

# **Отчет по второму этапу индивидуального проекта**

**Информационная безопасность**

Выполнила: Самсонова Мария Ильинична,  
НФИбд-02-21, 1032216526

# 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.

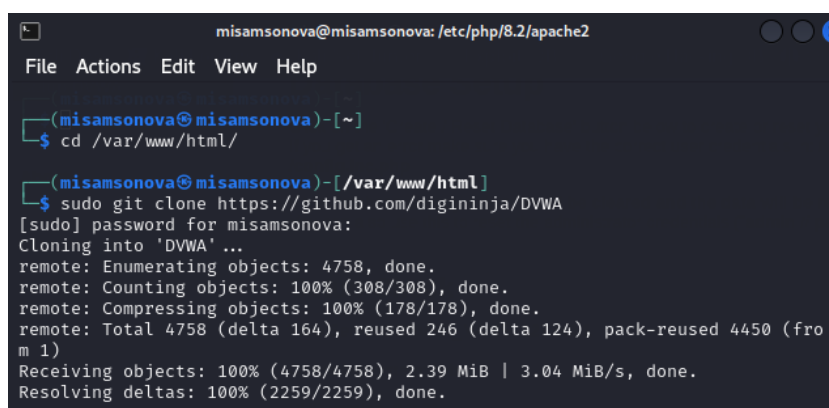
Некоторые из уязвимостей веб приложений, который содержит DVWA: - Брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования инструментов по атаке на пароль методом грубой силы и показывает небезопасность слабых паролей. - Исполнение (внедрение) команд: Выполнение команд уровня операционной 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.



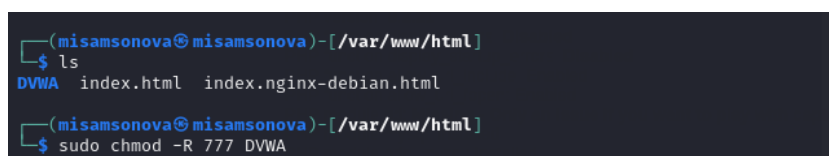
```
misamsonova@misamsonova: /etc/php/8.2/apache2
File Actions Edit View Help

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

(misamsonova@misamsonova)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA
[sudo] password for misamsonova:
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 | 3.04 MiB/s, done.
Resolving deltas: 100% (2259/2259), done.
```

Рис. 1: Клонирование репозитория DVWA

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



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

(misamsonova@misamsonova)-[/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)



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

(misamsonova@misamsonova)-[/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)

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

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

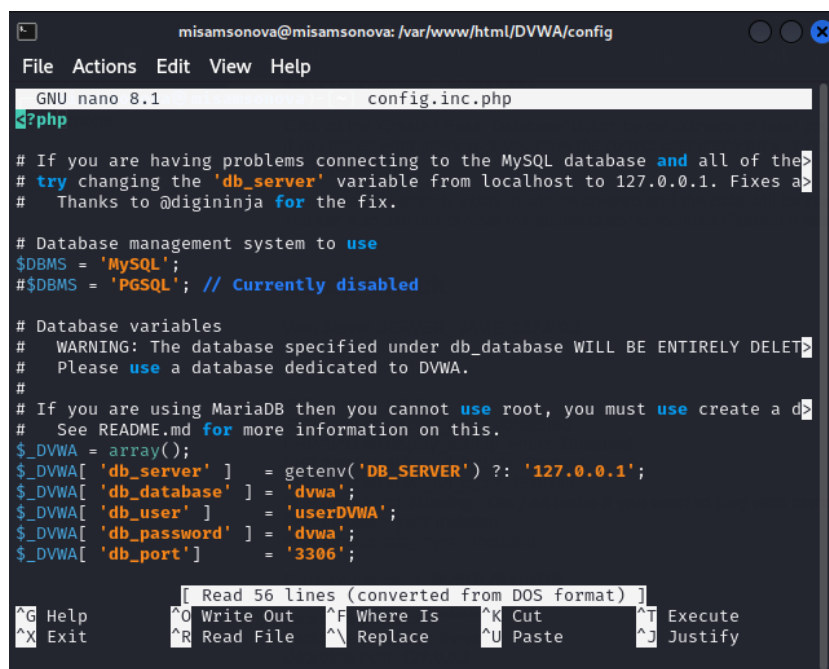
Рис. 4: Создание копии файла

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

```
(misamsonova@misamsonova)-[/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)



```
misamsonova@misamsonova: /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.

