

# **Отчет по первому этапу индивидуального проекта**

**Основы информационной безопасности**

Назармамадов Умед Джамshedович

# 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>15</b>
	<b>Список литературы</b>	<b>16</b>

## **Список иллюстраций**

## 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:

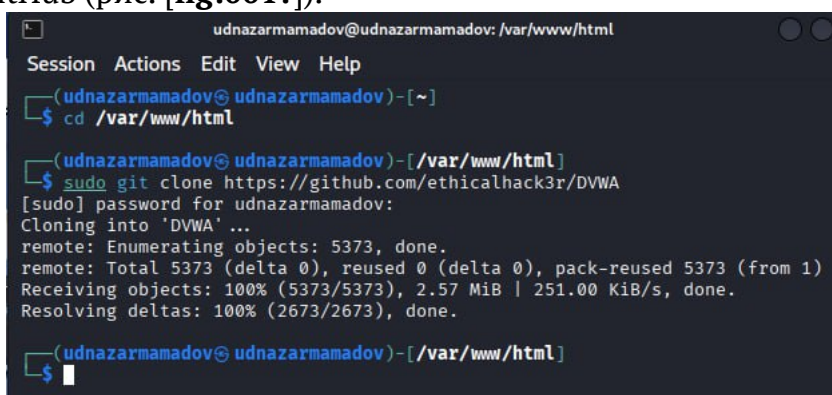
- Невозможный — этот уровень должен быть безопасным от всех уязвимостей. Он используется для сравнения уязвимого исходного кода с безопасным исходным кодом.
- Высокий — это расширение среднего уровня сложности, со смесью более сложных или альтернативных плохих практик в попытке обезопасить код. Уязвимости 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. [fig:001?]).



```
udnazarmamadov@udnazarmamadov: /var/www/html
Session Actions Edit View Help
(udnazarmamadov@udnazarmamadov)-[~]
$ cd /var/www/html
(udnazarmamadov@udnazarmamadov)-[/var/www/html]
$ sudo git clone https://github.com/ethicalhack3r/DVWA
[sudo] password for udnazarmamadov:
Cloning into 'DVWA' ...
remote: Enumerating objects: 5373, done.
remote: Total 5373 (delta 0), reused 0 (delta 0), pack-reused 5373 (from 1)
Receiving objects: 100% (5373/5373), 2.57 MiB | 251.00 KiB/s, done.
Resolving deltas: 100% (2673/2673), done.
(udnazarmamadov@udnazarmamadov)-[/var/www/html]
$
```

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



```
(udnazarmamadov@udnazarmamadov)-[/var/www/html]
$ ls
DVWA index.html index.nginx-debian.html
(udnazarmamadov@udnazarmamadov)-[/var/www/html]
$ sudo chmod -R 777 DVWA
(udnazarmamadov@udnazarmamadov)-[/var/www/html]
$
```

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

```

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

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

```

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

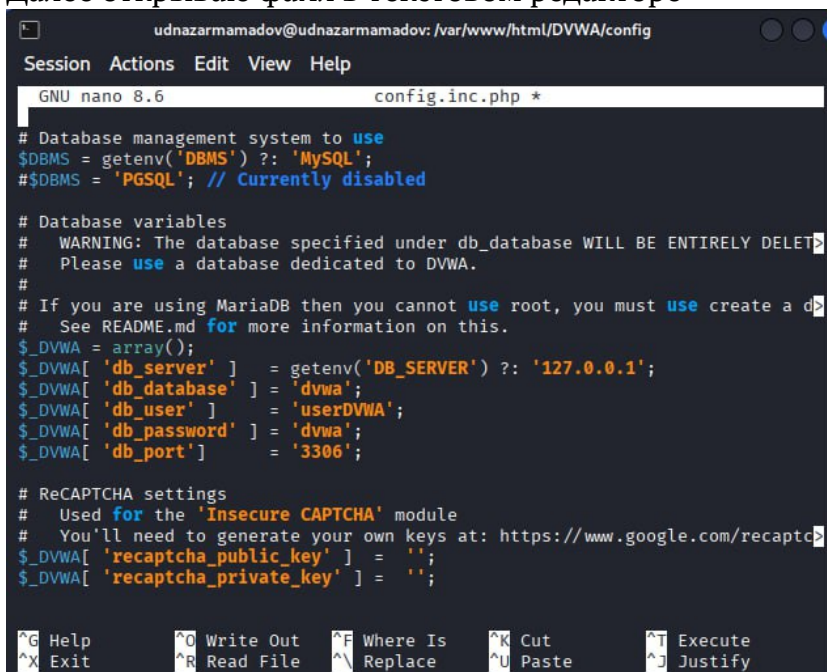
```

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

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

