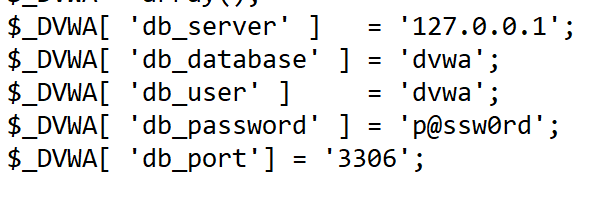
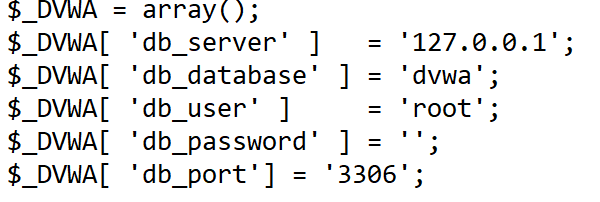
**PRACTICAL No. 6**

**AIM:** Simulate persistent cross-site Scripting Attack.

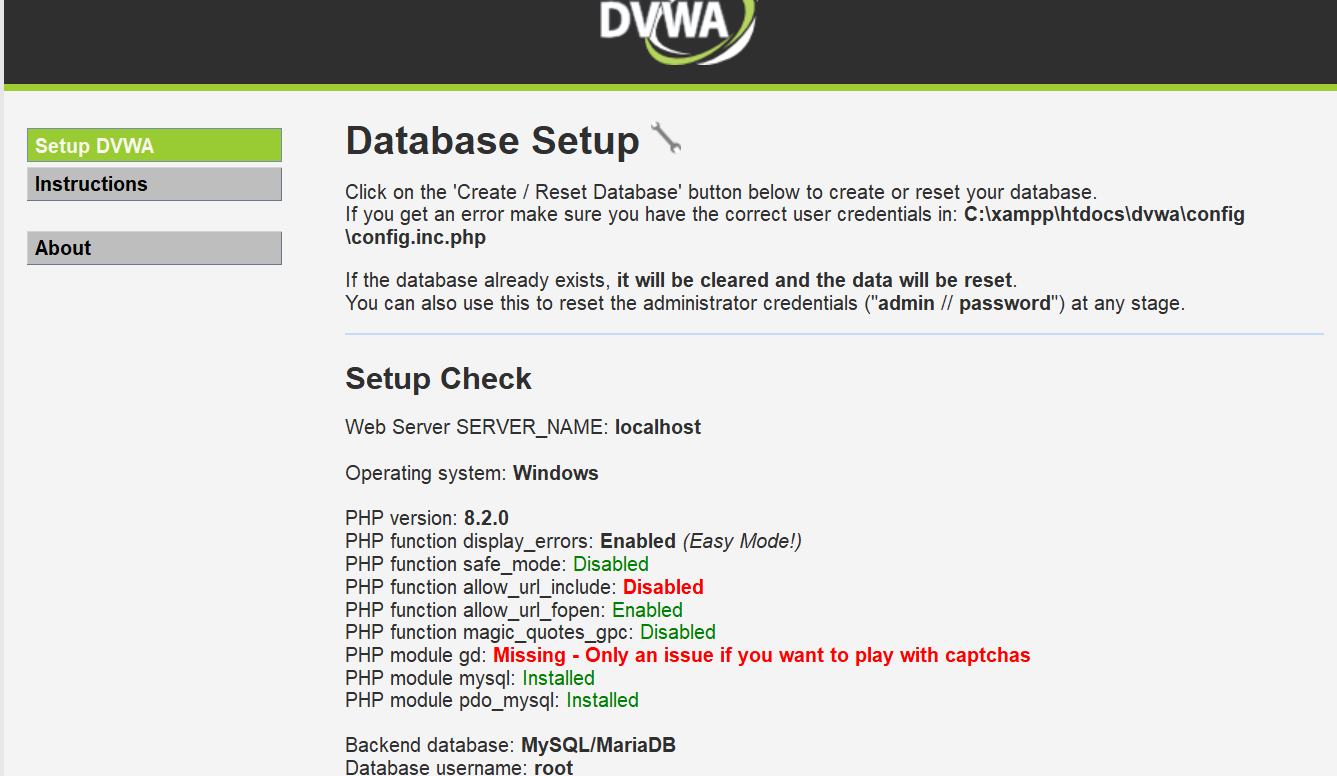
1. Download XAMPP.
2. Turn on Apache and MySQL.
3. Extract DVWA-master zip folder on desktop. Rename that folder & save as dvwa. Copy this newly created folder into C:\xampp\htdocs folder.
4. Go to dvwa copied folder. Go to config. Copy the config.inc.php.dist file. Paste that file in same folder. Rename the copied folder as config.inc.php. Automatically it is saved as php file.
5. Open the php file on notepad.