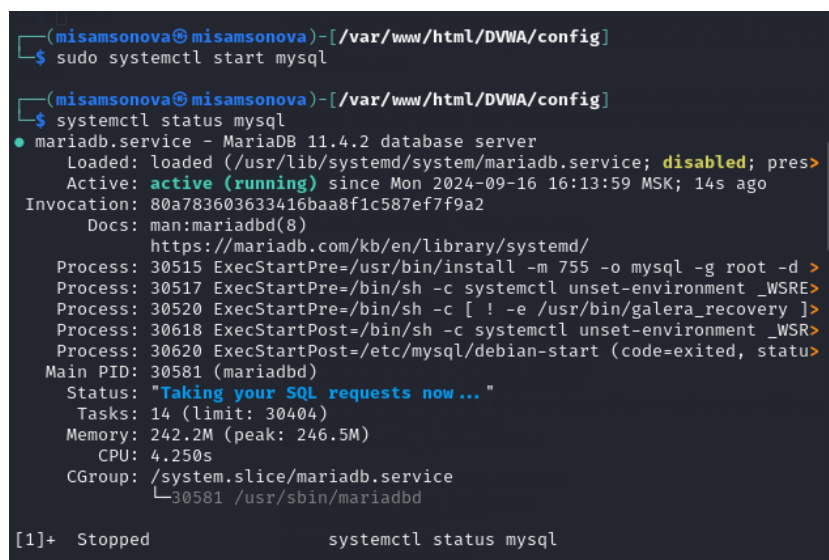
# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# 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 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';

[ Read 56 lines (converted from DOS format) ]
^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

Рис. 6: Редактирование файл

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



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

(misamsonova@misamsonova)-[/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 Mon 2024-09-16 16:13:59 MSK; 14s ago
  Invocation: 80a783603633416baa8f1c587ef7f9a2
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
   Process: 30515 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d >
   Process: 30517 ExecStartPre=/bin/sh -c systemctl unset-environment _WSRE>
   Process: 30520 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ]>
   Process: 30618 ExecStartPost=/bin/sh -c systemctl unset-environment _WSR>
   Process: 30620 ExecStartPost=/etc/mysql/debian-start (code=exited, statu>
  Main PID: 30581 (mariabdd)
    Status: "Taking your SQL requests now..."
     Tasks: 14 (limit: 30404)
  Memory: 242.2M (peak: 246.5M)
       CPU: 4.250s
   CGroup: /system.slice/mariadb.service
           └─30581 /usr/sbin/mariabdd

[1]+  Stopped                  systemctl status mysql
```

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)

```
(misamsonova@misamsonova)-[/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' identified by 'dvwa';
Query OK, 0 rows affected (0.005 sec)

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

Рис. 9: Изменение прав

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

```
(misamsonova@misamsonova)-[/var/www/html/DVWA/config]
$ cd /etc/php/8.2/
apache2/      cli/      mods-available/
(misamsonova@misamsonova)-[/var/www/html/DVWA/config]
$ cd /etc/php/8.2/apache2/

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

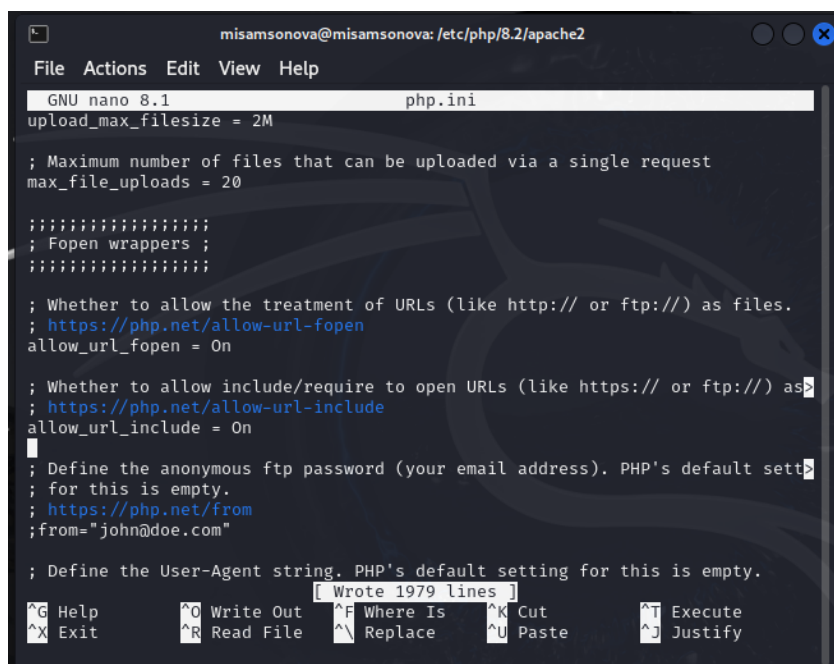
Рис. 10: Перемещение между директориями

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

```
(misamsonova@misamsonova)-[/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)



```
File Actions Edit View Help  
GNU nano 8.1 php.ini  
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  
; 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.  
[ Wrote 1979 lines ]  
^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute  
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

Рис. 12: Редактирование файла

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

