

Отчёт по второму этапу проекта

Дисциплина: Основы информационной безопасности

Ганина Таисия Сергеевна, НКАбд-01-22

Содержание

1 Цель работы	5
2 Задание	6
3 Теоретическое введение	7
4 Выполнение лабораторной работы	8
5 Выводы	18
Список литературы	19

Список иллюстраций

4.1	Задание	8
4.2	Клонирование	8
4.3	Перемещаю файлы	9
4.4	Запускаю страничку старта	9
4.5	Перемещаю файлы	10
4.6	Запускаю сервер	10
4.7	Перехожу к корневому пользователю	11
4.8	Соединение с сервером	11
4.9	Создаю базу данных	12
4.10	Создаю базу данных	13
4.11	Задаю пароль и логин пользователя	13
4.12	Сохраняю изменения	14
4.13	Создаю базу данных	14
4.14	Загрузка утилиты	15
4.15	Проверка настроек	15
4.16	Настраиваю	16
4.17	Меняю id	16
4.18	Настраиваю	17
4.19	Результат	17

Список таблиц

1 Цель работы

Установить DVWA и провести первичную настройку.

2 Задание

1. Скачать с репозитория DVWA.
2. Провести настройку и запустить.

3 Теоретическое введение

Веб-приложение Damn Vulnerable — это программный проект, который намеренно содержит уязвимости в системе безопасности и предназначен для образовательных целей.

4 Выполнение лабораторной работы

Смотрю задание (рис. 4.1).

Этап 2. Установка DVWA

- Установите DVWA в гостевую систему к Kali Linux.
- Репозиторий: <https://github.com/digijinji/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.
 - Исполнение (внедрение) команд: Выполнение команд уровня операционной системы.
 - Межсайтовая подделка запросов (CSRF): Позволяет «атакующему» изменить пароль администратора приложений.
 - Внедрение (инъекция) файлов: Позволяет «атакующему» присоединить удаленные/локальные файлы в веб приложение.
 - Небезопасная выгрузка файлов: Позволяет «атакующему» выгрузить вредоносные файлы на веб сервер.
 - Межсайтовый скрипты (XSS): «Атакующий» может внедрить свои скрипты в веб приложение/базу данных. DVWA включает отраженную 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.
 - Высокий — это расширение среднего уровня сложности, со смыслью более сложных или альтернативных плохих практик в попытке обезопасить код. Уязвимости не позволяют такой простор эксплуатации как на других уровнях.
 - Средний — этот уровень безопасности предназначенным 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.

Рис. 4.1: Задание

Клонирую репозиторий (рис. 4.2).

