

Отчёт по этапу №2 индивидуального проекта

Основы информационной безопасности

Мурашов Иван Вячеславович

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
5	Выводы	18

Список иллюстраций

4.1	Клонирование репозитория	9
4.2	Изменение прав доступа	9
4.3	Перемещение по директориям	10
4.4	Создание копии файла	10
4.5	Открытие файла в редакторе	10
4.6	Редактирование файл	11
4.7	Запуск mysql	11
4.8	Авторизация в базе данных	12
4.9	Изменение прав	12
4.10	Перемещение между директориями	13
4.11	Открытие файла в текстовом редакторе	13
4.12	Редактирование файла	14
4.13	Запуск arche	14
4.14	Запуск веб-приложения	15
4.15	“Создание базы данных”	15
4.16	Авторизация	16
4.17	Домашняя страница DVWA	17

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).

```
(kali@ivmurashov)-[/var/www/html]
$ sudo git clone https://github.com/ethicalhack3r/DVWA
[sudo] password for kali:
Cloning into 'DVWA'...
remote: Enumerating objects: 5105, done.
remote: Counting objects: 100% (91/91), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 5105 (delta 79), reused 67 (delta 67), pack-reused 5014
(from 4)
Receiving objects: 100% (5105/5105), 2.49 MiB | 3.70 MiB/s, done.
Resolving deltas: 100% (2489/2489), done.
```

Рис. 4.1: Клонирование репозитория

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

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

(kali@ivmurashov)-[/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 (рис. 3)

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

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

Рис. 4.3: 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. 4)

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

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

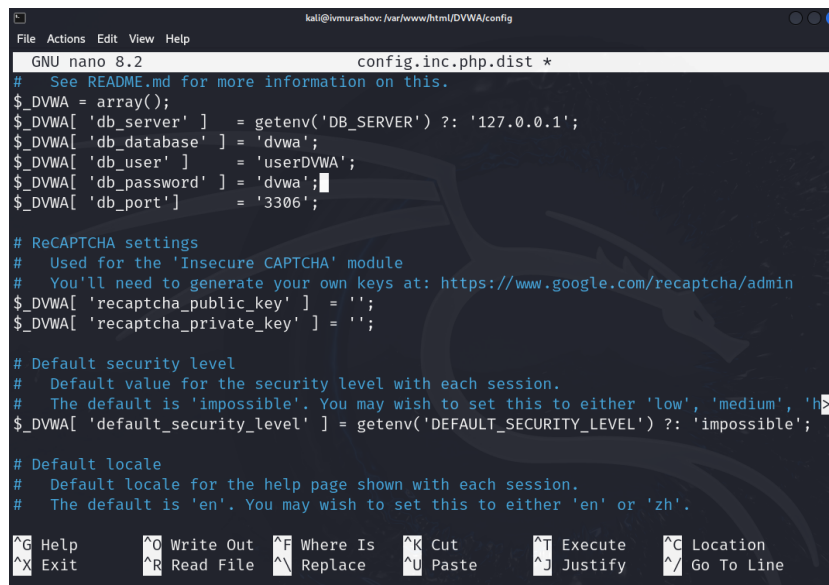
Рис. 4.4: Создание копии файла

Далее открываю файл в текстовом редакторе (рис. 5)

