

# **Отчет по второму этапу индивидуального проекта**

**Информационная безопасность**

Выполнила: Коняева Марина Александровна,  
НФИбд-01-21, 1032217044

# Содержание

<b>Цель работы</b>	<b>4</b>
<b>Задание</b>	<b>5</b>
<b>Теоретическое введение</b>	<b>6</b>
<b>Выполнение лабораторной работы</b>	<b>8</b>
<b>Выводы</b>	<b>16</b>
<b>Список литературы</b>	<b>17</b>

## Список иллюстраций

1	Клонирование репозитория DWVA . . . . .	8
2	Изменение прав доступа . . . . .	8
3	Перемещение по директориям . . . . .	9
4	Создание копии файла . . . . .	9
5	Открытие файла в редакторе . . . . .	9
6	Редактирование файл . . . . .	10
7	Запуск mysql . . . . .	10
8	Авторизация в базе данных . . . . .	11
9	Изменение прав . . . . .	11
10	Перемещение между директориями . . . . .	11
11	Открытие файла в текстовом редакторе . . . . .	12
12	Редактирование файла . . . . .	12
13	Запуск arche . . . . .	13
14	Запуск веб-приложения . . . . .	13
15	“Создание базы данных” . . . . .	14
16	Авторизация . . . . .	14
17	Домашняя страница DVWA . . . . .	15

## **Цель работы**

Приобретение практических навыков по установке DVWA.

# Задание

Установить DVWA на дистрибутив Kali Linux.

# Теоретическое введение

DVWA - это уязвимое веб-приложение, разработанное на PHP и MySQL.

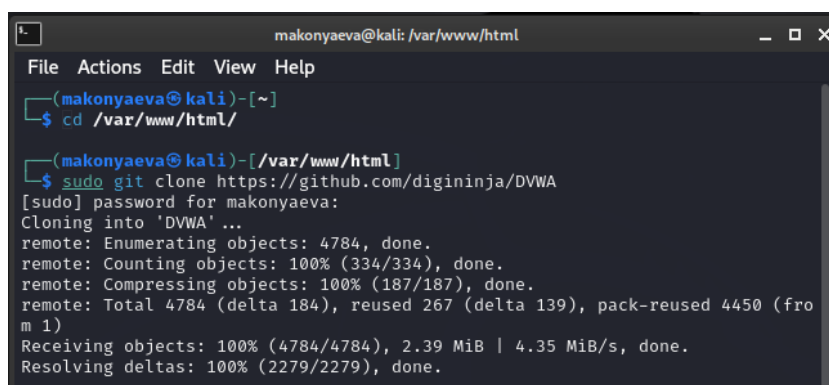
Некоторые из уязвимостей веб приложений, который содержит DVWA: - Брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования инструментов по атаке на пароль методом грубой силы и показывает небезопасность слабых паролей. - Исполнение (внедрение) команд: Выполнение команд уровня операционной 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 три уровня безопасности, они меняют уровень безопасности каждого веб приложения в DVWA: 1) 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. 2) 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. 3) 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.

# Выполнение лабораторной работы

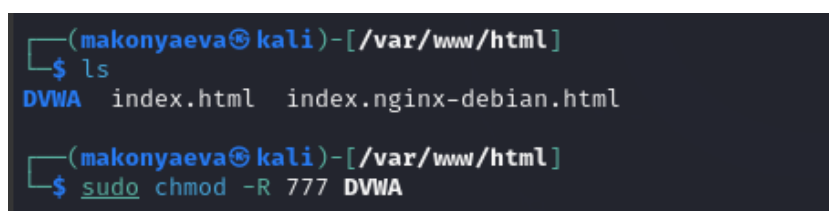
1. Переедем в директорию /var/www/html для настройки DVWA на локальном хосте.  
Далее клонируем нужный репозиторий GitHub.



```
makonyaeva@kali: /var/www/html
File Actions Edit View Help
(makonyaeva@kali)-[~]
$ cd /var/www/html/
(makonyaeva@kali)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA
[sudo] password for makonyaeva:
Cloning into 'DVWA' ...
remote: Enumerating objects: 4784, done.
remote: Counting objects: 100% (334/334), done.
remote: Compressing objects: 100% (187/187), done.
remote: Total 4784 (delta 184), reused 267 (delta 139), pack-reused 4450 (from 1)
Receiving objects: 100% (4784/4784), 2.39 MiB | 4.35 MiB/s, done.
Resolving deltas: 100% (2279/2279), done.
```

