

# Индивидуальный проект

## Этап 5

---

Ведьмина Александра Сергеевна

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Ведьмина Александра Сергеевна
- студентка
- Российский университет дружбы народов
- 1132236003@rudn.ru
- <https://asvedjmina.github.io/ru/>



## Вводная часть

---

Научиться использовать Burp Suite.

## Выполнение лабораторной работы

---

## Выполнение лабораторной работы

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

```
File Actions Edit View Help
└─(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
```

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]
$
```



## Выполнение лабораторной работы

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

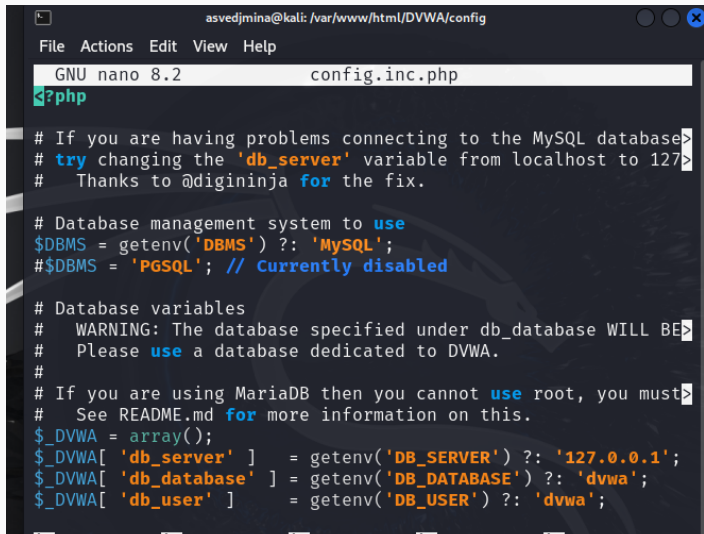
```
(asvedjmina@kali)-[/var/www/html/DVWA/config]
$ sudo cp config.inc.php.dist config.inc.php

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

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

## Выполнение лабораторной работы

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

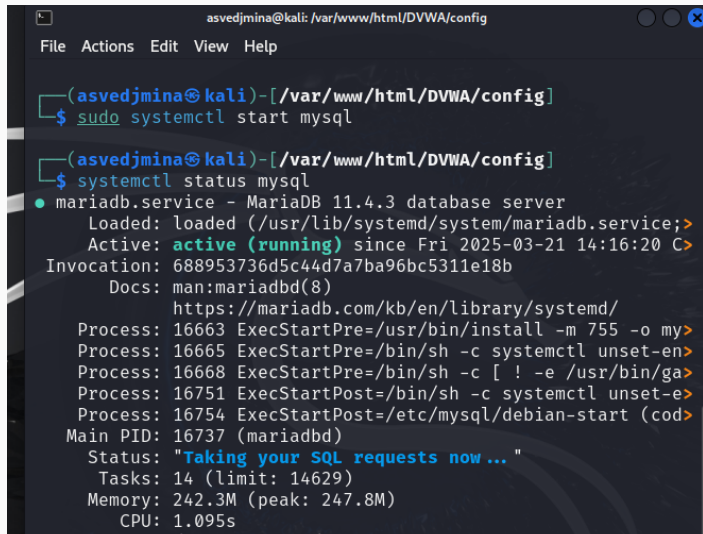
# If you are having problems connecting to the MySQL database>
# try changing the 'db_server' variable from localhost to 127>
# Thanks to @digininja for the fix.

# 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';
```

# Выполнение лабораторной работы

Проверяю запуск mysql.



```
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 (mariabdb)
    Status: "Taking your SQL requests now ..."
     Tasks: 14 (limit: 14629)
  Memory: 242.3M (peak: 247.8M)
    CPU: 1.095s
```

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.

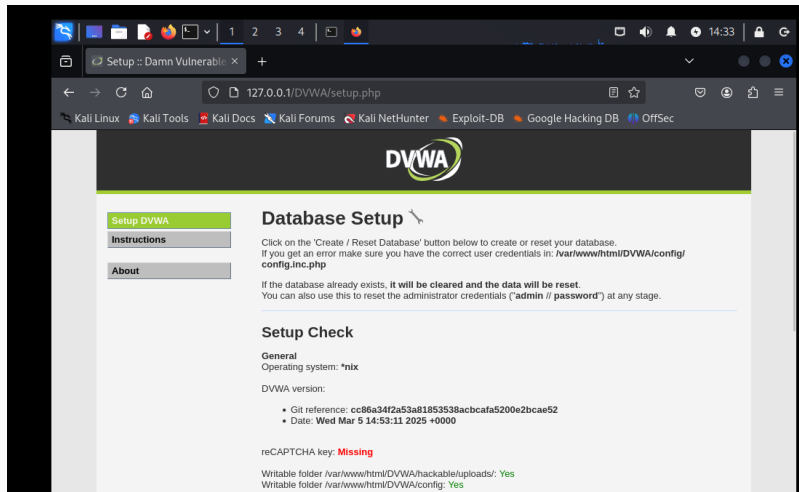
```
* to 'userDVWA'@'127.0.0.1' identified by "dvwa" at line 2
MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'
@'127.0.0.1' identified by 'dvwa';
Query OK, 0 rows affected (0.007 sec)
```

```
MariaDB [(none)]> exit
Bye
```

```
(asvedjmina@kali)-[~]
$
```

# Выполнение лабораторной работы

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`.



## Выводы

---

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