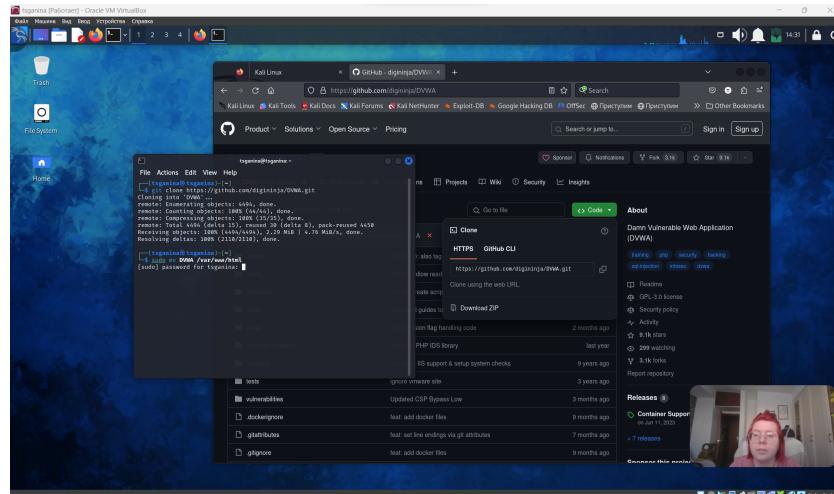
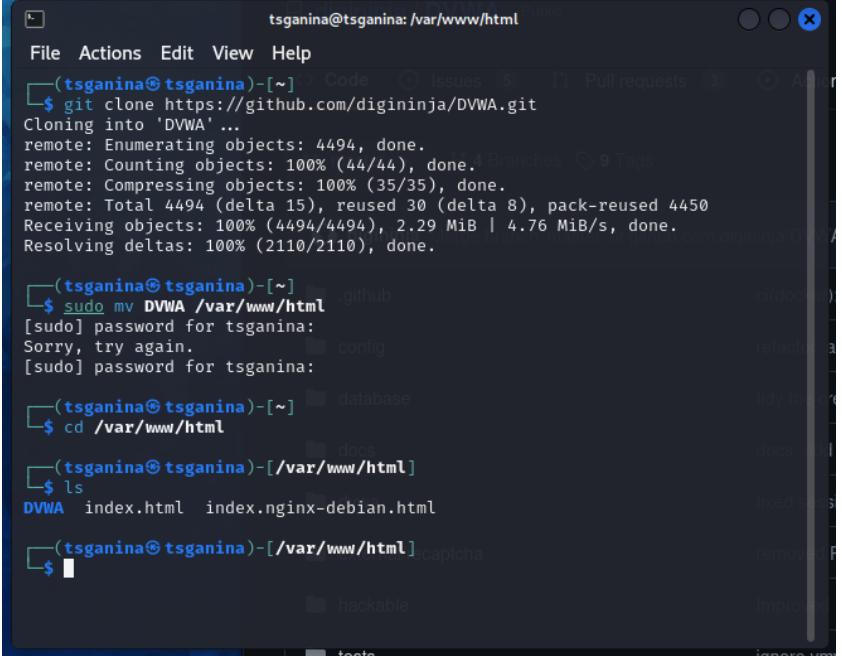


Рис. 4.2: Клонирование

Произвожу установку и настройку (рис. 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.14, 4.15, 4.16, 4.17, 4.18, 4.19).



```
tsganina@tsganina: /var/www/html
File Actions Edit View Help
└─(tsganina㉿tsganina)-[~] $ git clone https://github.com/digininja/DVWA.git
Cloning into 'DVWA' ...
remote: Enumerating objects: 4494, done.
remote: Counting objects: 100% (44/44), done.
remote: Compressing objects: 100% (35/35), done.
remote: Total 4494 (delta 15), reused 30 (delta 8), pack-reused 4450
Receiving objects: 100% (4494/4494), 2.29 MiB | 4.76 MiB/s, done.
Resolving deltas: 100% (2110/2110), done.

└─(tsganina㉿tsganina)-[~] $ sudo mv DVWA /var/www/html
[sudo] password for tsganina:
Sorry, try again.
[sudo] password for tsganina:

└─(tsganina㉿tsganina)-[~] $ cd /var/www/html
└─(tsganina㉿tsganina)-[/var/www/html] $ ls
DVWA index.html index.nginx-debian.html

└─(tsganina㉿tsganina)-[/var/www/html] $
```

