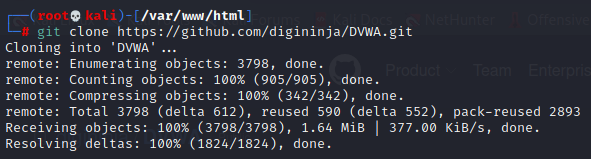
**Aryaman Mishra**

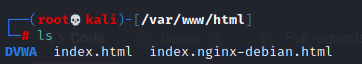
**19BCE1027**

DVWA is made with PHP and MySQL for security professionals or aspiring security professionals to discover as many issues as possible and exploit some of the most commons vulnerabilities of web platforms like **SQL injection**, **Cross Site Scripting** (XSS), **Cross Site Request Forgery** (CSRF), and more.

<https://github.com/digininja/DVWA.git>

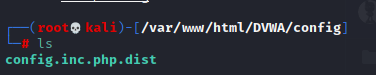








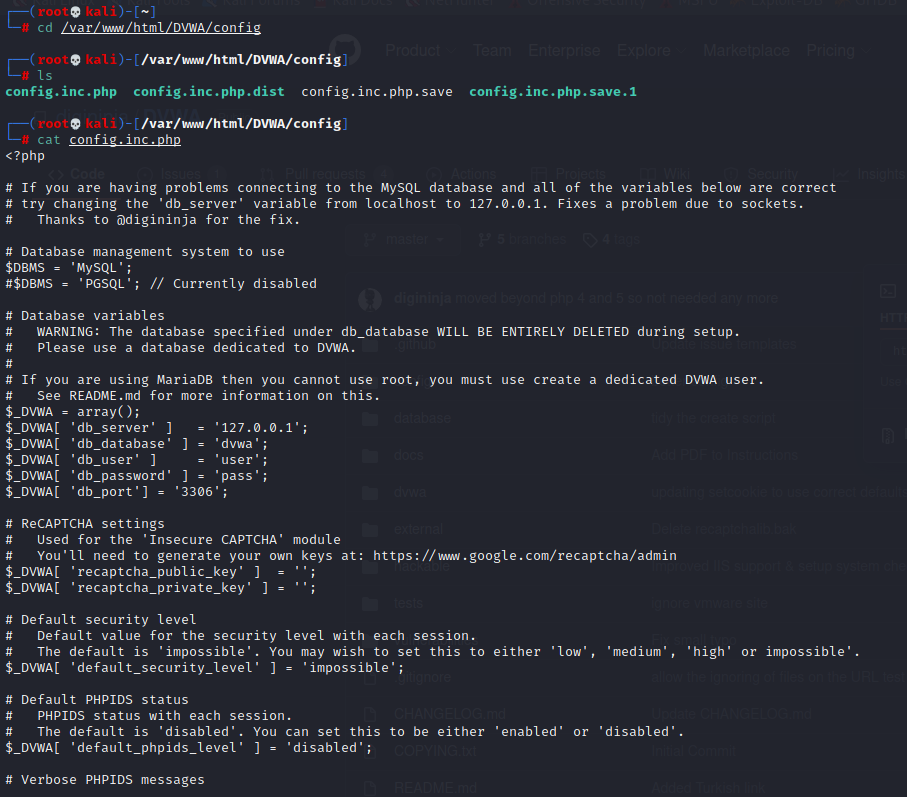
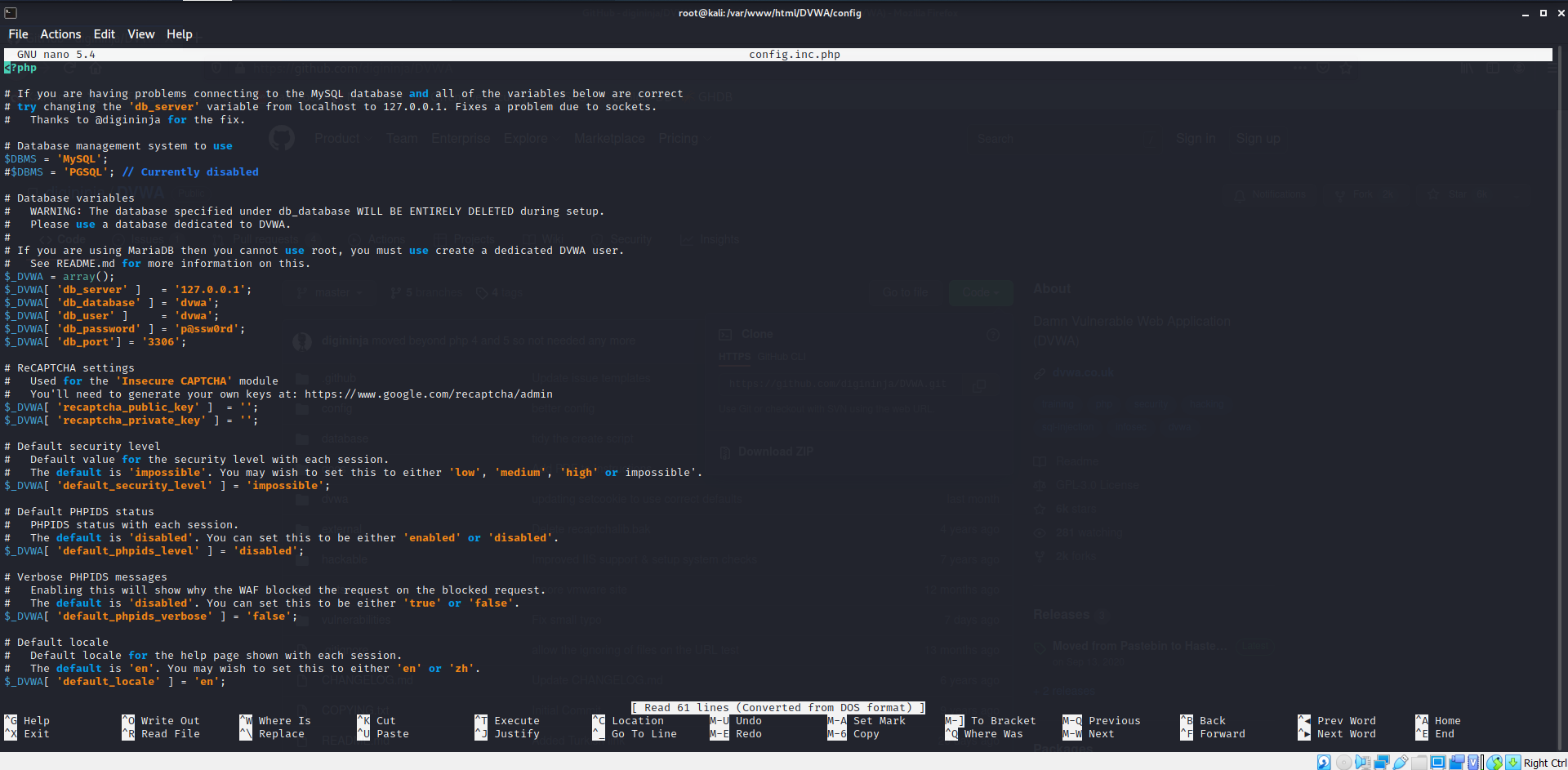


