Индивидуальный проект этап 2

Информационная безопасность

Ким И. В. НФИбд-01-21

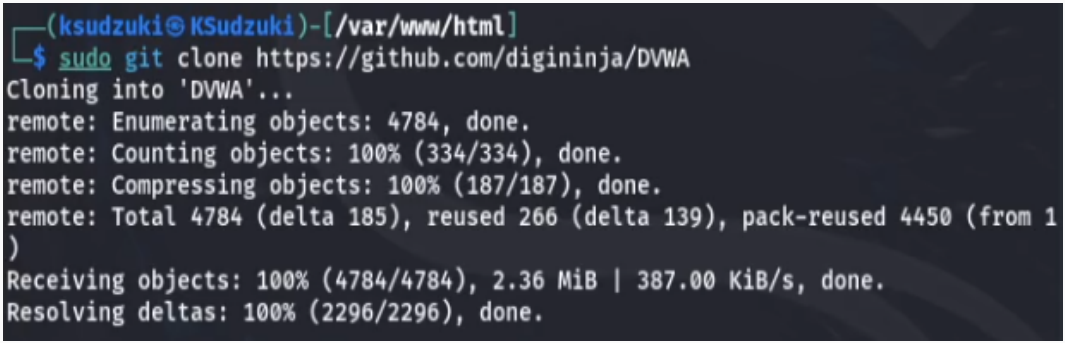
Российский университет дружбы народов, Москва, Россия

Цели и задачи

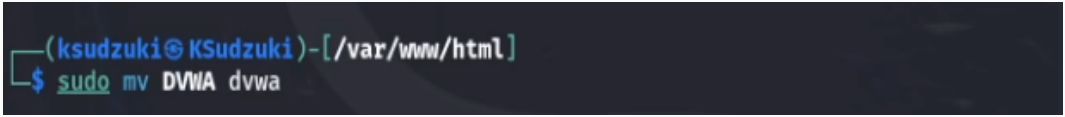
- Научиться основным способам тестирования веб приложений
- Установить и настроить DVWA на Kali linux

Выполнение работы

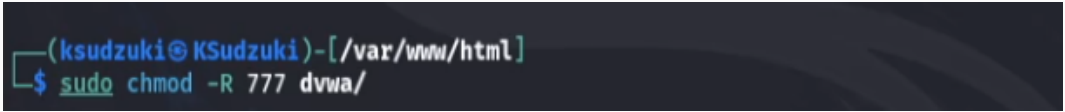
1. Клонировал DVWA с https://github.com/digininja/DVWA



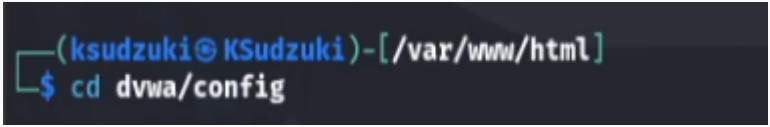
2. Переименовал директорию DVWA на dvwa



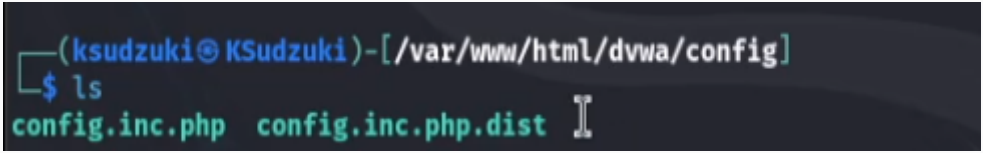
3. Задал права пользователя для директории



