

Индивидуальный проект. Этап 2

Основы информационной безопасности

Казаев Д. М.

Российский университет дружбы народов, Москва, Россия

Информация

- Казазаев Даниил Михайлович
- Студент бакалавриата
- Российский университет дружбы народов
- [1132231427@rudn.ru]
- <https://github.com/KazazaevDaniil>

Вводная часть

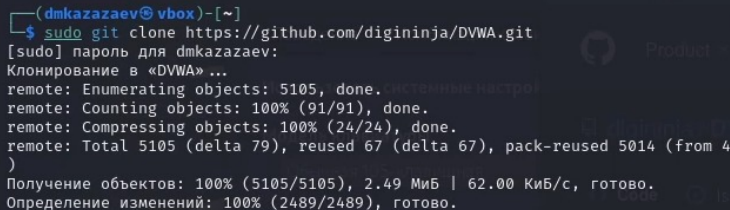
Установка ОС Kali Linux

Для выполнения лабораторной работы мы воспользуемся виртуальной машиной Oracle VM Virtual Box. Индивидуальный проект выполняется на домашнем оборудовании.

- Этапы работы
- 1. Установка DVWA

Выполнение индивидуального
проекта.

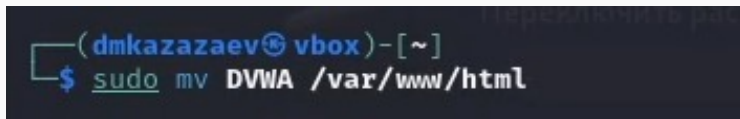
После запуска сисетмы клонирую репозиторий DVWA. (рис. 1).

A terminal window with a dark background and light-colored text. The prompt is '(dmkazazaev@vbox)-[~]'. The user enters the command 'sudo git clone https://github.com/digininja/DVWA.git'. The terminal shows the password prompt '[sudo] пароль для dmkazazaev:', the cloning progress 'Клонирование в «DVWA» ...', and the completion status 'Получение объектов: 100% (5105/5105), 2.49 МиБ | 62.00 КиБ/с, готово. Определение изменений: 100% (2489/2489), готово.'

```
(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. 1: Клонирование репозитория

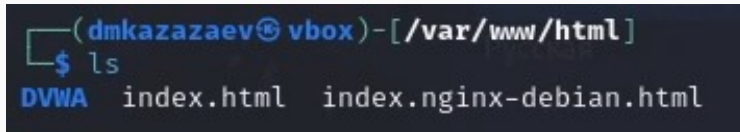
Переношу директорию DVWA в /var/www/html/. (рис. 2).

A terminal window with a dark background. The prompt shows the user 'dmkazazaev' on a 'vbox' machine in the home directory. The command 'sudo mv DVWA /var/www/html' is entered and highlighted in green.

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

Рис. 2: Перенос дирекции

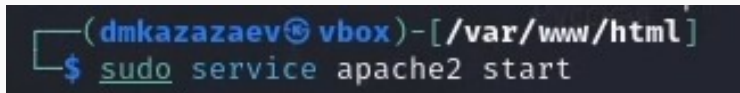
Проверяю, перенеслась ли директория. (рис. 3).

A terminal window with a dark background. The prompt is `(dmkazazaev@vbox) - [/var/www/html]`. The user enters `$ ls`. The output is `DVWA index.html index.nginx-debian.html`.

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

Рис. 3: Проверка

Запускаю apache2, чтобы сайт заработал. (рис. 4).

A terminal window with a dark background. The prompt is '(dmkazazaev@vbox)-[/var/www/html]'. The command '\$ sudo service apache2 start' is entered. The word 'sudo' is underlined.

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

Рис. 4: Запуск apache2

Выполнение индивидуального проекта.

Захожу на `https://localhost/`, чтобы убедиться в том, что наши файлы работают, и попадаю на сайт Apache2 (рис. 5).

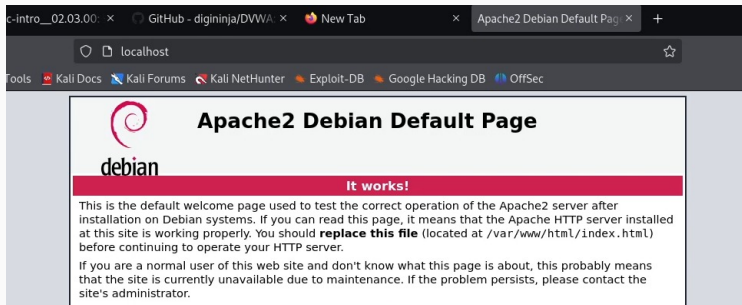


Рис. 5: Сайт с адресом localhost

Преходу на страницу <https://localhost/DVWA/>, чтобы убедиться, что файлы DVWA работают. (рис. 6).

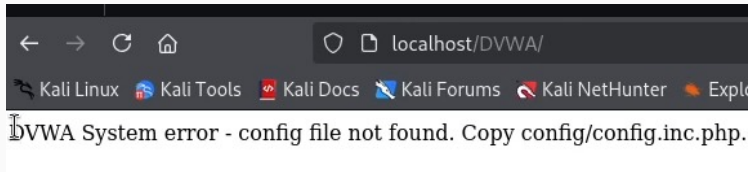



Рис. 6: Преход на https://localhost/DVWA

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

Копирую config файл, меняя его формат. (рис. 7).

A terminal window with a dark background. The prompt is `(dmkazazaev@vbox)-[/var/www/html/DVWA/config]`. The command entered is `$ sudo cp config.inc.php.dist config.inc.php`.

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

Рис. 7: Копирование конфиг файла

После обновления страницы, попадаю на дальнейшие указания по установке DVWA. (рис. 8).

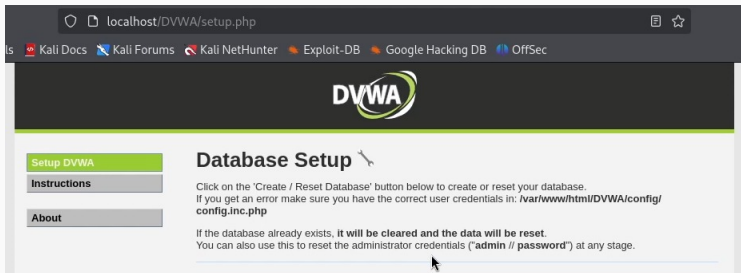


Рис. 8: Обновленная страница

Спускаюсь в самый низ страницы и жму кнопку создания базы данных. (рис. 9).

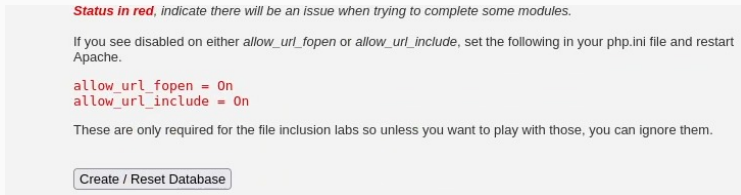
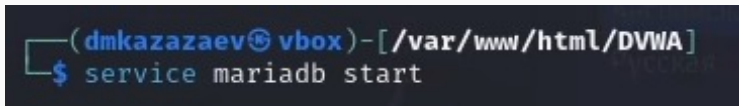


Рис. 9: Кнопка создания базы данных

База данных не создается.

Запускаю базу данных и настраиваю MySQL, который предустановлен в ОС Kali. Устанавливаю логин, пароль и права на базу данных. (рис. 10).

A terminal window with a dark background. The prompt is `(dmkazazaev@vbox) - [/var/www/html/DVWA]`. The command `$ service mariadb start` is entered and highlighted in blue.

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

Рис. 10: Запуск

Выполнение индивидуального проекта.