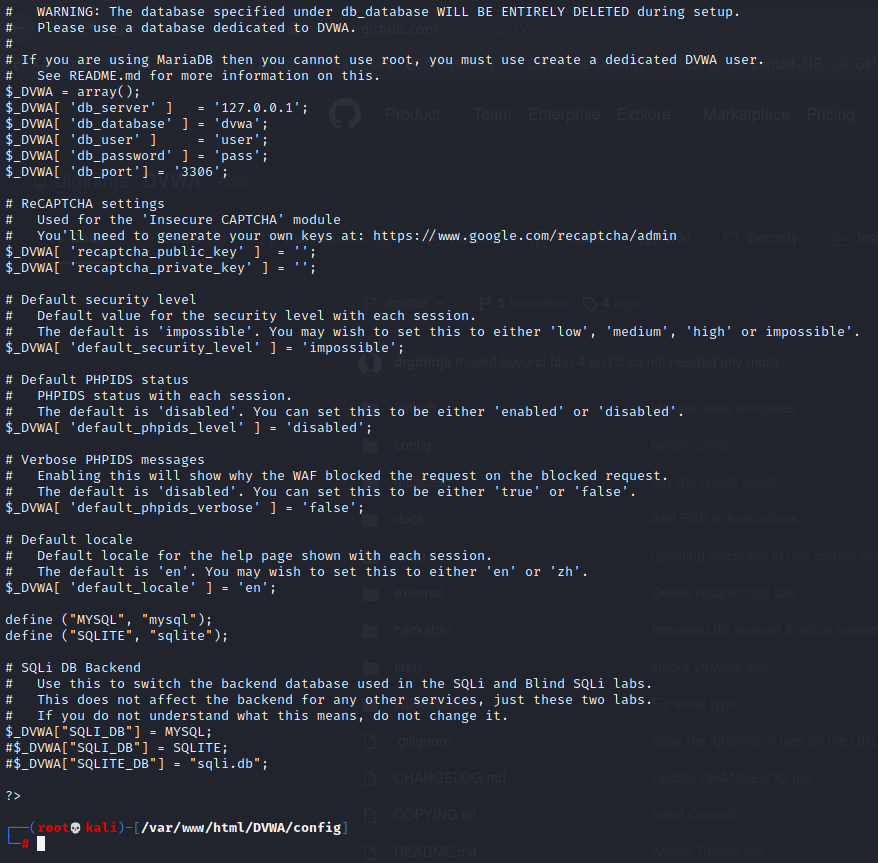


We will use the text editor to edit the configuration typing the following command:

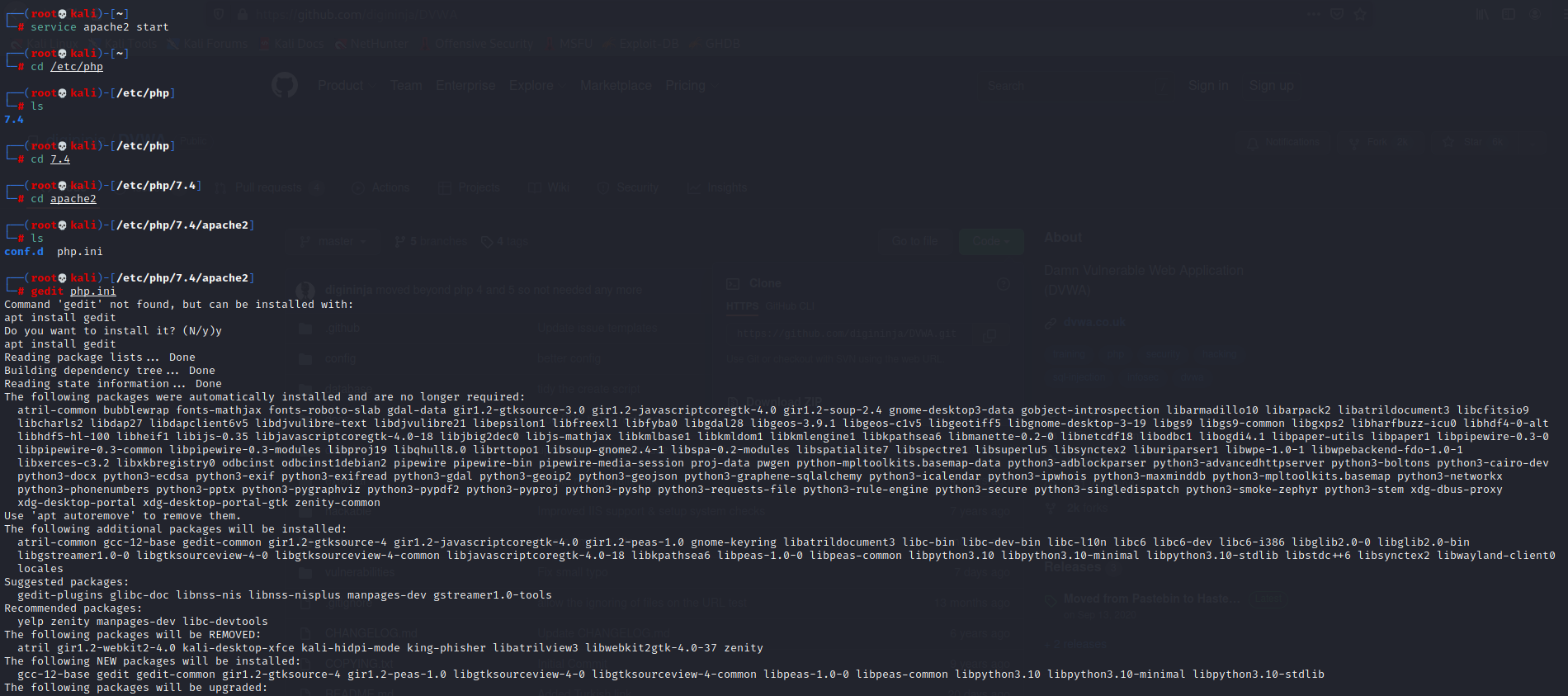
