

Отчет по второму этапу индивидуального проекта

Основы информационной безопасности

Курилко-Рюмин Е.М, НКАбд-02-23

Содержание

| | | |
|----------|---------------------------------------|-----------|
| 1 | Цель работы | 5 |
| 2 | Задание | 6 |
| 3 | Теоретическое введение | 7 |
| 4 | Выполнение лабораторной работы | 9 |
| 5 | Выводы | 18 |

Список иллюстраций

| | | |
|------|--|----|
| 4.1 | Клонирование репозитория | 9 |
| 4.2 | Изменение прав доступа | 10 |
| 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 | 15 |
| 4.15 | “Создание базы данных” | 15 |
| 4.16 | Авторизация | 16 |
| 4.17 | Домашняя страница DVWA | 17 |

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.

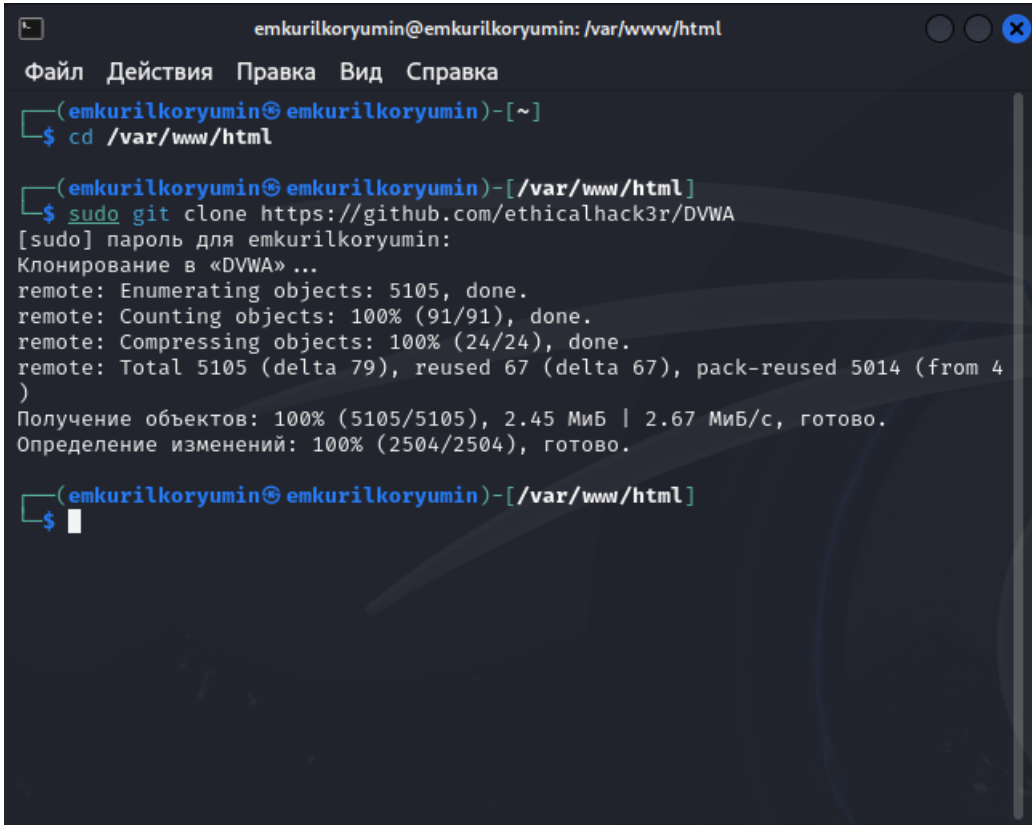
Некоторые из уязвимостей веб приложений, который содержит DVWA: - Брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования инструментов по атаке на пароль методом грубой силы и показывает небезопасность слабых паролей. - Исполнение (внедрение) команд: Выполнение команд уровня операционной 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 пред-

назначен 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. [parasram?]