4. Зашел в директорию dvwa/config

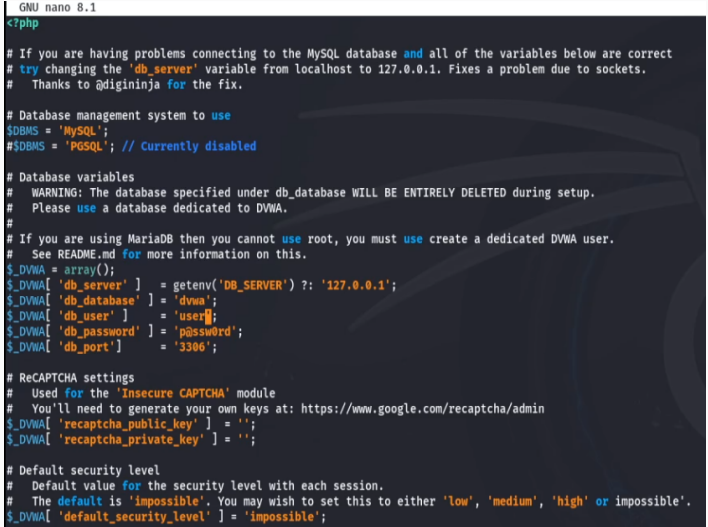


5. Проверил что в ней есть

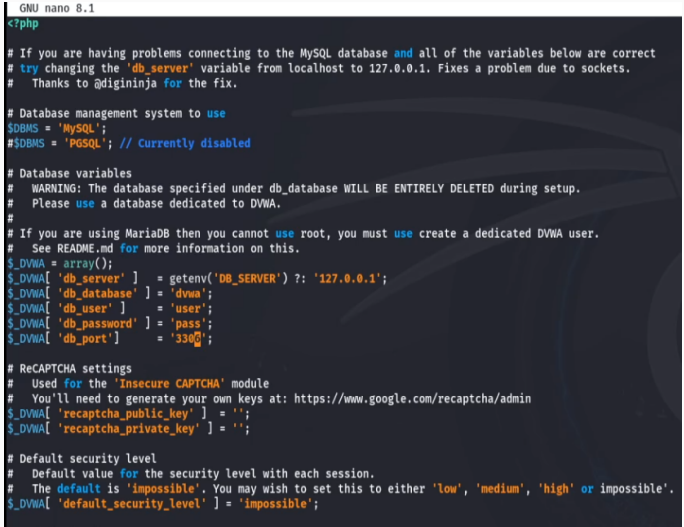


6. Открыл файл config.inc.php

7. Файл config.inc.php

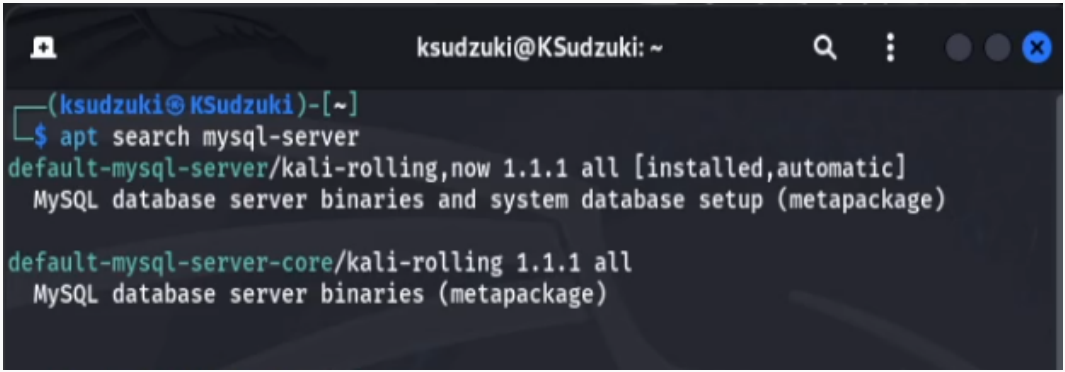


8. Заменил в нем db_user и db_password на user и pass

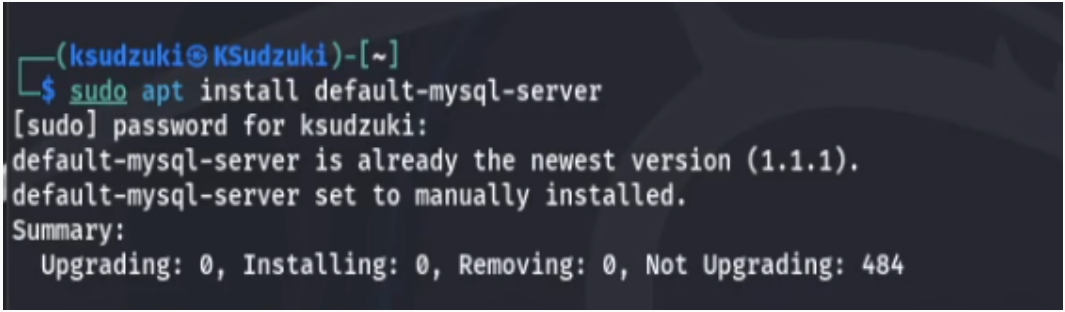


```
 GNU nano 8.1
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'user';
$_DVWA[ 'db_password' ] = 'pass';
$_DVWA[ 'db_port']      = '3306';

# ReCAPTCHA settings
#   Used for the 'Insecure CAPTCHA' module
#   You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA[ 'recaptcha_public_key' ]  = '';
$_DVWA[ 'recaptcha_private_key' ] = '';

# Default security level
#   Default value for the security level with each session.
#   The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or impossible'.
$_DVWA[ 'default_security_level' ] = 'impossible';
```