1. Rename db\_user as “root” and remove the db\_password.



1. Turn On Your XAMPP server and go to http://localhost:8080/dvwa/setup.php

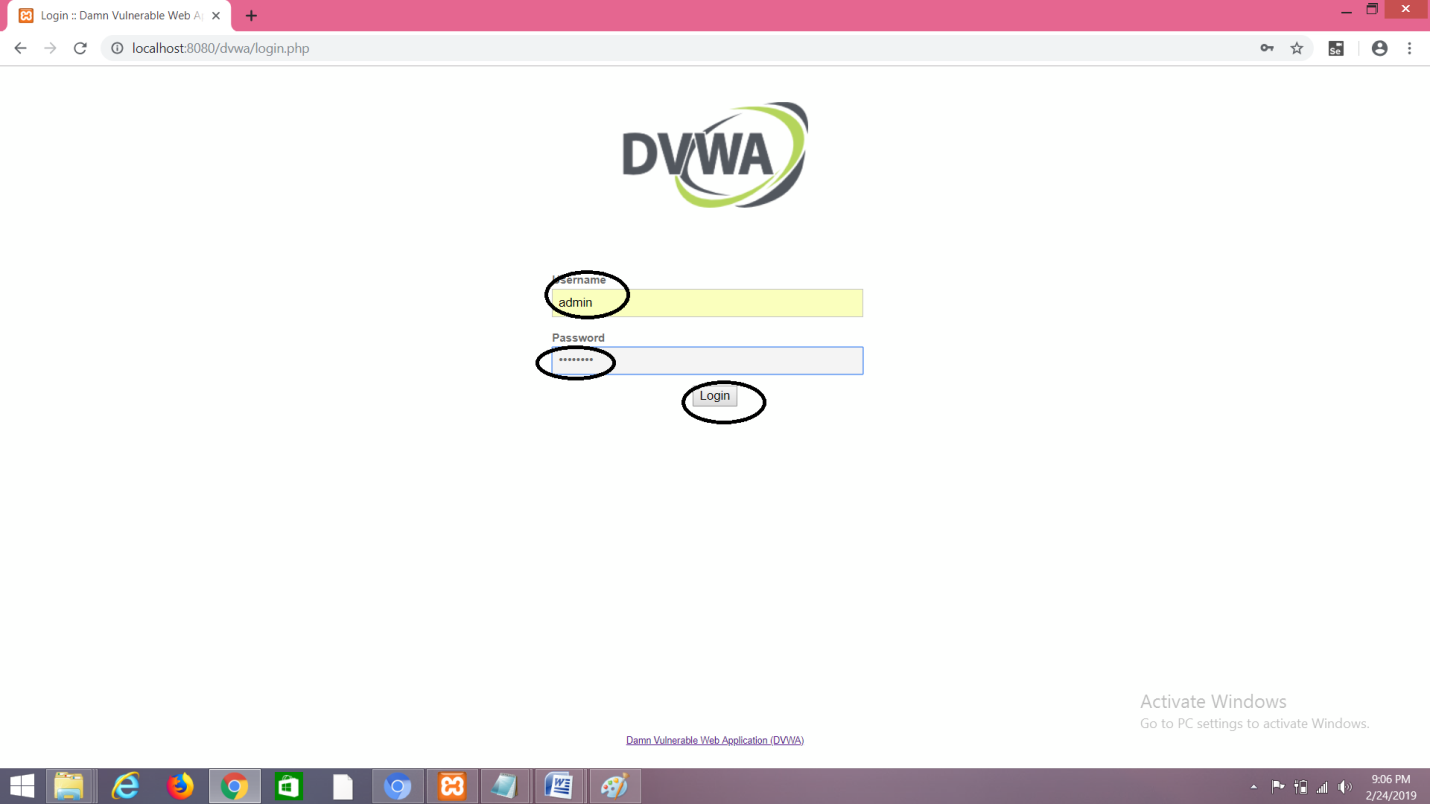




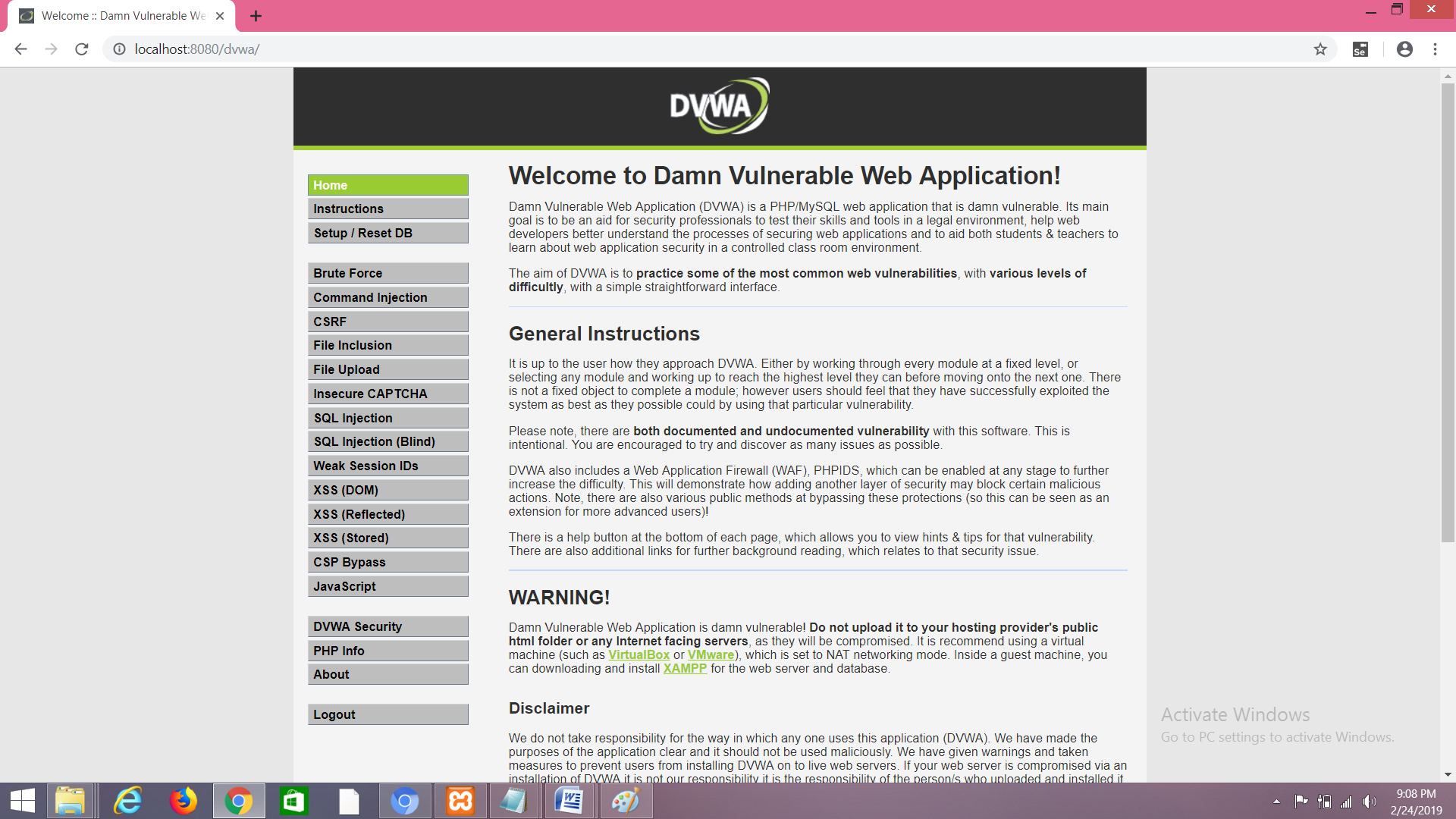
Click on Create/Reset Database.