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)

A screenshot of a terminal window with a dark background. The title bar at the top reads "emkurilkoryumin@emkurilkoryumin: /var/www/html". Below the title bar is a menu bar with "Файл", "Действия", "Правка", "Вид", and "Справка". The terminal shows the following commands and output:

```
(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]  
$
```

Рис. 4.1: Клонирование репозитория

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

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

(emkurilkoryumin@emkurilkoryumin)-[/var/www/html]
$ sudo chmod -R 666 DVWA
```

Рис. 4.2: Изменение прав доступа

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

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

(emkurilkoryumin@emkurilkoryumin)-[/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)

```
(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. 4.4: Создание копии файла

Далее открываю файл в текстовом редакторе (рис.5)

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

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

Рис. 4.5: Открытие файла в редакторе

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

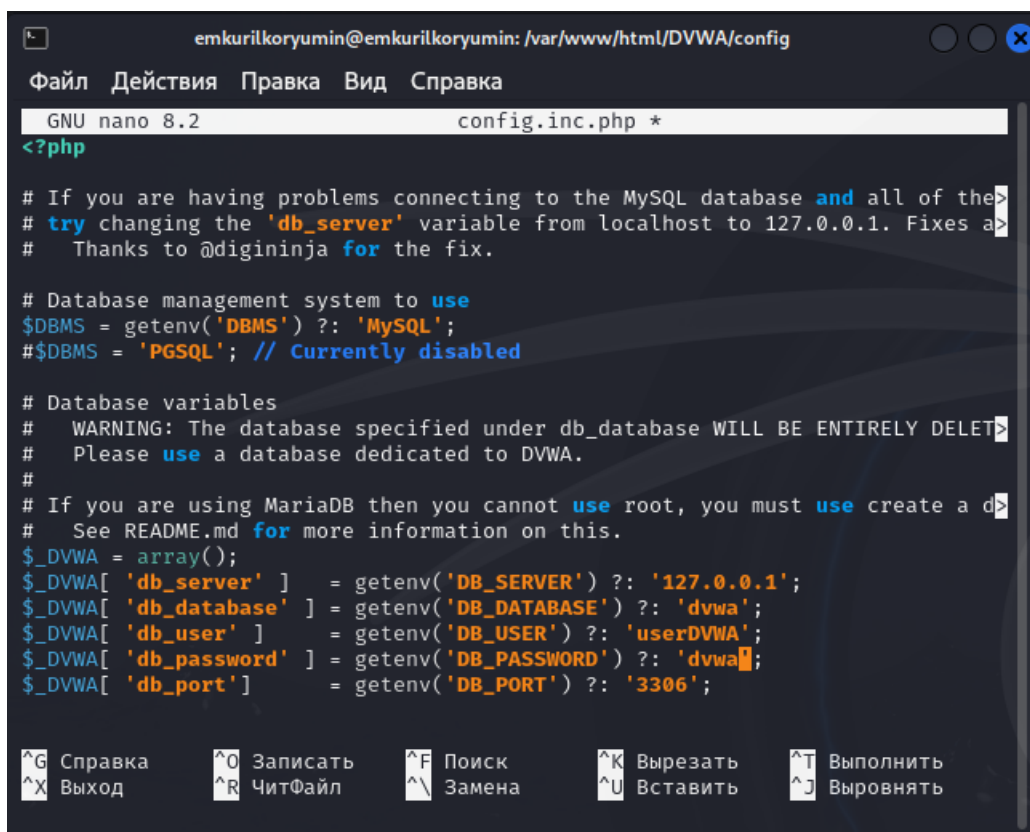


Рис. 4.6: Редактирование файл

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

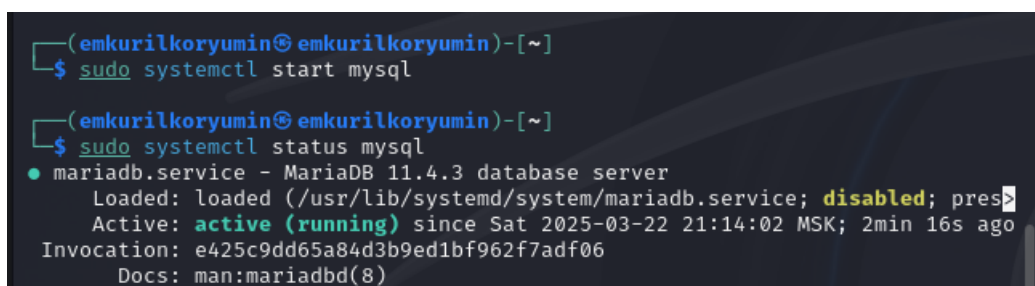


Рис. 4.7: Запуск mysql

Авторизуюсь 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)

```
(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)

MariaDB [(none)]> █
```

Рис. 4.8: Авторизация в базе данных

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

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

MariaDB [(none)]> exit
Bye

(emkurilkoryumin@emkurilkoryumin)-[~]
```

Рис. 4.9: Изменение прав

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

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

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

Рис. 4.10: Перемещение между директориями

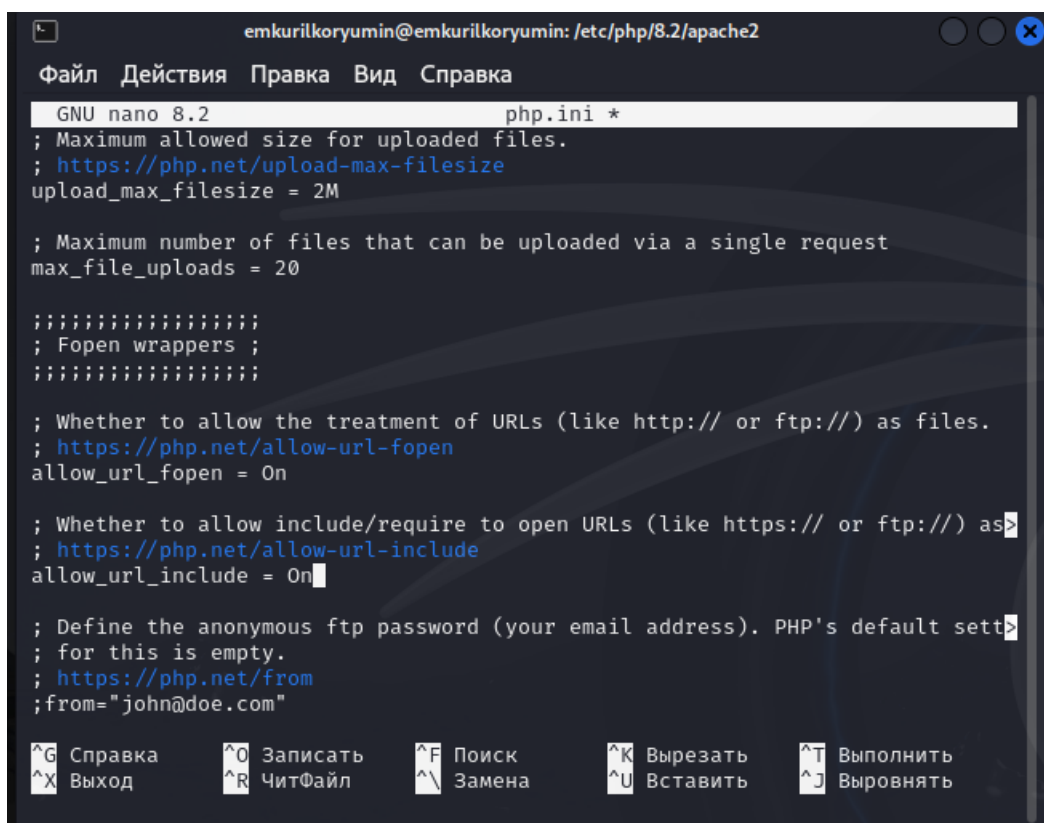
В файле `php.ini` нужно будет изменить один параметр, поэтому открываю файл в текстовом редакторе (рис.11)

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

(emkurilkoryumin@emkurilkoryumin)-[/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)



```
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
;from="john@doe.com"

