

Презентация ко 2 этапу индивидуального проекта

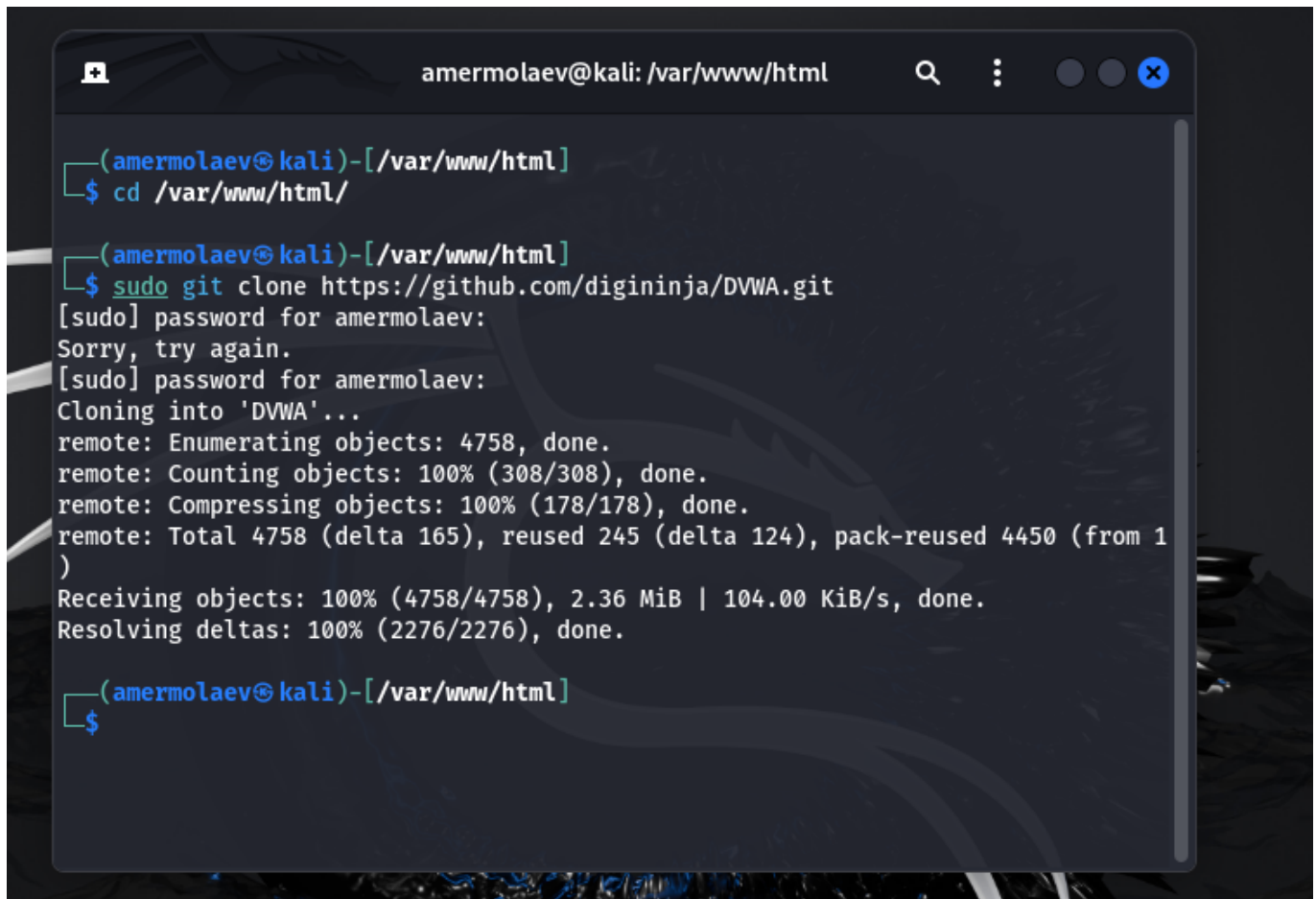
Цель работы

Приобретение практического навыка установки и развертывания веб-приложения DVWA в гостевую систему к Kali Linux.