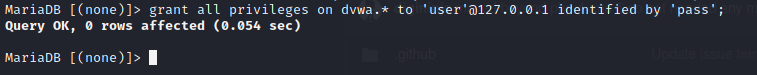
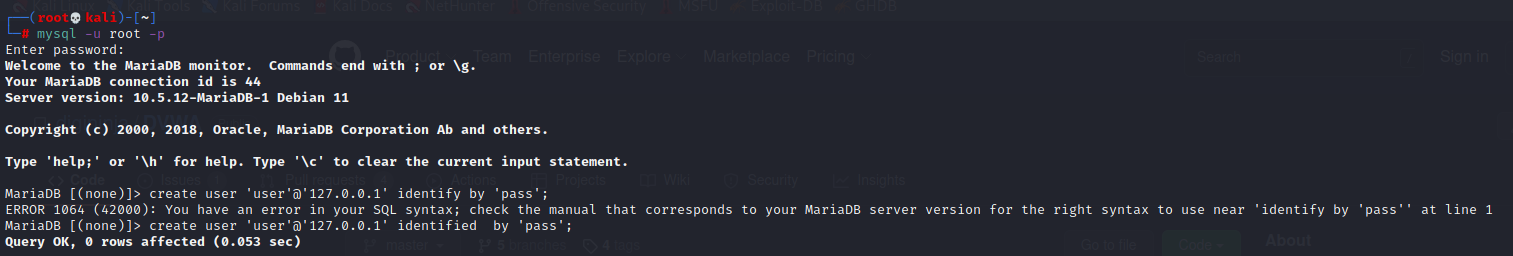
sudo vim /var/[www/html/dvwa/config/config.inc.php.dist](http://www/html/dvwa/config/config.inc.php.dist)