1. Now automatically you are redirected to login page.

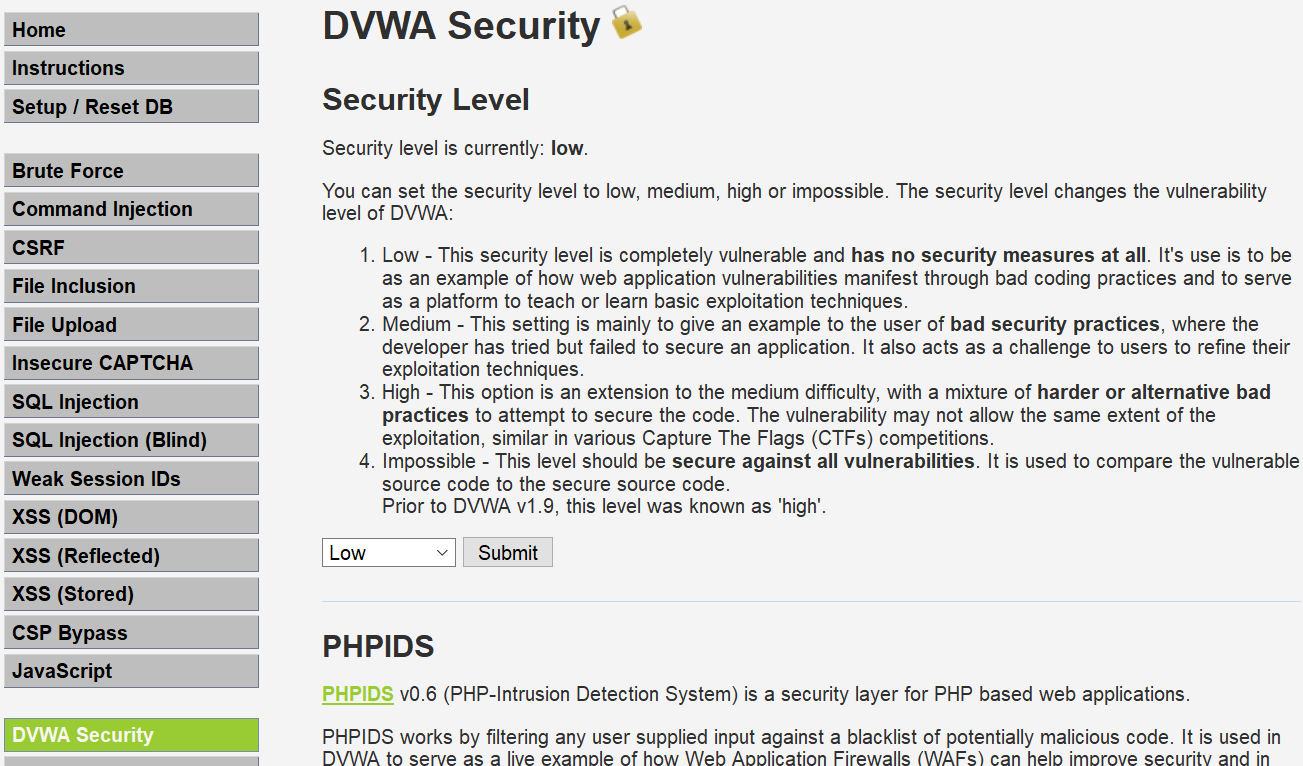
Enter username: admin and password: password



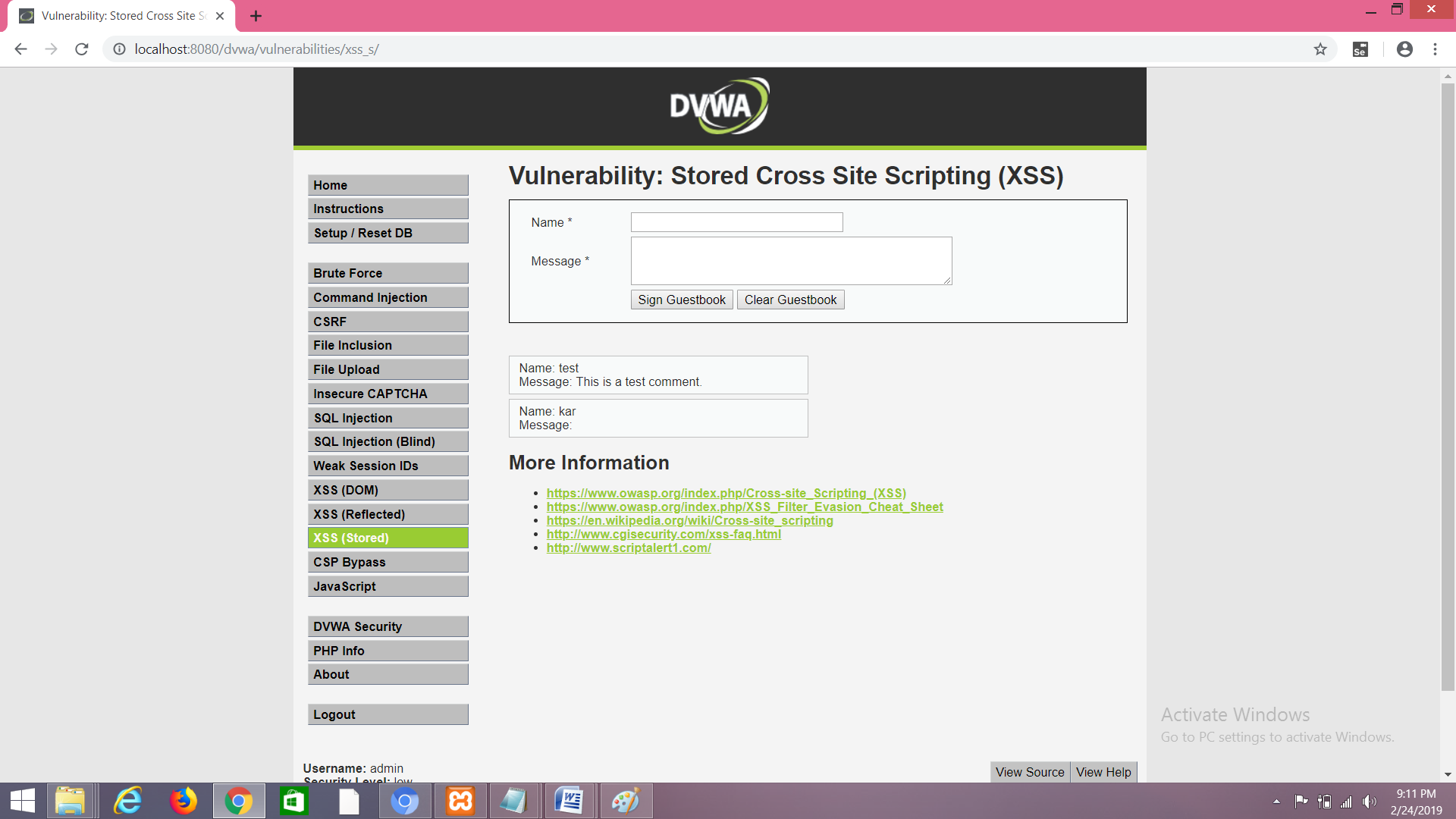
1. After successfully logging in you will be redirected to the homepage.

