

# Презентация по выполнению индивидуального проекта №2

Основы информационной безопасности

---

Курилко-Рюмин Е.М

22 марта 2025

Российский университет дружбы народов, Москва, Россия

# Информация

---

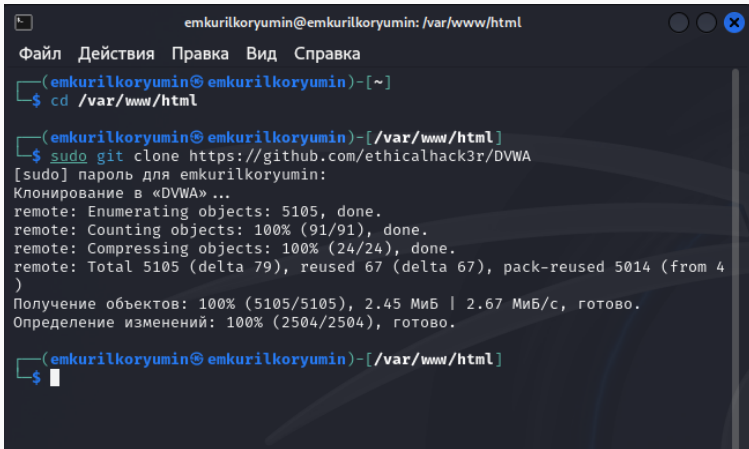
- Курилко-Рюмин Е.М
- студент группы НКАбд-02-23
- Российский университет дружбы народов

Приобретение практических навыков по установке DVWA.

# Выполнение лабораторной работы

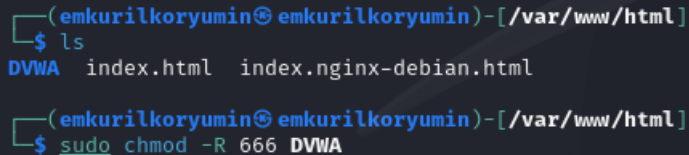
---

Настройка DVWA происходит на нашем локальном хосте, поэтому нужно перейти в директорию `/var/www/html`. Затем клонирую нужный репозиторий GitHub

A terminal window with a dark background and light text. The title bar shows the user 'emkurilkoryumin' and the current directory '/var/www/html'. The menu bar includes 'Файл', 'Действия', 'Правка', 'Вид', and 'Справка'. The terminal shows the user navigating to '/var/www/html' and cloning the 'DVWA' repository from GitHub. The output shows progress for enumerating, counting, and compressing objects, and finally the total size and reuse statistics.

```
emkurilkoryumin@emkurilkoryumin: /var/www/html
Файл Действия Правка Вид Справка
(emkurilkoryumin@emkurilkoryumin)-[~]
$ cd /var/www/html
(emkurilkoryumin@emkurilkoryumin)-[/var/www/html]
$ sudo git clone https://github.com/ethicalhack3r/DVWA
[sudo] пароль для emkurilkoryumin:
Клонирование в «DVWA» ...
remote: Enumerating objects: 5105, done.
remote: Counting objects: 100% (91/91), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 5105 (delta 79), reused 67 (delta 67), pack-reused 5014 (from 4)
Получение объектов: 100% (5105/5105), 2.45 МиБ | 2.67 МиБ/с, готово.
Определение изменений: 100% (2504/2504), готово.
(emkurilkoryumin@emkurilkoryumin)-[/var/www/html]
$
```

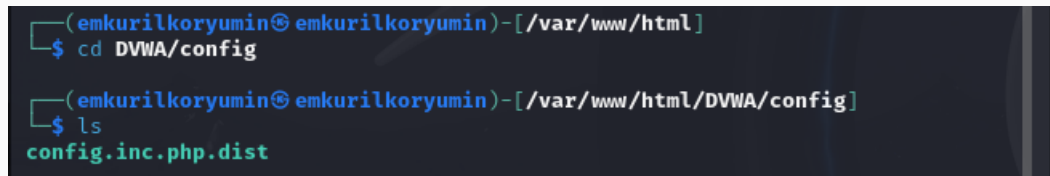
Повышаю права доступа к этой папке до 777

A terminal window with a dark background. The prompt is (emkurilkoryumin@emkurilkoryumin)-[/var/www/html]. The first command is \$ ls, which outputs DVWA index.html index.nginx-debian.html. The second command is \$ sudo chmod -R 666 DVWA.

```
(emkurilkoryumin@emkurilkoryumin)-[/var/www/html]  
$ ls  
DVWA index.html index.nginx-debian.html  
  
(emkurilkoryumin@emkurilkoryumin)-[/var/www/html]  
$ sudo chmod -R 666 DVWA
```

Рис. 2: Изменение прав доступа

Чтобы настроить DVWA, нужно перейти в каталог `/dvwa/config`

A terminal window with a dark background and light-colored text. The prompt is `(emkurilkoryumin@emkurilkoryumin)-[/var/www/html]`. The first command is `$ cd DVWA/config`. The prompt changes to `(emkurilkoryumin@emkurilkoryumin)-[/var/www/html/DVWA/config]`. The second command is `$ ls`, and the output is `config.inc.php.dist` in green text.

