

Индивидуальный проект.Этап 2

Установка и настройка DVWA

Хамдамова Айжана

Содержание

1	Цель работы	5
2	Выводы	18
	Список литературы	19

Список иллюстраций

1.1	Заходим в нужный каталог	7
1.2	Распаковываем DVWA	8
1.3	Статус	11
1.4	Результат	17

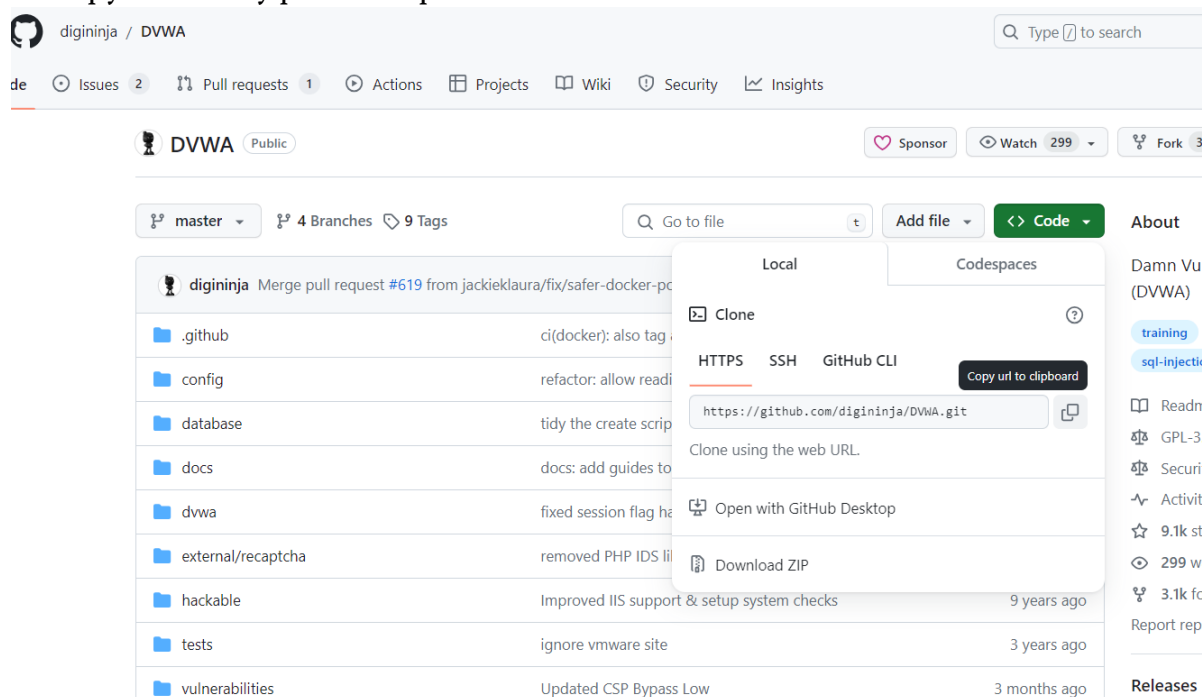
Список таблиц

1 Цель работы

Установить DVWA в гостевую систему к Kali Linux. # Теоретическое введение
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. 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: 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. 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. 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