Рис. 4.3: Перемещаю файлы

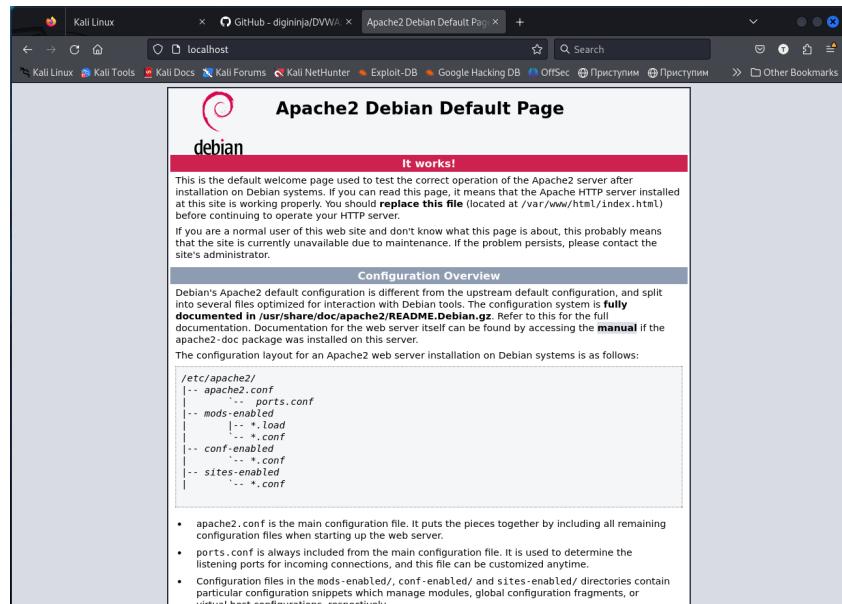


Рис. 4.4: Запускаю страничку старта

```
tsganina@tsganina: /var/www/html/DVWA
File Actions Edit View Help
(tsganina@tsganina)-[~]
$ cd /var/www/html
(tsganina@tsganina)-[/var/www/html]
$ ls
DVWA index.html index.nginx-debian.html
(tsganina@tsganina)-[/var/www/html]
$ sudo service apache2 start
(tsganina@tsganina)-[/var/www/html]
$ cd DVWA
(tsganina@tsganina)-[~/DVWA]
$ cp config/config.inc.php.dist config/config.inc.php
(tsganina@tsganina)-[~/DVWA]
$ service mariadb start
(tsganina@tsganina)-[~/DVWA]
$
```

Рис. 4.5: Перемещаю файлы

```
tsganina@tsganina: /var/www/html/DVWA
File Actions Edit View Help
About
(tsganina@tsganina)-[~/DVWA]
$ ls
DVWA index.html index.nginx-debian.html
(tsganina@tsganina)-[/var/www/html]
$ sudo service apache2 start
(tsganina@tsganina)-[/var/www/html]
$ cd DVWA
(tsganina@tsganina)-[~/DVWA]
$ ls /config
ls: cannot access '/config': No such file or directory
(tsganina@tsganina)-[~/DVWA]
$ ls config
config.inc.php.dist
(tsganina@tsganina)-[~/DVWA]
$ cp config/config.inc.php.dist config/config.inc.php
(tsganina@tsganina)-[~/DVWA]
$ service mariadb start
(tsganina@tsganina)-[~/DVWA]
$
```

Рис. 4.6: Запускаю сервер

```

Database Setup root@tsganina: ~
File Actions Edit View Help
Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: /var/www/html/DVWA/config
(tsganina㉿tsganina)-[~]
$ sudo su -
[sudo] password for tsganina: administrator credentials ("admin // password") at any stage.
(root㉿tsganina)-[~]
# mysql
Setup Check

Web Server SERVER_NAME: localhost

```

Рис. 4.7: Перехожу к корневому пользователю

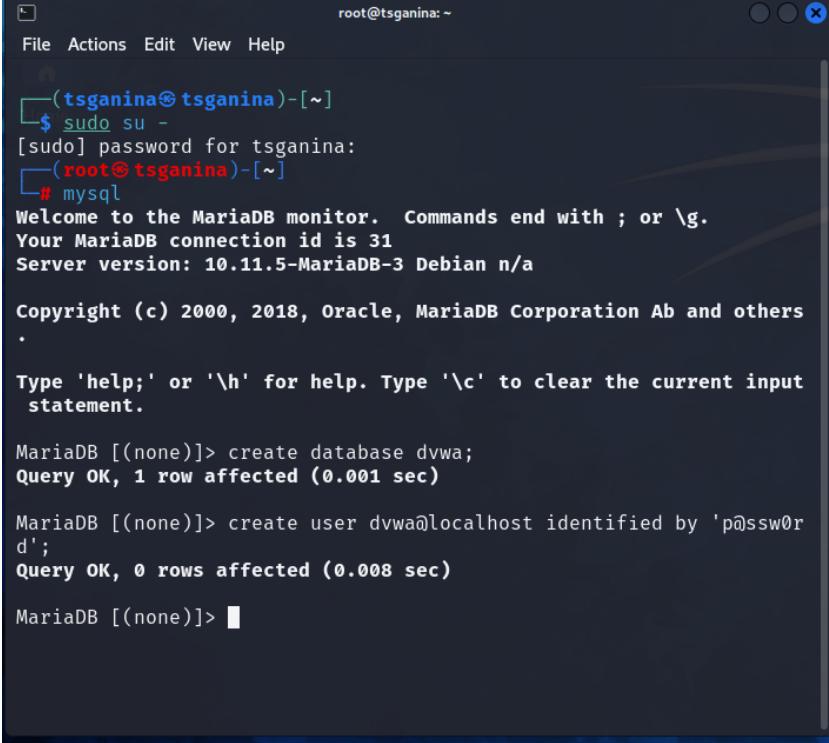
```

Database Setup root@tsganina: ~
File Actions Edit View Help
Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: /var/www/html/DVWA/config
(tsganina㉿tsganina)-[~]
$ sudo su -
[sudo] password for tsganina: administrator credentials ("admin // password") at any stage.
(root㉿tsganina)-[~]
# mysql
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31 [localhost]
Server version: 10.11.5-MariaDB-3 Debian n/a
Operating system: "nix"
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others
.
PHP function display_errors: Disabled
PHP function display_startup_errors: Disabled
PHP function allow_url_include: Disabled
Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.
.
PHP module gd: Missing - Only an issue if you want to play with captchas
PHP module mysqli: Installed
PHP module pdo_mysql: Installed
MariaDB [(none)]> status
Backend database: MySQL/MariaDB
Database username: dvwa
Database password: *****
Database database: dvwa
Database host: 127.0.0.1
Database port: 3306
reCAPTCHA key: Missing
Writable folder /var/www/html/DVWA/hackable/uploads/: No
Writable folder /var/www/html/DVWA/config: No
Status in red, indicate there will be an issue when trying to complete some modules.

If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php