Выполнение работы

Клонирование репозитория

A terminal window titled 'amermolaev@kali: /var/www/html' with standard window controls. The terminal shows the user navigating to the directory and cloning the DVWA repository from GitHub. The cloning process is successful, showing progress for enumerating, counting, and compressing objects, and finally receiving and resolving deltas.

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

(amermolaev@kali)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA.git
[sudo] password for amermolaev:
Sorry, try again.
[sudo] password for amermolaev:
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 165), reused 245 (delta 124), pack-reused 4450 (from 1)
Receiving objects: 100% (4758/4758), 2.36 MiB | 104.00 KiB/s, done.
Resolving deltas: 100% (2276/2276), done.

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

Копирование содержимого файла

```
Sep 17 / 23:01
amermolaev@kali: /var/www/html/DVWA/config

(amermolaev@kali)-[/var/www/html]
$ cd DVWA

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

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

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

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

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

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

Содержание файла config.inc.php

```
Sep 17 23:05
+ amermolaev@kali: /var/www/html/DVWA/config  Q  ⋮  ●  ●  ×
GNU nano 8.1 config.inc.php
<?php

# If you are having problems connecting to the MySQL database and all of the va>
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a pr>
# Thanks to @diginiinja 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 dedi>
# 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/>
[ Read 56 lines (converted from DOS format) ]
^G Help      ^O Write Out ^F Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line
```

Запуск сервиса MySQL

```
amermolaev@kali: /var/www/html/DVWA/config

(amermolaev@kali)-[/var/www/html/DVWA/config]
$ sudo service mysql status
○ mariadb.service - MariaDB 11.4.2 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset:▶
   Active: inactive (dead)
   Docs: man:mariadb(8)
         https://mariadb.com/kb/en/library/systemd/

(amermolaev@kali)-[/var/www/html/DVWA/config]
$ sudo service mysql start

(amermolaev@kali)-[/var/www/html/DVWA/config]
$ sudo service mysql status
● mariadb.service - MariaDB 11.4.2 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset:▶
   Active: active (running) since Tue 2024-09-17 23:07:35 MSK; 2s ago
   Invocation: a93f0149e2214a78802fe64d85caecc3
   Docs: man:mariadb(8)
         https://mariadb.com/kb/en/library/systemd/
   Process: 2510 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var>
   Process: 2512 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_ST>
   Process: 2514 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] 88>
   Process: 2588 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_S>
   Process: 2590 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/>
   Main PID: 2574 (mariadb)
   Status: "Taking your SQL requests now..."
   Tasks: 14 (limit: 30407)
   Memory: 241.6M (peak: 245.7M)
```

Вход в оболочку MySQL

```
Places Sep 17 23:10
root@kali: /var/www/html/DVWA/config

(amermolaev@kali)-[/var/www/html/DVWA/config]
$ sudo su
(root@kali)-[/var/www/html/DVWA/config]
# mysql

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)]> SELECT User FROM mysql.user;
+-----+
| User |
+-----+
| mariadb.sys |
| mysql |
| root |
+-----+
3 rows in set (0.001 sec)

MariaDB [(none)]> █
```

Создание базы данных и пользователя

```
Places Sep 17 23:14
root@kali: /var/www/html/DVWA/config

(root@kali)-[/var/www/html/DVWA/config]
# 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 (0.001 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.009 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.006 sec)

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

MariaDB [(none)]> 
```

```
Places Sep 17 23:15
root@kali: /var/www/html/DVWA/config

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)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| dvwa      |
| information_schema |
| mysql     |
| performance_schema |
| sys       |
+-----+
5 rows in set (0.001 sec)

MariaDB [(none)]> SELECT User FROM mysql.user;
+-----+
| User |
+-----+
| dvwa  |
| mariadb.sys |
| mysql |
| root  |
+-----+
4 rows in set (0.001 sec)

MariaDB [(none)]> 
```



```
ps  Places                               Sep 17/ 23:18
+-----+
+-----+ amermolaev@kali: /var/www/html/DVWA/config
+-----+
(amer-molaev@kali)-[/var/www/html/DVWA/config]
$ mysql -u dvwa -pp@ssw0rd
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 34
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]>
```

Настройка и запуск веб-сервера apache2