```
(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. 11: Настройка MySQL

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

Рис. 12: Настройка MySQL

После настройки проверяю, работают ли установленные логин и пароль. (рис. 13).

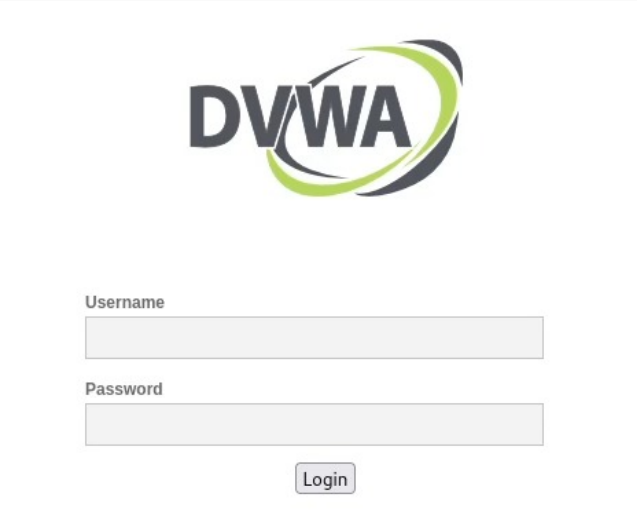
A terminal window with a dark background. The prompt is '(dmkazazaev@vbox)-[~]'. The user enters '\$ mysql -u dvwa -p'. The prompt changes to 'Enter password:'. The user enters a password (not visible). The terminal displays the following text: 'Welcome to the MariaDB monitor. Commands end with ; or \g.', 'Your MariaDB connection id is 33', and 'Server version: 11.4.3-MariaDB-1 Debian n/a'.

```
(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. 13: Проверка работы

Выполнение индивидуального проекта.

Захожу на сайт еще раз, где меня просят войти в аккаунт. (рис. 14).



The image shows a login form for DVWA (Damn Vulnerable Web Application). At the top center is the DVWA logo, which consists of the letters "DVWA" in a bold, dark grey font, with a stylized green and dark grey swoosh graphic to the right. Below the logo, there are two input fields. The first is labeled "Username" in a bold, dark grey font, and the second is labeled "Password" in a bold, dark grey font. Both labels are positioned to the left of their respective input fields. Below the password field is a "Login" button with a rounded rectangular shape and a light grey background.

DVWA


Username

Password

Login

Выполнение индивидуального проекта.

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

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

Выводы

При выполнении этого этапа индивидуального проекта мы установили ОС Kali Linux.