

Отчёт по 4 этапу индивидуального проекта

Использование nikto

Аристова Арина Олеговна

Содержание

1	Задание	4
2	Выполнение лабораторной работы	5
3	Выводы	13

Список иллюстраций

2.1	Клонирую заданный репозиторий по ссылке.	5
2.2	Перемещение файлов.	5
2.3	Заходим в эту директорию.	6
2.4	<i>https : //localhost</i>	6
2.5	Содержимое файла <i>config.inc.php</i>	7
2.6	Запуск <i>apache2</i>	8
2.7	Вход от имени администратора.	8
2.8	Выполняю команду <i>mysql</i> и некоторые команды внутри открыв- шегося MariaDB monitor.	9
2.9	Выполняю команду <i>mysql</i> и некоторые команды внутри открыв- шегося MariaDB monitor.	9
2.10	Вход с именем пользователя и паролем по умолчанию.	10
2.11	Страница входа.	10
2.12	Установка низкого уровня <i>DVWA Security</i> для дальнейшей ра- боты.	11
2.13	Выполнение команд от имени администратора.	11
2.14	Выполнение команд от имени администратора.	12

1 Задание

Установить DVWA в гостевую систему к Kali Linux.

2 Выполнение лабораторной работы

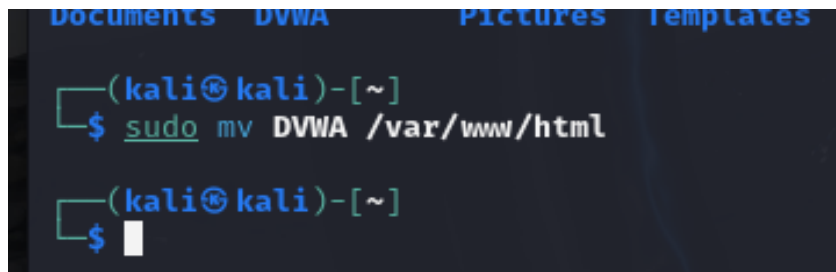
Клонирую заданный репозиторий по ссылке:

A terminal window on a Kali Linux system. The prompt is (kali@kali)-[~]. The user enters the command: git clone https://github.com/digininja/DVWA.git. The output shows the cloning process: Cloning into 'DVWA'..., remote: Enumerating objects: 4758, done., remote: Counting objects: 100% (308/308), done., remote: Compressing objects: 100% (180/180), done., remote: Total 4758 (delta 167), reused 241 (delta 122), pack-reused 4450 (from 1), Receiving objects: 100% (4758/4758), 2.39 MiB | 947.00 KiB/s, done., Resolving deltas: 100% (2262/2262), done. The prompt returns to (kali@kali)-[~].

```
(kali@kali)-[~]  
$ git clone https://github.com/digininja/DVWA.git  
Cloning into 'DVWA' ...  
remote: Enumerating objects: 4758, done.  
remote: Counting objects: 100% (308/308), done.  
remote: Compressing objects: 100% (180/180), done.  
remote: Total 4758 (delta 167), reused 241 (delta 122), pack-reused 4450 (from 1)  
Receiving objects: 100% (4758/4758), 2.39 MiB | 947.00 KiB/s, done.  
Resolving deltas: 100% (2262/2262), done.  
  
(kali@kali)-[~]  
$
```

Рис. 2.1: Клонирую заданный репозиторий по ссылке.

Далее перемещаем необходимые файлы согласно примеру:

A terminal window on a Kali Linux system. The prompt is (kali@kali)-[~]. The user enters the command: sudo mv DVWA /var/www/html. The prompt returns to (kali@kali)-[~].

```
(kali@kali)-[~]  
$ sudo mv DVWA /var/www/html  
  
(kali@kali)-[~]  
$
```

Рис. 2.2: Перемещение файлов.

И заходим в эту директорию:

```
(kali㉿kali)-[~]
$ cd /var/www/html

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

(kali㉿kali)-[/var/www/html]
$
```

Рис. 2.3: Заходим в эту директорию.

