

Индивидуальный проект

Этап 4

Ведьмина Александра Сергеевна

Содержание

1	Цель работы	1
2	Задание.....	1
3	Выполнение лабораторной работы	1
4	Выводы.....	5

1 Цель работы

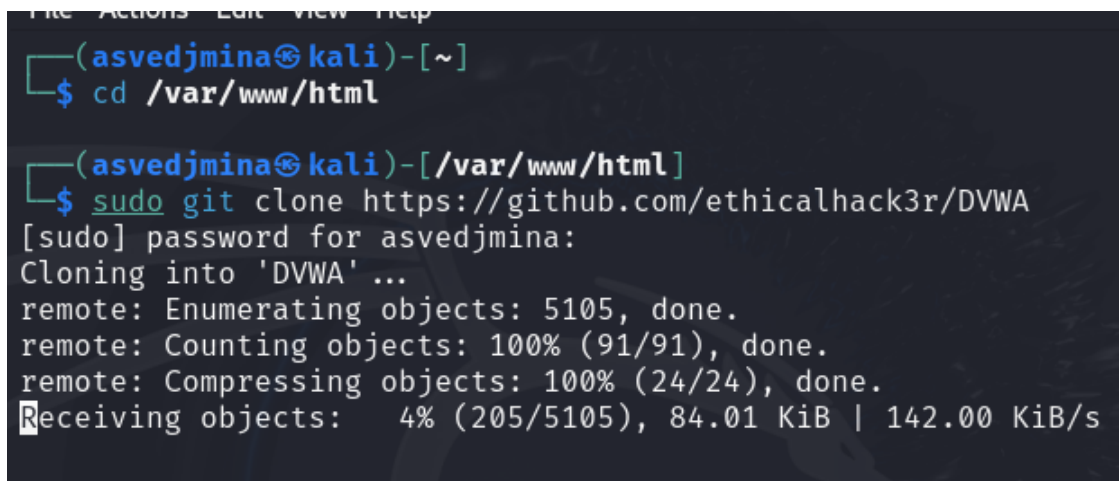
Приобретение практических навыков по установке nikto.

2 Задание

Разобраться в использовании nikto.

3 Выполнение лабораторной работы

Перехожу в директорию /var/www/html. Клонировать нужный репозиторий.



```

(asvedjmina@kali)-[~]
$ cd /var/www/html

(asvedjmina@kali)-[/var/www/html]
$ sudo git clone https://github.com/ethicalhack3r/DVWA
[sudo] password for asvedjmina:
Cloning into 'DVWA' ...
remote: Enumerating objects: 5105, done.
remote: Counting objects: 100% (91/91), done.
remote: Compressing objects: 100% (24/24), done.
Receiving objects: 4% (205/5105), 84.01 KiB | 142.00 KiB/s
```

Рис. 1: Директория /var/www/html

Повышаю права доступа к этой папке до 777.

```
(asvedjmina@kali)-[/var/www/html]
$ ls
DVWA index.html index.nginx-debian.html

(asvedjmina@kali)-[/var/www/html]
$ sudo chmod -R 777 DVWA

(asvedjmina@kali)-[/var/www/html]
$
```

Рис. 2: Изменение прав доступа

Создаем копию файла, используемого для настройки DVWA config.inc.php.dist с именем config.inc.php. Делаю копию.