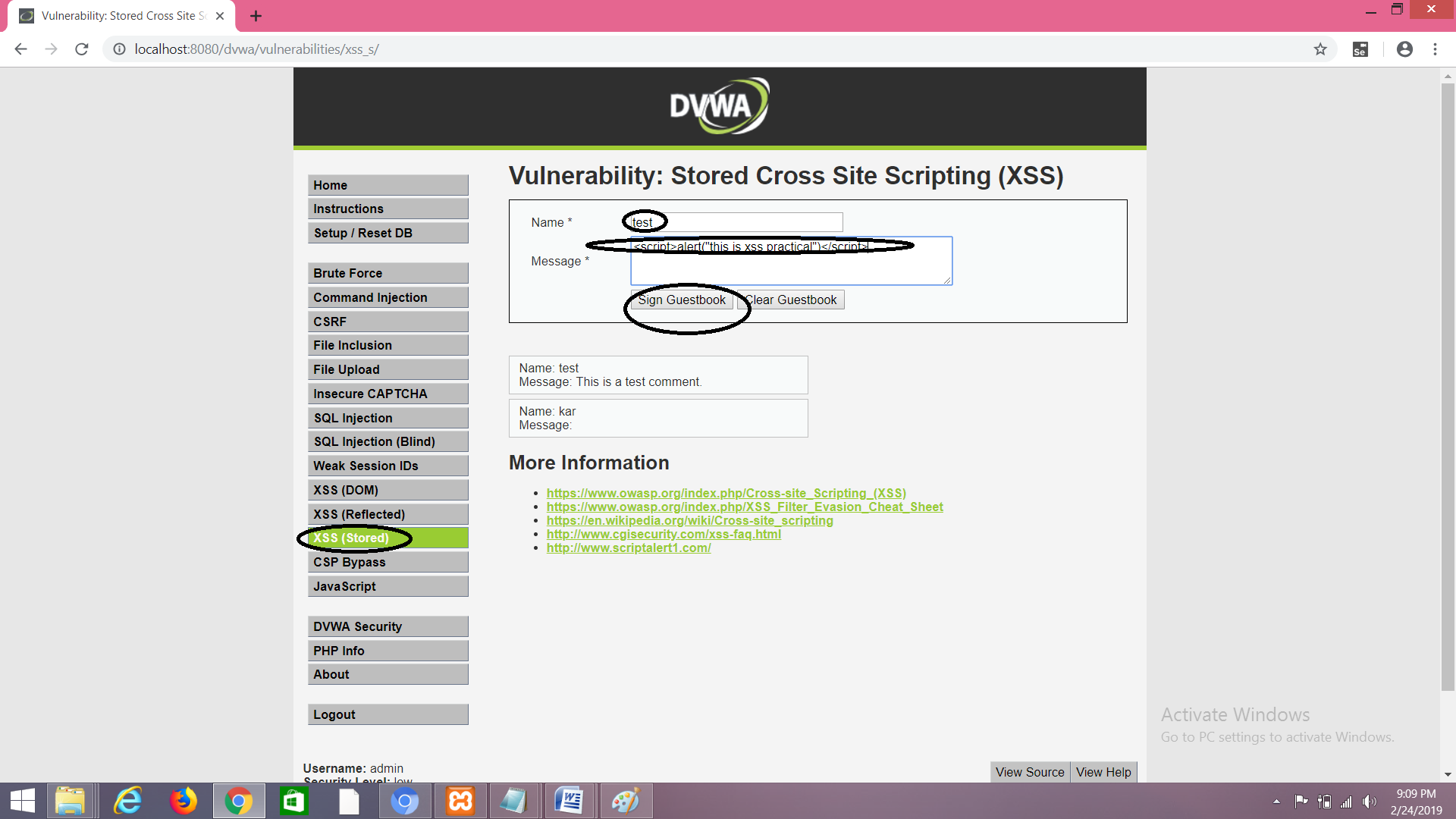


Go to DVWA security and set it as “low”.