```

Рис. 4.8: Соединение с сервером



root@tsganina: ~

```
[File Actions Edit View Help]
[(tsganina㉿tsganina)-[~]
$ sudo su -
[sudo] password for tsganina:
[(root㉿tsganina)-[~]
# mysql
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.5-MariaDB-3 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 (0.001 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0r
d';
Query OK, 0 rows affected (0.008 sec)

MariaDB [(none)]> #
```

Рис. 4.9: Создаю базу данных

```
root@tsganina:~  
File Actions Edit View Help  
└$ sudo su -  
[sudo] password for tsganina:  
└─(root@tsganina)-[~]  
# mysql  
Welcome to the MariaDB monitor. Commands end with ; or \g.  
Your MariaDB connection id is 31  
Server version: 10.11.5-MariaDB-3 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 (0.001 sec)  
  
MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0r  
d';  
Query OK, 0 rows affected (0.008 sec)  
  
MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;  
Query OK, 0 rows affected (0.005 sec)  
  
MariaDB [(none)]> flush privileges;  
Query OK, 0 rows affected (0.002 sec)  
  
MariaDB [(none)]>
```

Рис. 4.10: Создаю базу данных

```
tsganina@tsganina:~  
File Actions Edit View Help  
ERROR 1045 (28000): Access denied for user 'dvwa'@'localhost' (using password: YES)  
└─(tsganina@tsganina)-[~]  
$ mysql -u dvwa -p  
Enter password:  
Welcome to the MariaDB monitor. Commands end with ; or \g.  
Your MariaDB connection id is 33  
Server version: 10.11.5-MariaDB-3 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.  
|> create database dvwa;  
MariaDB [(none)]>
```

Рис. 4.11: Задаю пароль и логин пользователя

```
tsganina@tsganina: ~
File Actions Edit View Help
(tsganina@tsganina)-[~]
$ mysql -u dvwa -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ;
; or \g.
Your MariaDB connection id is 33
Server version: 10.11.5-MariaDB-3 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)]> use dvwa
Database changed
MariaDB [dvwa]>
```

Рис. 4.12: Сохраняю изменения

```
root@tsganina: ~
File Actions View Help
(root@tsganina)-[~]
# mysql
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.5-MariaDB-3 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 (0.001 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0r
d';
Query OK, 0 rows affected (0.008 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.005 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> create database dvwa;
ERROR 1007 (HY000): Can't create database 'dvwa'; database exists
MariaDB [(none)]>
```