^G Справка      ^O Записать     ^F Поиск       ^K Вырезать    ^T Выполнить
^X Выход        ^R ЧитФайл    ^\ Замена     ^U Вставить    ^J Выровнять
```

Рис. 4.12: Редактирование файла

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

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

(emkurilkoryumin@emkurilkoryumin)-[/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; pres>
   Active: active (running) since Sat 2025-03-22 21:25:24 MSK; 23s ago
 Invocation: 2b043cb51e4f4226bfa96f3cd6df7def
    Docs: https://httpd.apache.org/docs/2.4/
  Process: 14654 ExecStart=/usr/sbin/apachectl start (code=exited, status=>
 Main PID: 14670 (apache2)
    Tasks: 6 (limit: 4557)
  Memory: 20.2M (peak: 20.3M)
     CPU: 194ms
   CGroup: /system.slice/apache2.service
           └─14670 /usr/sbin/apache2 -k start
             └─14673 /usr/sbin/apache2 -k start
               └─14674 /usr/sbin/apache2 -k start
                 └─14675 /usr/sbin/apache2 -k start
                   └─14676 /usr/sbin/apache2 -k start
                     └─14677 /usr/sbin/apache2 -k start

map 22 21:25:24 emkurilkoryumin systemd[1]: Starting apache2.service - The A>
map 22 21:25:24 emkurilkoryumin systemd[1]: Started apache2.service - The Ap>
lines 1-21/21 (END)
```

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)