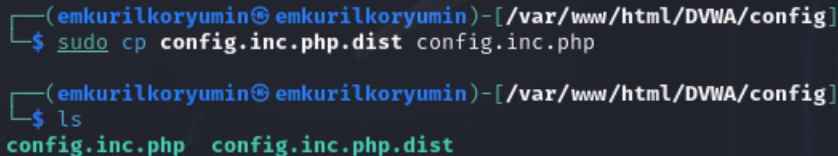
```
(emkurilkoryumin@emkurilkoryumin)-[/var/www/html]
$ cd DVWA/config

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

Рис. 3: Перемещение по директориям



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

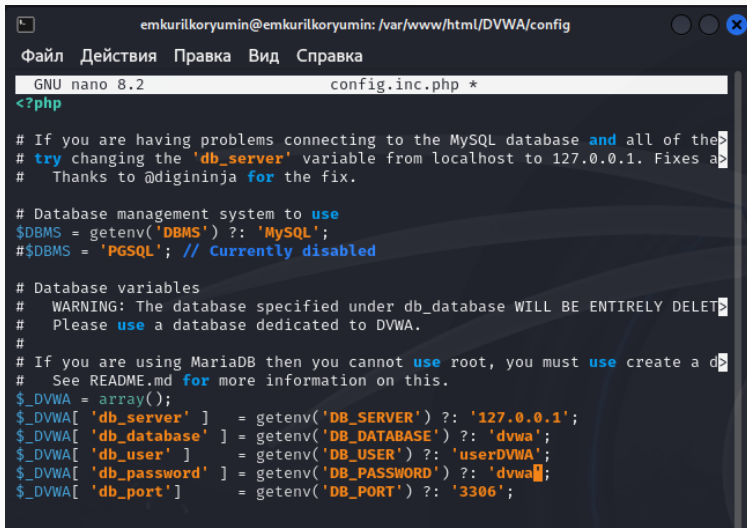
A terminal window with a dark background and light-colored text. The prompt is `(emkurilkoryumin@emkurilkoryumin)-[/var/www/html/DVWA/config]`. The first command is `$ sudo cp config.inc.php.dist config.inc.php`. The second command is `$ ls`, followed by the output `config.inc.php config.inc.php.dist`.

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

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

Рис. 4: Создание копии файла

## Изменяю данные об имени пользователя и пароле



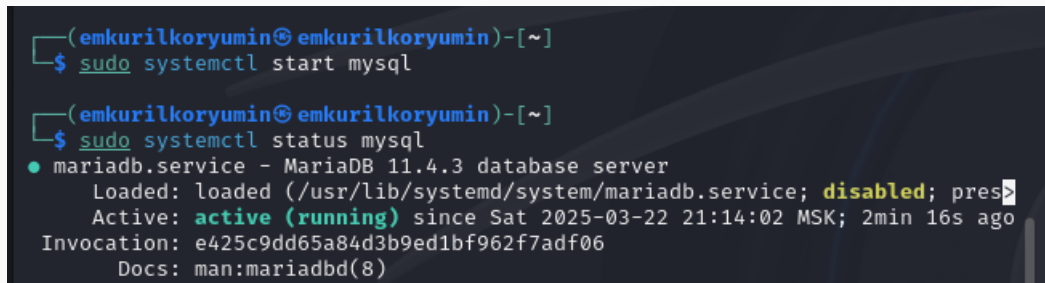
```
emkurilkoryumin@emkurilkoryumin: /var/www/html/DVWA/config
Файл Действия Правка Вид Справка
GNU nano 8.2 config.inc.php *
<?php