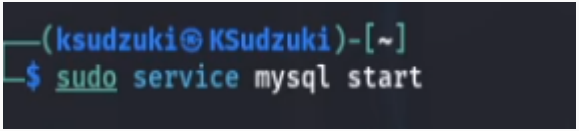
9. Посмотрел мой mysql-server



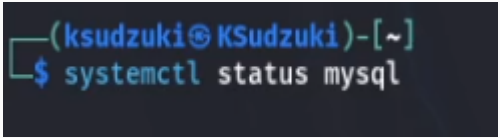
10. Установил mysql-server



11. Запустил mysql

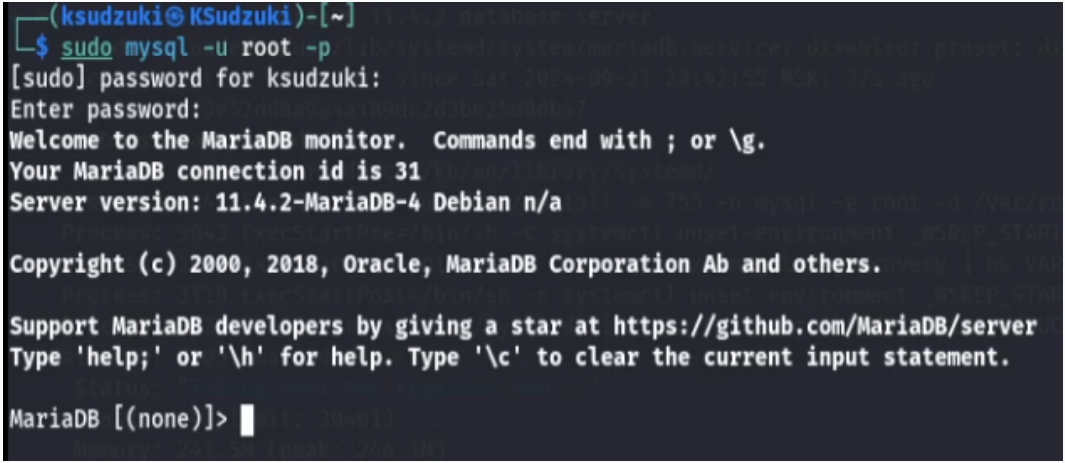


12. Посмотрел статус mysql



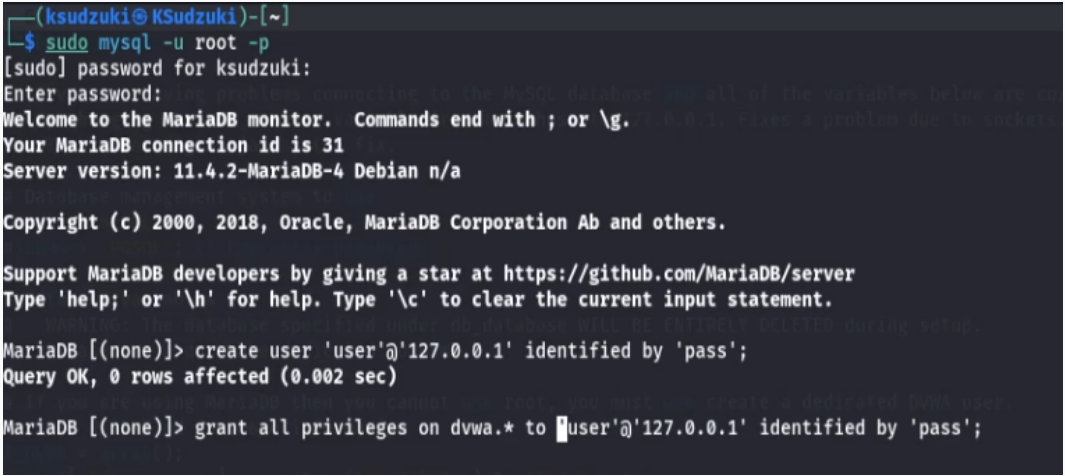

```
● mariadb.service - MariaDB 11.4.2 database server
     Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
     Active: active (running) since Sat 2024-09-21 20:42:55 MSK; 37s ago
 Invocation: 0f9e52dd8a9a4a189dc2d3be25d0db47
       Docs: man:mariadbd(8)
             https://mariadb.com/kb/en/library/systemd/
    Process: 3041 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, status=0/SUCCESS)
    Process: 3043 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
    Process: 3046 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= ||   VAR=`cd /usr/bin/..; /usr/bin/galera_recovery`; [ $? -eq 0 ]  && systemctl set-environment _WSREP_START_POSITION=$VAR || exit 1 (code=exited, statu>
    Process: 3119 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
    Process: 3121 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
   Main PID: 3105 (mariadbd)
     Status: "Taking your SQL requests now..."
      Tasks: 14 (limit: 30401)