```

Далее открываю файл в текстовом редакторе



```

udnazarmamadov@udnazarmamadov: /var/www/html/DVWA/config
Session Actions Edit View Help
GNU nano 8.6 config.inc.php *

# Database management system to use
$DBMS = getenv('DBMS') ?: 'MySQL';
#$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 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'] = '';

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

```

Изменяю данные об имени пользователя и пароле

```

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

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

```

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

```

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

(udnazarmamadov@udnazarmamadov)-[/var/www/html/DVWA/config]
$ systemctl status mysql
● mariadb.service - MariaDB 11.8.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; pres>
   Active: active (running) since Sun 2025-09-21 16:26:33 EDT; 15s ago
   Invocation: a63e5b51f926413582cfdb63b7e50b8b
   Docs: man:mariadb(8)
         https://mariadb.com/kb/en/library/systemd/
   Process: 229856 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d>
   Process: 229858 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery >
   Process: 229933 ExecStartPost=/bin/rm -f /run/mysqld/wsrep-start-positio>
   Process: 229943 ExecStartPost=/etc/mysql/debian-start (code=exited, stat>
   Main PID: 229910 (mariabdd)
   Status: "Taking your SQL requests now..."
   Tasks: 14 (limit: 30005)

```

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

```

(udnazarmamadov@udnazarmamadov)-[/var/www/html/DVWA/config]
$ sudo mysql -u root -p
[sudo] password for udnazarmamadov:
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.8.3-MariaDB-1+b1 from Debian -- Please help get to 10k sta
rs at https://github.com/MariaDB/Server

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)]>

```

Теперь нужно пользователю предоставить привилегии для работы с этой базой данных

```

(udnazarmamadov@udnazarmamadov)-[/var/www/html/DVWA/config]
$ sudo mysql -u root -p
[sudo] password for udnazarmamadov:
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.8.3-MariaDB-1+b1 from Debian -- Please help get to 10k s
rs at https://github.com/MariaDB/Server

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

Type 'help;' or '\h' for help. Type '\c' to clear the current input stateme
.

MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1'
Query OK, 0 rows affected (0.005 sec)

MariaDB [(none)]> exit
Bye