```
(misamsonova@misamsonova)-[/etc/php/8.2/apache2]
$ sudo systemctl start apache2
(misamsonova@misamsonova)-[/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 16:22:36 MSK; 23s ago
 Invocation: a7754b38a5fb41ae9b7295a379b0760c
    Docs: https://httpd.apache.org/docs/2.4/
 Process: 35193 ExecStart=/usr/sbin/apachectl start (code=exited, status=>
 Main PID: 35209 (apache2)
   Tasks: 6 (limit: 4606)
  Memory: 19.9M (peak: 20.3M)
    CPU: 137ms
   CGroup: /system.slice/apache2.service
           └─35209 /usr/sbin/apache2 -k start
             └─35211 /usr/sbin/apache2 -k start
               └─35212 /usr/sbin/apache2 -k start
                 └─35213 /usr/sbin/apache2 -k start
                   └─35214 /usr/sbin/apache2 -k start
                     └─35215 /usr/sbin/apache2 -k start
```

Рис. 13: Запуск арче

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

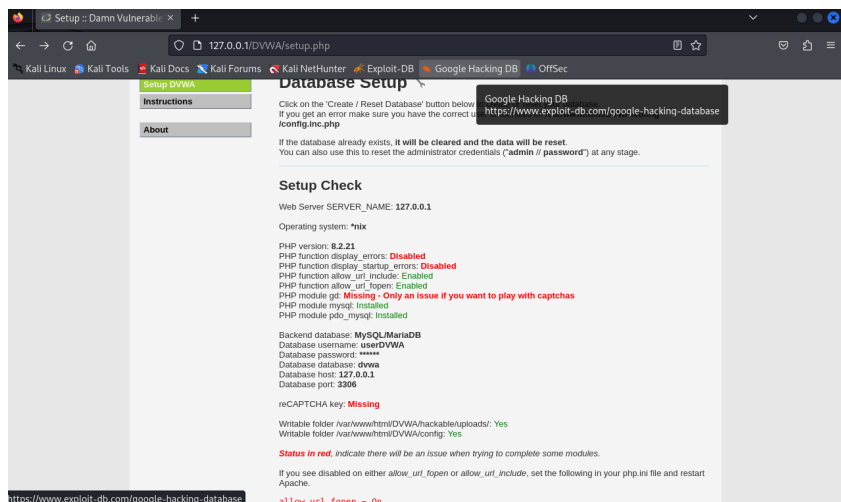


Рис. 14: Запуск веб-приложения

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

If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the following in your `php.ini` file and restart Apache.

```
allow_url_fopen = On
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

[Create / Reset Database](#)

---

Database has been created.

'users' table was created.

Data inserted into 'users' table.

'guestbook' table was created.

Data inserted into 'guestbook' table.


Backup file `/config/config.inc.php.bak` automatically created

**Setup successful!**

Please [login](#).

Рис. 15: “Создание базы данных”

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



Username

admin

Password

.....

[Login](#)

Рис. 16: Авторизация

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

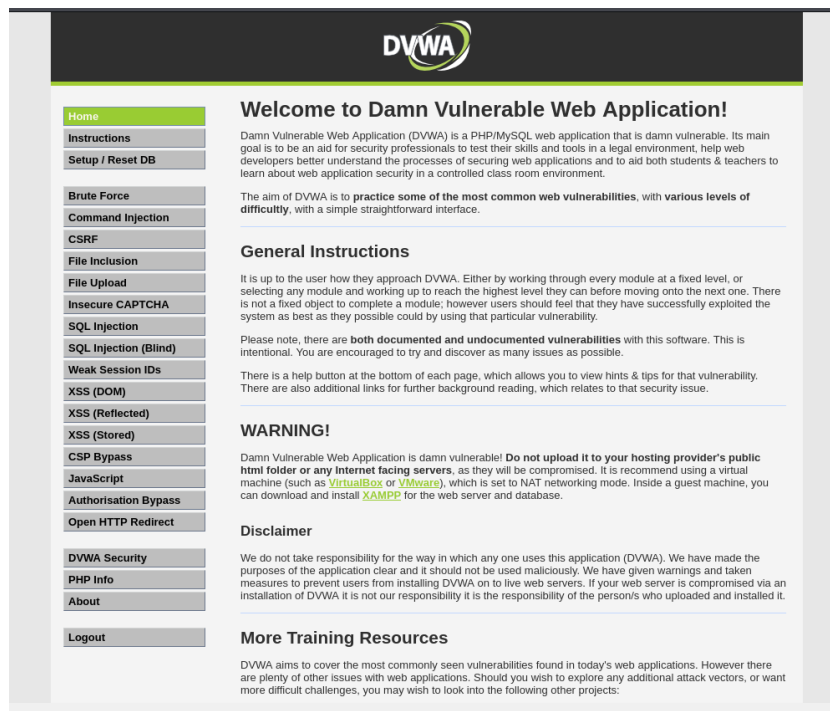


Рис. 17: Домашняя страница DVWA

## **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>