

# Презентация по 2 этапу индивидуального проекта

Установка DVWA

---

Танрибергенов Э.

2024 г.

Российский университет дружбы народов, Москва, Россия

# Информация

---

- Танрибергенов Эльдар
- студент 4 курса из группы НПИбд-02-21
- ФМиЕН, кафедра прикладной информатики и теории вероятностей
- Российский университет дружбы народов

## Цели и задачи

---

Установить DVWA в гостевую систему к Kali Linux и ознакомиться.

- Установить DVWA в гостевую систему к Kali Linux и ознакомиться.

## Результаты

---

```
[sudo] password for etanribergenov:
(root@etanribergenov)-[/home/etanribergenov]
# apt-get install dvwa
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libapache2-mod-php8.2 php8.2 php8.2-cli php8.2-common p
  php8.2-readline
Suggested packages:
```

**Рис. 1:** Загрузка DVWA



```
(root@etanribergenov)-[/home/etanribergenov]  
# apt-get install -y apache2 mariadb-server mariadb-client php php-mysqli php-gd libapache2-mod-php  
Reading package lists... Done  
Building dependency tree... Done
```

**Рис. 2:** Установка необходимых пакетов

```
(root@etanribergenov)-[/var/www/html]
# git clone https://github.com/digininja/DVWA.git
Cloning into 'DVWA' ...
remote: Enumerating objects: 4857, done.
remote: Counting objects: 100% (17/17), done.
remote: Compressing objects: 100% (13/13), done.
remote: Total 4857 (delta 5), reused 11 (delta 4), pack-reused 4840 (from 1)
Receiving objects: 100% (4857/4857), 2.43 MiB | 1.10 MiB/s, done.
Resolving deltas: 100% (2342/2342), done.
```

**Рис. 3:** Клонирование репозитория DVWA

```
(root@etanribergenov)-[/var/www/html/DVWA/config]
# cd /var/www/html

(root@etanribergenov)-[/var/www/html]
# mv DVWA dvwa

(root@etanribergenov)-[/var/www/html]
# chmod -R 777 dvwa
```

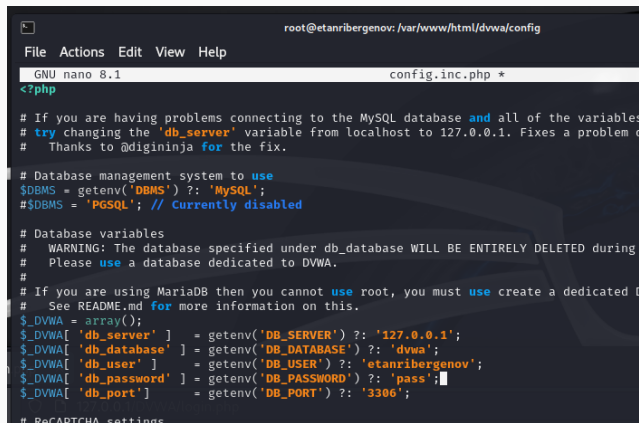
Рис. 4: Изменение имени и прав директории

```
(root@etanribergenov)-[/var/www/html]
# cd DVWA/config

(root@etanribergenov)-[/var/www/html/DVWA/config]
# cp config.inc.php.dist config.inc.php

(root@etanribergenov)-[/var/www/html/DVWA/config]
# nano config.inc.php
```

Рис. 5: Редактирование конфиг. файла



```
root@etanribergenov: /var/www/html/dvwa/config
File Actions Edit View Help
GNU nano 8.1 config.inc.php *
<?php

# If you are having problems connecting to the MySQL database and all of the variables
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem d
# 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 ENTIRELY DELETED during
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated D
# 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') ?: 'etanribergenov';
$_DVWA[ 'db_password' ] = getenv('DB_PASSWORD') ?: 'pass';
$_DVWA[ 'db_port' ] = getenv('DB_PORT') ?: '3306';

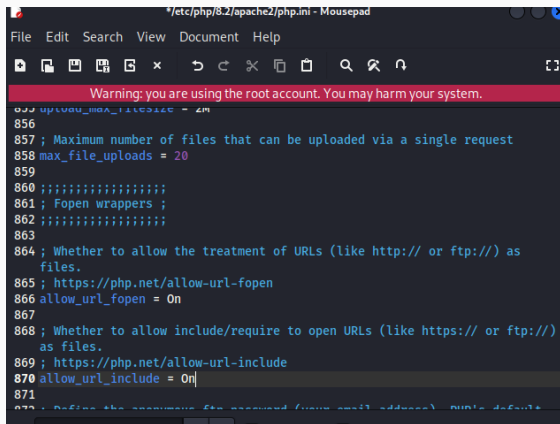
# ReCAPTCHA settings
```