Копируем ссылку репозитория



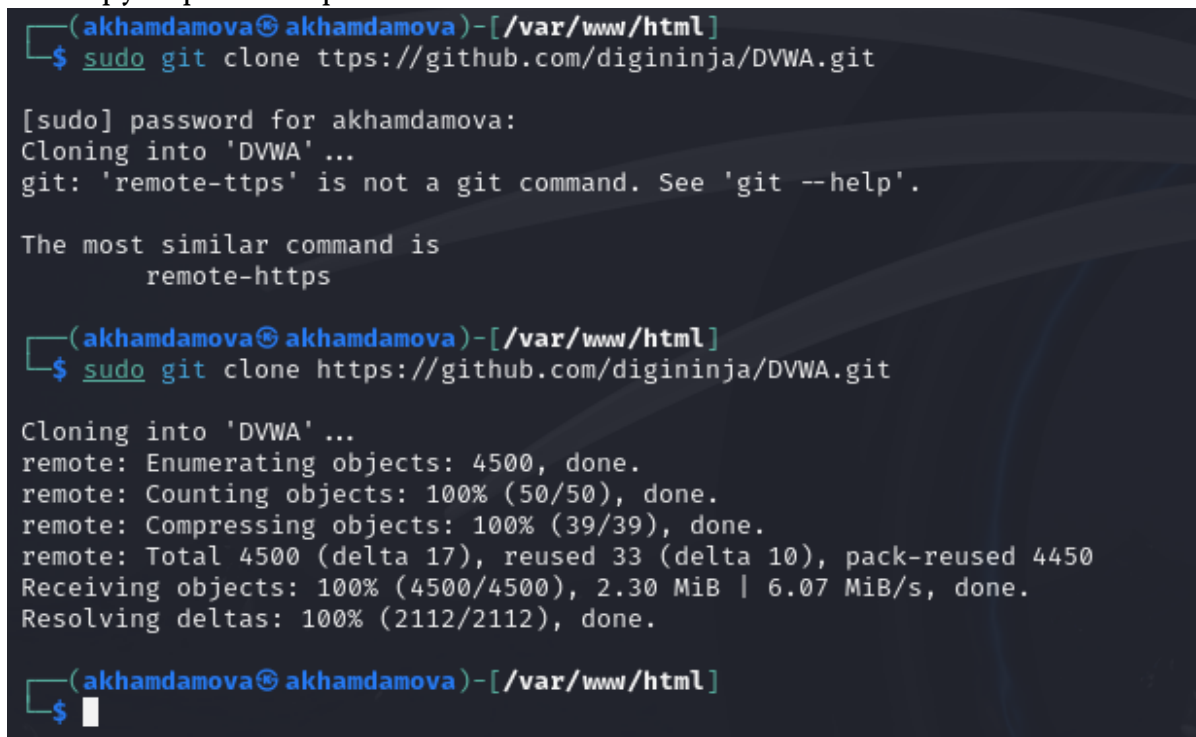
The screenshot shows the GitHub interface for the repository `digininja / DVWA`. The repository is public and has 299 watchers and 3 forks. The `Code` dropdown menu is open, displaying the `Clone` option with the `HTTPS` tab selected. The URL `https://github.com/digininja/DVWA.git` is shown and copied to the clipboard. The repository file list is visible in the background, showing folders like `.github`, `config`, `database`, `docs`, `dvwa`, `external/recaptcha`, `hackable`, `tests`, and `vulnerabilities`.



```
akhamdamova@akhamdamova: /var/www/html
File Actions Edit View Help
(akhamdamova@akhamdamova)-[~]
$ cd /var/www/html
(akhamdamova@akhamdamova)-[/var/www/html]
$ git clone https://github.com/digininja/DVWA.git
fatal: could not create work tree dir 'DVWA': Permission denied
(akhamdamova@akhamdamova)-[/var/www/html]
$
```

Рис. 1.1: Заходим в нужный каталог

Клонируем репозиторий в нем



```
(akhamdamova@akhamdamova)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA.git
[sudo] password for akhamdamova:
Cloning into 'DVWA' ...
git: 'remote-ttps' is not a git command. See 'git --help'.

The most similar command is
remote-https
(akhamdamova@akhamdamova)-[/var/www/html]
$ sudo 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), 2.30 MiB | 6.07 MiB/s, done.
Resolving deltas: 100% (2112/2112), done.
(akhamdamova@akhamdamova)-[/var/www/html]
$
```

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

(akhamdamova@akhamdamova)-[/var/www/html]
$ sudo chmod -R 777 DVWA

(akhamdamova@akhamdamova)-[/var/www/html]
$ sudo chmod -R 777 DVWA

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

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

Рис. 1.2: Распаковываем DVWA

Настраиваем права доступа


```
(akhamdamova® akhamdamova)-[/var/www/html]
$ cd DVWA

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

(akhamdamova® akhamdamova)-[/var/www/html/DVWA]
$ cd config

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

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

(akhamdamova® akhamdamova)-[/var/www/html/DVWA/config]
$ sudo mousepad config.inc.php
```