Рис. 4.13: Создаю базу данных

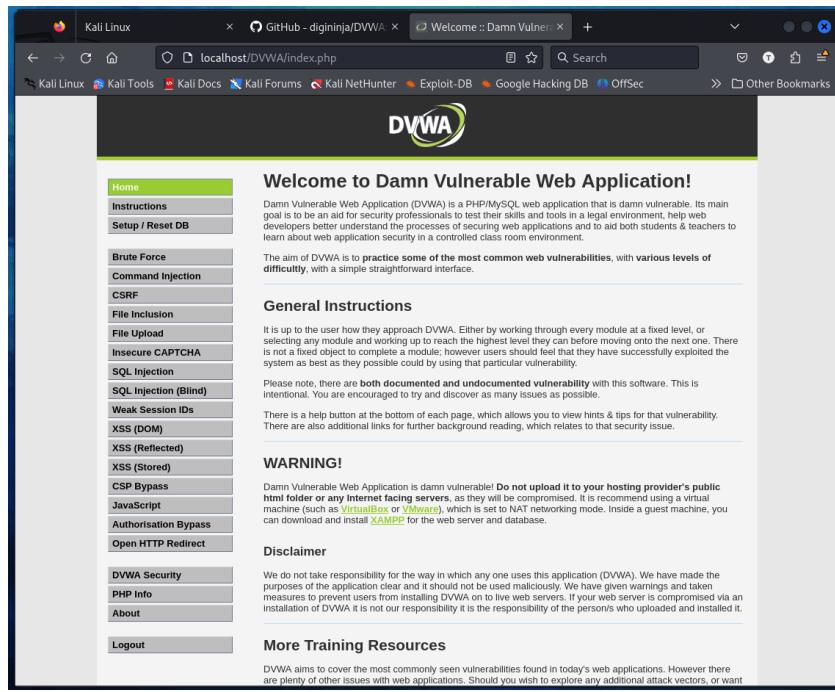


Рис. 4.14: Загрузка утилиты

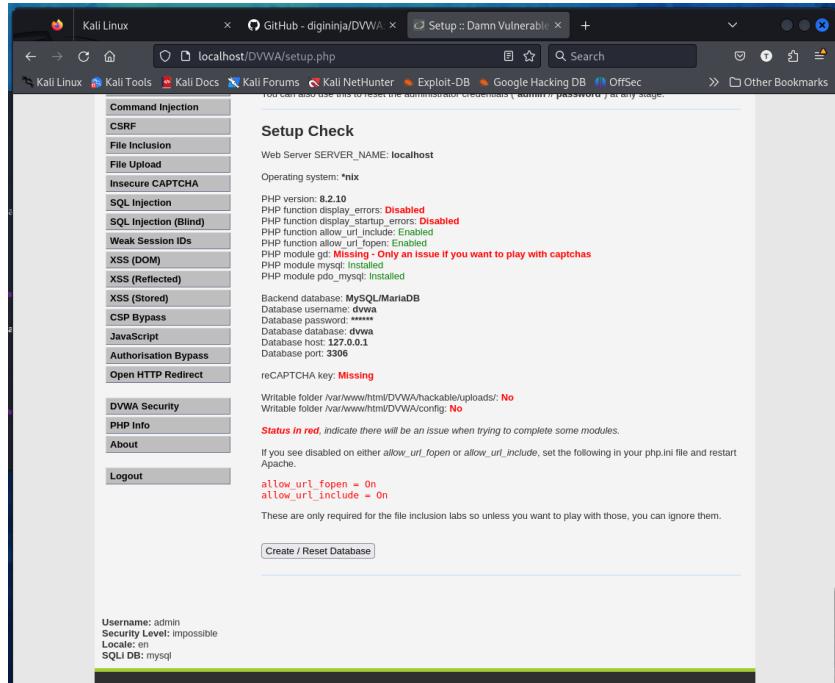


Рис. 4.15: Проверка настроек

```
root@tsganina: /etc/php/8.2/apache2
File Actions Edit View Help
(tsganina㉿tsganina)~
$ su -
Password:
su: Authentication failure
(tsganina㉿tsganina)~
$ sudo su -
[sudo] password for tsganina:
(root㉿tsganina)~
# /etc/php/8.2
(root㉿tsganina)~/etc/php/8.2
# ls
apache2 cli mods-available
(root㉿tsganina)~/etc/php/8.2
# cd apache2
(root㉿tsganina)~/etc/php/8.2/apache2
# ls
conf.d php.ini
(root㉿tsganina)~/etc/php/8.2/apache2
# nano php.ini
(root㉿tsganina)~/etc/php/8.2/apache2
```