     Memory: 241.5M (peak: 246.1M)
        CPU: 1.170s
     CGroup: /system.slice/mariadb.service
             └─3105 /usr/sbin/mariadbd

Sep 21 20:42:54 KSudzuki mariadbd[3105]: 2024-09-21 20:42:54 0 [Note] Plugin 'wsrep-provider' is disabled.
Sep 21 20:42:54 KSudzuki mariadbd[3105]: 2024-09-21 20:42:54 0 [Note] InnoDB: Buffer pool(s) load completed at 240921 20:42:54
Sep 21 20:42:55 KSudzuki mariadbd[3105]: 2024-09-21 20:42:55 0 [Note] Server socket created on IP: '127.0.0.1'.
Sep 21 20:42:55 KSudzuki mariadbd[3105]: 2024-09-21 20:42:55 0 [Note] mariadbd: Event Scheduler: Loaded 0 events
Sep 21 20:42:55 KSudzuki mariadbd[3105]: 2024-09-21 20:42:55 0 [Note] /usr/sbin/mariadbd: ready for connections.
Sep 21 20:42:55 KSudzuki mariadbd[3105]: Version: '11.4.2-MariaDB-4'  socket: '/run/mysqld/mysqld.sock'  port: 3306  Debian n/a
Sep 21 20:42:55 KSudzuki systemd[1]: Started mariadb.service - MariaDB 11.4.2 database server.
Sep 21 20:42:55 KSudzuki /etc/mysql/debian-start[3124]: Upgrading MariaDB tables if necessary.
Sep 21 20:42:55 KSudzuki /etc/mysql/debian-start[3130]: Checking for insecure root accounts.
Sep 21 20:42:55 KSudzuki /etc/mysql/debian-start[3140]: Triggering myisam-recover for all MyISAM tables and aria-recover for all Aria tables
```