```
+-----+                               amermolaev@kali: /etc/php/8.2/apache2
+-----+
GNU nano 8.1                               php.ini
+-----+

; 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.
; https://php.net/from
;from="john@doe.com"

; Define the User-Agent string. PHP's default setting for this is empty.
; https://php.net/user-agent
user_agent="PHP"

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

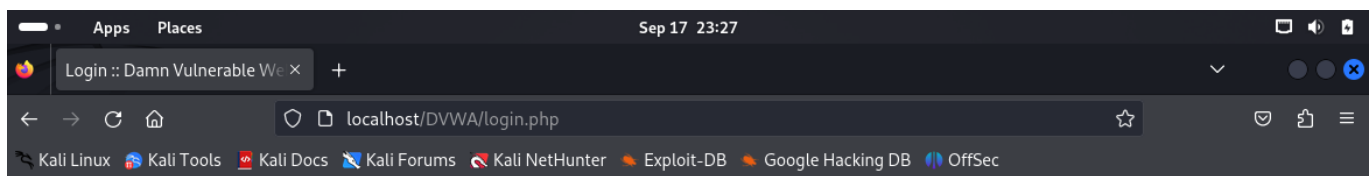
```
amermolaev@kali: /etc/php/8.2/apache2

(amermolaev@kali)-[/etc/php/8.2/apache2]
$ sudo service apache2 status
○ apache2.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
  Active: inactive (dead)
  Docs: https://httpd.apache.org/docs/2.4/

(amermolaev@kali)-[/etc/php/8.2/apache2]
$ sudo service apache2 start

(amermolaev@kali)-[/etc/php/8.2/apache2]
$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
  Active: active (running) since Tue 2024-09-17 23:25:23 MSK; 8s ago
  Invocation: 1cc91747562043299b5436820299b43a
  Docs: https://httpd.apache.org/docs/2.4/
  Process: 3267 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 3283 (apache2)
  Tasks: 7 (limit: 4607)
  Memory: 20.5M (peak: 20.8M)
  CPU: 135ms
  CGroup: /system.slice/apache2.service
          └─3283 /usr/sbin/apache2 -k start
            └─3286 /usr/sbin/apache2 -k start
              └─3287 /usr/sbin/apache2 -k start
                └─3288 /usr/sbin/apache2 -k start
                  └─3289 /usr/sbin/apache2 -k start
                    └─3290 /usr/sbin/apache2 -k start
```