По ссылке *https : //localhost* ничего нет

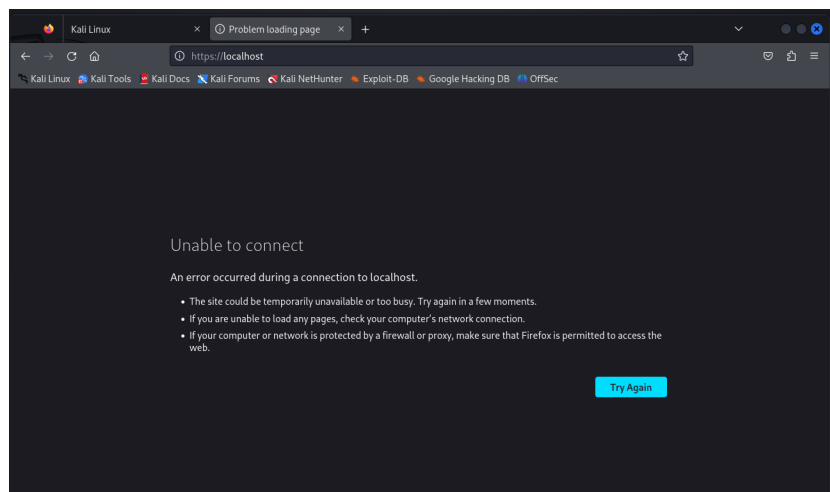


Рис. 2.4: *https : //localhost*.

Открываем файл *config.inc.php* в *config*:

```
GNU nano 8.1 config/config.inc.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 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' ] = 'dvwa';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';
$_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 'high'.
$_DVWA[ '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'.
$_DVWA[ 'default_locale' ] = 'en';

[ 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. 2.5: Содержимое файла *config.inc.php*.

Запускаем *apache2* и выполняем следующие действия:

```
(kali㉿kali)-[/var/www/html]
$ sudo service apache2 start

(kali㉿kali)-[/var/www/html]
$ cd DVWA

(kali㉿kali)-[/var/www/html/DVWA]
$ ls
about.php      dvwa          phpinfo.php   README.md     security.txt
CHANGELOG.md   external      php.ini       README.pt.md  setup.php
compose.yml    favicon.ico   README.ar.md  README.tr.md  tests
config         hackable     README.es.md  README.vi.md  vulnerabilities
COPYING.txt    index.php    README.fa.md  README.zh.md
database       instructions.php README.fr.md  robots.txt
Dockerfile     login.php    README.id.md  SECURITY.md
docs           logout.php   README.ko.md  security.php

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

(kali㉿kali)-[/var/www/html/DVWA]
$ cp config/config.inc.php.dist config/config.inc.php

(kali㉿kali)-[/var/www/html/DVWA]
$
```

Рис. 2.6: Запуск *apache2*.

Чтобы зайти от имени администратора я сначала устанавливаю пароль *root*, а потом уже захожу от имени администратора:

```
(kali㉿kali)-[~]
$

(kali㉿kali)-[~]
$ sudo passwd root

[sudo] password for kali:
New password:
Retype new password:
passwd: password updated successfully

(kali㉿kali)-[~]
$ su -
Password:
(kali㉿kali)-[~]
#
```

Рис. 2.7: Вход от имени администратора.

Затем выполняю команду *mysql* и ввожу там следующие команды:


```
File Actions Edit View Help /var/www/html
(kali@kali)-[~]
└─$ mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
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 database dvwa;
Query OK, 1 row affected (0.002 sec)

MariaDB [(none)]> create database dvw'asdfa;
> ;
> ;
→ ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
corresponds to your MariaDB server version for the right syntax to use near
''asdfa;
;
'' at line 1
MariaDB [(none)]> dreate database dvwa;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
corresponds to your MariaDB server version for the right syntax to use near
'r 'dreate database dvwa' at line 1
MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
ERROR 1133 (28000): Can't find any matching row in the user table
MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.011 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.009 sec)

MariaDB [(none)]> flush privileges;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
corresponds to your MariaDB server version for the right syntax to use near
'r 'priveleges' at line 1
MariaDB [(none)]>
```

Рис. 2.8: Выполняю команду *mysql* и некоторые команды внутри открывшегося MariaDB monitor.

