

# **Отчет по первому этапу индивидуального проекта**

**Основы информационной безопасности**

Дворкина Ева, НКАбд-01-22

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>7</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>9</b>
<b>5</b>	<b>Выводы</b>	<b>17</b>
	<b>Список литературы</b>	<b>18</b>

## Список иллюстраций

4.1	Клонирование репозитория . . . . .	9
4.2	Изменение прав доступа . . . . .	9
4.3	Перемещение по директориям . . . . .	10
4.4	Создание копии файла . . . . .	10
4.5	Открытие файла в редакторе . . . . .	10
4.6	Редактирование файл . . . . .	11
4.7	Запуск mysql . . . . .	11
4.8	Авторизация в базе данных . . . . .	12
4.9	Изменение прав . . . . .	12
4.10	Перемещение между директориями . . . . .	12
4.11	Открытие файла в текстовом редакторе . . . . .	13
4.12	Редактирование файла . . . . .	13
4.13	Запуск arche . . . . .	14
4.14	Запуск веб-приложения . . . . .	14
4.15	“Создание базы данных” . . . . .	15
4.16	Авторизация . . . . .	15
4.17	Домашняя страница DVWA . . . . .	16

## **Список таблиц**

# 1 Цель работы

Приобретение практических навыков по установке DVWA.

## 2 Задание

1. Установить DVWA на дистрибутив Kali Linux.

### 3 Теоретическое введение

DVWA - это уязвимое веб-приложение, разработанное на PHP и MySQL.

Некоторые из уязвимостей веб приложений, который содержит DVWA: - Брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования инструментов по атаке на пароль методом грубой силы и показывает небезопасность слабых паролей. - Исполнение (внедрение) команд: Выполнение команд уровня операционной системы. - Межсайтовая подделка запроса (CSRF): Позволяет «атакующему» изменить пароль администратора приложений. - Внедрение (инклюд) файлов: Позволяет «атакующему» присоединить удалённые/локальные файлы в веб приложение. - SQL внедрение: Позволяет «атакующему» внедрить SQL выражения в HTTP из поля ввода, DVWA включает слепое и основанное на ошибке SQL внедрение. - Небезопасная выгрузка файлов: Позволяет «атакующему» выгрузить вредоносные файлы на веб сервер. - Межсайтовый скриптинг (XSS): «Атакующий» может внедрить свои скрипты в веб приложение/базу данных. DVWA включает отражённую и хранимую XSS. - Пасхальные яйца: раскрытие полных путей, обход аутентификации и некоторые другие.

DVWA имеет четыре уровня безопасности, они меняют уровень безопасности каждого веб приложения в DVWA: - Невозможный — этот уровень должен быть безопасным от всех уязвимостей. Он используется для сравнения уязвимого исходного кода с безопасным исходным кодом. - Высокий — это расширение среднего уровня сложности, со смесью более сложных или альтернативных плохих практик в попытке обезопасить код. Уязвимости не позволяют такой простор

эксплуатации как на других уровнях. - Средний — этот уровень безопасности предназначен главным образом для того, чтобы дать пользователю пример плохих практик безопасности, где разработчик попытался сделать приложение безопасным, но потерпел неудачу. - Низкий — этот уровень безопасности совершенно уязвим и совсем не имеет защиты. Его предназначение быть примером среди уязвимых веб приложений, примером плохих практик программирования и служить платформой обучения базовым техникам эксплуатации. [2]



## 4 Выполнение лабораторной работы

Настройка DVWA происходит на нашем локальном хосте, поэтому нужно перейти в директорию `/var/www/html`. Затем клонирую нужный репозиторий GitHub (рис. 1).

```
(evdvorkina@evdvorkina)-[~]
$ cd /var/www/html

(evdvorkina@evdvorkina)-[/var/www/html]
$ sudo git clone https://github.com/ethicalhack3r/DVWA
[sudo] password for evdvorkina:
Cloning into 'DVWA' ...
remote: Enumerating objects: 4500, done.
remote: Counting objects: 100% (50/50), done.
remote: Compressing objects: 100% (39/39), done.
remote: Total 4500 (delta 17), reused 33 (delta 10), pack-reused 4450
Receiving objects: 100% (4500/4500), 2.30 MiB | 6.03 MiB/s, done.
Resolving deltas: 100% (2112/2112), done.
```

Рис. 4.1: Клонирование репозитория

Проверяю, что файлы скопировались правильно, далее повышаю права доступа к этой папке до 777 (рис. 2.)

