

# **Индивидуальный проект**

**Этап 2**

Казазаев Даниил Михайлович

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>3</b>	<b>Выводы</b>	<b>12</b>

# Список иллюстраций

2.1	Клонирование репозитория . . . . .	6
2.2	Перенос директории . . . . .	6
2.3	Проверка . . . . .	6
2.4	Запуск apache2 . . . . .	7
2.5	Сайт с адресом localhost . . . . .	7
2.6	Преход на https://localhost/DVWA . . . . .	7
2.7	Копирование конфиг файла . . . . .	7
2.8	Обновленная страница . . . . .	8
2.9	Кнопка создания базы данных . . . . .	8
2.10	Запуск . . . . .	8
2.11	Настройка MySQL . . . . .	9
2.12	Настройка MySQL . . . . .	9
2.13	Проверка работы . . . . .	9
2.14	Обновленная страница . . . . .	10
2.15	Главная страница . . . . .	11

## **Список таблиц**

# 1 Цель работы

Установить DVWA.

## 2 Выполнение лабораторной работы

После запуска системы клонирую репозиторий DVWA. (рис. 2.1).

```
(dmkazazaev@vbox)-[~]
$ sudo git clone https://github.com/digininja/DVWA.git
[sudo] пароль для dmkazazaev:
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), 2.49 МиБ | 62.00 КиБ/с, готово.
Определение изменений: 100% (2489/2489), готово.
```

Рис. 2.1: Клонирование репозитория

Переношу директорию DVWA в /var/www/html/. (рис. 2.2).

```
(dmkazazaev@vbox)-[~]
$ sudo mv DVWA /var/www/html
```

Рис. 2.2: Перенос директории

Проверяю, перенеслась ли директория. (рис. 2.3).

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

Рис. 2.3: Проверка

Запускаю apache2, чтобы сайт заработал. (рис. 2.4).

```
(dmkazazaev@vbox)-[/var/www/html]
$ sudo service apache2 start
```

Рис. 2.4: Запуск apache2

Захожу на <https://localhost/>, чтобы убедиться в том, что наши файлы работают, и попадаю на сайт Apache2 (рис. 2.5).

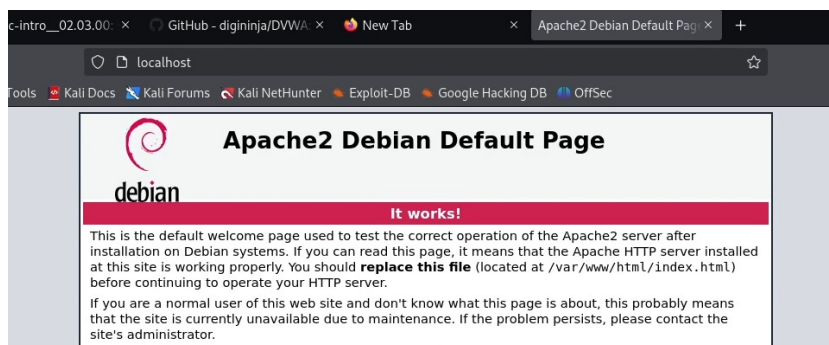


Рис. 2.5: Сайт с адресом localhost

Преходу на страницу <https://localhost/DVWA/>, чтобы убедиться, что файлы DVWA работают. (рис. 2.6).

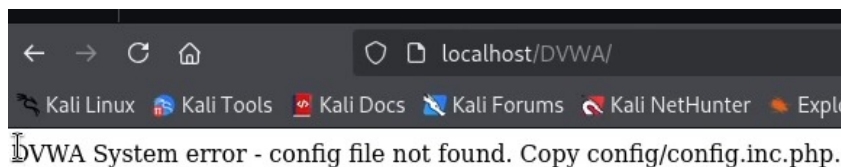


Рис. 2.6: Преход на <https://localhost/DVWA/>

На открывшейся вкладке меня настойчиво попросили отредактировать формат config файла, чтобы его настройки вступили в силу.

Копирую config файл, меняя его формат. (рис. 2.7).

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

Рис. 2.7: Копирование конфиг файла

После обновления страницы, попадаю на дальнейшие указания по установке DVWA. (рис. 2.8).

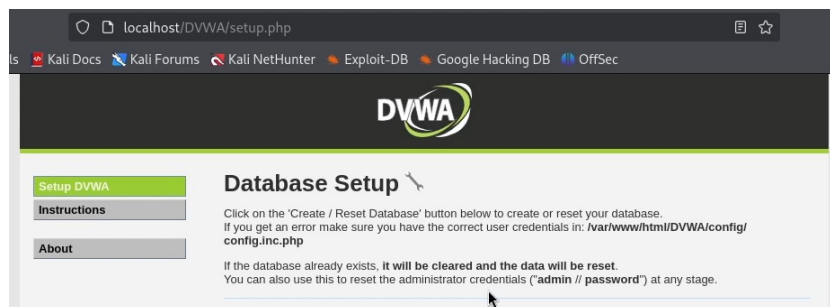


Рис. 2.8: Обновленная страница

Спускаюсь в самый низ страницы и жму кнопку создания базы данных. (рис. 2.9).

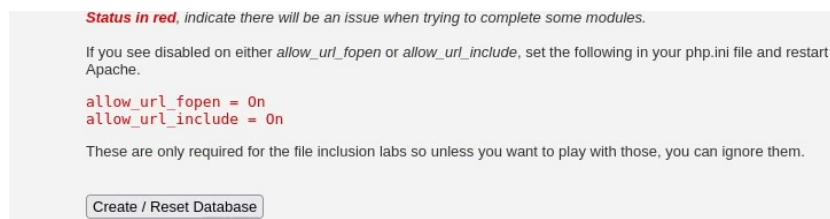


Рис. 2.9: Кнопка создания базы данных

База данных не создается.

Запускаю базу данных и настраиваю MySQL, который предустановлен в ОС Kali. Устанавливаю логин, пароль и права на базу данных. (рис. 2.10).

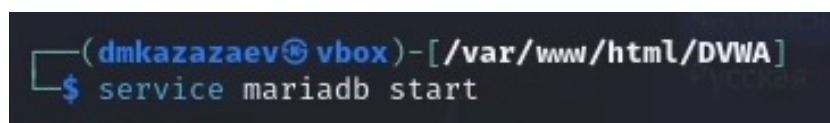


Рис. 2.10: Запуск



```
(root@vbox)-[~]
mysql
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 database dvwa;
Query OK, 1 row affected (0,001 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0,005 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost
→
```

Рис. 2.11: Настройка MySQL

```
MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0,002 sec)
```

Рис. 2.12: Настройка MySQL

После настройки проверяю, работают ли установленные логин и пароль. (рис. 2.13).

```
(dmkazazaev@vbox)-[~]
$ mysql -u dvwa -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 33
Server version: 11.4.3-MariaDB-1 Debian n/a
```

Рис. 2.13: Проверка работы

Захожу на сайт еще раз, где меня просят войти в аккаунт. (рис. 2.14).



**Username**


**Password**

Login

Login failed

Рис. 2.14: Обновленная страница

После захода в аккаунт попадаю на главную страницу DVWA. (рис. 2.15).



Home

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

Cryptography

API

DVWA Security

## 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 vulnerabilities** 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 recommend 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 your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

Рис. 2.15: Главная страница

## **3 Выводы**

При выполнении этого этапа индивидуального проекта мы установили DVWA.