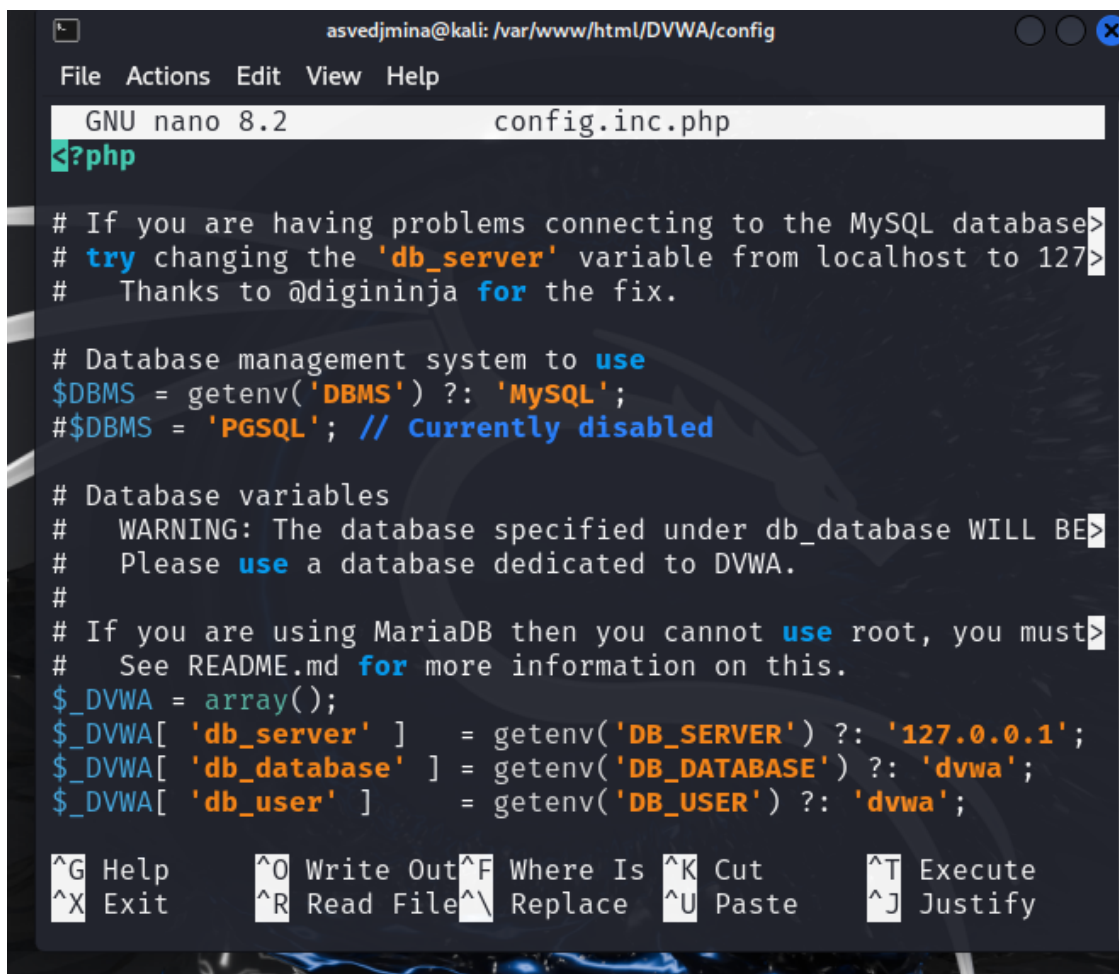
```
(asvedjmina@kali)-[/var/www/html/DVWA/config]
$ sudo cp config.inc.php.dist config.inc.php

(asvedjmina@kali)-[/var/www/html/DVWA/config]
$ ls
config.inc.php config.inc.php.dist

(asvedjmina@kali)-[/var/www/html/DVWA/config]
$
```