Меняем пароль и имя пользователя


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

(akhamdamova@akhamdamova)~[/var/www/html/DVWA/config]
$ sudo systemctl status mysql
● mariadb.service - MariaDB 10.11.6 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; pres>
   Active: active (running) since Fri 2024-03-15 15:59:55 EDT; 7s ago
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
   Process: 6727 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d />
   Process: 6729 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP>
   Process: 6731 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] >
   Process: 6811 ExecStartPost=/bin/sh -c systemctl unset-environment _WSRE>
   Process: 6813 ExecStartPost=/etc/mysql/debian-start (code=exited, status>
  Main PID: 6792 (mariabdd)
    Status: "Taking your SQL requests now..."
     Tasks: 12 (limit: 2274)
    Memory: 218.1M (peak: 222.0M)
       CPU: 836ms
    CGroup: /system.slice/mariadb.service
            └─6792 /usr/sbin/mariabdd
```

Рис. 1.3: Статус

```
(akhamdamova@akhamdamova)~[/var/www/html/DVWA/config]
$ sudo su
(root@akhamdamova)~[/var/www/html/DVWA/config]
# mysql -u root -p
Enter password:
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 (0.025 sec)

MariaDB [(none)]> create user 'admin'@'127.0.0.1' identified by 'password';
Query OK, 0 rows affected (0.030 sec)

MariaDB [(none)]> █
```

```
File Actions Edit View Help
└─6792 /usr/sbin/mariabdd

Mar 15 15:59:55 akhamdamova mariabdd[6792]: 2024-03-15 15:59:55 0 [Note] Plu>
Mar 15 15:59:55 akhamdamova mariabdd[6792]: 2024-03-15 15:59:55 0 [Note] Inn>
Mar 15 15:59:55 akhamdamova mariabdd[6792]: 2024-03-15 15:59:55 0 [Warning] >
Mar 15 15:59:55 akhamdamova mariabdd[6792]: 2024-03-15 15:59:55 0 [Note] Ser>
Mar 15 15:59:55 akhamdamova mariabdd[6792]: 2024-03-15 15:59:55 0 [Note] /us>
Mar 15 15:59:55 akhamdamova mariabdd[6792]: Version: '10.11.6-MariaDB-2' so>
Mar 15 15:59:55 akhamdamova systemd[1]: Started mariadb.service - MariaDB 10>
Mar 15 15:59:55 akhamdamova /etc/mysql/debian-start[6817]: Upgrading MariaDB>
Mar 15 15:59:55 akhamdamova /etc/mysql/debian-start[6828]: Checking for inse>

(akhamdamova@akhamdamova)-[/var/www/html/DVWA/config]
$ sudo su
(root@akhamdamova)-[/var/www/html/DVWA/config]
# mysql -u root -p
Enter password:
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 (0.025 sec)

MariaDB [(none)]> create user 'admin'@'127.0.0.1' identified by 'password';
Query OK, 0 rows affected (0.030 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'admin'@'127.0.0.1';
```

Смотрим статус сервиса

```

(root@akhamdamova)-[/var/www/html/DVWA/config]
# systemctl start apache2

(root@akhamdamova)-[/var/www/html/DVWA/config]
# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Fri 2024-03-15 16:06:08 EDT; 11s ago
     Docs: https://httpd.apache.org/docs/2.4/
  Process: 9952 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 9968 (apache2)
    Tasks: 6 (limit: 2274)
   Memory: 19.7M (peak: 20.0M)
      CPU: 116ms
   CGroup: /system.slice/apache2.service
           └─9968 /usr/sbin/apache2 -k start
             └─9971 /usr/sbin/apache2 -k start
               └─9972 /usr/sbin/apache2 -k start
                 └─9973 /usr/sbin/apache2 -k start
                   └─9974 /usr/sbin/apache2 -k start
                     └─9975 /usr/sbin/apache2 -k start

Mar 15 16:06:08 akhamdamova systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Mar 15 16:06:08 akhamdamova systemd[1]: Started apache2.service - The Apache HTTP Server.