Рис. 1: Клонирование репозитория DVWA

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



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

Рис. 2: Изменение прав доступа

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



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

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

Рис. 3: Перемещение по директориям

4. 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)

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

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

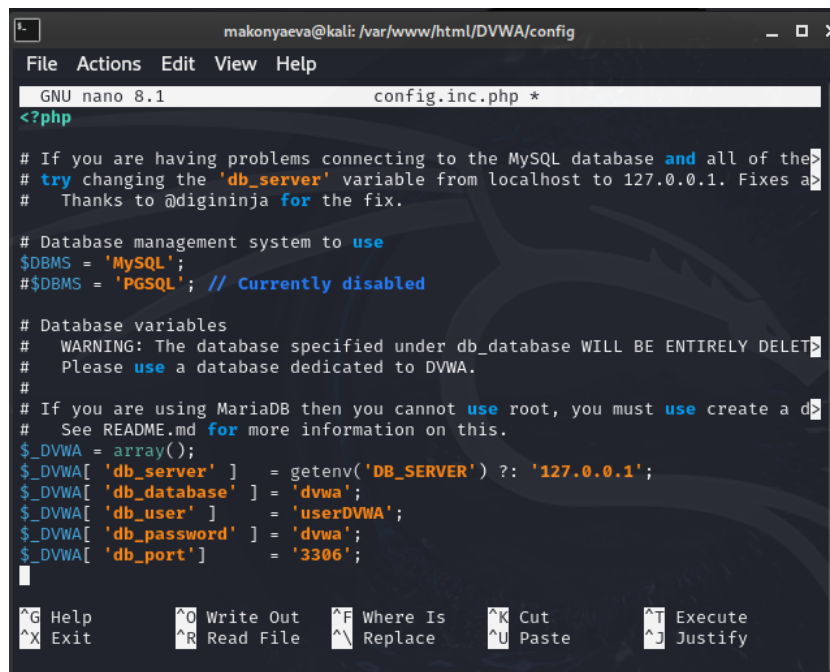
Рис. 4: Создание копии файла

5. Далее открываем файл в текстовом редакторе (рис. 5)

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

Рис. 5: Открытие файла в редакторе

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



```
makonyaeva@kali: /var/www/html/DVWA/config
File Actions Edit View Help
GNU nano 8.1 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.

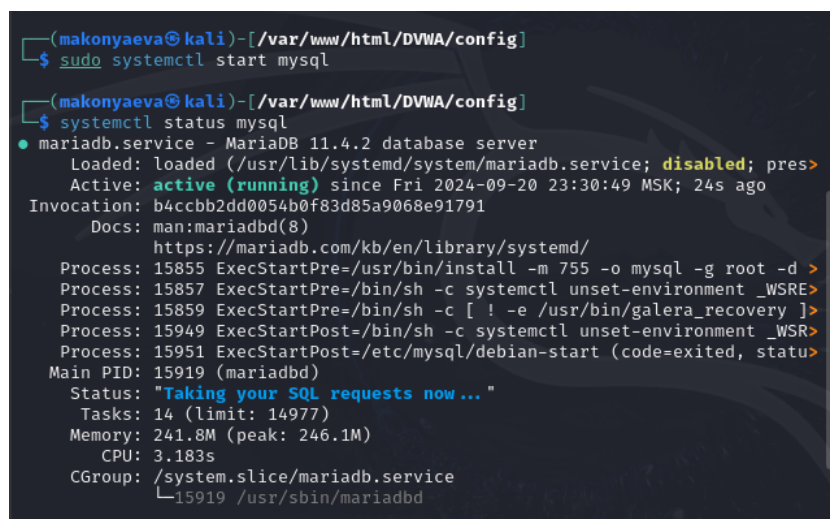
# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# 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 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';

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

Рис. 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)



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

(makonyaeva@kali)-[/var/www/html/DVWA/config]
$ systemctl status mysql
● mariadb.service - MariaDB 11.4.2 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; pres>
   Active: active (running) since Fri 2024-09-20 23:30:49 MSK; 24s ago
   Invocation: b4ccbb2dd0054b0f83d85a9068e91791
   Docs: man:mariadb(8)
        https://mariadb.com/kb/en/library/systemd/
   Process: 15855 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d >
   Process: 15857 ExecStartPre=/bin/sh -c systemctl unset-environment _WSRE>
   Process: 15859 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ]>
   Process: 15949 ExecStartPost=/bin/sh -c systemctl unset-environment _WSR>
   Process: 15951 ExecStartPost=/etc/mysql/debian-start (code=exited, statu>
   Main PID: 15919 (mariabdd)
   Status: "Taking your SQL requests now ..."
   Tasks: 14 (limit: 14977)
   Memory: 241.8M (peak: 246.1M)
   CPU: 3.183s
   CGroup: /system.slice/mariadb.service
           └─15919 /usr/sbin/mariabdd
```

