

# **Индивидуальный проект - Этап 2**

**Основы информационной безопасности**

Оразгелдиев Язгелди

# 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>14</b>

## Список иллюстраций

4.1	Клонирование репозитория . . . . .	9
4.2	Изменение прав доступа . . . . .	9
4.3	Открытие файла в редакторе . . . . .	10
4.4	Запуск mysql . . . . .	10
4.5	Изменение прав . . . . .	11
4.6	Перемещение между директориями . . . . .	11
4.7	Редактирование файла . . . . .	12
4.8	Запуск apache . . . . .	12
4.9	Домашняя страница DVWA . . . . .	13

## 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).

```
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 | 4.37 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.)

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

(yazgeldi@kali)-[/var/www/html]
$ DVWA

(yazgeldi@kali)-[/var/www/html/DVWA]
$ cd

(yazgeldi@kali)-[~]
$ cd /var/www/html

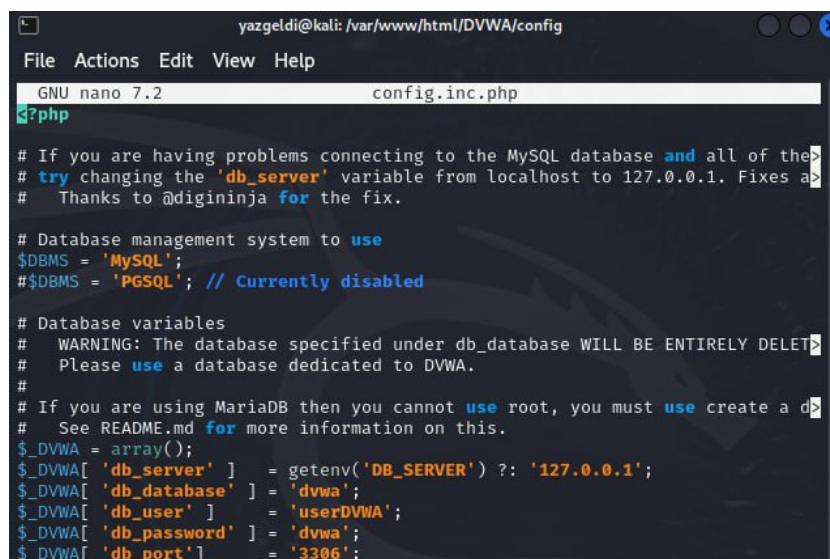
(yazgeldi@kali)-[/var/www/html]
$ sudo chmod -R 777 DVWA
```

Рис. 4.2: Изменение прав доступа

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

Далее открываю файл в текстовом редакторе



```
yazgeldi@kali: /var/www/html/DVWA/config
File Actions Edit View Help
GNU nano 7.2 config.inc.php
config.inc.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.

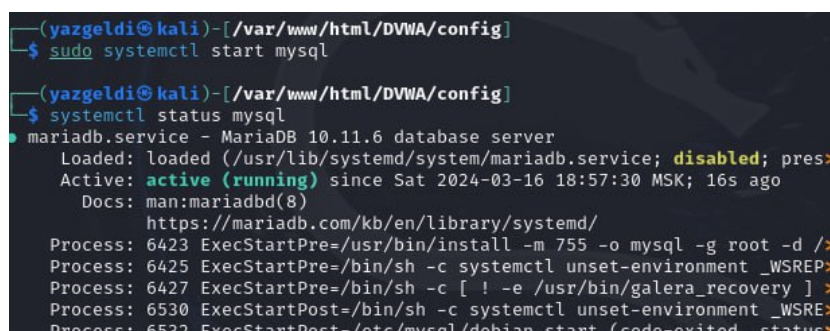
# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# 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 d
# 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';
```

Рис. 4.3: Открытие файла в редакторе

Изменяю данные об имени пользователя и пароле

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



```
(yazgeldi@kali)-[/var/www/html/DVWA/config]
$ sudo systemctl start mysql

(yazgeldi@kali)-[/var/www/html/DVWA/config]
$ 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 18:57:30 MSK; 16s ago
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
   Process: 6423 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d />
   Process: 6425 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP>
   Process: 6427 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] >
   Process: 6530 ExecStartPost=/bin/sh -c systemctl unset-environment _WSRE>
   Process: 6532 ExecStartPost=/etc/mysql/debian-start (code=exited, status>
```

