

# Отчет по второму этапу индивидуального проекта

Основы информационной безопасности

Кабанова Варвара, НПМбд02-21

## Содержание

Цель работы .....	1
Задание .....	1
Теоретическое введение .....	1
Выполнение лабораторной работы .....	2
Выводы.....	8
Список литературы.....	8

## Цель работы

Приобретение практических навыков по установке DVWA.

## Задание

1. Установить DVWA на дистрибутив Kali Linux.

## 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. [@guide, @parasram]

## Выполнение лабораторной работы

Настройка DVWA происходит на нашем локальном хосте, поэтому нужно перейти в директорию /var/www/html. Затем клонирую нужный репозиторий GitHub (рис. 1-2).

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

(kali@kali)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA
Cloning into 'DVWA' ...
remote: Enumerating objects: 4758, done.
remote: Counting objects: 100% (308/308), done.
remote: Compressing objects: 100% (178/178), done.
remote: Total 4758 (delta 164), reused 246 (delta 124), pack-reused 4450 (from 1)
Receiving objects: 100% (4758/4758), 2.39 MiB | 6.53 MiB/s, done.
Resolving deltas: 100% (2259/2259), done.
```

Проверяю, что файлы склонировались правильно, далее повышаю права доступа к этой папке до 777 (рис. 3)

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

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

### *Изменение прав доступа*

Чтобы настроить DVWA, нужно перейти в каталог /dvwa/config, затем проверяю содержимое каталога (рис. 4)

```
(kali㉿kali)-[/var/www/html]
$ cd DVWA/config

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

### *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. 5)

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

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

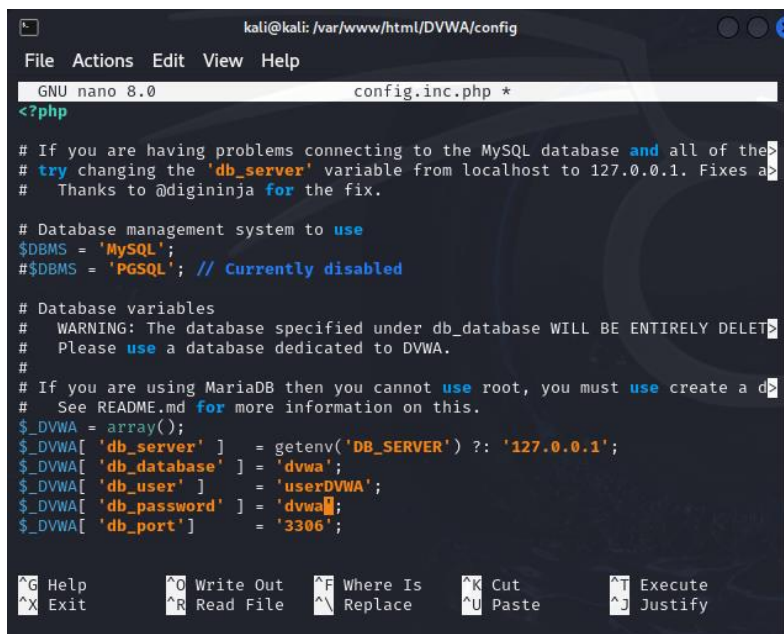
### *Создание копии файла*

Далее открываю файл в текстовом редакторе (рис. 6)

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

### *Открытие файла в редакторе*

Изменяю данные об имени пользователя и пароле (рис. 7)



```
kali@kali: /var/www/html/DVWA/config
File Actions Edit View Help
GNU nano 8.0 config.inc.php *
<?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.

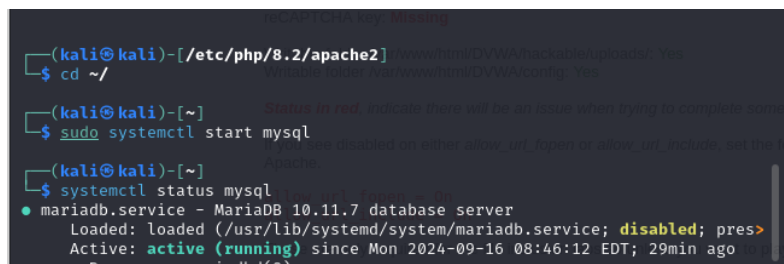
# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# 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 db
# 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';

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

## Редактирование файл

По умолчанию в Kali Linux установлен mysql, поэтому можно его запустить без предварительного скачивания, далее выполняю проверку, запущен ли процесс (рис. 8)



```
(kali@kali)-[/etc/php/8.2/apache2] $ cd ~/
(kali@kali)-[~/var/www/html/DVWA/config] $ sudo systemctl start mysql
(kali@kali)-[~/var/www/html/DVWA/config] $ systemctl status mysql
● mariadb.service - MariaDB 10.11.7 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; pres>
   Active: active (running) since Mon 2024-09-16 08:46:12 EDT; 29min ago
     Docs: man:mariadb(8)
```

## 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. 9)