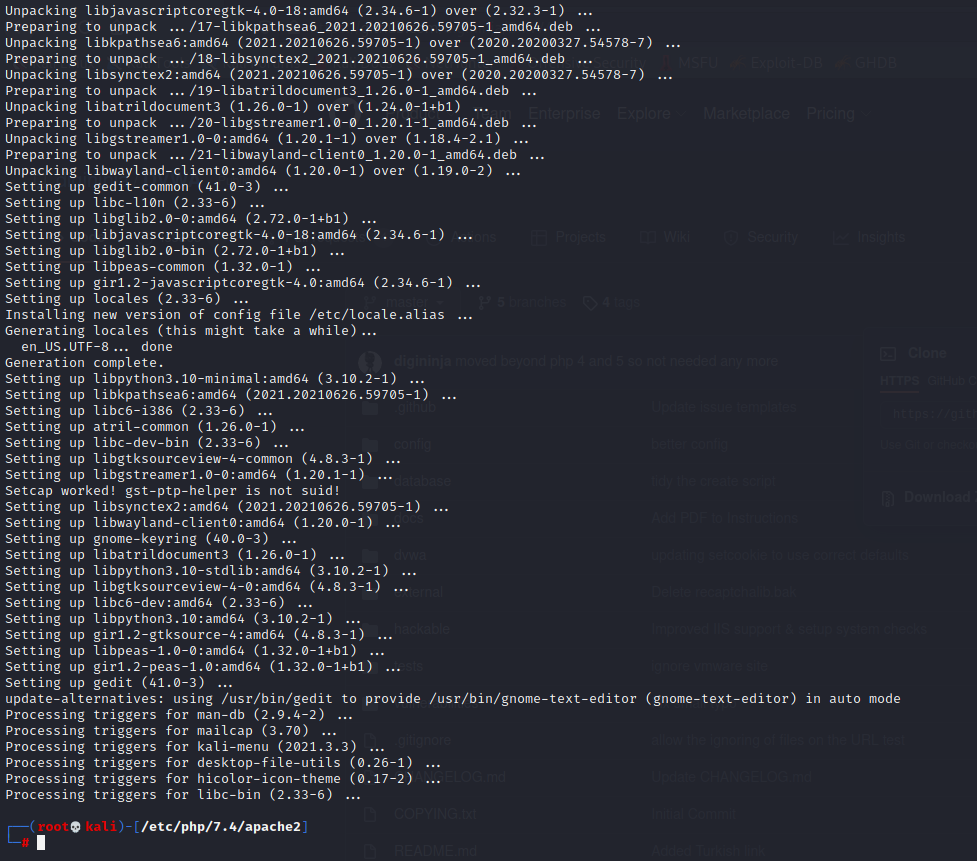


Change username and password as required by you. 



