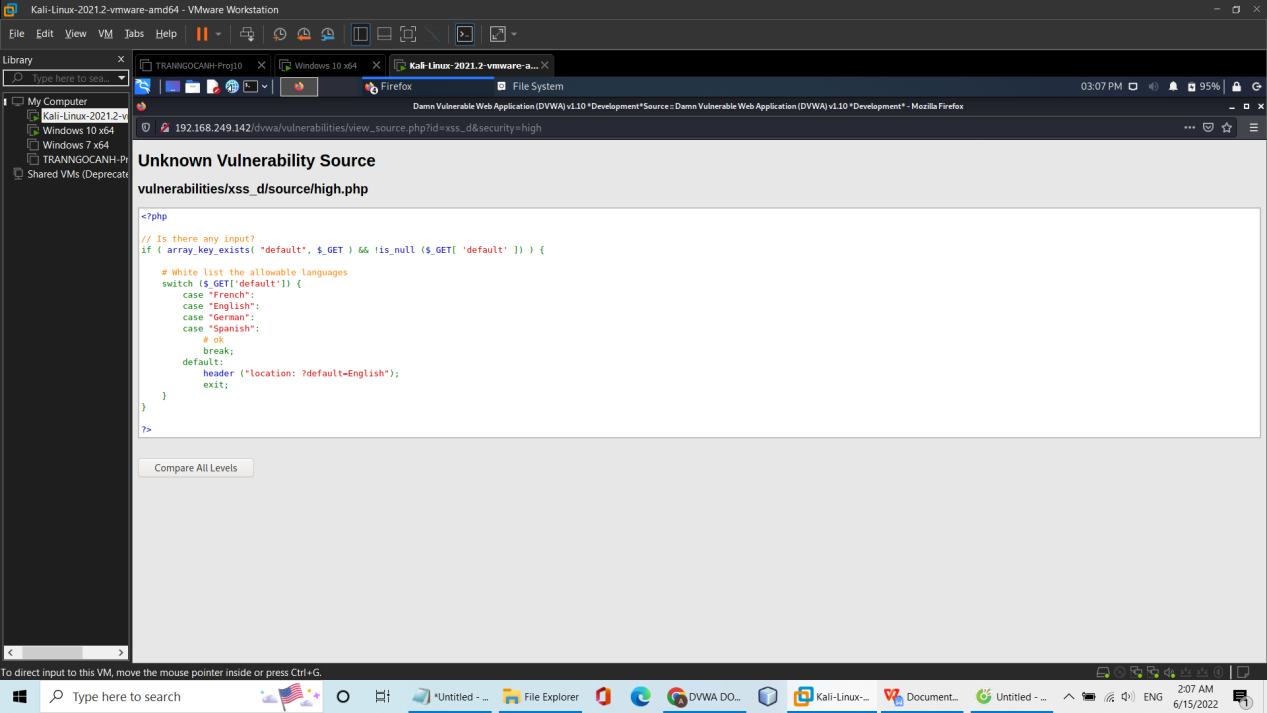


- Chúng ta tiến hành lấy cookie #<script>alert(document.cookie)</script> hoàn thành mức medium.



1. **High**

- Ở mức high thì người ta có tạo ra một danh sách whilelist để tránh bị nhập đầu vào không mong muốn.



- Ta có thể dùng payload &</select><svg onload=alert('HE151461')> để khai thác thành công sau đó dùng #<script>alert(document.cookie)</script> để lấy được cookie hoàn thành mức high.

