

# **Этап 2. Установка DVWA**

**Установка DVWA**

Сагдеров Камал

# Содержание

<b>1</b>	<b>Выполнение лабораторной работы</b>	<b>5</b>
<b>2</b>	<b>Выводы</b>	<b>11</b>

# Список иллюстраций

1.1	1	. . . . .	5
1.2	2	. . . . .	5
1.3	3	. . . . .	6
1.4	4	. . . . .	7
1.5	5	. . . . .	7
1.6	6	. . . . .	8
1.7	7	. . . . .	9
1.8	8	. . . . .	9
1.9	9	. . . . .	10
1.10	10	. . . . .	10

## **Список таблиц**

# 1 Выполнение лабораторной работы

Установите DVWA в гостевую систему к Kali Linux.

```
(sagderovk@kali)-[~]
$ git clone https://github.com/digininja/DVWA.git
Cloning into 'DVWA' ...
remote: Enumerating objects: 4500, done.
remote: Counting objects: 100% (50/50), done.
remote: Compressing objects: 100% (39/39), done.
remote: Total 4500 (delta 17), reused 33 (delta 10), pack-reused 4450
Receiving objects: 100% (4500/4500), 2.27 MiB | 2.54 MiB/s, done.
Resolving deltas: 100% (2128/2128), done.

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

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

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

(sagderovk@kali)-[/var/www/html]
$
```

Рис. 1.1: 1

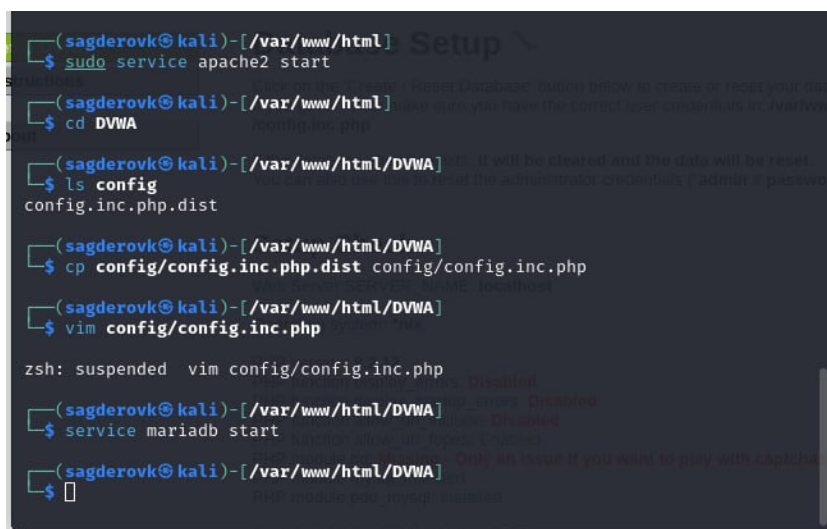
Репозиторий: <https://github.com/digininja/DVWA>. Некоторые из уязвимостей веб приложений, который содержит DVWA: Брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования инструментов по атаке на пароль методом грубой силы и показывает небезопасность слабых паролей.

```
root@kali: ~
File Actions Edit View Help

(sagderovk@kali)-[~]
$ sudo su -
[sudo] password for sagderovk:
(root@kali)-[~]
#
```

Рис. 1.2: 2

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.



```
(sagderovk@kali)-[/var/www/html] Setup
$ sudo service apache2 start
(sagderovk@kali)-[/var/www/html]
$ cd DVWA
(sagderovk@kali)-[/var/www/html/DVWA]
$ ls config
config.inc.php.dist
(sagderovk@kali)-[/var/www/html/DVWA]
$ cp config/config.inc.php.dist config/config.inc.php
(sagderovk@kali)-[/var/www/html/DVWA]
$ vim config/config.inc.php
zsh: suspended vim config/config.inc.php
(sagderovk@kali)-[/var/www/html/DVWA]
$ service mariadb start
(sagderovk@kali)-[/var/www/html/DVWA]
$
```

Рис. 1.3: 3

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: Невозможный — этот уровень должен быть безопасным от всех уязвимостей. Он используется для сравнения уязвимого исходного кода с безопасным исходным кодом.