Start Mysql server.

Create a user in MariaBD and grant all priviledges to ‘user’@127.0.0.1

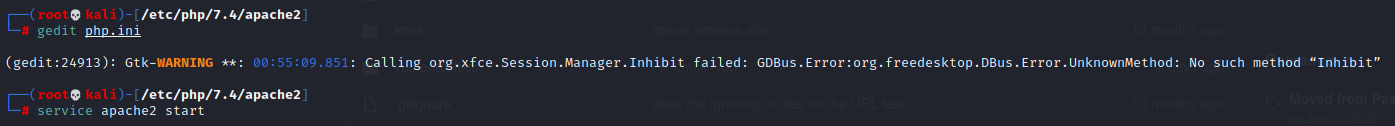


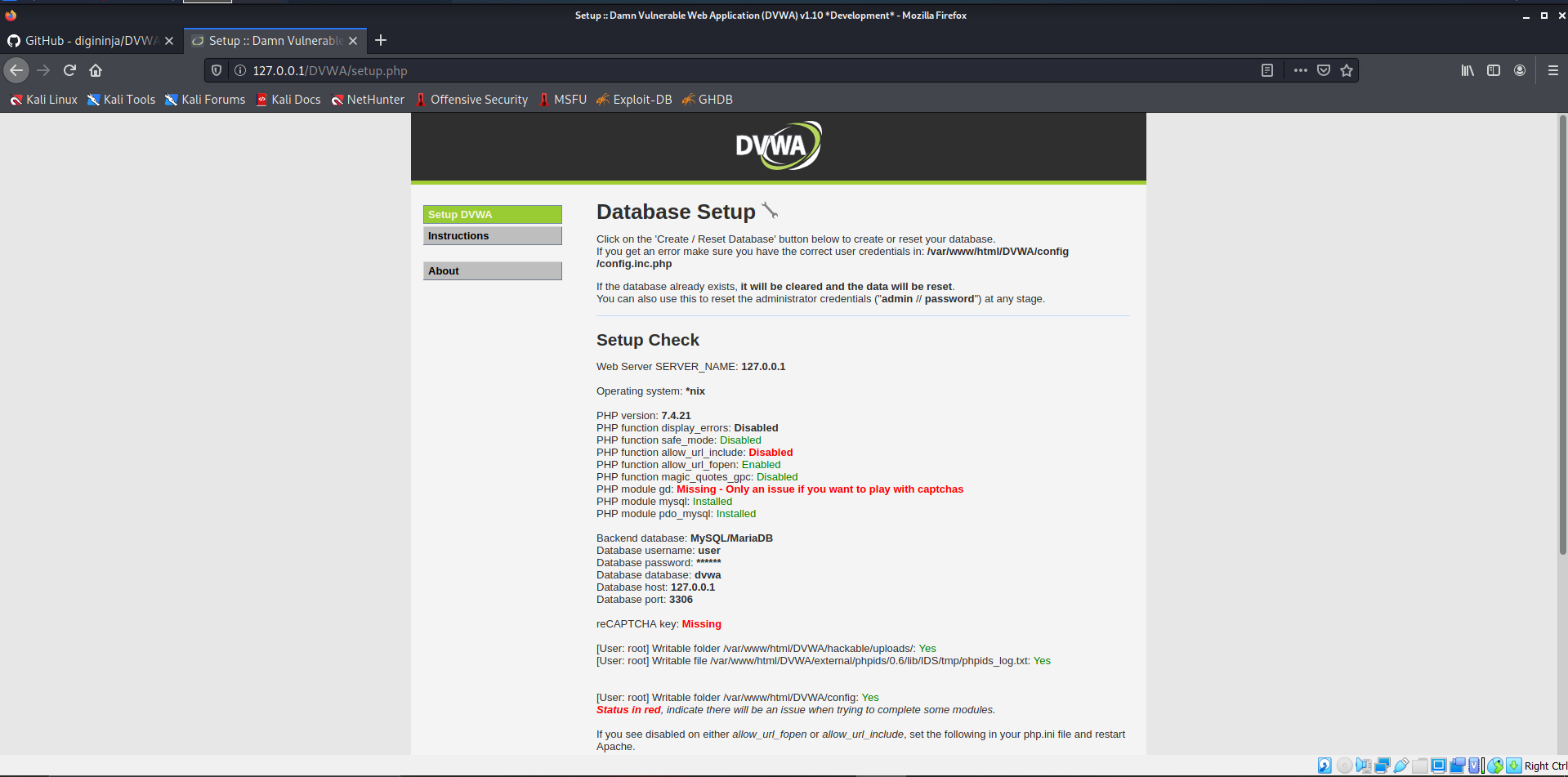
Once done, we need to edit the main config (***php.ini***) file for apache2, which is not correctly overridden for **DVWA** by default.