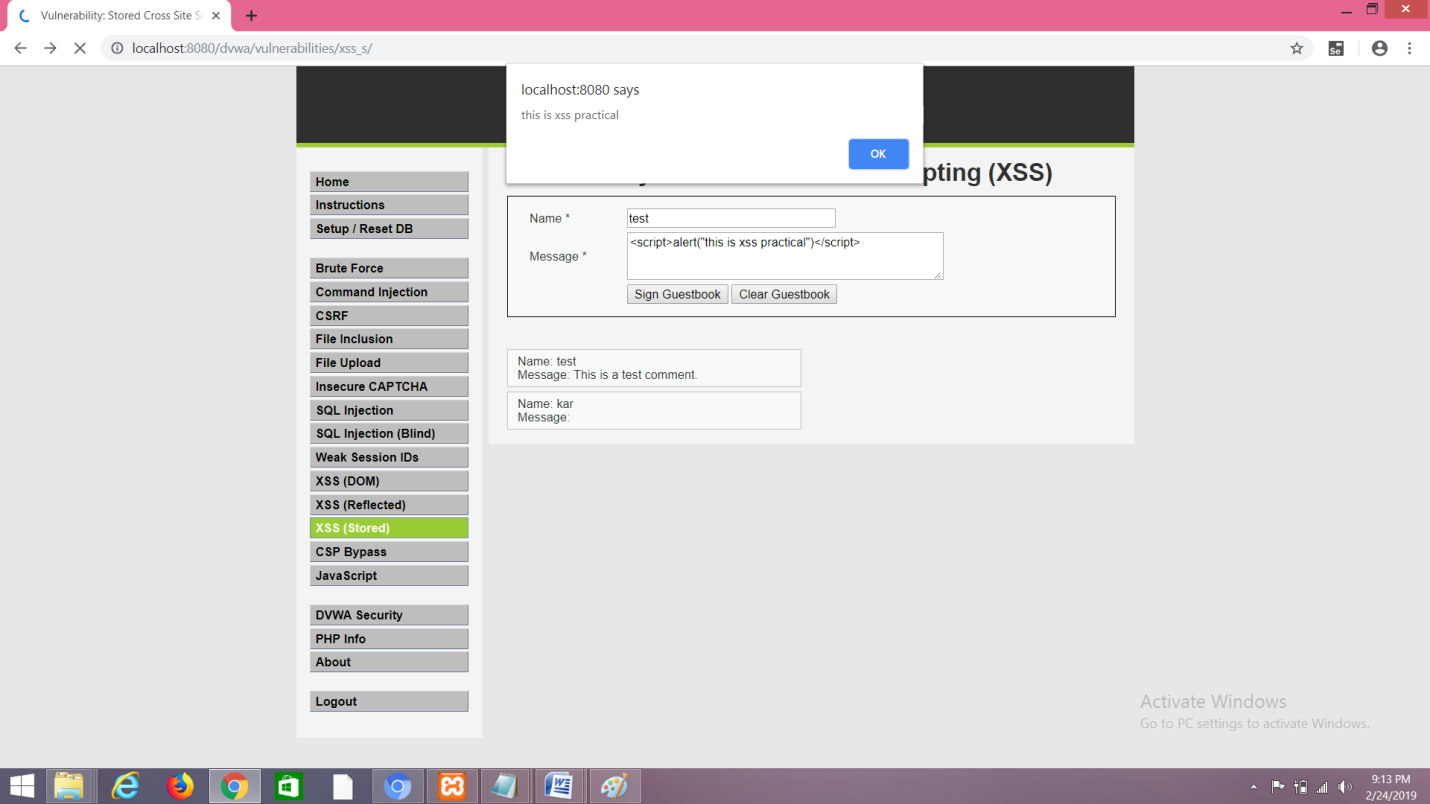


1. Go to XSS (stored)



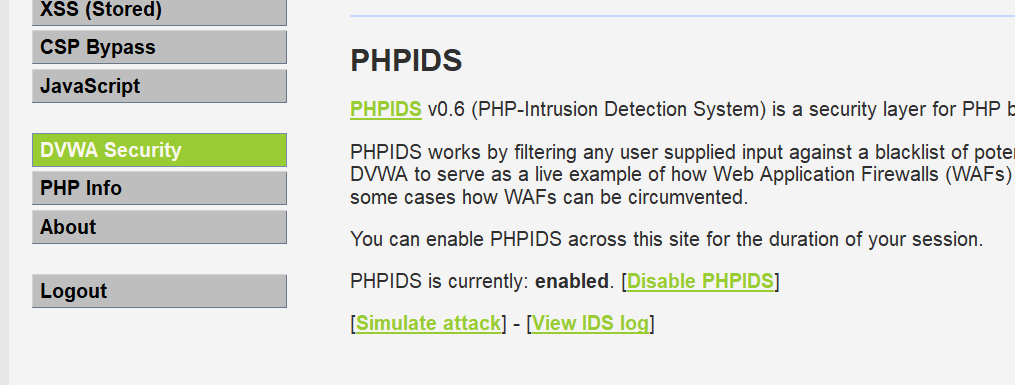
(11) Enter name: test message:<script>alert("this is xss practical")</script>