Форма авторизации



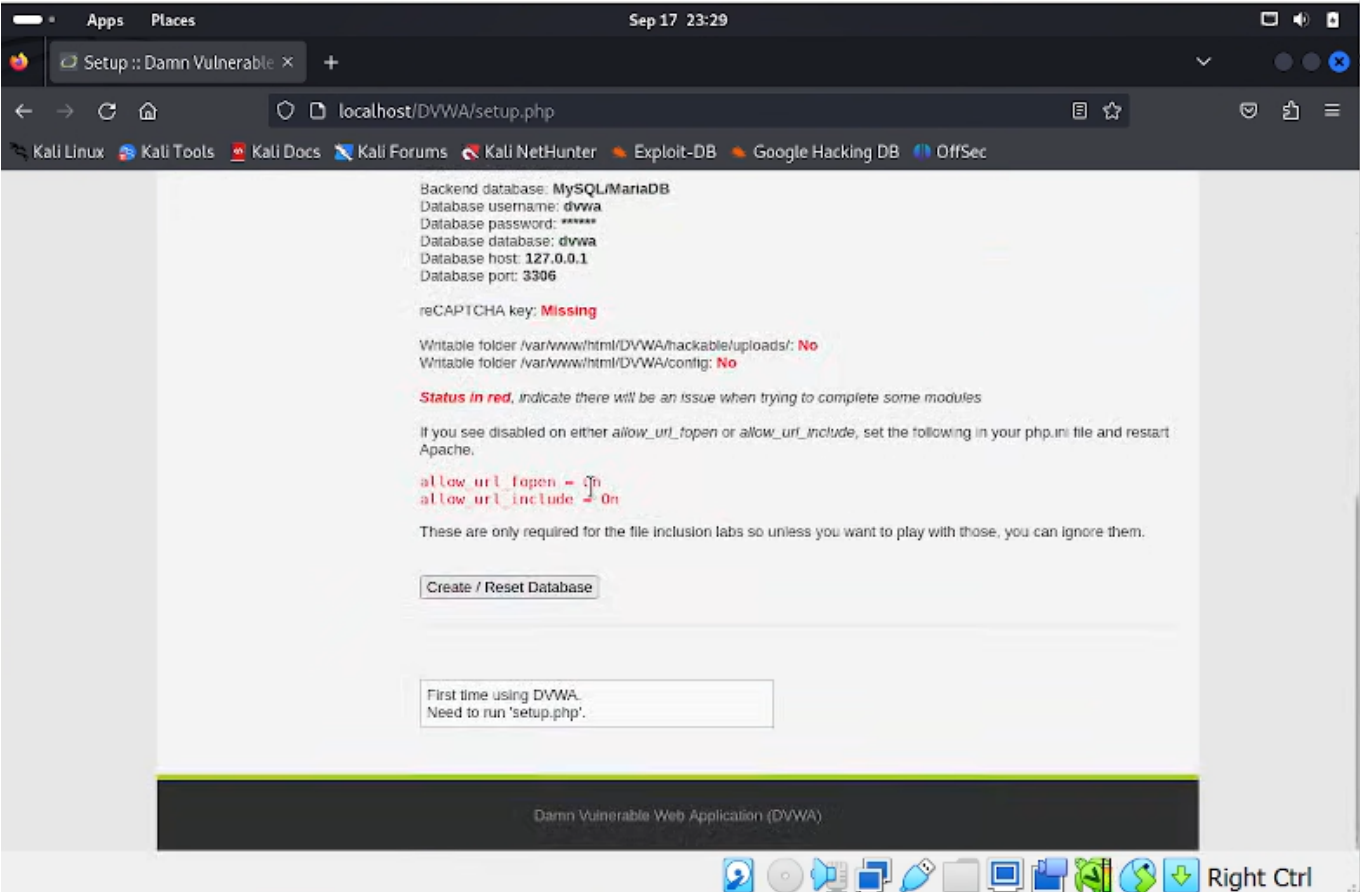
Username

Password

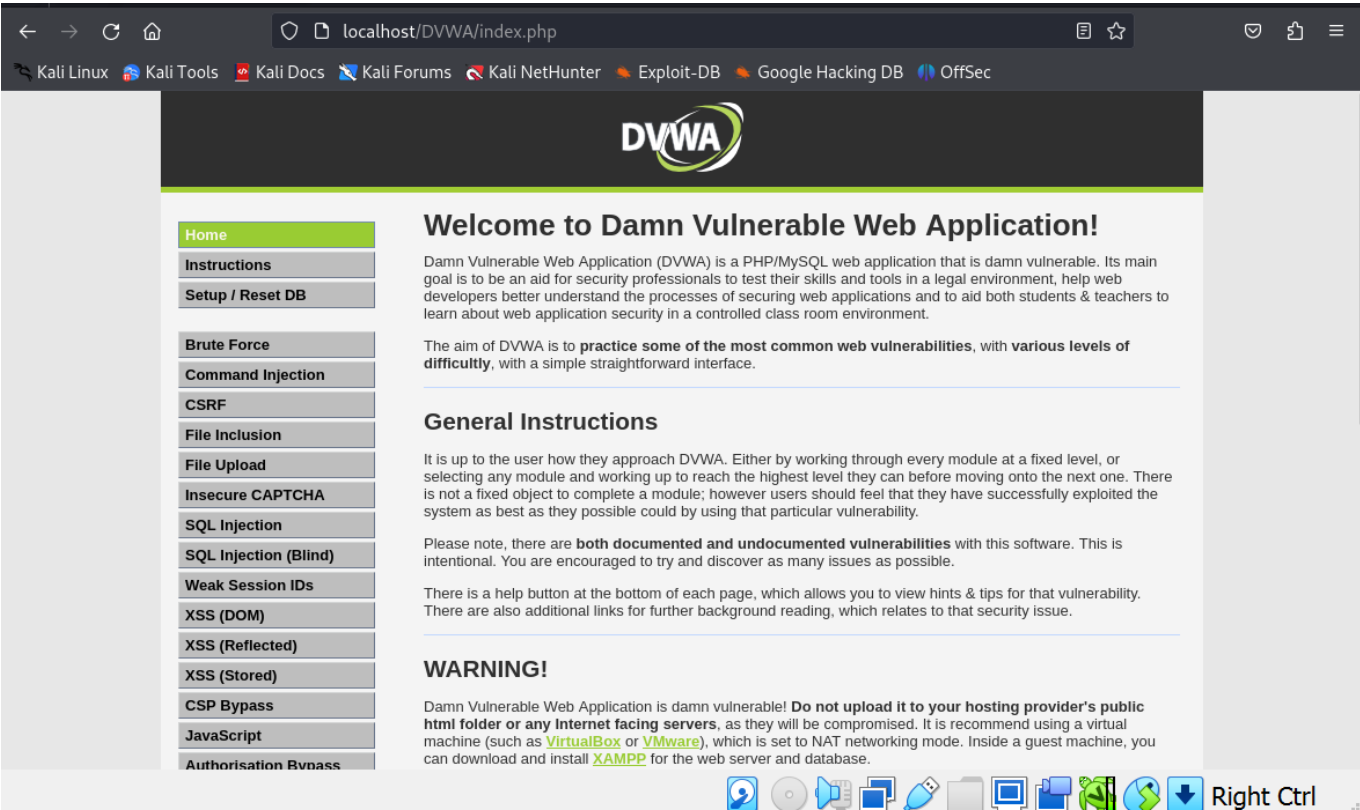
Login

[Damn Vulnerable Web Application \(DVWA\)](#)

Создание баз данных