*sudo vim /etc/php5/apache2/php.ini*

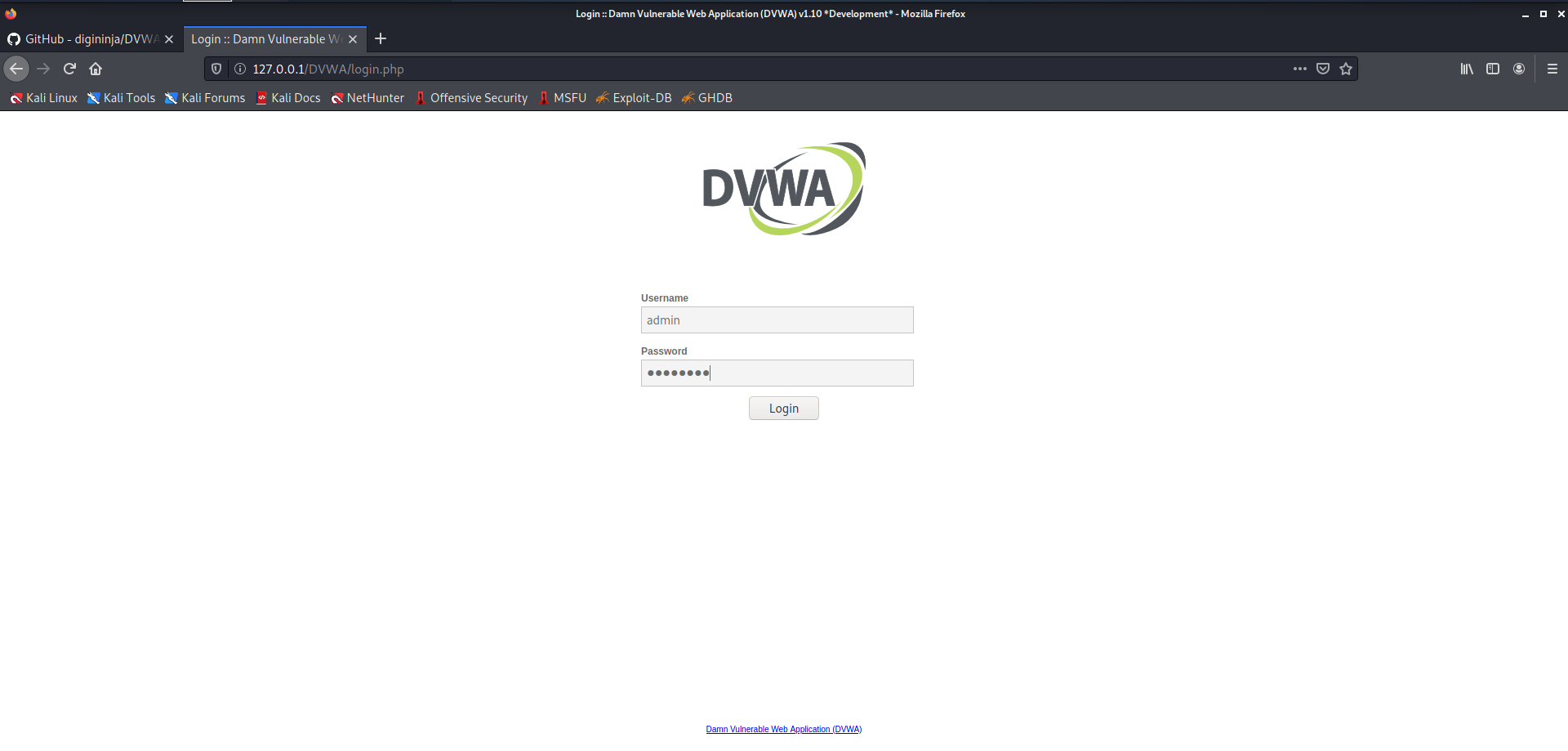
* Enable Allow\_url\_fopen
* Enable Allow\_url\_include

This is necessary to exploit the file upload vulnerability. Here’s a screenshot for ***php.ini*** after making changes.