13. Зашел в mysql

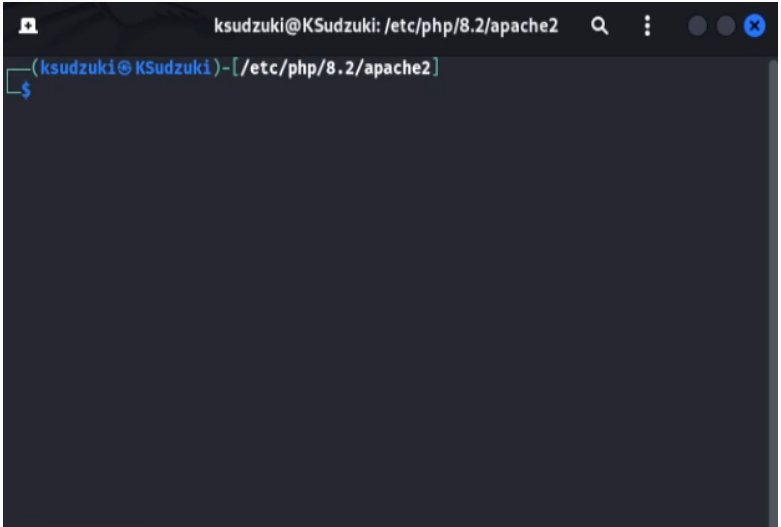


Выполнение работы

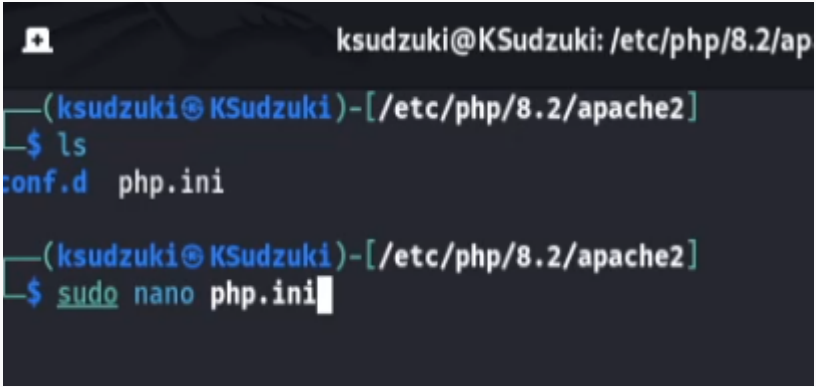
14. Создал пользователя и дал ему все права