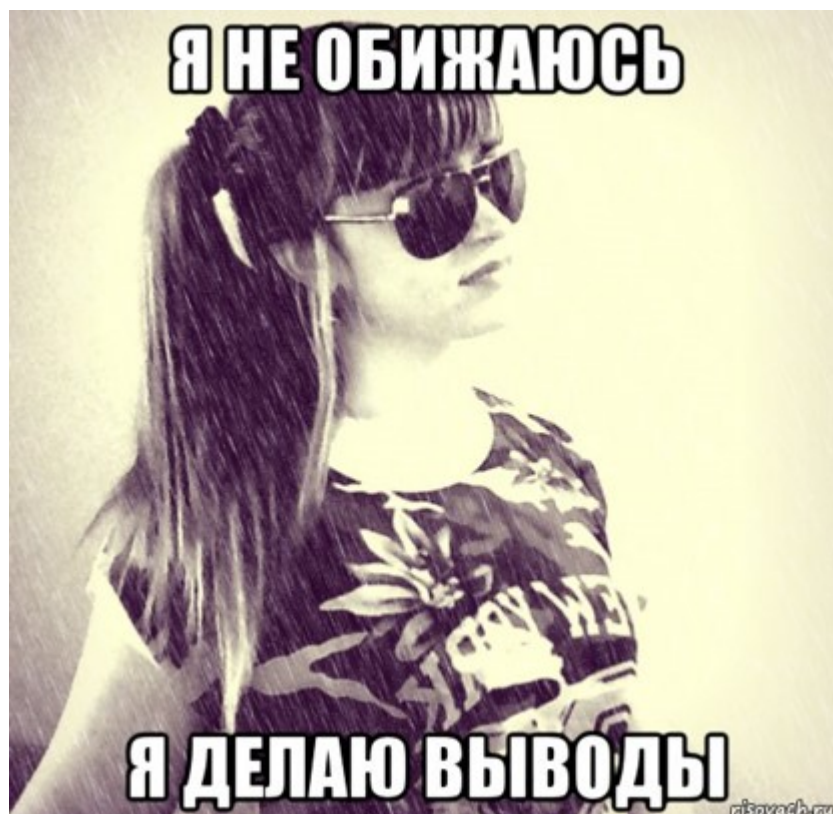


Развернутое приложение



Вывод

В рамках выполнения работы я получил практический навык установки и развертывания веб-приложения DVWA в гостевую систему к Kali Linux.



Финал