Рис. 7: Запуск mysql

8. Авторизируемся 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)

```
(makonyaeva@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: 11.4.2-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)]> create user 'userDVWA'@'127.0.0.1' identified by 'dvwa';
Query OK, 0 rows affected (0.005 sec)
```

Рис. 8: Авторизация в базе данных

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

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1' id
Query OK, 0 rows affected (0.007 sec)

MariaDB [(none)]> exit
```

Рис. 9: Изменение прав


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

```
(makonyaeva@kali)-[/etc/php/8.2]
$ cd /etc/php/8.2/apache2/

(makonyaeva@kali)-[/etc/php/8.2/apache2]
$ ls
conf.d  php.ini
```

Рис. 10: Перемещение между директориями

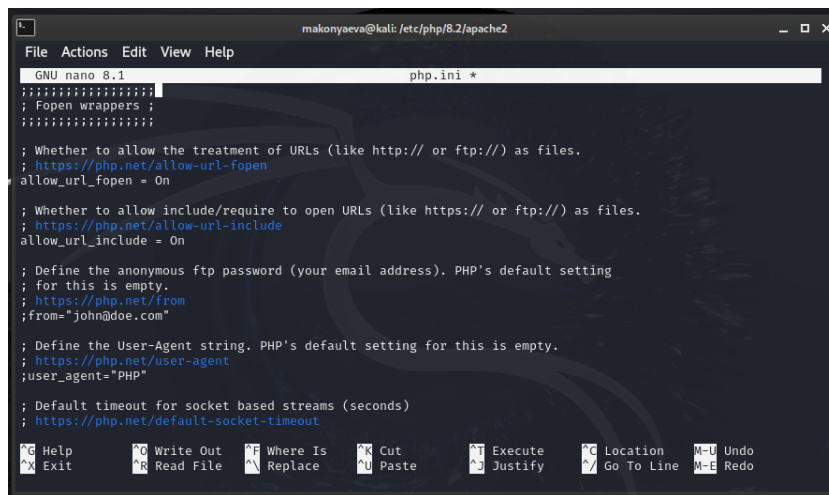
11. В файле `php.ini` нужно будет изменить один параметр, поэтому открываем файл в текстовом редакторе (рис. 11)



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

Рис. 11: Открытие файла в текстовом редакторе

12. В файле параметры `allow_url_fopen` и `allow_url_include` должны быть поставлены как `On` (рис. 12)



```
GNU nano 8.1 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 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"