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

(evdvorkina@evdvorkina)-[/var/www/html]
$ sudo chmod -R 777 DVWA
```

Рис. 4.2: Изменение прав доступа

Чтобы настроить DVWA, нужно перейти в каталог `/dvwa/config`, затем проверить содержимое каталога (рис. 3)

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

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

Рис. 4.3: Перемещение по директориям

Создаем копию файла, используемого для настройки DVWA `config.inc.php.dist` с именем `config.inc.php`. Копируем файл, а не изменяем его, чтобы у нас был запасной вариант, если что-то пойдет не так (рис. 4)

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

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

Рис. 4.4: Создание копии файла

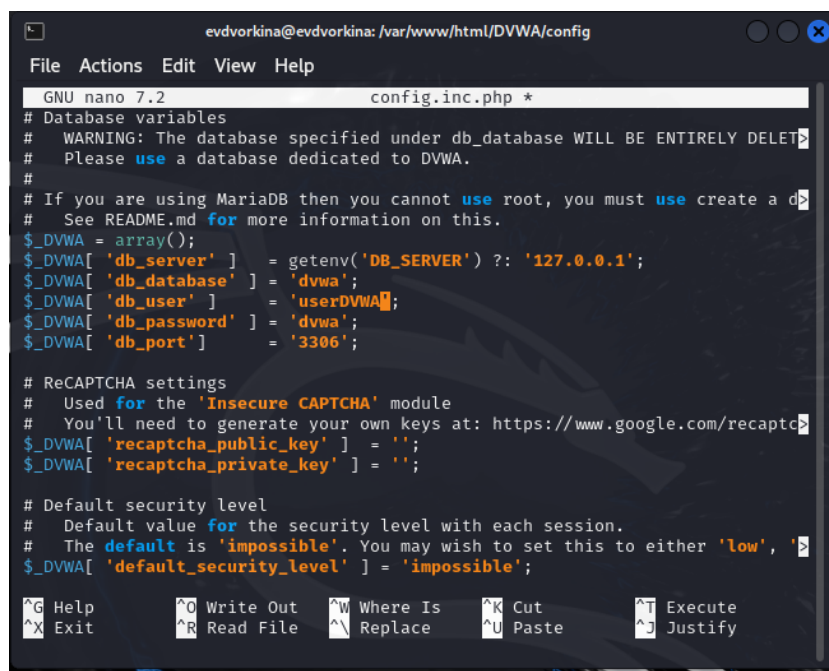
Далее открываю файл в текстовом редакторе (рис. 5)

```
(evdvorkina@evdvorkina)-[/var/www/html/DVWA/config]
$ sudo nano config.inc.php

(evdvorkina@evdvorkina)-[/var/www/html/DVWA/config]
$ █
```

Рис. 4.5: Открытие файла в редакторе

Изменяю данные об имени пользователя и пароле (рис. 6)



```
evdvorkina@evdvorkina: /var/www/html/DVWA/config
File Actions Edit View Help
GNU nano 7.2 config.inc.php *
# 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' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'userDVWA';
$_DVWA[ 'db_password' ] = 'dvwa';
$_DVWA[ 'db_port' ] = '3306';

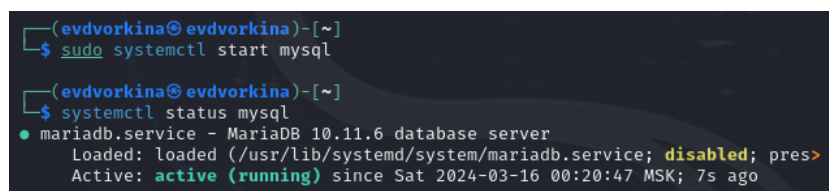
# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptcha
$_DVWA[ 'recaptcha_public_key' ] = '';
$_DVWA[ 'recaptcha_private_key' ] = '';

# Default security level
# Default value for the security level with each session.
# The default is 'impossible'. You may wish to set this to either 'low', 'medium', or 'high'
$_DVWA[ 'default_security_level' ] = 'impossible';

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^_ Replace    ^U Paste      ^J Justify
```

Рис. 4.6: Редактирование файла

По умолчанию в Kali Linux установлен mysql, поэтому можно его запустить без предварительного скачивания, далее выполняю проверку, запущен ли процесс (рис. 7)



```
(evdvorkina@evdvorkina)-[~]
$ sudo systemctl start mysql

(evdvorkina@evdvorkina)-[~]
$ systemctl status mysql
● mariadb.service - MariaDB 10.11.6 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; pres>
   Active: active (running) since Sat 2024-03-16 00:20:47 MSK; 7s ago
```

Рис. 4.7: Запуск mysql

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 (рис. 8)