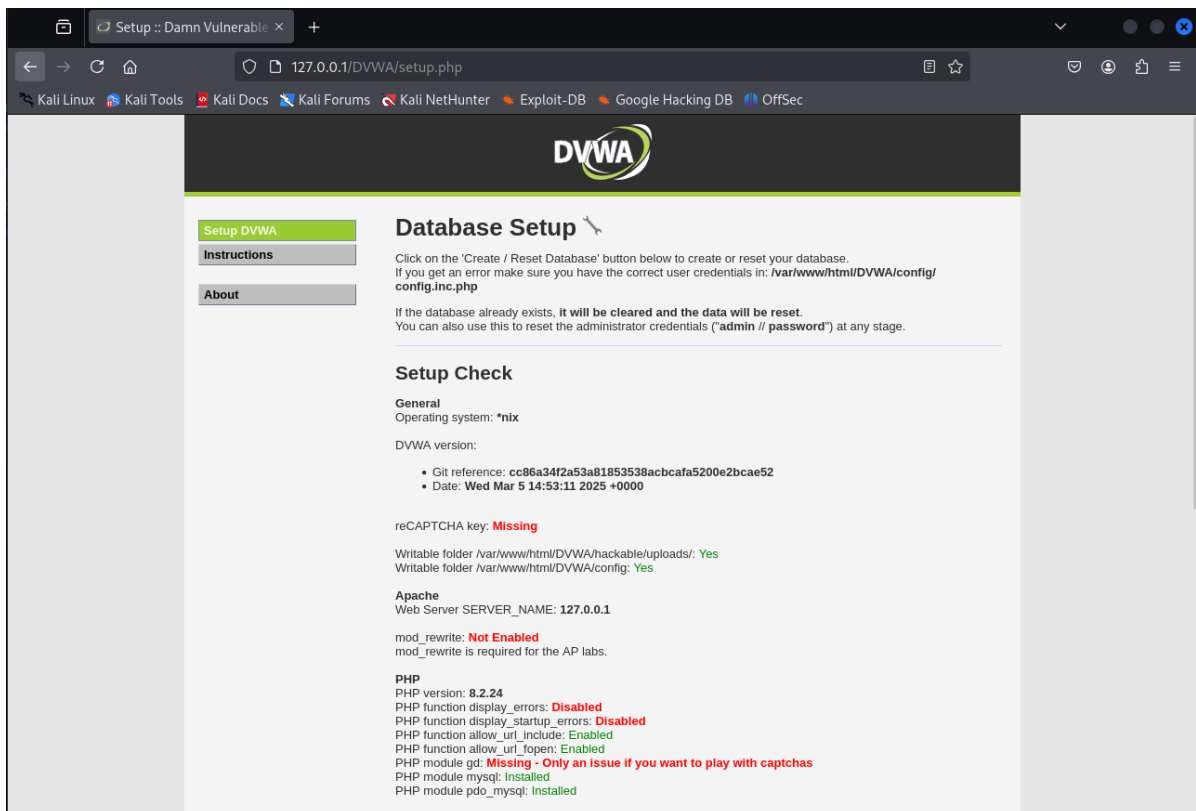


Рис. 4.14: Запуск веб-приложения

Прокручиваем страницу вниз и нажимаем на кнопку create\reset database (рис.15)

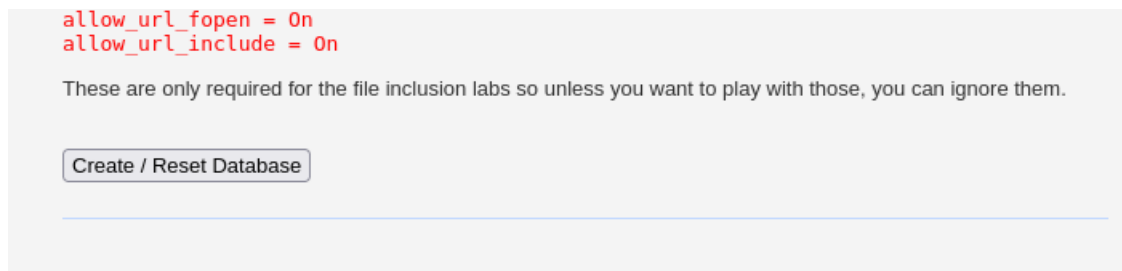


Рис. 4.15: “Создание базы данных”

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

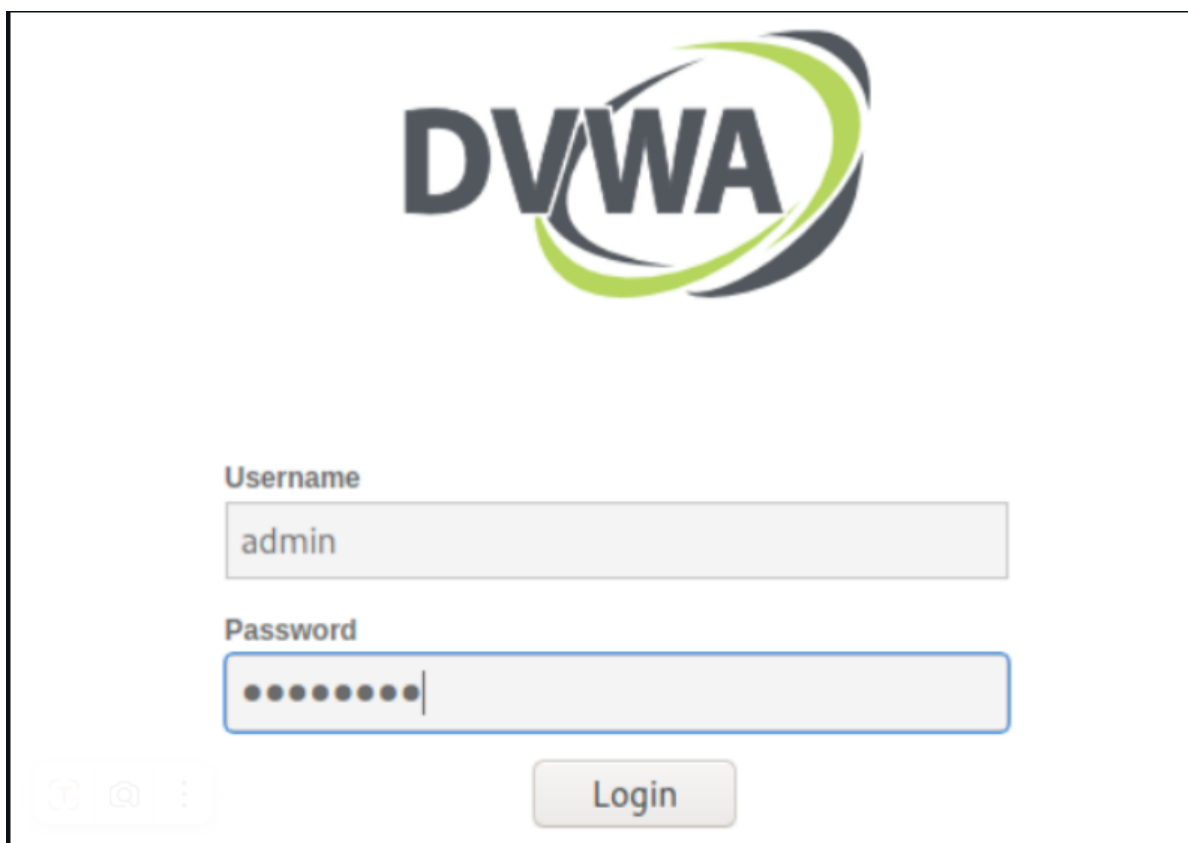
The image shows the DVWA (Damn Vulnerable Web Application) login interface. At the top center is the DVWA logo, which consists of the letters 'DVWA' in a bold, dark blue font, with a stylized green and blue swoosh graphic to the right. Below the logo, there are two input fields. The first is labeled 'Username' and contains the text 'admin'. The second is labeled 'Password' and contains ten black dots, indicating a masked password. Below the password field is a 'Login' button. In the bottom left corner, there are three small, faint icons: a Twitter bird, a camera, and a vertical ellipsis.

