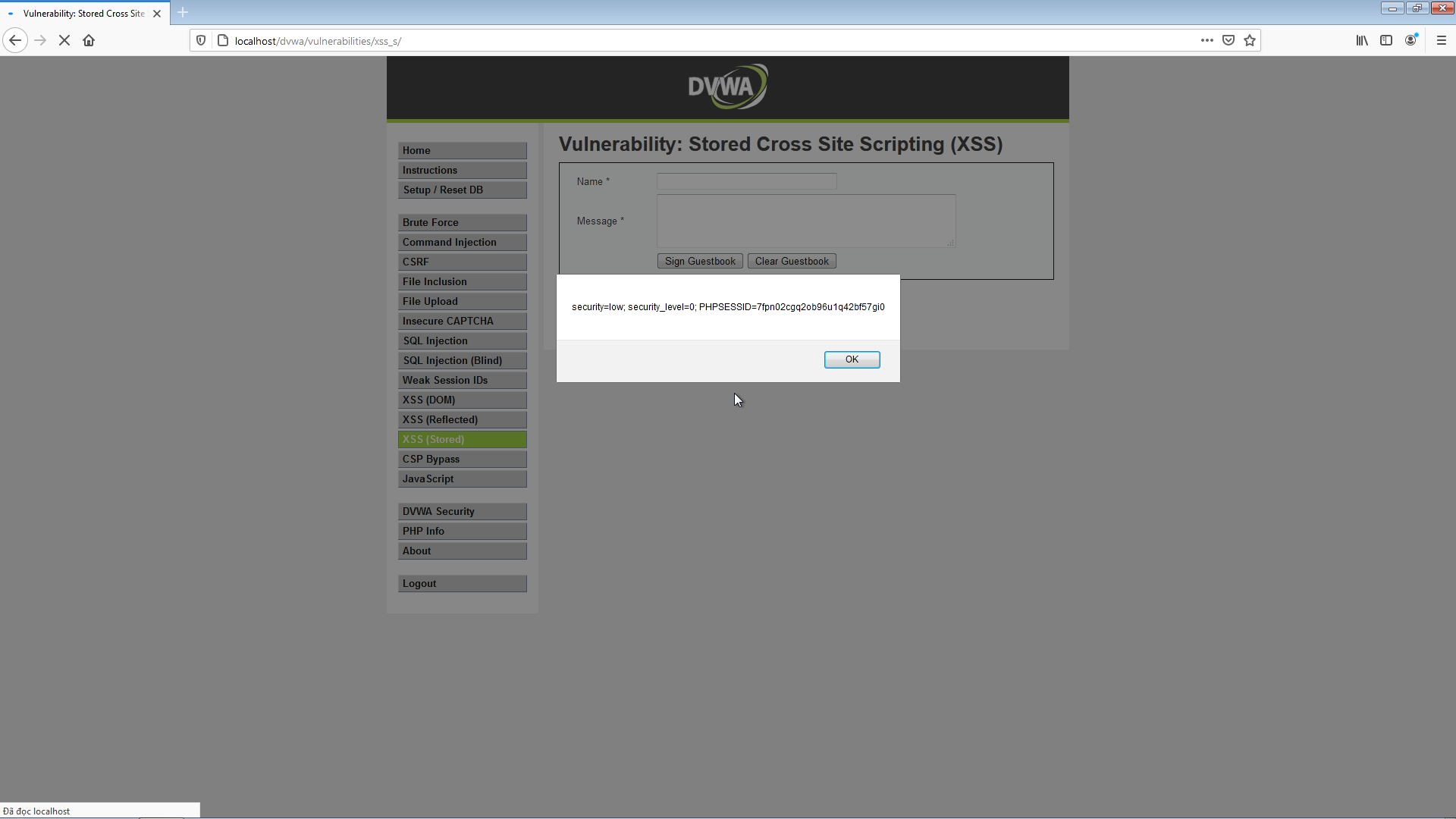
|  |  |
| --- | --- |
| Class & Module | IAW301  Lab 16: Stored Cross Site Scripting |
| Name | Nguyễn Đức Kiên |
| IC No. | HE141763 |
| Date & Time | October 20, 2020 |