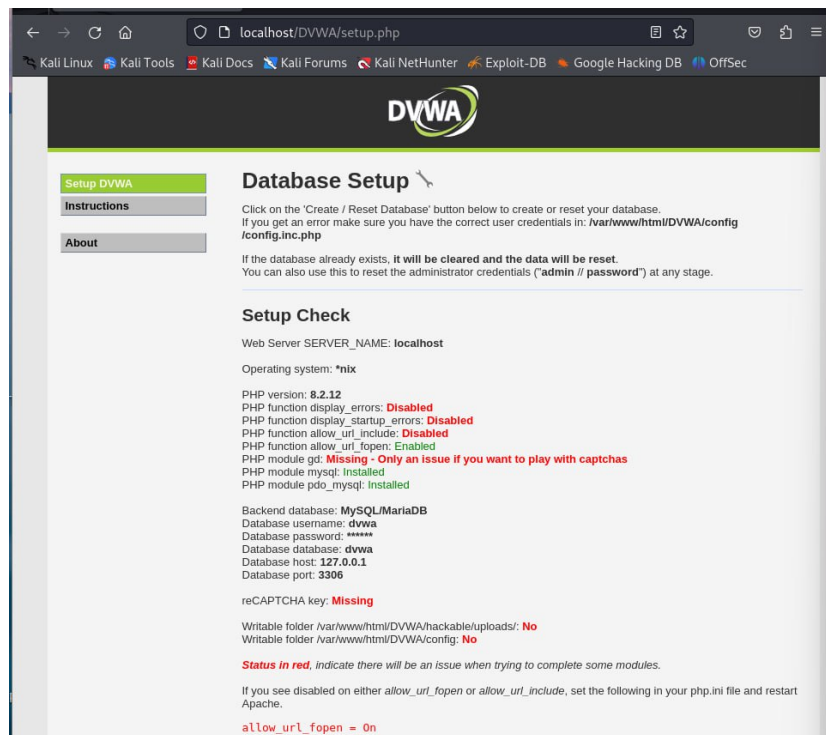


Рис. 1.4: 4

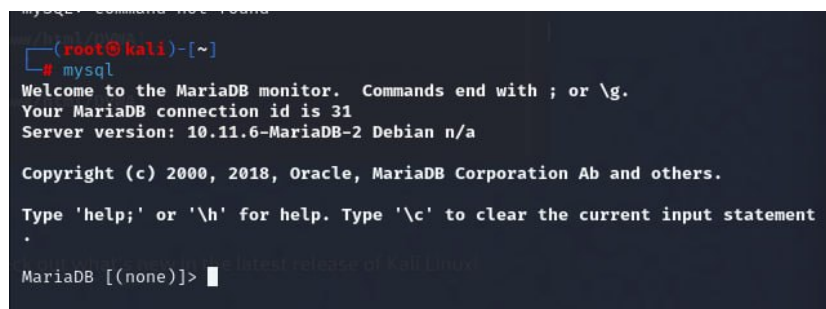


Рис. 1.5: 5

```
(root@kali)~# mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.6-MariaDB-2 Debian n/a

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)]> create database dvwa;
Query OK, 1 row affected (0.002 sec)

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 (0.008 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> 
```

Рис. 1.6: 6

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.



```
sagderovk@kali: ~  
File Actions Edit View Help  
sagderovk@kali: ~  
$ mysql -u dvwa -p  
Enter password:  
ERROR 1045 (28000): Access denied for user 'dvwa'@'localhost' (using password : YES)  
$ mysql -u dvwa -p  
Enter password:  
Welcome to the MariaDB monitor. Commands end with ; or \g.  
Your MariaDB connection id is 33  
Server version: 10.11.6-MariaDB-2 Debian n/a  
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)]>
```