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

Рис. 4.5: Открытие файла в редакторе

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



```
GNU nano 8.2 config.inc.php.dist *
# 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/admin
$_DVWA[ 'recaptcha_public_key' ] = '';
$_DVWA[ 'recaptcha_private_key' ] = '';

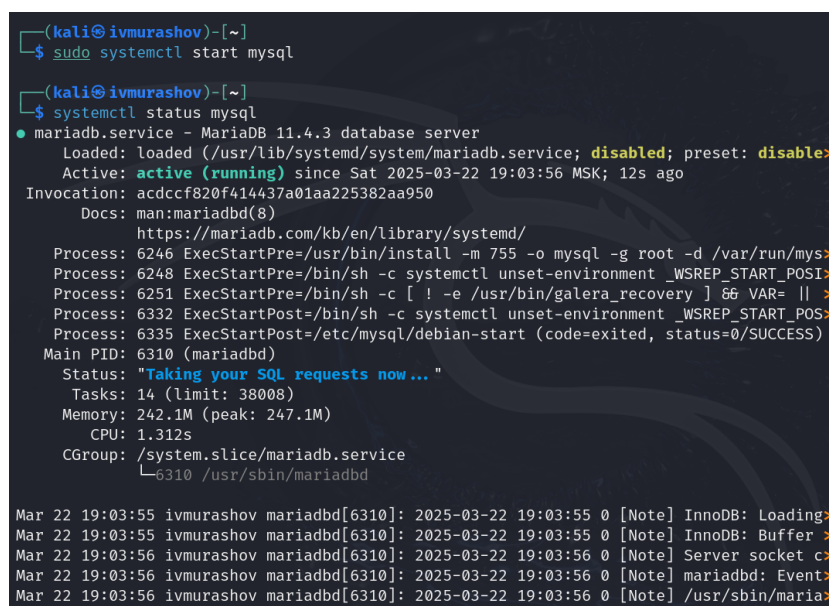
# Default security level
# Default value for the security level with each session.
# The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high'
$_DVWA[ 'default_security_level' ] = getenv('DEFAULT_SECURITY_LEVEL') ?: 'impossible';

# Default locale
# Default locale for the help page shown with each session.
# The default is 'en'. You may wish to set this to either 'en' or 'zh'.

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

Рис. 4.6: Редактирование файла

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



```
(kali@ivmurashov)-[~]
$ sudo systemctl start mysql

(kali@ivmurashov)-[~]
$ systemctl status mysql
● mariadb.service - MariaDB 11.4.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disable>
   Active: active (running) since Sat 2025-03-22 19:03:56 MSK; 12s ago
   Invocation: acdcef820f414437a01aa225382aa950
   Docs: man:mariadb(8)
        https://mariadb.com/kb/en/library/systemd/
   Process: 6246 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mys>
   Process: 6248 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSI>
   Process: 6251 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || >
   Process: 6332 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POS>
   Process: 6335 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
   Main PID: 6310 (mariabdd)
   Status: "Taking your SQL requests now..."
   Tasks: 14 (limit: 38008)
   Memory: 242.1M (peak: 247.1M)
   CPU: 1.312s
   CGroup: /system.slice/mariadb.service
           └─6310 /usr/sbin/mariabdd

Mar 22 19:03:55 ivmurashov mariabdd[6310]: 2025-03-22 19:03:55 0 [Note] InnoDB: Loading>
Mar 22 19:03:55 ivmurashov mariabdd[6310]: 2025-03-22 19:03:55 0 [Note] InnoDB: Buffer >
Mar 22 19:03:56 ivmurashov mariabdd[6310]: 2025-03-22 19:03:56 0 [Note] Server socket c>
Mar 22 19:03:56 ivmurashov mariabdd[6310]: 2025-03-22 19:03:56 0 [Note] mariabdd: Event>
Mar 22 19:03:56 ivmurashov mariabdd[6310]: 2025-03-22 19:03:56 0 [Note] /usr/sbin/maria>
```

Рис. 4.7: 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 (рис. 8)

