**Practical -06**

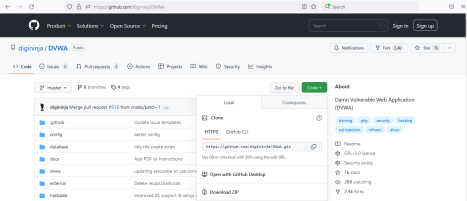
**Aim :-**Simulate persistent cross-site scripting attack.

**Steps:-**

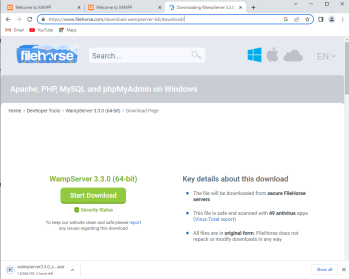
**https://www.youtube.com/watch?v=VE0OJrGfr\_Y**

1. Search DVWA in browser, download zip and extract.

https://github.com/digininja/DVWA

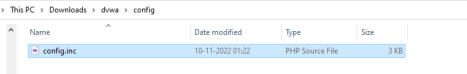
2. Download and install wamp server.

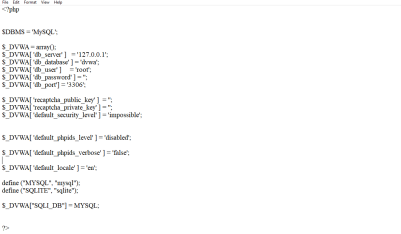
https://www.filehorse.com/download-wampserver-64/download/



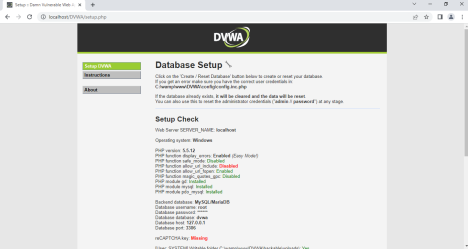
3.rename extracted dvwa master to DVWA.Copy this file and paste in c:drive/wamp64/www folder.

4. Open DVWA folder inside config folder rename config file by removing .dist extension.

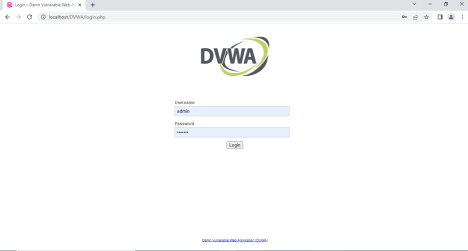
5. Open config file with notepad , Change username to “root” and keep password empty.

6.search for xss payload github and copy malicious script. <script>alert('XSS')</script>

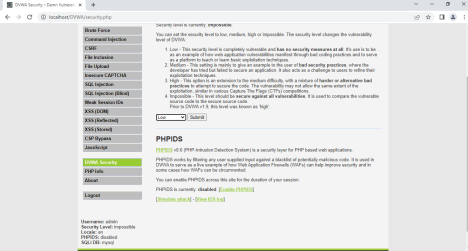
7.Open wamp and type(http://localhost/DVWA/setup.php)click on create/reset Database.

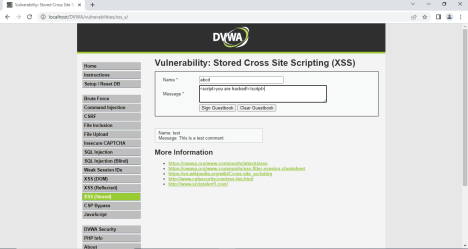


8.Give username as admin and password as password.You will be logged in successfully.



8.Click on DVWA security and set security Level as low.



9.Click on XXS(Stored) -> type name and malicious script in message box. 10.Click on Sign GuestBook.