**Рис. 6:** Редактирование конфиг. файла: задание имени и пароля пользователя

```
(root@etanribergenov)-[/var/www/html/DVWA/config]
# cd /etc/php/8.2/apache2

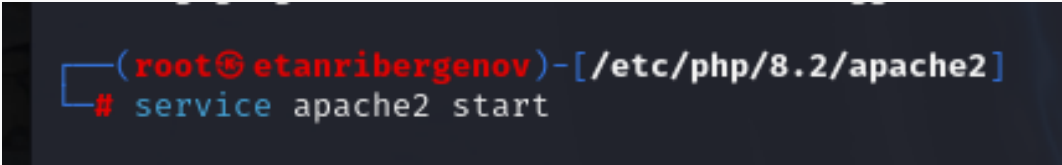
(root@etanribergenov)-[/etc/php/8.2/apache2]
# mousepad php.ini
```

Рис. 7: Конфигурирование apache2



```
*/etc/php/8.2/apache2/php.ini - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.
856
857 ; Maximum number of files that can be uploaded via a single request
858 max_file_uploads = 20
859
860 ;;;;;;;;;;;;;;;;;
861 ; Fopen wrappers ;
862 ;;;;;;;;;;;;;;;;;
863
864 ; Whether to allow the treatment of URLs (like http:// or ftp://) as
    files.
865 ; https://php.net/allow-url-fopen
866 allow_url_fopen = On
867
868 ; Whether to allow include/require to open URLs (like https:// or ftp://)
    as files.
869 ; https://php.net/allow-url-include
870 allow_url_include = On|
871
872 ; Define the anonymous ftp password (your email address). Define default
```

**Рис. 8:** Конфигурирование apache2



```
(root@etanribergenov)-[/etc/php/8.2/apache2]  
# service apache2 start
```

**Рис. 9:** Запуск apache2



```
(root@etanribergenov)-[/var/www/html/dvwa/config]
# service mysql start

(root@etanribergenov)-[/var/www/html/dvwa/config]
# systemctl status mysql
● mariadb.service - MariaDB 11.4.2 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
   Active: active (running) since Mon 2024-11-18 08:29:57 MSK; 14s ago
     Invocation: adbf9338834bc3bd3ecb30c7069555
       Docs: man:mariadb(8)
             https://mariadb.com/kb/en/library/systemd/
   Process: 103425 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, stat>
   Process: 103427 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, sta>
   Process: 103429 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || VAR=`cd /usr/bin/..;>
   Process: 103512 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, st>
   Process: 103514 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
 Main PID: 103490 (mariabdd)
   Status: "Taking your SQL requests now..."
    Tasks: 14 (limit: 62286)
  Memory: 239.7M (peak: 244.4M)
    CPU: 2.046s
   CGroup: /system.slice/mariadb.service
           └─103490 /usr/sbin/mariabdd
```

Рис. 10: Проверка запуска apache2



A terminal window showing a user at a root prompt in a directory `/var/www/html/dvwa/config`. The user runs the command `# mysql -u root -p`. The terminal displays the MySQL monitor welcome message, connection ID 31, and server version 11.4.2-MariaDB-4 Debian n/a. It then shows the command `create user 'etanribergenov'@'127.0.0.1' identified by 'pass';` being executed successfully. The prompt returns to `MariaDB [(none)]>`.

```
(root@etanribergenov) [/var/www/html/dvwa/config]
# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.4.2-MariaDB-4 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

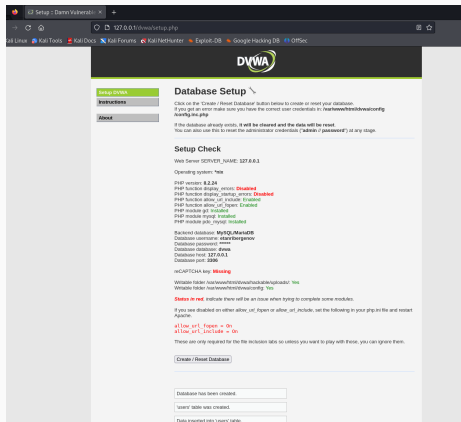
MariaDB [(none)]> create user 'etanribergenov'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.008 sec)

MariaDB [(none)]> 
```