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

## Запускаю mysql

A terminal window with a dark background and light-colored text. The prompt is (emkurilkoryumin@emkurilkoryumin)-[~]. The first command is \$ sudo systemctl start mysql. The second command is \$ sudo systemctl status mysql. The output shows the status of the mariadb.service, which is loaded, disabled, and pres> (truncated). It is active (running) since Sat 2025-03-22 21:14:02 MSK; 2min 16s ago. The invocation ID is e425c9dd65a84d3b9ed1bf962f7adf06 and the docs are man:mariadb(8).

```
(emkurilkoryumin@emkurilkoryumin)-[~]  
$ sudo systemctl start mysql  
  
(emkurilkoryumin@emkurilkoryumin)-[~]  
$ sudo systemctl status mysql  
● mariadb.service - MariaDB 11.4.3 database server  
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; pres>  
   Active: active (running) since Sat 2025-03-22 21:14:02 MSK; 2min 16s ago  
 Invocation: e425c9dd65a84d3b9ed1bf962f7adf06  
    Docs: man:mariadb(8)
```

Рис. 6: Запуск mysql

## 2.2

Авторизируюсь в базе данных от имени пользователя root. Создаем нового пользователя, используя учетные данные из файла config.inc.php

```
(emkurilkoryumin@emkurilkoryumin)-[~]
$ sudo mysql -u root -p
[sudo] пароль для emkurilkoryumin:
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.4.3-MariaDB-1 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 'userDVWA'@'127.0.0.1' identified by "dvwa";
Query OK, 0 rows affected (0,005 sec)
```

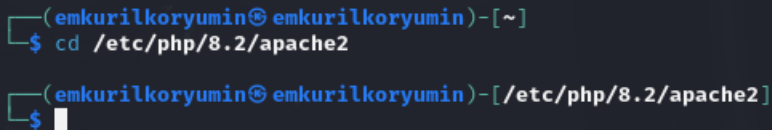
Теперь нужно пользователю предоставить привилегии для работы с этой базой данных

```
MariaDB [(none)]> create user 'userDVWA'@'127.0.0.1' identified by "dvwa";  
Query OK, 0 rows affected (0,005 sec)
```

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

Рис. 8: Изменение прав

Необходимо настроить сервер apache2, перехожу в соответствующую директорию

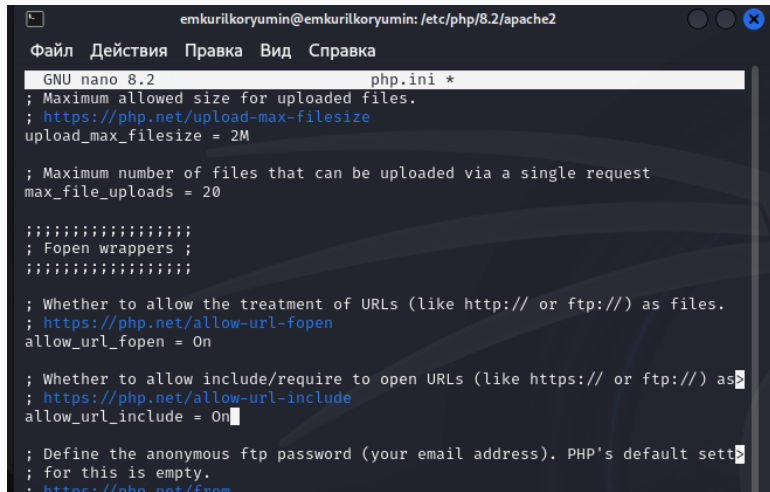
A terminal window with a dark background and light blue text. The prompt is (emkurilkoryumin@emkurilkoryumin)-[~]. The first command is \$ cd /etc/php/8.2/apache2. The second prompt is (emkurilkoryumin@emkurilkoryumin)-[/etc/php/8.2/apache2] followed by a dollar sign and a cursor.

```
(emkurilkoryumin@emkurilkoryumin)-[~]  
$ cd /etc/php/8.2/apache2  
  
(emkurilkoryumin@emkurilkoryumin)-[/etc/php/8.2/apache2]  
$
```