```

(kali@kali)-[/var/www/html/DVWA/config]
$ 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: 10.11.7-MariaDB-4 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)]> ^C
MariaDB [(none)]> create user 'userDVWA' '@'127.0.0.1' identified by "dvwa"
→
→ ^C
MariaDB [(none)]> create user 'userDVWA' '@'127.0.0.1' identified by "dvwa";
Query OK, 0 rows affected (0.833 sec)

MariaDB [(none)]> █

```

### *Авторизация в базе данных*

Теперь нужно пользователю предоставить привилегии для работы с этой базой данных (рис. 10)

```

MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA' '@'127.0.0.1' i
identified by 'dvwa';
Query OK, 0 rows affected (0.059 sec)

MariaDB [(none)]> exit
Bye

```

### *Изменение прав*

Необходимо настроить сервер apache2, перехожу в соответствующую директорию (рис. 11)

```

(kali@kali)-[/var/www/html/DVWA/config]
$ cd /etc/php/8.2/apache2

```

### *Перемещение между директориями*

В файле php.ini нужно будет изменить один параметр, поэтому открываю файл в текстовом редакторе (рис. 12)

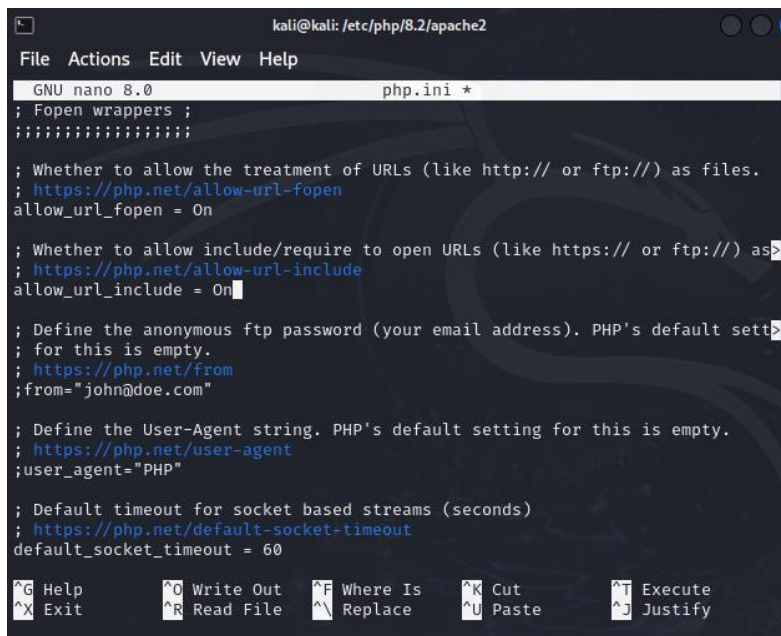
```

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

```

### *Открытие файла в текстовом редакторе*

В файле параметры allow\_url\_fopen и allow\_url\_include должны быть поставлены как On (рис. 13)



```
kali@kali: /etc/php/8.2/apache2
File Actions Edit View Help
GNU nano 8.0 php.ini *
; 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"

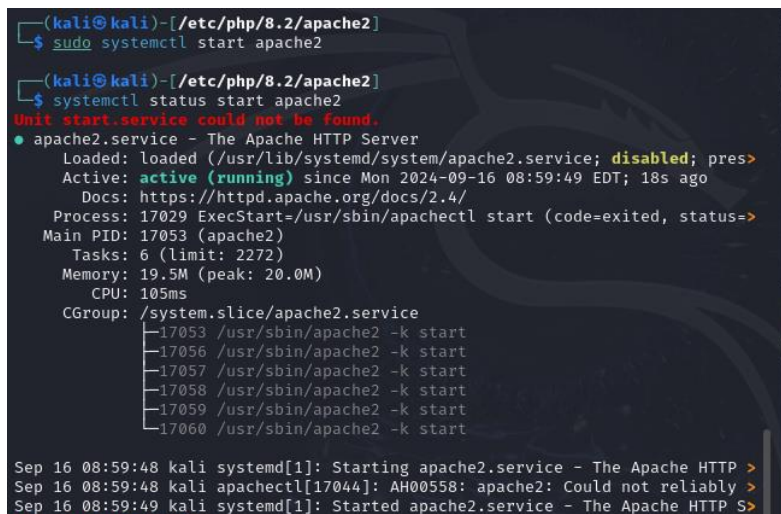
; Define the User-Agent string. PHP's default setting for this is empty.
; https://php.net/user-agent
user_agent="PHP"

; Default timeout for socket based streams (seconds)
; https://php.net/default-socket-timeout
default_socket_timeout = 60

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

## Редактирование файла

Запускаем службу веб-сервера apache и проверяем, запущена ли служба (рис. 14)