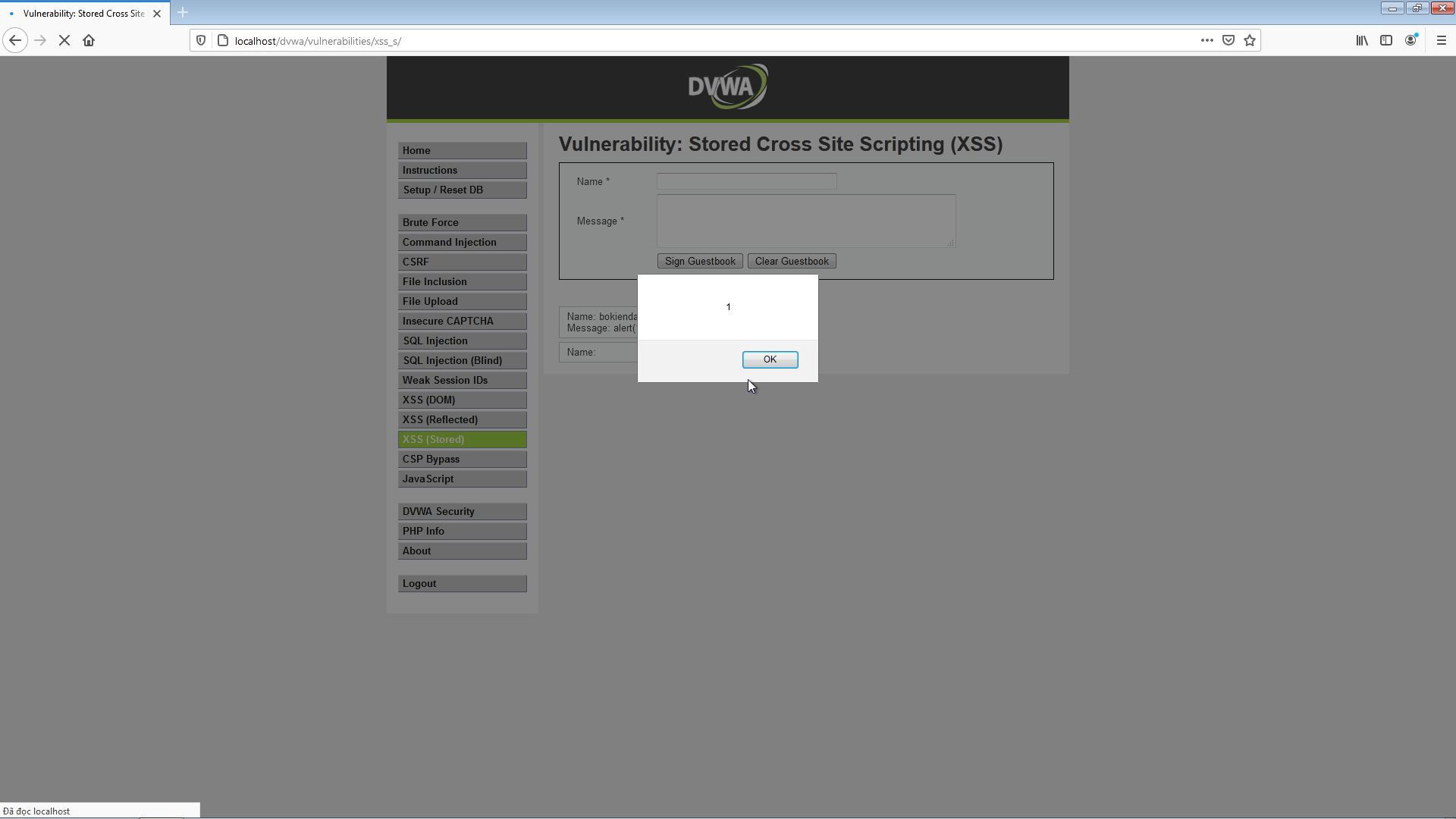
#### Exercise 1.1 Low Security

Script used: <script>alert(document.cookie)</script>

**Exercise 1.2 Medium Security**

Script used: <Script>alert(1)</script>

First we need to change the value of **maxlength** element in the name field, by right clicking the name field and choose inspect element as html, change this from 10 to 100. By checking the source code we see that the “<script>” tag is filtered, bypass this by using sensitive case(‘s’ to ‘S’) and we have the result.



**Exercise 1.3 High Security**

Script used: <img src = “#” onclick = alert(document.cookie)>

Checking the source code we see that now dvwa filter all input by adding slash and check for every single character, can no longer use ‘script’ tag, so we use the ‘img’ insert method, have the result. However we still need to change the maxlength attribute in name field to inject the script. By simply clicking on the image we have the alert, we can use “onerror” instead of “onclick” to have instant alert pop-up on the screen.