Рис. 3: Создание копии файла

Далее открываю файл в текстовом редакторе.



```
asvedjmina@kali: /var/www/html/DVWA/config
File Actions Edit View Help
GNU nano 8.2 config.inc.php
<?php
# If you are having problems connecting to the MySQL database>
# try changing the 'db_server' variable from localhost to 127>
# Thanks to @digininja for the fix.

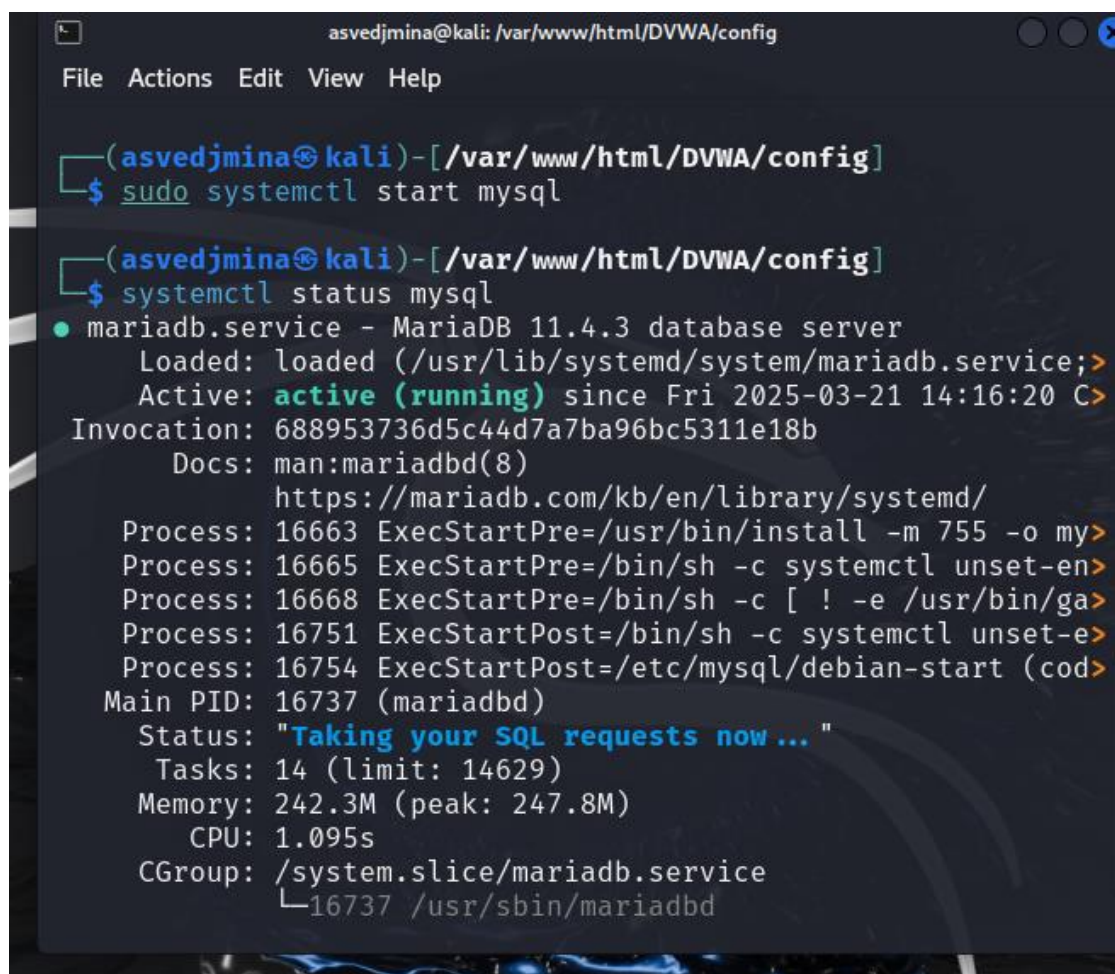
# Database management system to use
$DBMS = getenv('DBMS') ?: 'MySQL';
#$DBMS = 'PGSQL'; // currently disabled

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

^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify
```

Рис. 4: Открытие файла в редакторе

Проверяю запуск mysql.

A terminal window titled 'asvedjmina@kali: /var/www/html/DVWA/config'. The window shows the execution of two commands: 'sudo systemctl start mysql' and 'systemctl status mysql'. The output of the second command shows that the 'mariadb.service' is active and running. The status output includes details about the service's loaded state, active state, invocation ID, documentation, process list, main PID, status message, tasks, memory usage, CPU usage, and cgroup.

```
asvedjmina@kali: /var/www/html/DVWA/config
File Actions Edit View Help

(asvedjmina@kali)-[/var/www/html/DVWA/config]
$ sudo systemctl start mysql

(asvedjmina@kali)-[/var/www/html/DVWA/config]
$ systemctl status mysql
● mariadb.service - MariaDB 11.4.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; >
   Active: active (running) since Fri 2025-03-21 14:16:20 C>
 Invocation: 688953736d5c44d7a7ba96bc5311e18b
    Docs: man:mariadb(8)
          https://mariadb.com/kb/en/library/systemd/
   Process: 16663 ExecStartPre=/usr/bin/install -m 755 -o my>
   Process: 16665 ExecStartPre=/bin/sh -c systemctl unset-en>
   Process: 16668 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/ga>
   Process: 16751 ExecStartPost=/bin/sh -c systemctl unset-e>
   Process: 16754 ExecStartPost=/etc/mysql/debian-start (cod>
 Main PID: 16737 (mariabdd)
   Status: "Taking your SQL requests now ..."
    Tasks: 14 (limit: 14629)
  Memory: 242.3M (peak: 247.8M)
     CPU: 1.095s
   CGroup: /system.slice/mariadb.service
           └─16737 /usr/sbin/mariabdd
```

Рис. 5: Запуск mysql

Авторизируюсь в базе данных от имени пользователя root. Появляется командная строка с приглашением "MariaDB", далее создаем в ней нового пользователя, используя учетные данные из файла config.inc.php. Затем предоставляем привилегии для работы с этой базой данных.