```

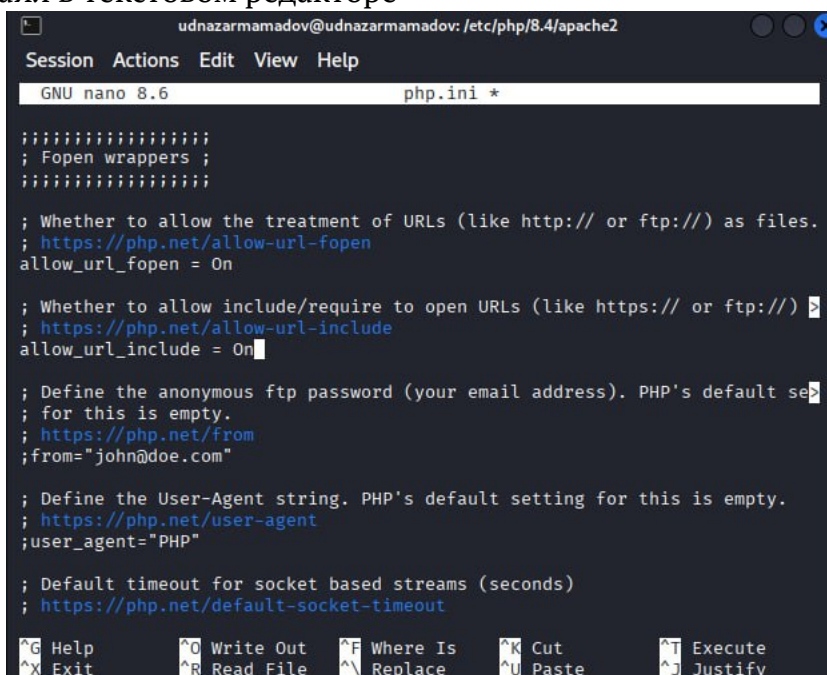
Необходимо настроить сервер apache2, перехожу в соответствующую директорию



```
(udnazarmamadov@udnazarmamadov)-[/var/www/html/DVWA/config]
$ cd /etc/php/8.4/apache2

(udnazarmamadov@udnazarmamadov)-[/etc/php/8.4/apache2]
$
```

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



```
udnazarmamadov@udnazarmamadov: /etc/php/8.4/apache2
Session Actions Edit View Help
GNU nano 8.6 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://)
; https://php.net/allow-url-include
allow_url_include = On

; Define the anonymous ftp password (your email address). PHP's default se
; 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

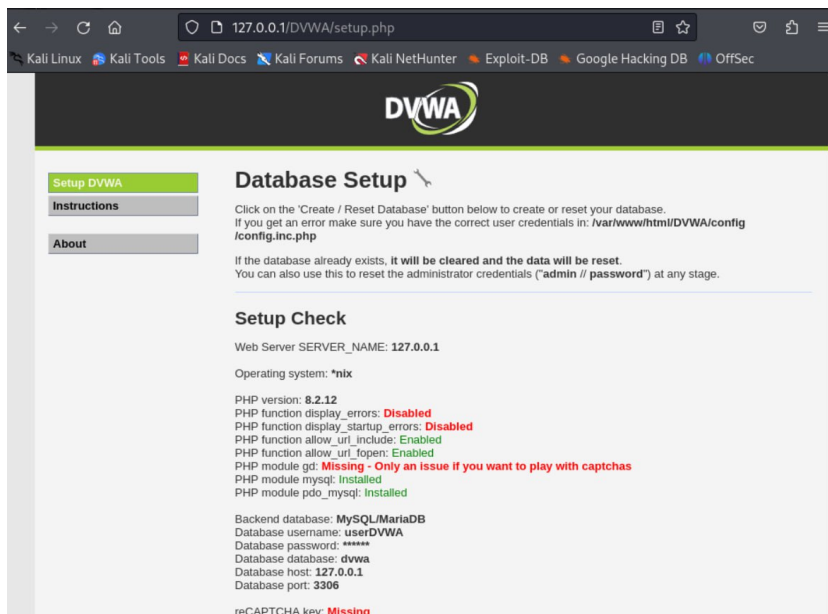
^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

В файле параметры `allow_url_fopen` и `allow_url_include` должны быть поставлены как `On`

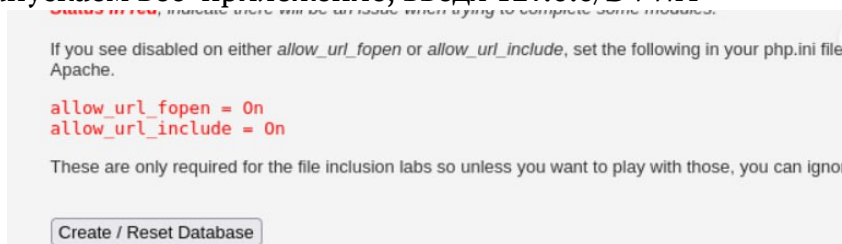
```
(udnazarmamadov@udnazarmamadov)-[/etc/php/8.4/apache2]
$ sudo systemctl start apache2