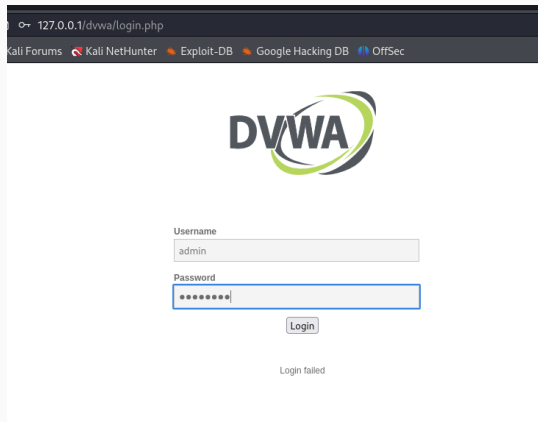
**Рис. 11:** Создание пользователя в базе данных

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'etanribergenov'@'127.0.0.1' identified by 'pass';  
Query OK, 0 rows affected (0.007 sec)  
  
MariaDB [(none)]> █
```

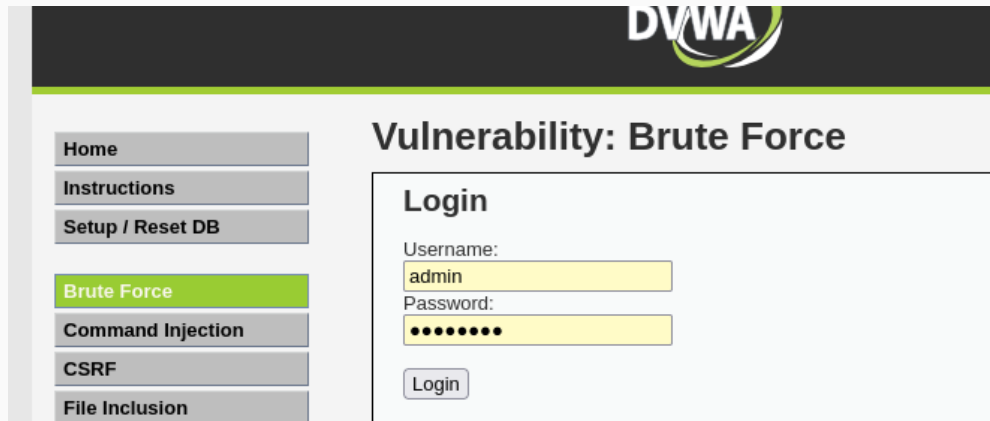
**Рис. 12:** Предоставление пользователю всех привелегий



**Рис. 13:** Открытие DVWA в браузере, создание/сброс базы данных



**Рис. 14:** Вход от имени admin



The screenshot shows the DVWA web application interface. At the top, there is a dark header with the DVWA logo. Below the header, on the left, is a sidebar with a list of navigation links: Home, Instructions, Setup / Reset DB, Brute Force (highlighted in green), Command Injection, CSRF, and File Inclusion. The main content area is titled "Vulnerability: Brute Force". Below this title, there is a "Login" section. It contains two input fields: "Username:" with the value "admin" and "Password:" with masked characters (dots). Below the password field is a "Login" button.

**DVWA**

Home  
Instructions  
Setup / Reset DB  
**Brute Force**  
Command Injection  
CSRF  
File Inclusion

## Vulnerability: Brute Force

### Login

Username:

Password:

Login

**Рис. 15:** Проверка brute force

Instructions

Setup / Reset DB

**Brute Force**

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

.....


## Login

Username:

Password:

Login

Welcome to the password protected area **admin**



## More Information

**Рис. 16:** Проверка brute force: результат

Home

Instructions

Setup / Reset DB

Brute Force

**Command Injection**

CSRF

File Inclusion

File Upload

## Vulnerability: Command Injection

### Ping a device

Enter an IP address:

PING 93.171.221.0 (93.171.221.0) 56(84) bytes of data.

--- 93.171.221.0 ping statistics ---

4 packets transmitted, 0 received, 100% packet loss, time 3059ms

**Рис. 17:** Проверка командной вставки



## **Вывод**

---

В результате выполнения работы я ознакомился с дистрибутивом Kali Linux, установив его на виртуальную машину VirtualBox.