(12) You will be able to see the following output:

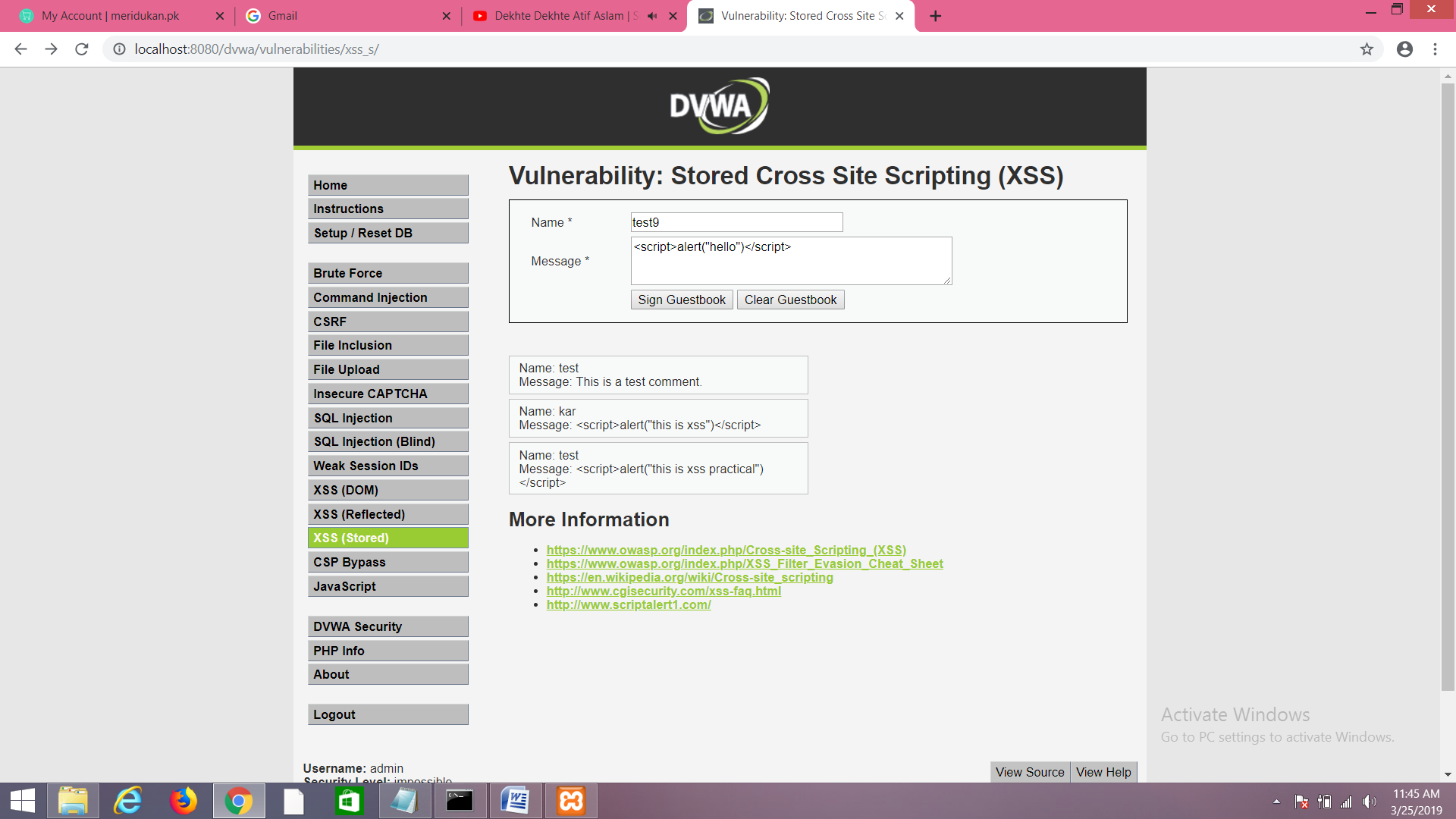


(13)To insert any malicious code do the following:

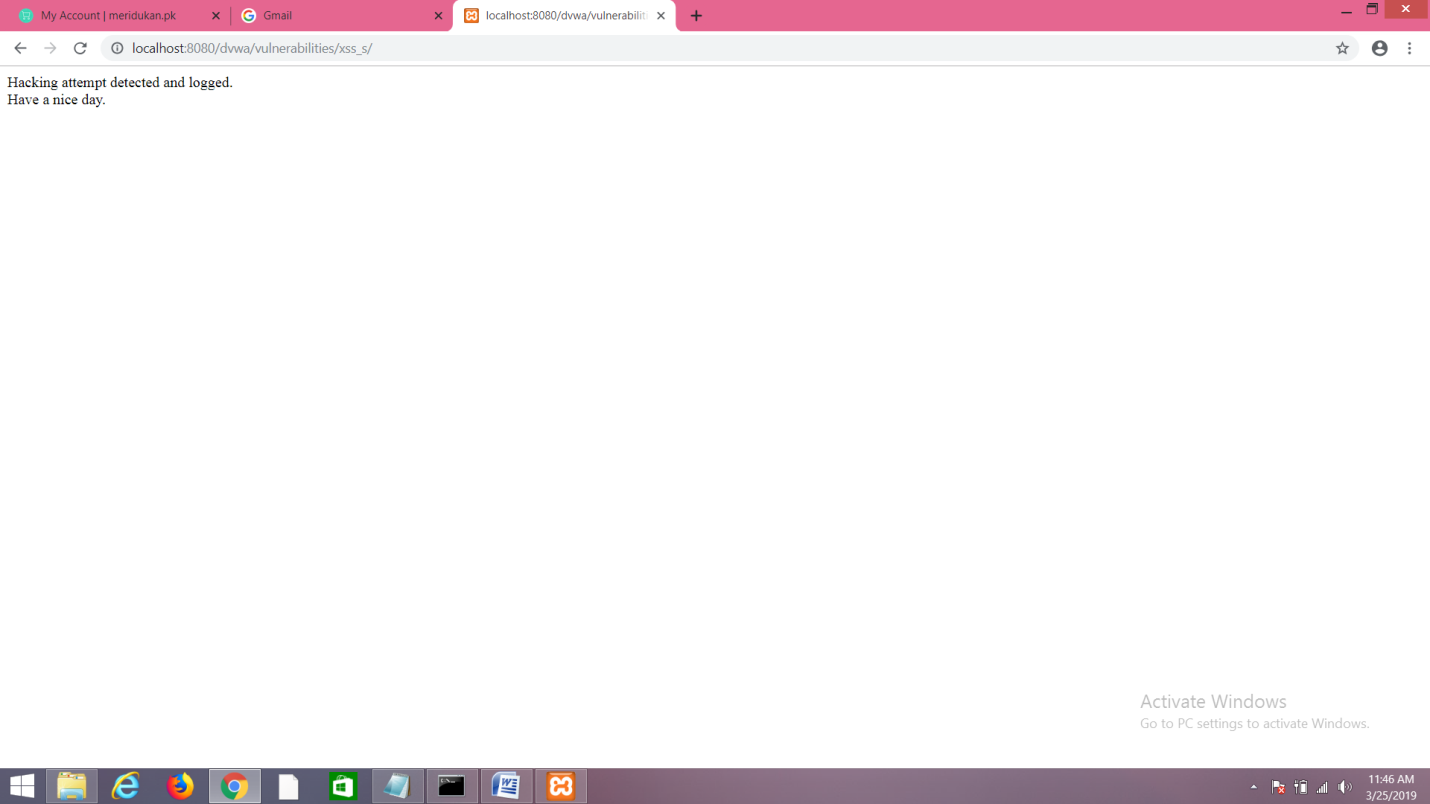
Go to dvwa security > enable PHPIDS



Go to XSS (stored) > message > type any malicious code as shown below.



And then click on "Sign GuestBook" you will be able to see the following message



(14) To view intrusion detection go to dvwa security > view IDS log