```
(kali@ivmurashov)-[~]
$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 11.4.3-MariaDB-1 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 (0.004 sec)
```

Рис. 4.8: Авторизация в базе данных

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' identified by "dvwa";
Query OK, 0 rows affected (0.002 sec)

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

Рис. 4.9: Изменение прав

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

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

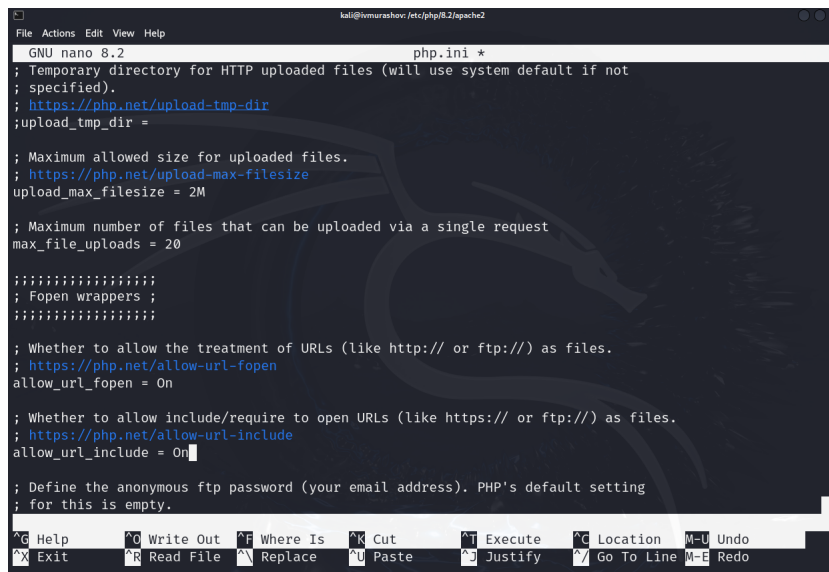
Рис. 4.10: Перемещение между директориями

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

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

Рис. 4.11: Открытие файла в текстовом редакторе

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



```
File Actions Edit View Help
GNU nano 8.2 php.ini *
; Temporary directory for HTTP uploaded files (will use system default if not
; specified).
; https://php.net/upload-tmp-dir
upload_tmp_dir =

; Maximum allowed size for uploaded files.
; https://php.net/upload-max-filesize
upload_max_filesize = 2M

; Maximum number of files that can be uploaded via a single request
max_file_uploads = 20

;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;

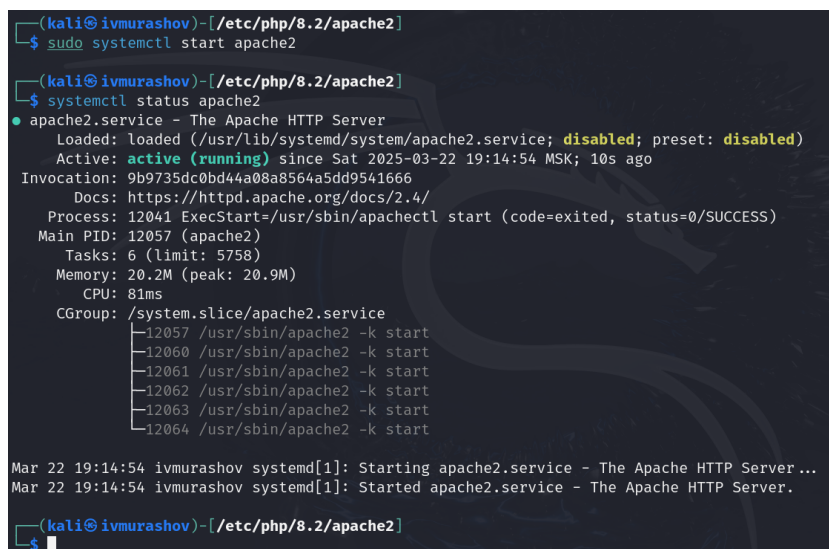
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

; 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.
```

Рис. 4.12: Редактирование файла

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



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

(kali@ivmurashov)-[/etc/php/8.2/apache2]
$ systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Sat 2025-03-22 19:14:54 MSK; 10s ago
     Invocation: 9b9735dc0bd44a08a8564a5dd9541666
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 12041 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 12057 (apache2)
      Tasks: 6 (limit: 5758)
     Memory: 20.2M (peak: 20.9M)
        CPU: 81ms
    CGroup: /system.slice/apache2.service
            └─12057 /usr/sbin/apache2 -k start
              12060 /usr/sbin/apache2 -k start
              12061 /usr/sbin/apache2 -k start
              12062 /usr/sbin/apache2 -k start
              12063 /usr/sbin/apache2 -k start
              12064 /usr/sbin/apache2 -k start

Mar 22 19:14:54 ivmurashov systemd[1]: Starting apache2.service - The Apache HTTP Server...
Mar 22 19:14:54 ivmurashov systemd[1]: Started apache2.service - The Apache HTTP Server.
```