Рис. 4.16: Авторизация

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

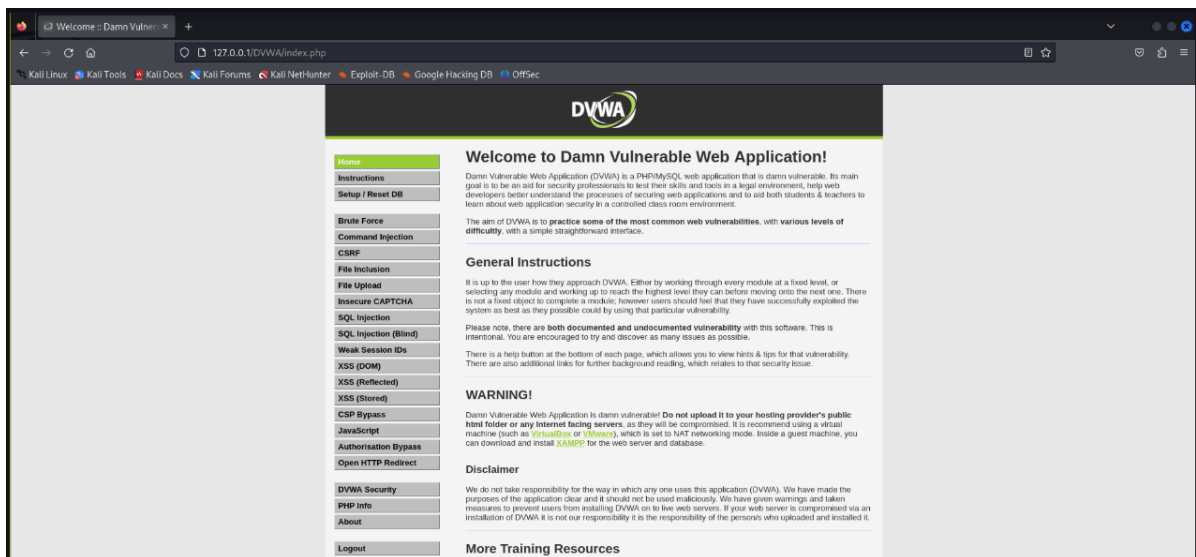


Рис. 4.17: Домашняя страница DVWA

5 Выводы

Приобрел практические навыки по установке уязвимого веб-приложения DVWA.

...