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

Рис. 12: Редактирование файла

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

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

(makonyaeva@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; preset: disabled)
   Active: active (running) since Fri 2024-09-20 23:48:34 MSK; 27s ago
  Invocation: 5e77e98349d349cc86520f42cfef2b87
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 24731 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 24747 (apache2)
    Tasks: 6 (limit: 2269)
   Memory: 19.7M (peak: 19.9M)
      CPU: 114ms
   CGroup: /system.slice/apache2.service
           └─24747 /usr/sbin/apache2 -k start
             └─24750 /usr/sbin/apache2 -k start
               └─24751 /usr/sbin/apache2 -k start
                 └─24752 /usr/sbin/apache2 -k start
                   └─24753 /usr/sbin/apache2 -k start
                     └─24754 /usr/sbin/apache2 -k start
```

Рис. 13: Запуск архе

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

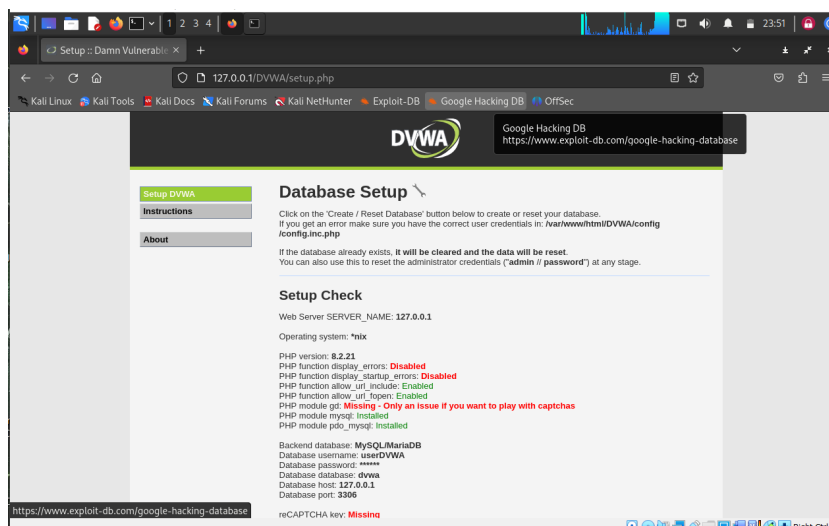


Рис. 14: Запуск веб-приложения

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

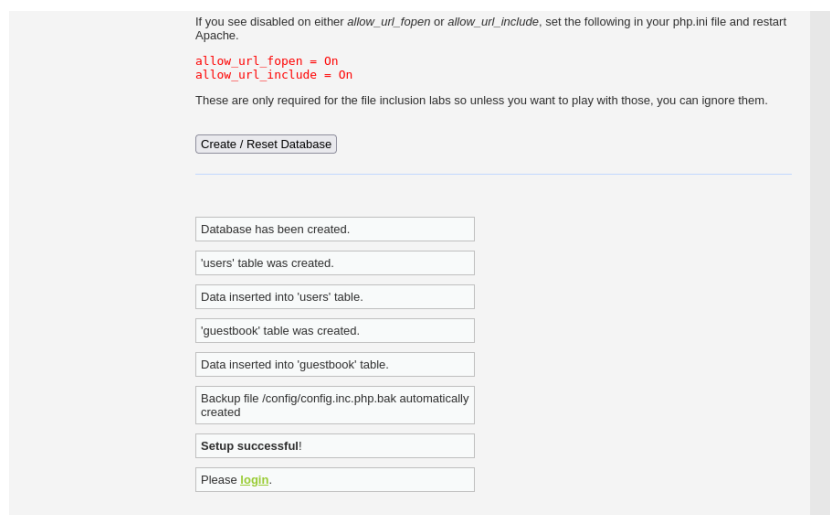


Рис. 15: “Создание базы данных”

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

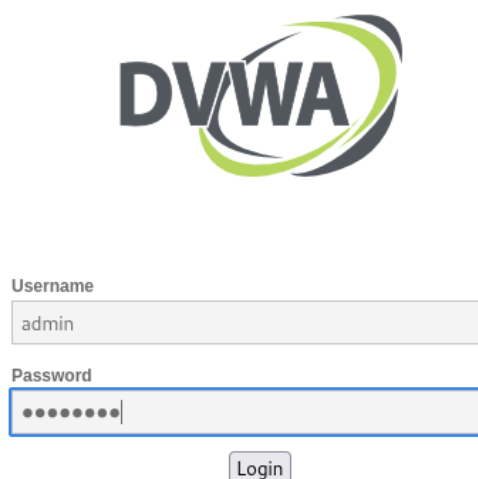



Рис. 16: Авторизация

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



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Authorisation Bypass

Open HTTP Redirect

DVWA Security

PHP Info

About

Logout

## Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficulty**, with a simple straightforward interface.

### General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerabilities** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

### WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest machine, you can download and install [XAMPP](#) for the web server and database.

### Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

### More Training Resources

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want

Рис. 17: Домашняя страница DVWA

## **Выводы**

Выполнив первый этап индивидуального проекта, мы приобрели практические навыки по установке уязвимого веб-приложения DVWA.



## **Список литературы**

[1] Документация по Virtual Box: <https://www.virtualbox.org/wiki/Documentation>