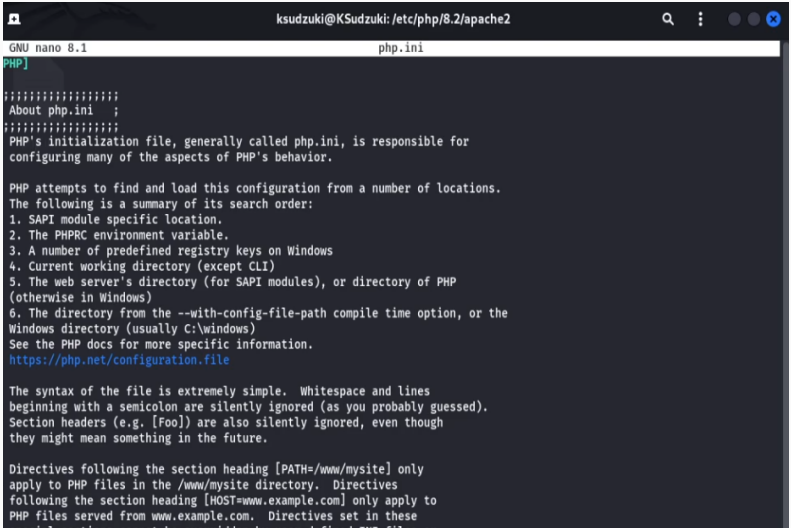
15. Зашёл в папку /etc/php/8.2/apache2



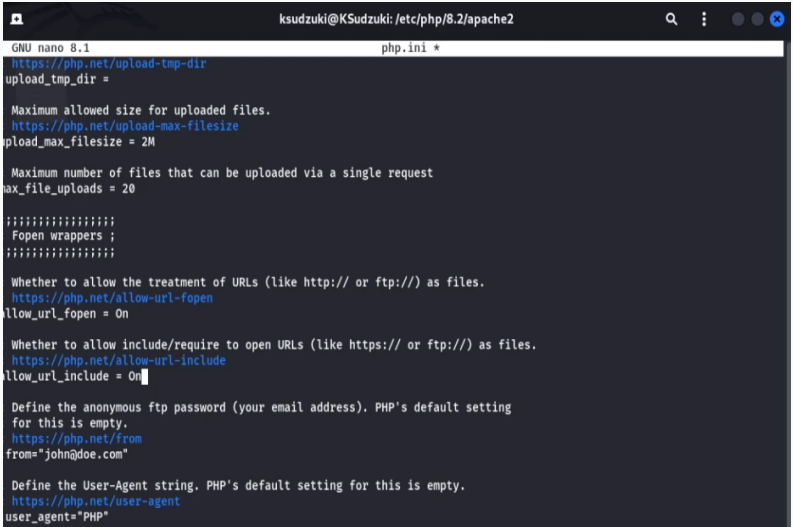
16. Посмотрел что в ней есть и открыл файл php.ini



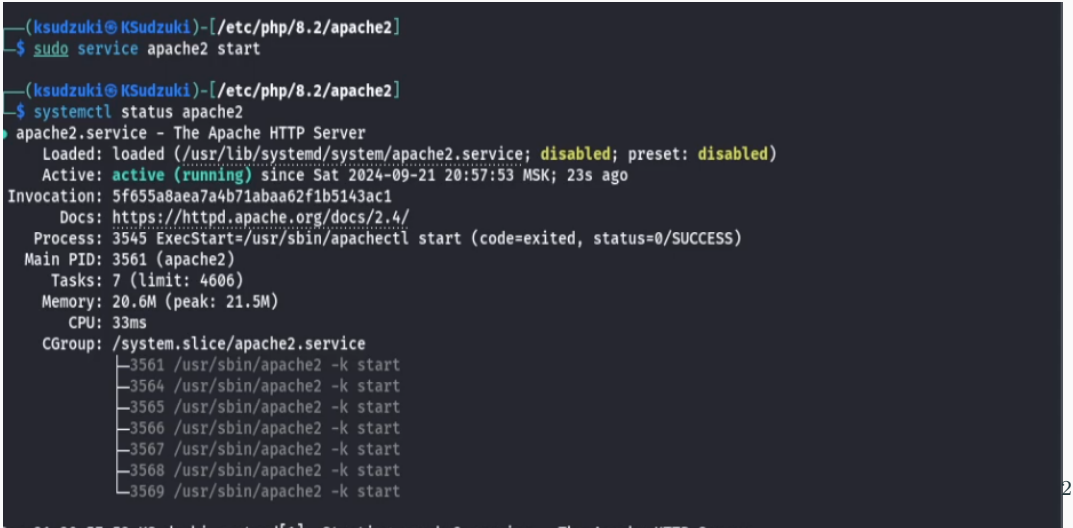
17. Файл php.ini



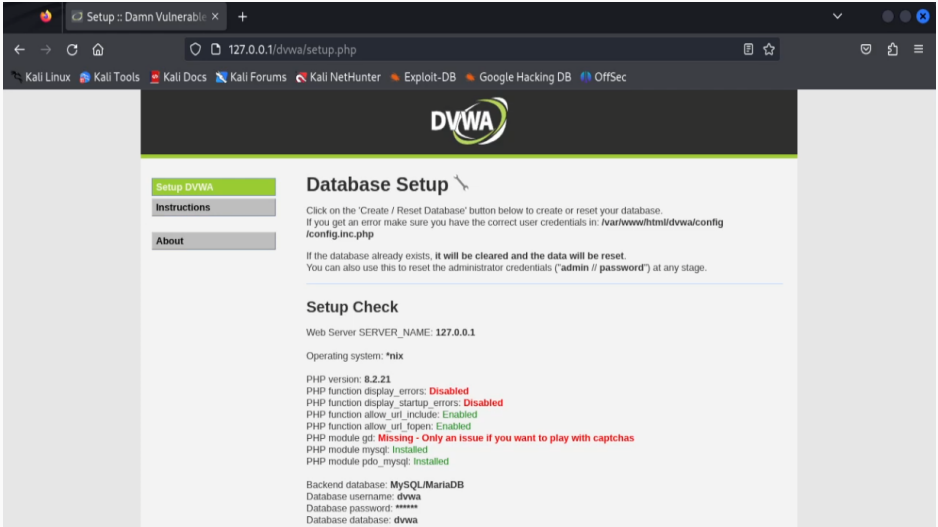
18. Нашел в нем allow_url_fopen и allow_url_include и поменял на “On”