Настраиваю apache2.

[Настройка apache2](image/Screenshot from 2025-03-21 22-26-30.png{#fig:006 width=100%})

Мы настроили DVWA, Apache и базу данных, поэтому открываем браузер и запускаем веб-приложение, введя 127.0.0/DVWA. Нажимаю на кнопку create\reset database.

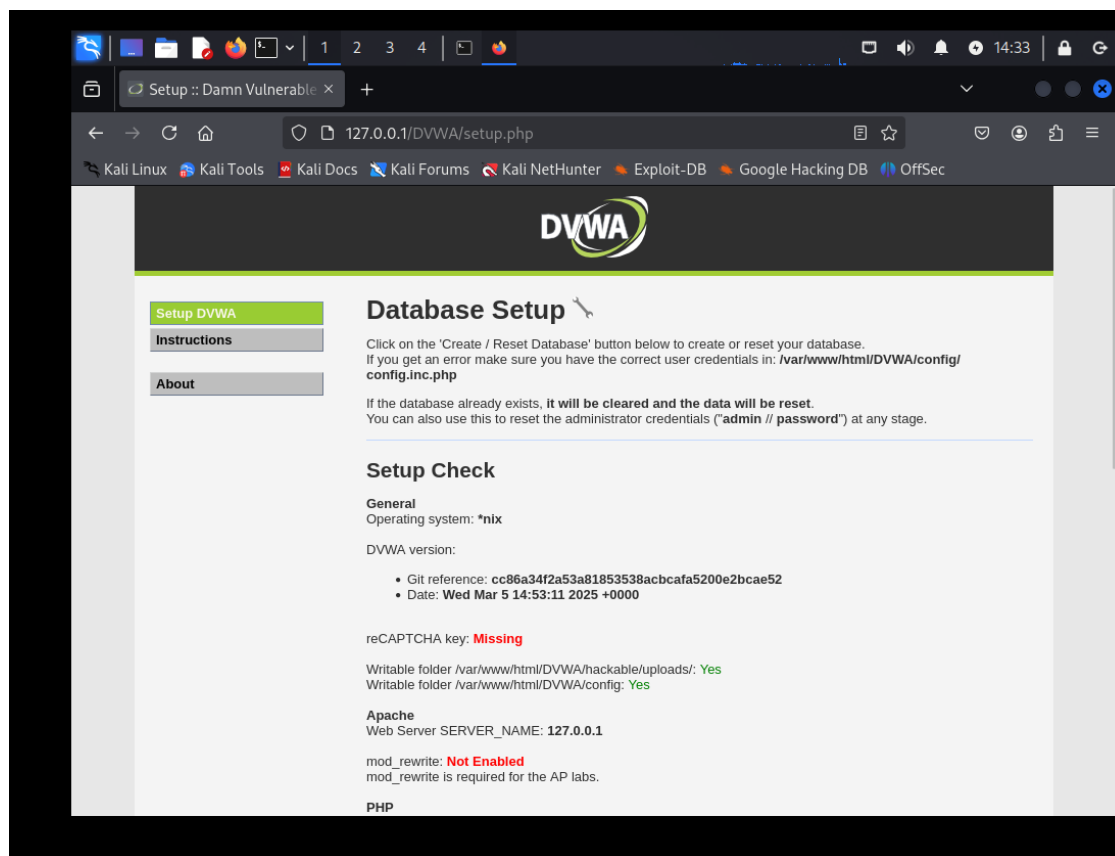


Рис. 6: Запуск веб-приложения

4 Выводы

В ходе выполнения лабораторной работы я приобрела практические навыки по установке уязвимого веб-приложения DVWA.