```
(evdvorkina@evdvorkina)-[~]
$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.6-MariaDB-2 Debian n/a

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

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 (0.010 sec)
```

Рис. 4.8: Авторизация в базе данных

Теперь нужно пользователю предоставить привилегии для работы с этой базой данных (рис. 9)

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1' identified by 'dvwa';
Query OK, 0 rows affected (0.006 sec)

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

Рис. 4.9: Изменение прав

Необходимо настроить сервер apache2, перехожу в соответствующую директорию (рис. 10)

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

(evdvorkina@evdvorkina)-[/etc/php/8.2/apache2]
$
```

Рис. 4.10: Перемещение между директориями

В файле `php.ini` нужно будет изменить один параметр, поэтому открываю файл в текстовом редакторе (рис. 11)

```
(evdvorkina@evdvorkina)-[/etc/php/8.2/apache2]
$ sudo nano php.ini

(evdvorkina@evdvorkina)-[/etc/php/8.2/apache2]
$
```

Рис. 4.11: Открытие файла в текстовом редакторе

В файле параметры `allow_url_fopen` и `allow_url_include` должны быть поставлены как `On` (рис. 12)

```
evdvorkina@evdvorkina: /etc/php/8.2/apache2
File Actions Edit View Help
GNU nano 7.2 php.ini *
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 files.
; https://php.net/allow-url-include
allow_url_include = On

; Define the anonymous ftp password (your email address). PHP's default setting
; for this is empty.
; https://php.net/from
;from="john@doe.com"

; Define the User-Agent string. PHP's default setting for this is empty.
; https://php.net/user-agent
user_agent="PHP"
```

Рис. 4.12: Редактирование файла

Запускаем службу веб-сервера `apache` и проверяем, запущена ли служба (рис. 13)

```
(evdvorkina@evdvorkina)-[/etc/php/8.2/apache2]
$ sudo systemctl start apache2

(evdvorkina@evdvorkina)-[/etc/php/8.2/apache2]
$ systemctl status start apache2
Unit start.service could not be found.
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Sat 2024-03-16 00:31:47 MSK; 11s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 11911 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 11927 (apache2)
      Tasks: 6 (limit: 4611)
     Memory: 23.8M (peak: 24.1M)
        CPU: 101ms
    CGroup: /system.slice/apache2.service
            └─11927 /usr/sbin/apache2 -k start
              11930 /usr/sbin/apache2 -k start
              11931 /usr/sbin/apache2 -k start
              11932 /usr/sbin/apache2 -k start
              11933 /usr/sbin/apache2 -k start
              11934 /usr/sbin/apache2 -k start

Mar 16 00:31:47 evdvorkina systemd[1]: Starting apache2.service - The Apache HTTP Server...
Mar 16 00:31:47 evdvorkina systemd[1]: Started apache2.service - The Apache HTTP Server.

(evdvorkina@evdvorkina)-[/etc/php/8.2/apache2]
```

Рис. 4.13: Запуск apache

Мы настроили DVWA, Apache и базу данных, поэтому открываем браузер и запускаем веб-приложение, введя 127.0.0/DVWA (рис. 14)