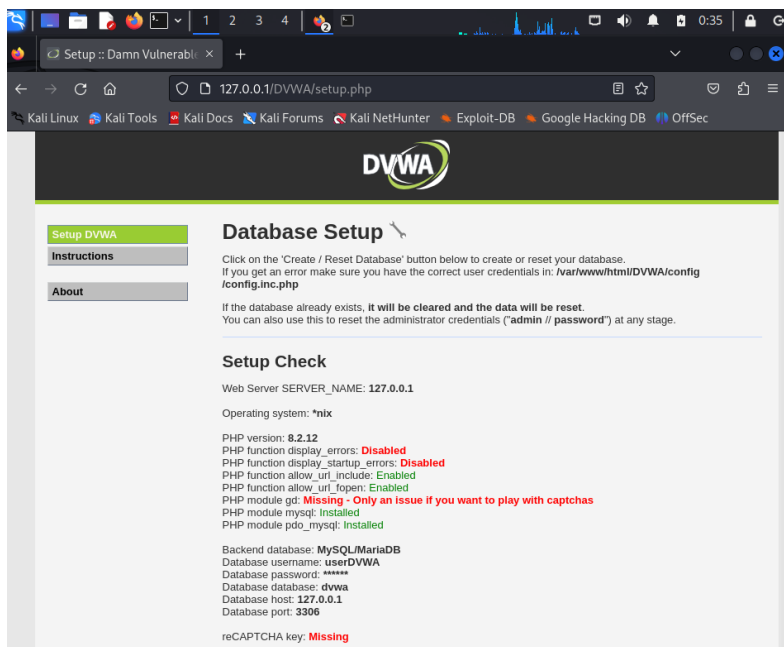
```
(kali@kali)-[/etc/php/8.2/apache2]
$ sudo systemctl start apache2

(kali@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 Mon 2024-09-16 08:59:49 EDT; 18s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 17029 ExecStart=/usr/sbin/apachectl start (code=exited, status=>
  Main PID: 17053 (apache2)
    Tasks: 6 (limit: 2272)
   Memory: 19.5M (peak: 20.0M)
      CPU: 105ms
   CGroup: /system.slice/apache2.service
           └─17053 /usr/sbin/apache2 -k start
             └─17056 /usr/sbin/apache2 -k start
               └─17057 /usr/sbin/apache2 -k start
                 └─17058 /usr/sbin/apache2 -k start
                   └─17059 /usr/sbin/apache2 -k start
                     └─17060 /usr/sbin/apache2 -k start

Sep 16 08:59:48 kali systemd[1]: Starting apache2.service - The Apache HTTP >
Sep 16 08:59:48 kali apachectl[17044]: AH00558: apache2: Could not reliably >
Sep 16 08:59:49 kali systemd[1]: Started apache2.service - The Apache HTTP S>
```

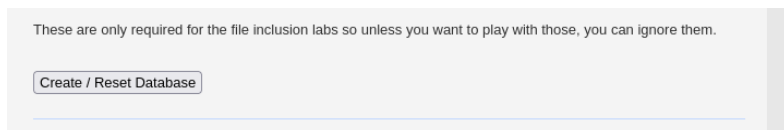
## Запуск apache

Мы настроили DVWA, Apache и базу данных, поэтому открываем браузер и запускаем веб-приложение, введя 127.0.0/DVWA (рис. 15)



## Запуск веб-приложения

Прокручиваем страницу вниз и нажимаем на кнопку create\reset database (рис. 16)



## “Создание базы данных”

Авторизуюсь с помощью предложенных по умолчанию данных (рис. 17)



Username

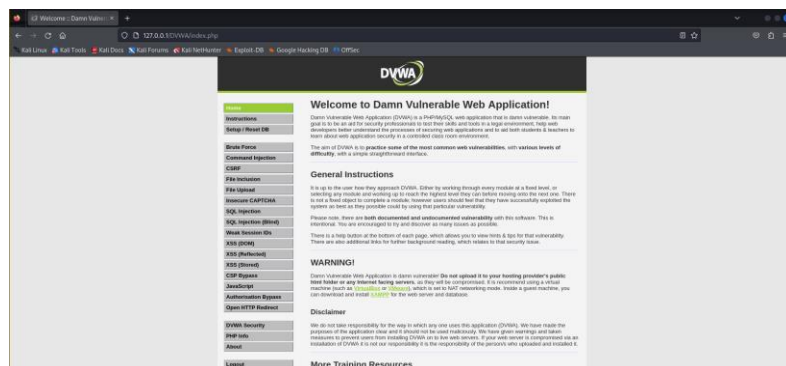
  
  

Password

## Авторизация

Оказываюсь на домашней странице веб-приложения, на этом установка окончена (рис. 18)



Домашняя страница DVWA

## Выводы

Приобрела практические навыки по установке уязвимого веб-приложения DVWA.

## Список литературы