Рис. 4.13: Запуск apache

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

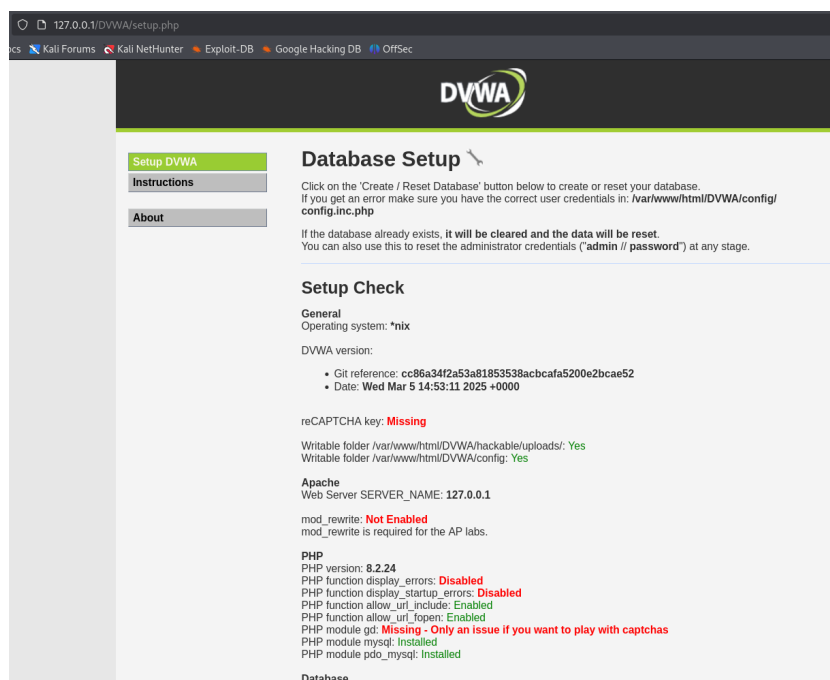


Рис. 4.14: Запуск веб-приложения

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

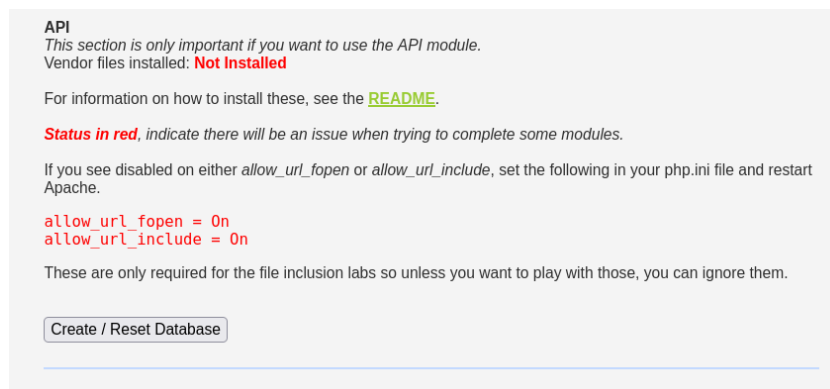



Рис. 4.15: “Создание базы данных”

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



Username


Password

Login

Login failed

Рис. 4.16: Авторизация

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

Cryptography

API

DVWA Security

PHP Info

About

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 [Vikware](#)), 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 Trainina Resources

Рис. 4.17: Домашняя страница DVWA

5 Выводы

Приобретены практические навыки по установке уязвимого веб-приложения DVWA.