

# Отчет по первому этапу индивидуального проекта

## Основы информационной безопасности

Авдадаев Джамал, НКАбд-01-23

### Содержание

1	Цель работы .....	1
2	Задание .....	1
3	Теоретическое введение.....	1
4	Выполнение лабораторной работы.....	2
5	Выводы.....	5
	Список литературы .....	5

### 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

### *Клонирование репозитория*

Проверяю, что файлы склонировались правильно, далее повышаю права доступа к этой папке до 777

### *Изменение прав доступа*

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

### *Перемещение по директориям*

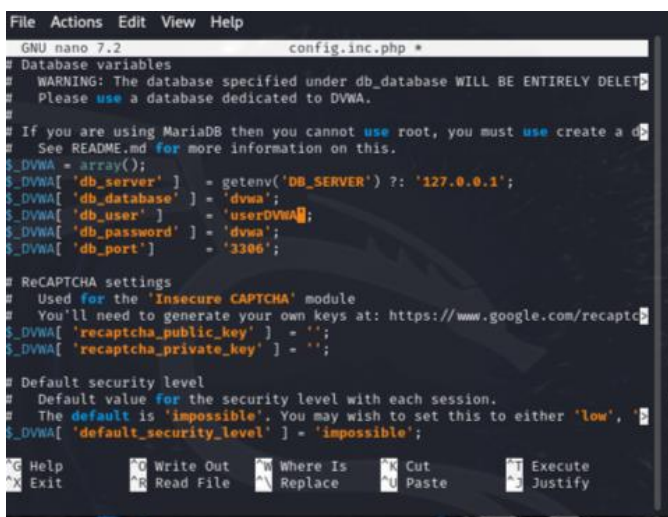
Создаем копию файла, используемого для настройки DVWA `config.inc.php.dist` с именем `config.inc.php`. Копируем файл, а не изменяем его, чтобы у нас был запасной вариант, если что-то пойдет не так

### *Создание копии файла*

Далее открываю файл в текстовом редакторе

### *Открытие файла в редакторе*

Изменяю данные об имени пользователя и пароле



```
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 'impossible'.
$DVWA['default_security_level'] = 'impossible';

Help Exit Write Out Read File Where Is Replace Cut Paste Execute Justify
```

### *Редактирование файла*

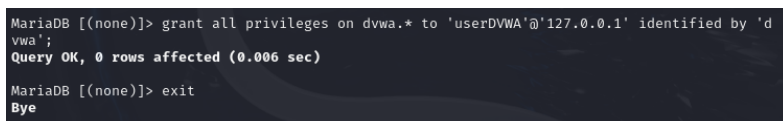
По умолчанию в Kali Linux установлен mysql, поэтому можно его запустить без предварительного скачивания, далее выполняю проверку, запущен ли процесс (рис. 1)

### *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

### *Авторизация в базе данных*

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 (0.006 sec)

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

### *Изменение прав*

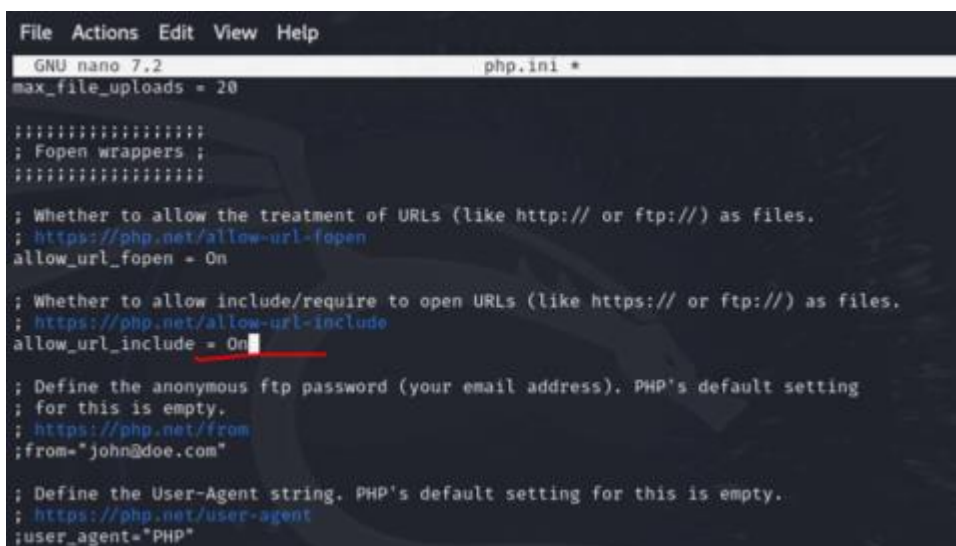
Необходимо настроить сервер apache2, перехожу в соответствующую директорию

### *Перемещение между директориями*

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

### *Открытие файла в текстовом редакторе*

В файле параметры allow\_url\_fopen и allow\_url\_include должны быть поставлены как On



```
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"
```

### *Редактирование файла*

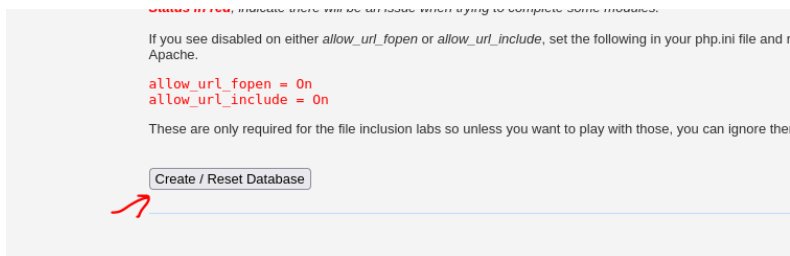
Запускаем службу веб-сервера apache и проверяем, запущена ли служба

### *Запуск apache*

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

### *Запуск веб-приложения*

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



### *“Создание базы данных”*

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



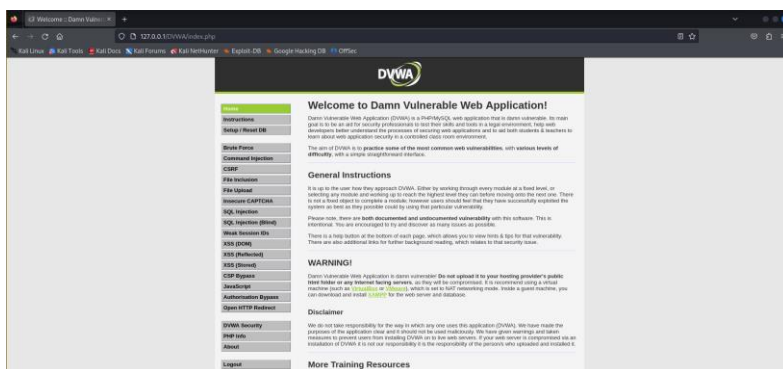
Username

Password

Login

## Авторизация

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