Рис. 4.4: Запуск mysql

Авторизируюсь в базе данных от имени пользователя root. Появляется команд-

ная строка с приглашением “MariaDB”, далее создаем в ней нового пользователя, используя учетные данные из файла config.inc.php

Теперь нужно пользователю предоставить привилегии для работы с этой базой данных

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1' identified by 'dvwa';  
Query OK, 0 rows affected (0.020 sec)  
  
MariaDB [(none)]> █
```

Рис. 4.5: Изменение прав

Необходимо настроить сервер apache2, перехожу в соответствующую директорию

```
(yazgeldi@kali)-[~]  
$ cd /etc/php/8.2/apache2  
  
(yazgeldi@kali)-[/etc/php/8.2/apache2]  
$ █
```

Рис. 4.6: Перемещение между директориями

В файле php.ini нужно будет изменить один параметр, поэтому открываю файл в текстовом редакторе. В файле параметры allow\_url\_fopen и allow\_url\_include должны быть поставлены как On

```

;;;;;;;;;;;;;;;;
; 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"

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

```

Рис. 4.7: Редактирование файла

Запускаем службу веб-сервера apache и проверяем, запущена ли служба

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

(yazgeldi@kali)-[/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 2024-03-16 19:08:16 MSK; 17s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 11972 ExecStart=/usr/sbin/apachectl start (code=exited, status=>
   Main PID: 11996 (apache2)
     Tasks: 6 (limit: 9215)
    Memory: 19.7M (peak: 20.0M)
       CPU: 172ms
   CGroup: /system.slice/apache2.service
           └─11996 /usr/sbin/apache2 -k start
             └─11999 /usr/sbin/apache2 -k start
               └─12000 /usr/sbin/apache2 -k start
                 └─12001 /usr/sbin/apache2 -k start
                   └─12002 /usr/sbin/apache2 -k start
                     └─12003 /usr/sbin/apache2 -k start

Mar 16 19:08:15 kali systemd[1]: Starting apache2.service - The Apache HTTP >
Mar 16 19:08:16 kali systemd[1]: Started apache2.service - The Apache HTTP >
```

Рис. 4.8: Запуск apache

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

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

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

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

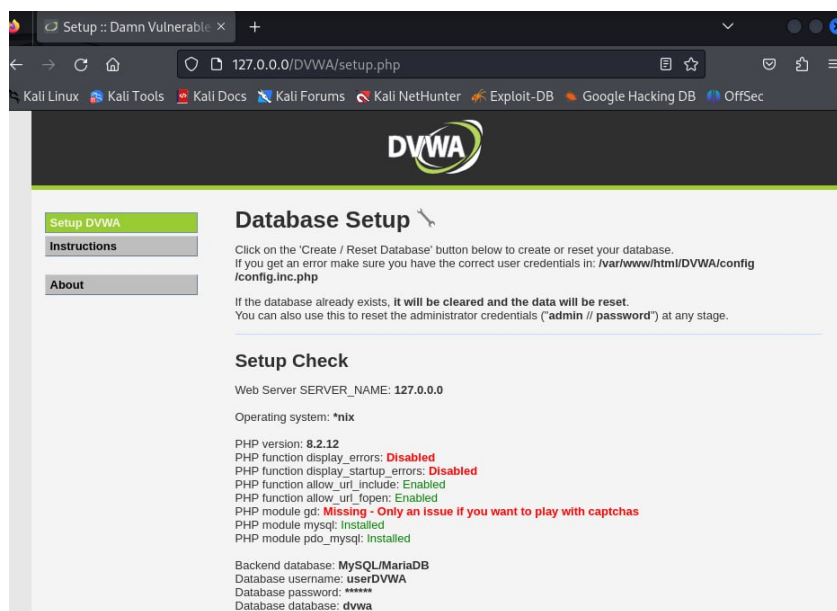


Рис. 4.9: Домашняя страница DVWA

## 5 Выводы

Приобрел практические навыки по установке уязвимого веб-приложения DVWA.