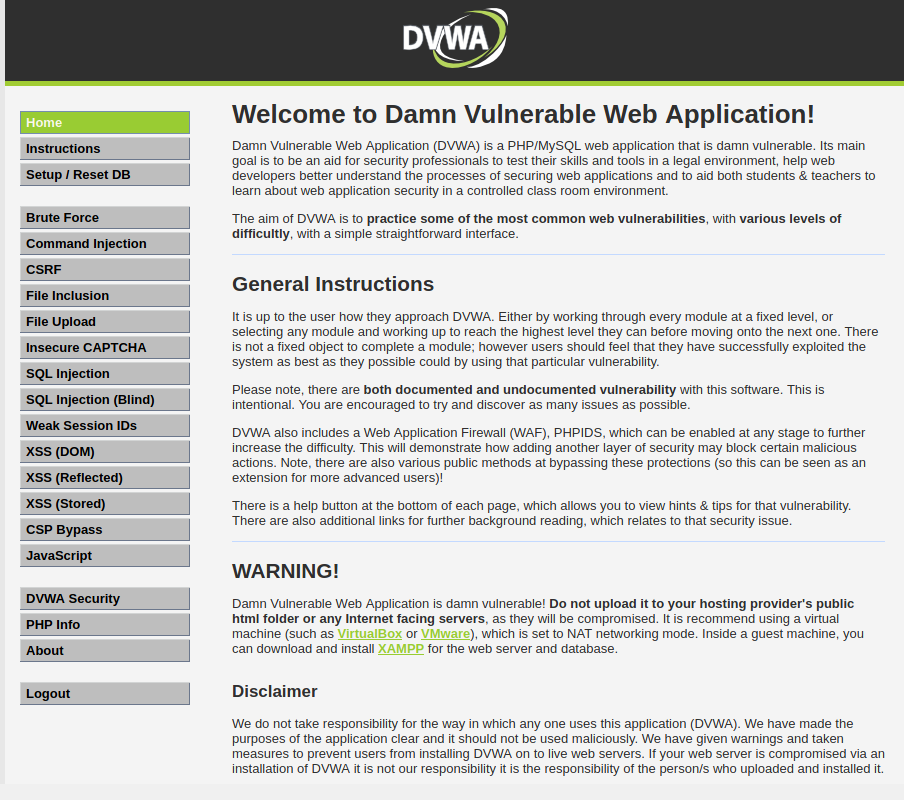
Access localhost/DVWA and work with DVWA Application.

Scroll and click ‘recreate database’ option and you will be redirected to login page.