```
(kali@kali)-[/var/www/html/DVWA]
└─$ mysql -u dvwa -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 33
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)]> use dvwa;
Database changed
MariaDB [dvwa]> bye;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
```

Рис. 2.9: Выполняю команду *mysql* и некоторые команды внутри открывшегося MariaDB monitor.

Теперь по адресу *localhost/DVWA/login.php* создаю базу данных с помо-

щью кнопки на сайте “Create/Change Database”. И захожу с именем пользователя и паролем по умолчанию:

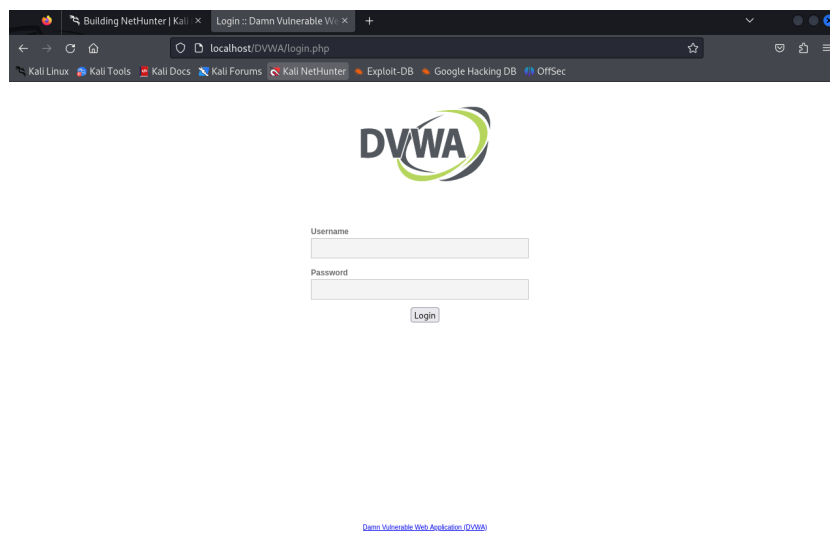


Рис. 2.10: Вход с именем пользователя и паролем по умолчанию.

Оказываемся на следующей странице:

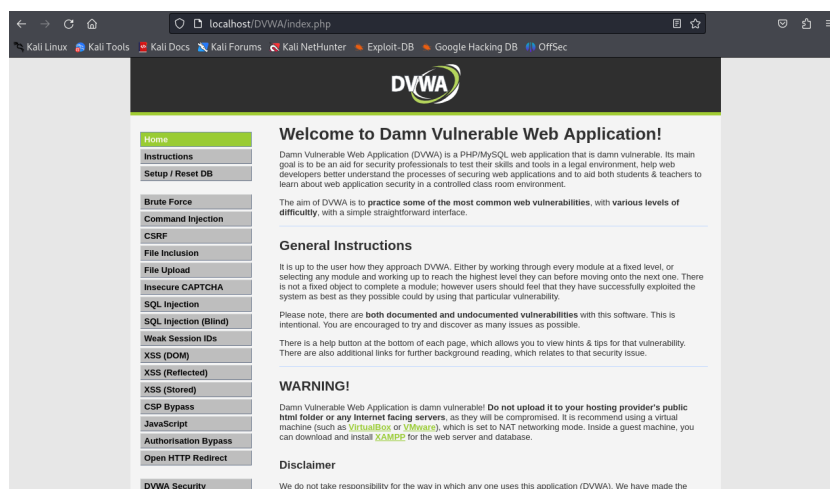


Рис. 2.11: Страница входа.

Устанавливаем низкий уровень *DVWASecurity* для дальнейшей работы.

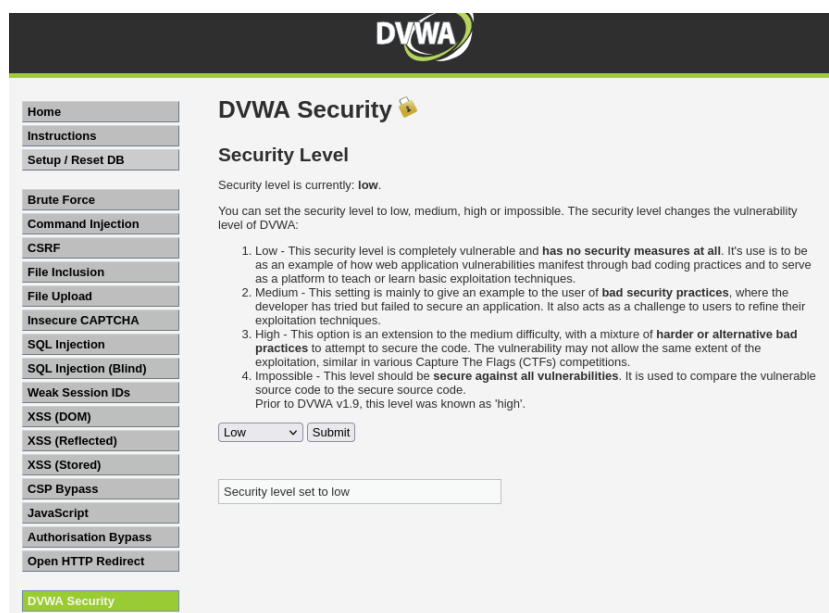


Рис. 2.12: Установка низкого уровня *DVWA Security* для дальнейшей работы.

Затем выполняем ряд команд по примеру:

```
(root@kali)~# cd /etc/php

(root@kali)~/etc/php# ls
8.2

(root@kali)~/etc/php# cd 8.2

(root@kali)~/etc/php/8.2# ls
in your SQL syntax, check the manual to
version for the right syntax to use near
apache2 cli mods-available

(root@kali)~/etc/php/8.2# cd apache2

(root@kali)~/etc/php/8.2/apache2# ls
conf.d  php.ini

(root@kali)~/etc/php/8.2/apache2# nano php.ini

(root@kali)~/etc/php/8.2/apache2# apachectl restart
AH00558: apache2: Could not reliably determine the server's fully qualified d
omain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppr
ess this message

(root@kali)~/etc/php/8.2/apache2# apt install php-gd
Error: Unable to locate package php-gd
```

Рис. 2.13: Выполнение команд от имени администратора.

```

(root@kali)-[/etc/php/8.2/apache2]
# apachectl restart
AH00558: apache2: Could not reliably determine the server's fully qualified d
omain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppr
ess this message

(root@kali)-[/etc/php/8.2/apache2]
# id www.data
id: 'www.data': no such user

(root@kali)-[/etc/php/8.2/apache2]
# ls -sl /var/www/html/DVWA/hackable/uploads
total 4
4 -rw-rw-r-- 1 kali kali 667 Sep 20 09:46 dvwa_email.png

(root@kali)-[/etc/php/8.2/apache2]
# chown www-data
chown: missing operand after 'www-data'
Try 'chown --help' for more information.

(root@kali)-[/etc/php/8.2/apache2]
# chown www-data /var/www/html/DVWA/hackable/uploads

(root@kali)-[/etc/php/8.2/apache2]
# id www.data
id: 'www.data': no such user

(root@kali)-[/etc/php/8.2/apache2]
# id www-data
uid=33(www-data) gid=33(www-data) groups=33(www-data)

(root@kali)-[/etc/php/8.2/apache2]
#

```

Рис. 2.14: Выполнение команд от имени администратора.

3 Выводы

В результате выполнения второго этапа индивидуального проекта я установила DVWA в гостевую систему Kali Linux.