Рис. 4.16: Настраиваю

```
root@tsganina: /etc/php/8.2/apache2
File Actions Edit View Help
conf.d php.ini
(root㉿tsganina)~/etc/php/8.2/apache2
# nano php.ini
(root㉿tsganina)~/etc/php/8.2/apache2
# vim php.ini
(root㉿tsganina)~/etc/php/8.2/apache2
# apachectl restart
(root㉿tsganina)~/etc/php/8.2/apache2
# id WWW-data
id: 'WWW-data': no such user
(root㉿tsganina)~/etc/php/8.2/apache2
# id www-data
uid=33(www-data) gid=33(www-data) groups=33(www-data)
(root㉿tsganina)~/etc/php/8.2/apache2
# ls -al /var/www/html/DVWA/hackable/uploads/
total 12
drwxr-xr-x 2 tsganina tsganina 4096 Mar  9 14:29 .
drwxr-xr-x 5 tsganina tsganina 4096 Mar  9 14:29 ..
-rw-r--r-- 1 tsganina tsganina  667 Mar  9 14:29 dvwa_email.png
(root㉿tsganina)~/etc/php/8.2/apache2
```

Рис. 4.17: Меняю id

```

root@tsganina: /etc/php/8.2/apache2
File Actions Edit View Help
└─(root@tsganina)-[/etc/php/8.2/apache2]
# id www-data
id: 'WWW-data': no such user

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

└─(root@tsganina)-[/etc/php/8.2/apache2]
# ls -al /var/www/html/DVWA/hackable/uploads/
total 12
drwxr-xr-x 2 tsganina tsganina 4096 Mar  9 14:29 .
drwxr-xr-x 5 tsganina tsganina 4096 Mar  9 14:29 ..
-rw-r--r-- 1 tsganina tsganina 667 Mar  9 14:29 dvwa_email.png

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

└─(root@tsganina)-[/etc/php/8.2/apache2]
# ls -al /var/www/html/DVWA/hackable/uploads/
total 12
drwxr-xr-x 2 www-data tsganina 4096 Mar  9 14:29 .
drwxr-xr-x 5 tsganina tsganina 4096 Mar  9 14:29 ..
-rw-r--r-- 1 tsganina tsganina 667 Mar  9 14:29 dvwa_email.png

└─(root@tsganina)-[/etc/php/8.2/apache2]
#

```

Рис. 4.18: Настраиваю

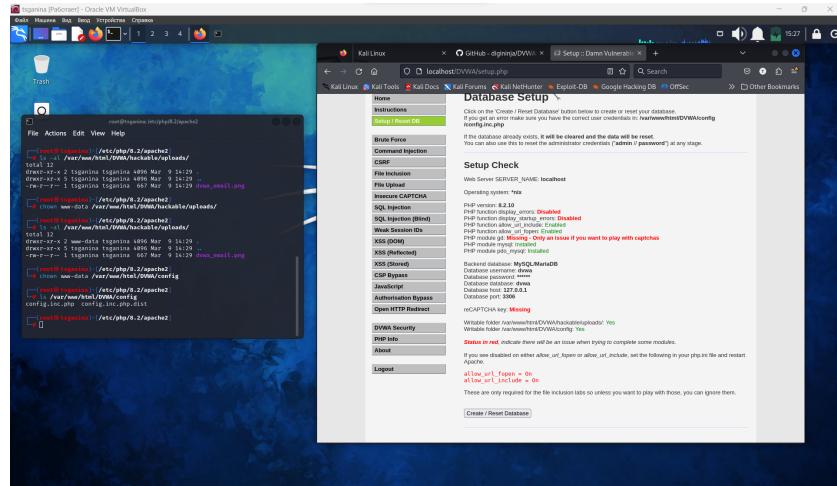


Рис. 4.19: Результат

5 Выводы

Установила DVWA.

Список литературы

1. Видео