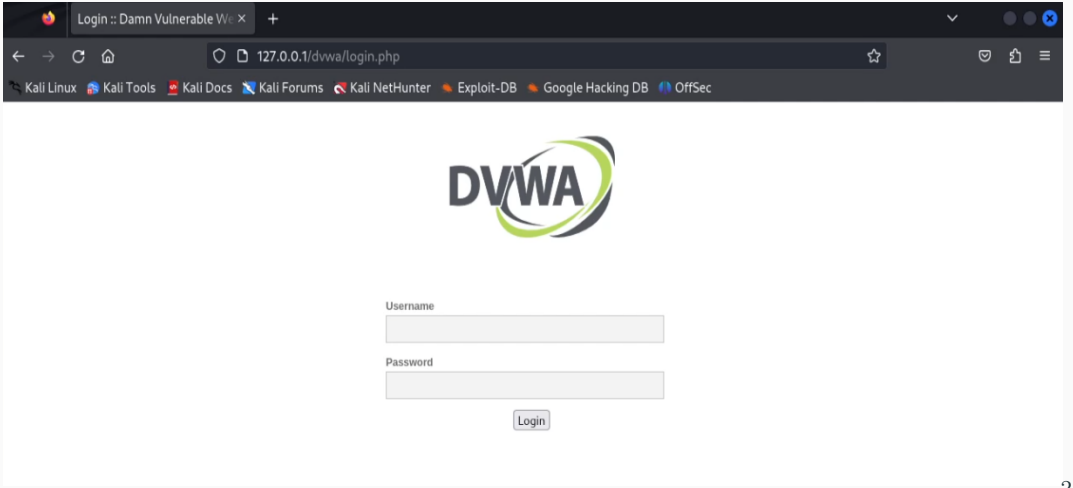
19. Запустил apache2 и проверил его статус



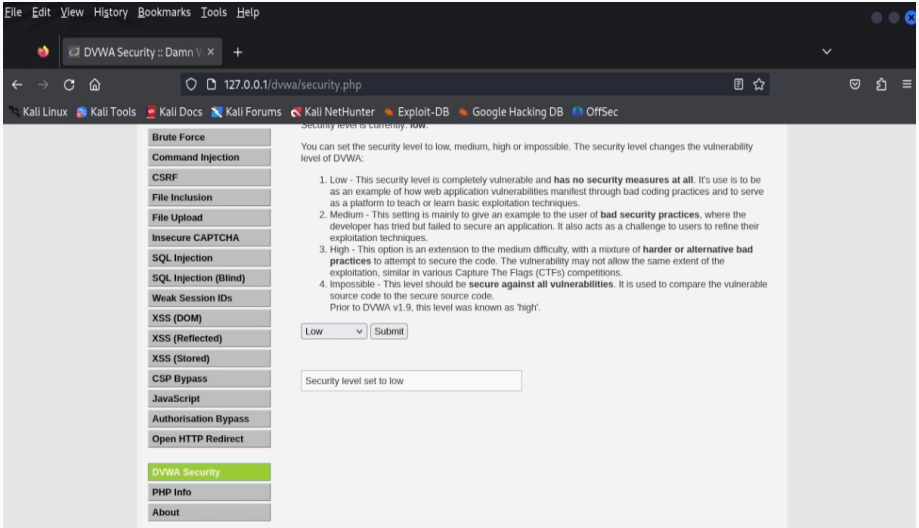
20. Зашёл на Localhost 127.0.0.1/dvwa/setup.php



21. Ввёл логин и пароль admin password



22. Поменял защиту на low



Выводы

- Установил и настроил DVWA на Kali linux