Рис. 1.7: 7

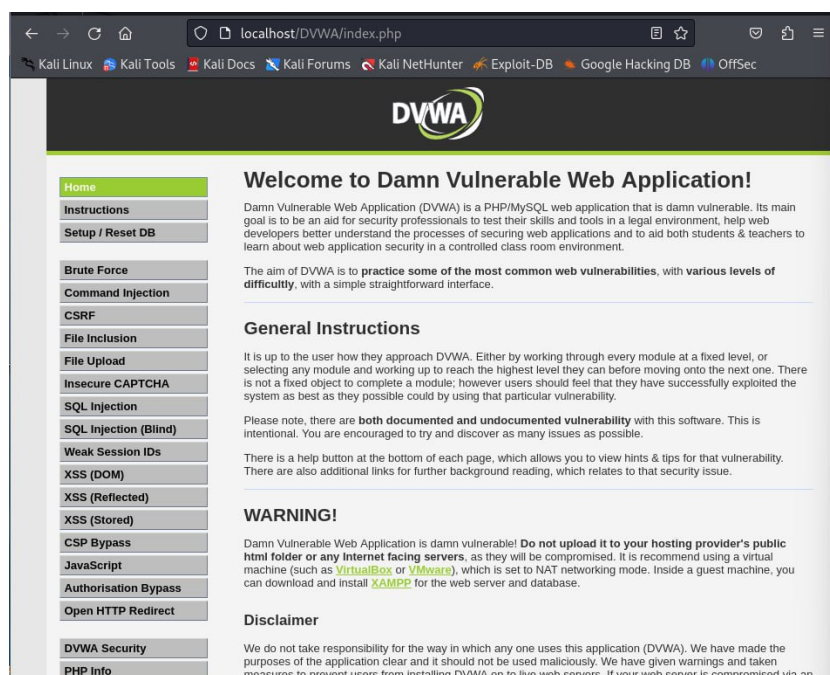


Рис. 1.8: 8

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.

```
(sagderovk@kali)-[/etc/php/8.2/apache2]
$ apt install php-gd
E: Could not open lock file /var/lib/dpkg/lock-frontent - open (13: Permission denied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontent), are you root?

(sagderovk@kali)-[/etc/php/8.2/apache2]
$ apt update
Reading package lists... Done
E: Could not open lock file /var/lib/apt/lists/lock - open (13: Permission denied)
E: Unable to lock directory /var/lib/apt/lists/
W: Problem unlinking the file /var/cache/apt/pkgcache.bin - RemoveCaches (13: Permission denied)
W: Problem unlinking the file /var/cache/apt/srcpkgcache.bin - RemoveCaches (13: Permission denied)

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

Рис. 1.9: 9

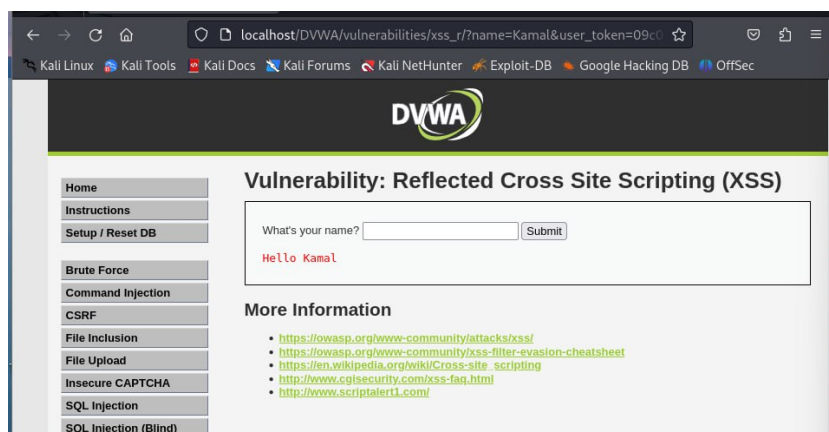


Рис. 1.10: 10

## 2 Выводы

Я научился устанавливать DVWA на Linux