Рис. 9: Перемещение между директориями

## 3.2

В файле параметры `allow_url_fopen` и `allow_url_include` должны быть поставлены как `On`



```
emkurilkoryumin@emkurilkoryumin: /etc/php/8.2/apache2
Файл Действия Правка Вид Справка
GNU nano 8.2 php.ini *
; Maximum allowed size for uploaded files.
; https://php.net/upload-max-filesize
upload_max_filesize = 2M

; Maximum number of files that can be uploaded via a single request
max_file_uploads = 20

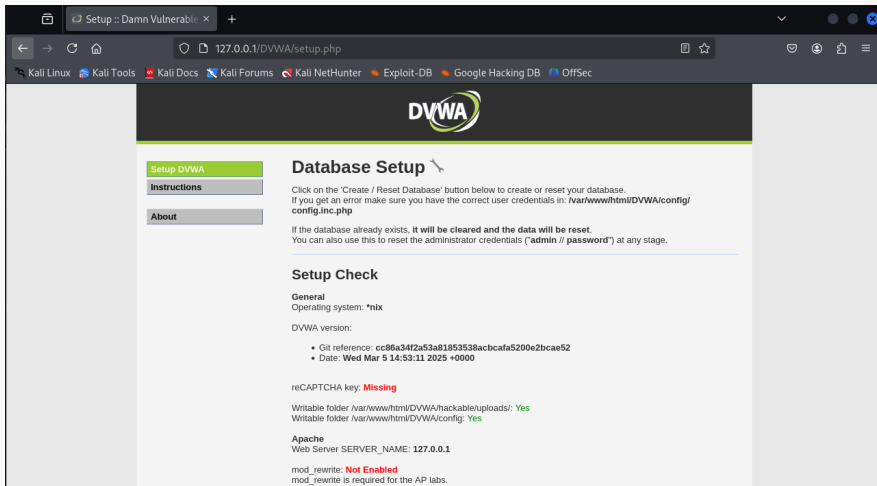
;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;

; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like https:// or ftp://) as
; https://php.net/allow-url-include
allow_url_include = On

; Define the anonymous ftp password (your email address). PHP's default sett
; for this is empty.
; https://php.net/from
```

Мы настроили DVWA, Apache и базу данных, поэтому открываем браузер и запускаем веб-приложение, введя 127.0.0/DVWA





Прокручиваем страницу вниз и нажимаем на кнопку `create\reset database`

```
allow_url_fopen = On  
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Create / Reset Database

---

**Рис. 12:** “Создание базы данных”

## 4.3

Авторизуюсь с помощью предложенных по умолчанию данных

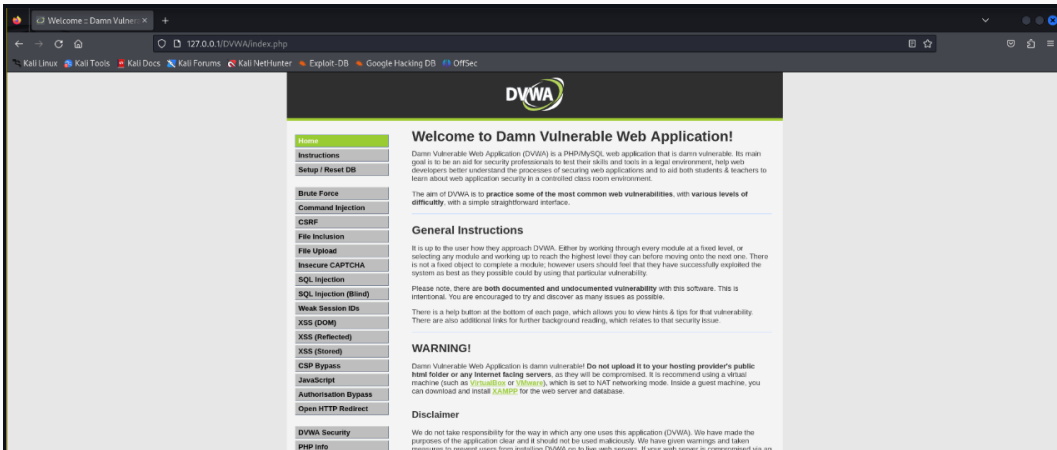


The DVWA logo features the text "DVWA" in a bold, dark blue font. To the right of the text is a stylized circular graphic composed of two curved, overlapping lines: a light green one on the outside and a dark blue one on the inside, creating a sense of motion or a sphere.

Username

Password

## Оказываюсь на домашней странице веб-приложения, на этом установка окончена



The screenshot shows a web browser window with the address bar displaying `127.0.0.1/DVWA/index.php`. The browser's bookmark bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The DVWA homepage features a dark header with the DVWA logo. A left sidebar contains a menu with the following items: Home (highlighted), Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, Authorisation Bypass, Open HTTP Redirect, DVWA Security, and PHP Info. The main content area has a heading "Welcome to Damn Vulnerable Web Application!" followed by a paragraph describing DVWA as a PHP/MySQL web application for learning web security. Below this is a section titled "General Instructions" with three paragraphs of advice for users. A "WARNING!" section follows, warning against uploading the application to public servers. Finally, a "Disclaimer" section states that the application is provided as-is and the user assumes all responsibility.

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with various levels of difficulty, with a simple straightforward interface.

### General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

### WARNING!

Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing servers, as they will be compromised. It is recommended using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.

### Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If any web server is compromised via an

Приобрел практические навыки по установке уязвимого веб-приложения DVWA.

**Спасибо за внимание**

---

