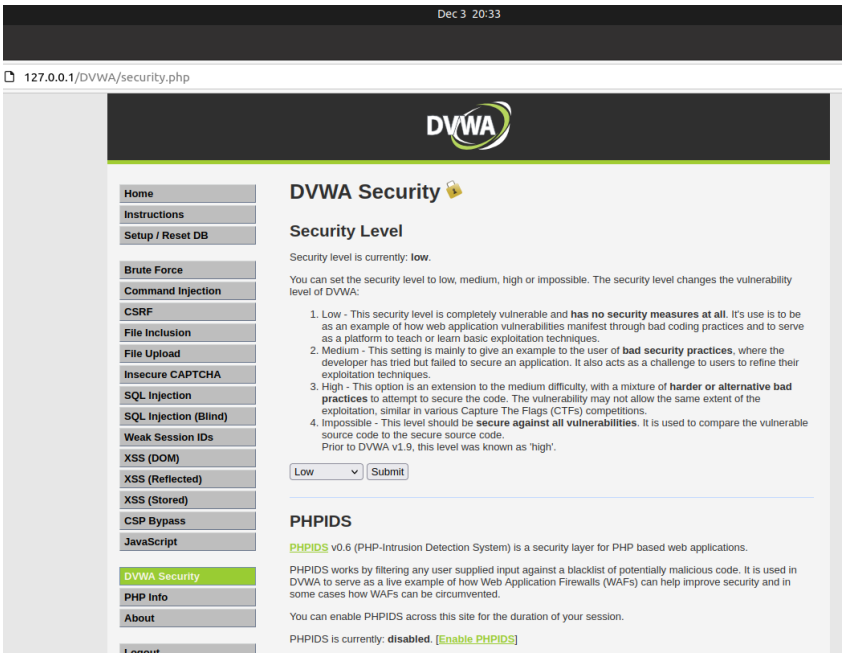
Assignment 3

Team members:

Zhicheng Zhao: 015221102

Xuewei Zheng: 012066314

Setup security level:



Question 1: Describe the SQLi attack you used, how did you cause the user table to be dumped? What was the input string you used?

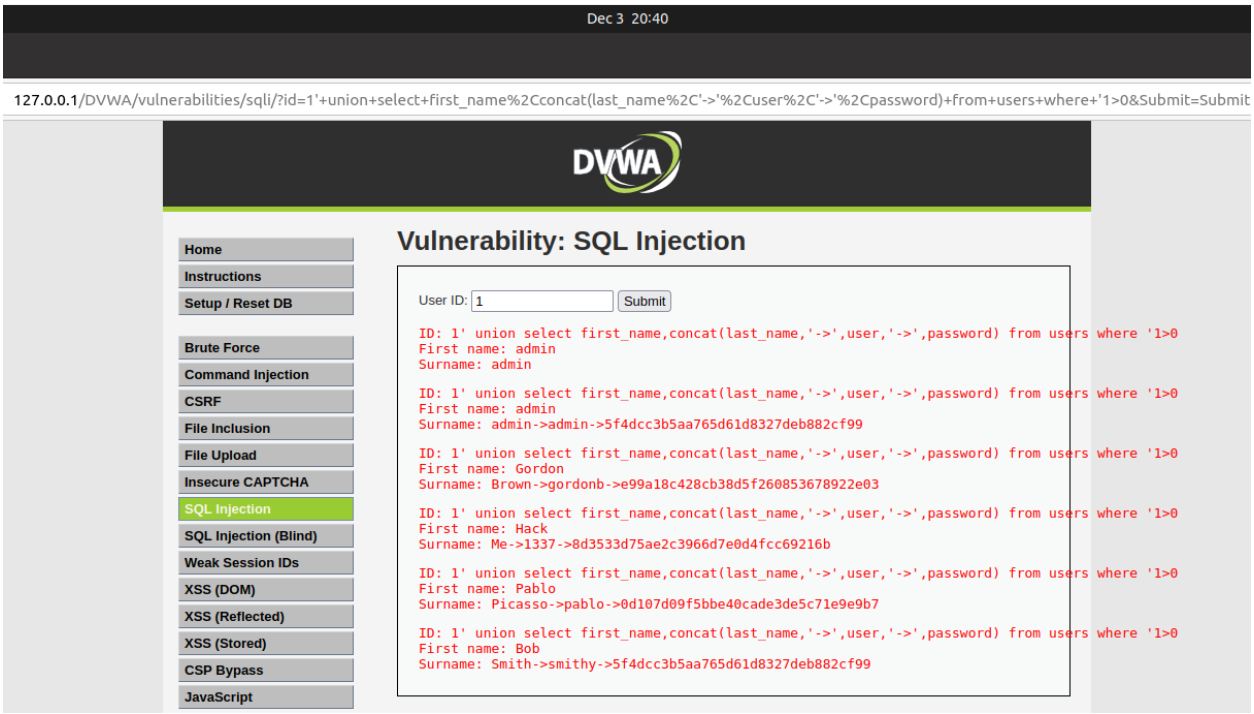
In SQL Injecton section on the left:

We can input the user ID to get the first name and last name

If we input

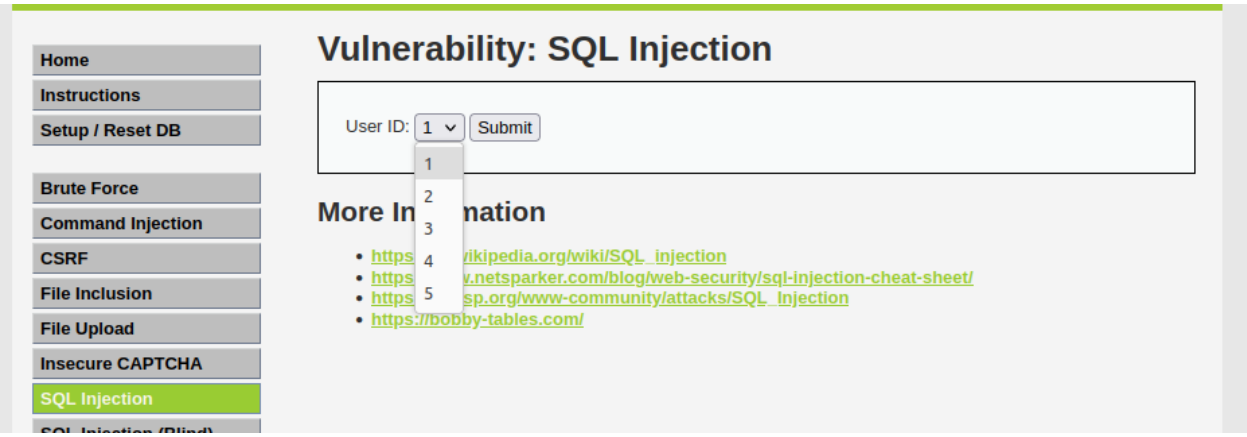
1' union select first_name,concat(last_name,'->',user,'->',password) from users where '1>0

Inside Surname, we can get lastname -> username -> password



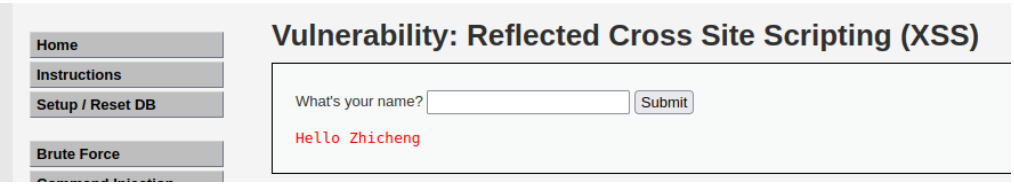
Question 2: If you switch the security level in DVWA to “Medium”, does the SQLi attack still work?

If we set security level to medium, there is a drop down instead of an input box. So, we cannot do SQLi attack.



Question 3: Describe the reflected XSS attack you used; how did it work?

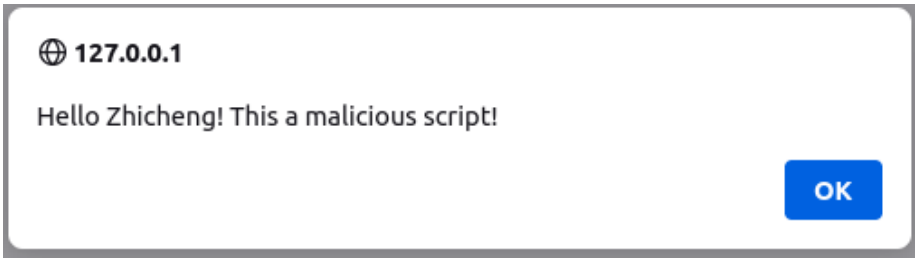
Set security level to low, select XSS (Reflected) section on the left, input the name in the text box, and submit, a hello message will show up include the name you input.



If we input the following inside text box:

<script>alert('Hello Zhicheng! This a malicious script!')</script>

We will get this alert jump out



Question 4: If you switch the security level in DVWA to “Medium”, does the XSS attack still work?

Set security to medium, input <script>alert('Hello Zhicheng! This a malicious script!')</script>

The script inside <script> </script> tag was rendered as characters and will not execute as code. The XSS attack doesn’t work.