Username:**admin**

Password:**password**

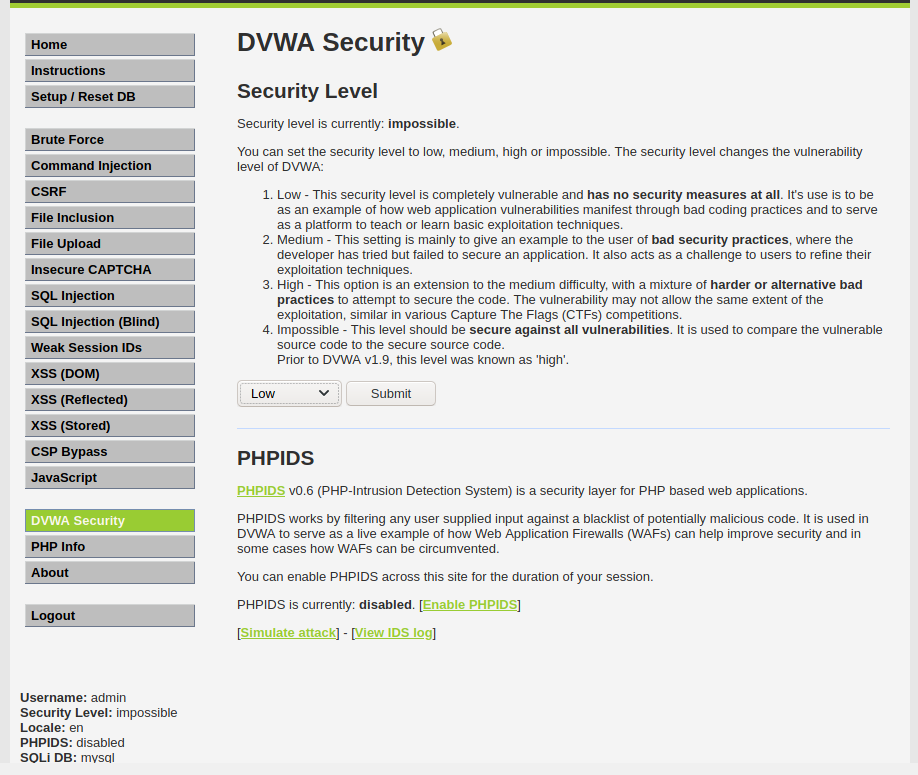


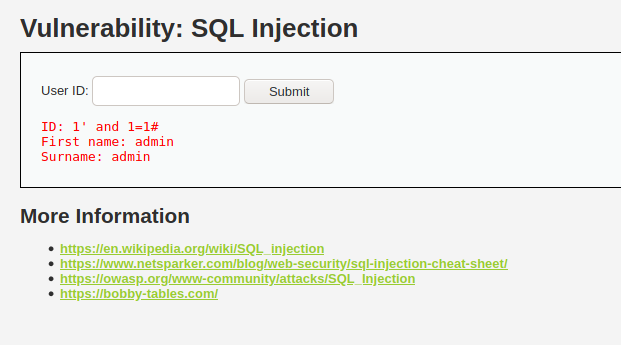
Now, login to change the strength of vulnerabilities by clicking on “DVWA Security”.

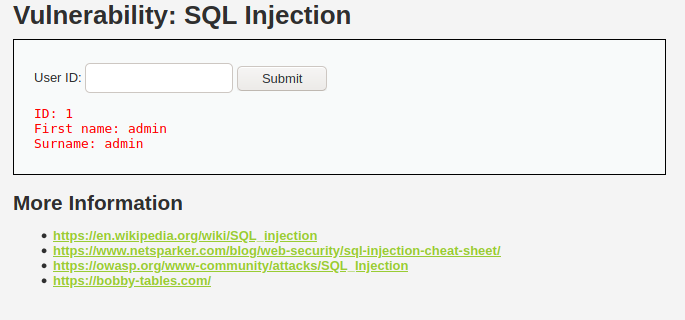
**Low Level:** Low-Level Security gives you the freedom to exploit all known vulnerabilities means there will be no security in a given framework and hence you can try all attacks if you are using it first Time.

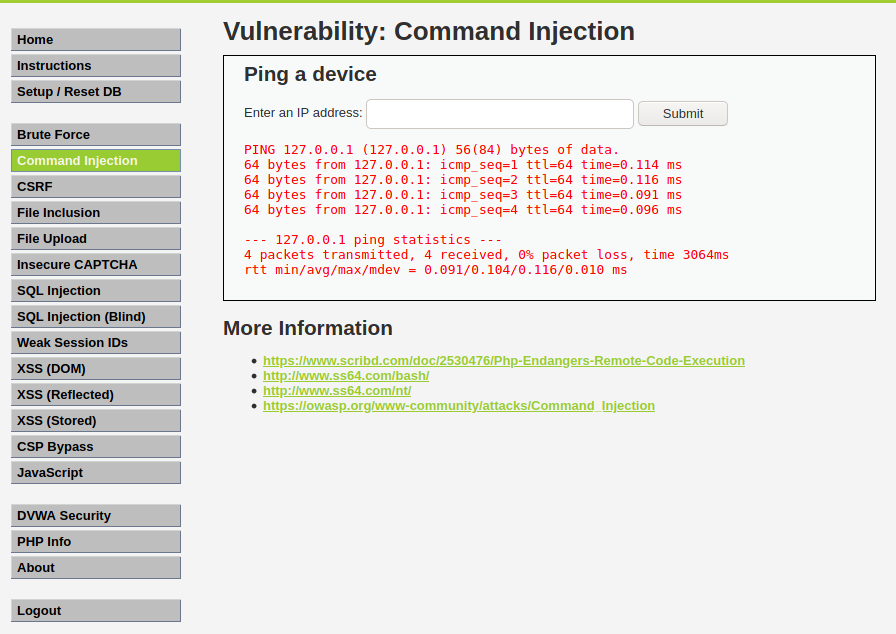
**Medium Level:** Medium security will have all entry-level validations and filtration which can stop any script kiddie to get the benefit of available vulnerabilities.

**High Level:** High Level is kind of Zero Day environment and if you can breach it then that means you are on the right track to becoming a VAPT Expert.









**Conclusion:**DVWA has been successfully configured and SQL and Command Injection can be implemented using the web tool.