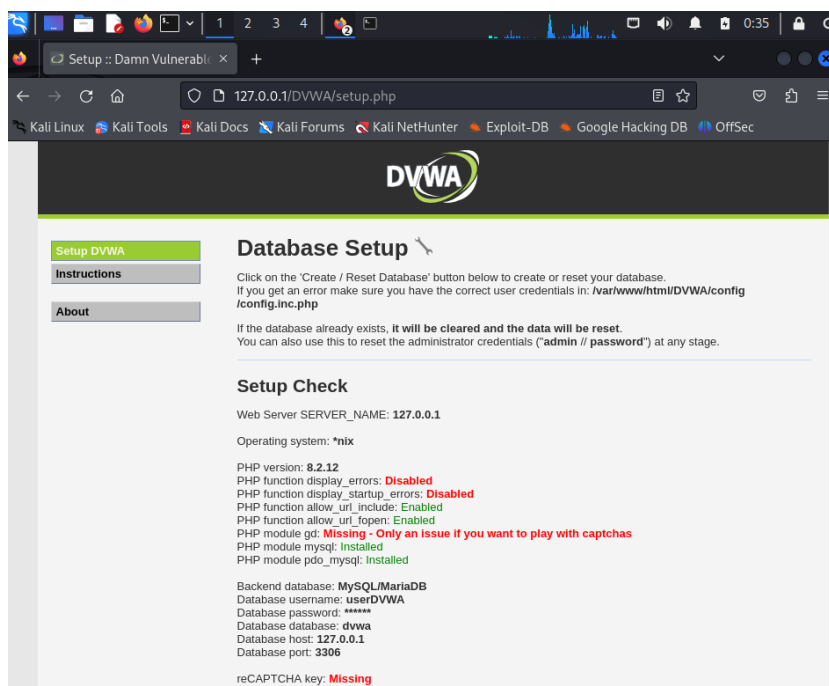


Рис. 4.14: Запуск веб-приложения

Прокручиваем страницу вниз и нажмем на кнопку create\reset database

(рис. 15)

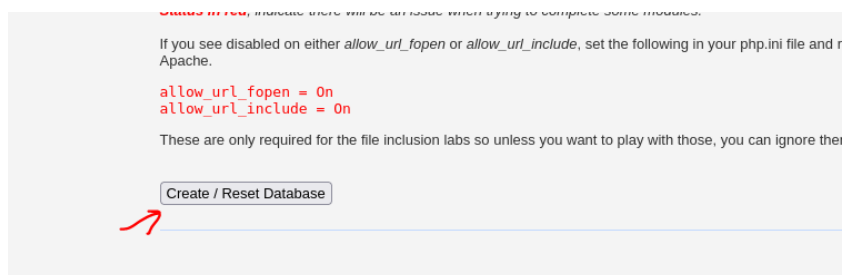


Рис. 4.15: “Создание базы данных”

Авторизуюсь с помощью предложенных по умолчанию данных (рис. 16)

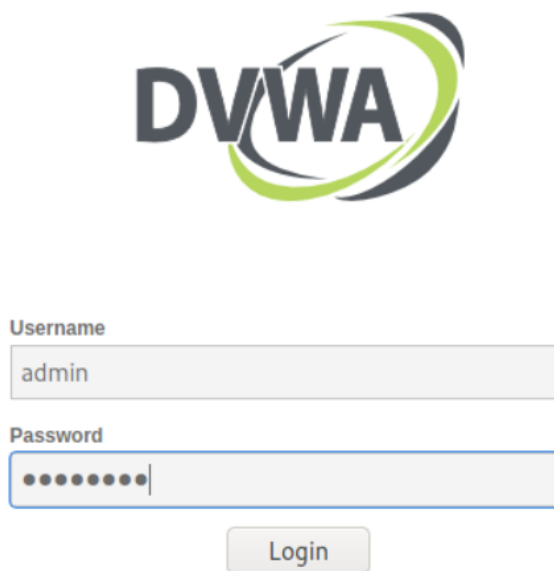


Рис. 4.16: Авторизация

Оказываюсь на домашней странице веб-приложения, на этом установка окончена (рис. 17)

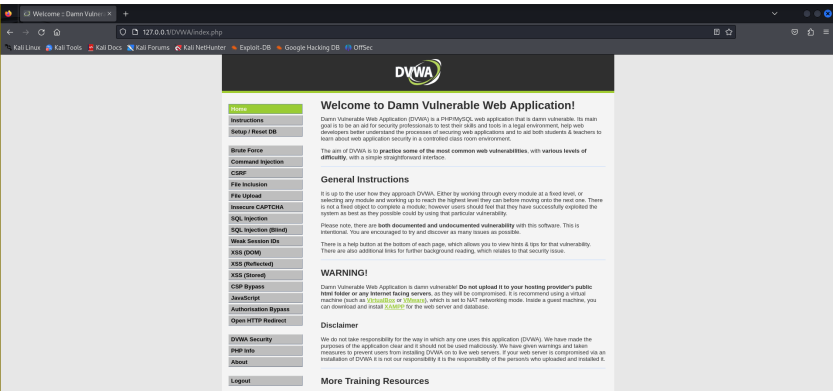


Рис. 4.17: Домашняя страница DVWA



## 5 Выводы

Приобрела практические навыки по установке уязвимого веб-приложения DVWA.

## Список литературы

1. How to install DVWA on Kali-Linux for pentesting practice [Электронный ресурс]. 2021. URL: <http://nooblinux.com/how-to-install-dvwa/>.
2. Ш. Парасрам Т.Х.и.др. А. Замм. Kali Linux: Тестирование на проникновение и безопасность: для профессионалов. Питер, 2022. 448 с.