(udnazarmamadov@udnazarmamadov)-[/etc/php/8.4/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; pr>
   Active: active (running) since Sun 2025-09-21 16:39:02 EDT; 29s ago
  Invocation: b1ed58ac61174625a5d07d50ca5a86e0
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 236217 ExecStart=/usr/sbin/apachectl start (code=exited, stat>
    Main PID: 236263 (apache2)
      Tasks: 6 (limit: 4546)
    Memory: 20.8M (peak: 21.2M)
       CPU: 73ms
    CGroup: /system.slice/apache2.service
            └─236263 /usr/sbin/apache2 -k start
              236266 /usr/sbin/apache2 -k start
              236267 /usr/sbin/apache2 -k start
              236268 /usr/sbin/apache2 -k start
```

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



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



Прокручиваем страницу вниз и нажимаем на кнопку create/reset database

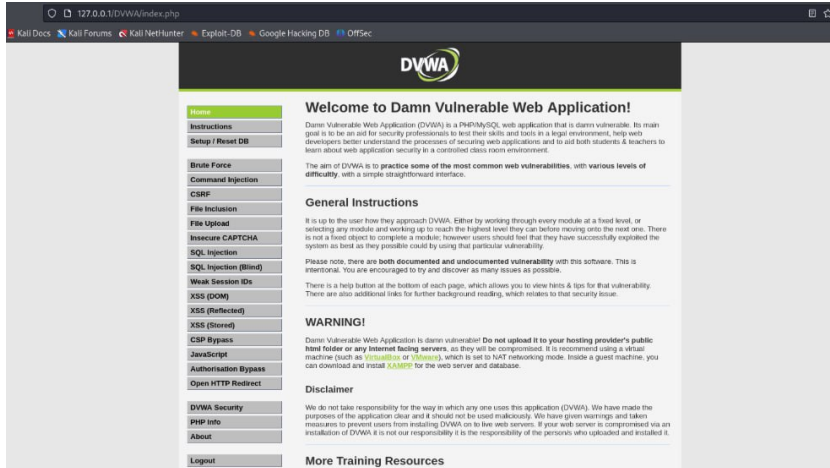


Username

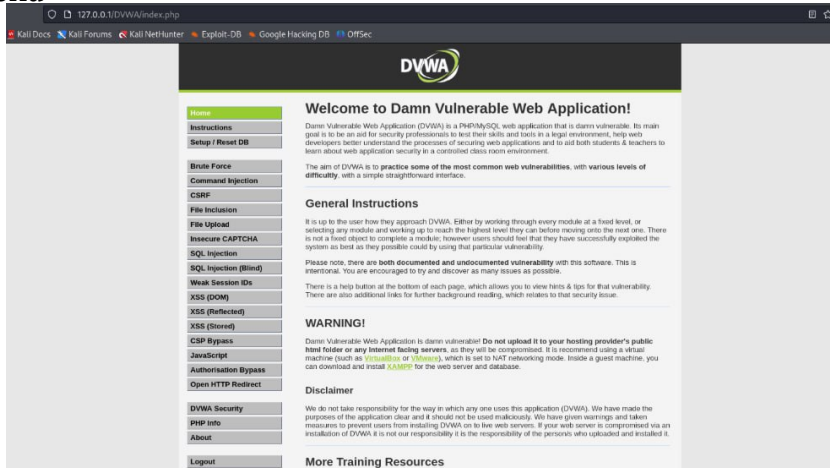
Password

Login

## Авторизуюсь с помощью предложенных по умолчанию данных



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



## 5 Выводы

Приобрел 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.