(root@akhamdamova)-[/var/www/html/DVWA/config]
# █

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.025 sec)

MariaDB [(none)]> create user 'admin'@'127.0.0.1' identified by 'password';
Query OK, 0 rows affected (0.030 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'admin'@'127.0.0.1';
Query OK, 0 rows affected (0.024 sec)

MariaDB [(none)]> exit
Bye

(root@akhamdamova)-[/var/www/html/DVWA/config]
# systemctl start apache2

(root@akhamdamova)-[/var/www/html/DVWA/config]
# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Fri 2024-03-15 16:06:08 EDT; 11s ago
     Docs: https://httpd.apache.org/docs/2.4/
  Process: 9952 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 9968 (apache2)
    Tasks: 6 (limit: 2274)
   Memory: 19.7M (peak: 20.0M)
      CPU: 116ms
   CGroup: /system.slice/apache2.service
           └─9968 /usr/sbin/apache2 -k start
             └─9971 /usr/sbin/apache2 -k start
               └─9972 /usr/sbin/apache2 -k start
                 └─9973 /usr/sbin/apache2 -k start
                   └─9974 /usr/sbin/apache2 -k start
                     └─9975 /usr/sbin/apache2 -k start

Mar 15 16:06:08 akhamdamova systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Mar 15 16:06:08 akhamdamova systemd[1]: Started apache2.service - The Apache HTTP Server.

(root@akhamdamova)-[/var/www/html/DVWA/config]
# █

```

```
(root@akhamdamova)-[/var/www/html/DVWA/config]
# cd /etc/php
```

```
(root@akhamdamova)-[/etc/php]
# ls
```

8.2

```
(root@akhamdamova)-[/etc/php]
# cd 8.2
```

```
(root@akhamdamova)-[/etc/php/8.2]
# cd apache2
```

```
(root@akhamdamova)-[/etc/php/8.2/apache2]
# ls
conf.d  php.ini
```

```
(root@akhamdamova)-[/etc/php/8.2/apache2]
# mousepad php.ini
```

```
356
357 ; Maximum number of files that can be uploaded via a single request
358 max_file_uploads = 20
359
360 ;;;;;;;;;;;;;;;;;
361 ; Fopen wrappers ;
362 ;;;;;;;;;;;;;;;;;
363
364 ; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
365 ; https://php.net/allow-url-fopen
366 allow_url_fopen = On
367
368 ; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
369 ; https://php.net/allow-url-include
370 allow_url_include = On
371
372 ; Define the anonymous ftp password (your email address). PHP's default setting
373 ; for this is empty.
374 ; https://php.net/from
375 ;from="john@doe.com"
376
377 ; Define the User-Agent string. PHP's default setting for this is empty.
378 ; https://php.net/user-agent
379 ;user_agent="PHP"
380
381 ; Default timeout for socket based streams (seconds)
```

Kali Linux

127.0.0.1/DVWA

http://127.0.0.1/DVWA

KALI

127.0.0.1/DVWA/setup.php

Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Setup DVWA

Instructions

About

Database Setup

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/config.inc.php`

If the database already exists, **it will be cleared and the data will be reset.**
You can also use this to reset the administrator credentials ("admin // password") at any stage.

Setup Check

Web Server SERVER_NAME: 127.0.0.1

Operating system: *nix

PHP version: 8.2.12

PHP function display_errors: Disabled

PHP function display_startup_errors: Disabled

PHP function allow_url_include: Enabled

PHP function allow_url_fopen: Enabled

PHP module gd: Missing - Only an issue if you want to play with captchas

PHP module mysql: Installed

PHP module pdo_mysql: Installed

Backend database: MySQL/MariaDB

Database username: admin

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/: Yes

Writable folder /var/www/html/DVWA/config: Yes

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.ini` file and restart Apache.

`allow url fopen = On`



Username

Password

Login

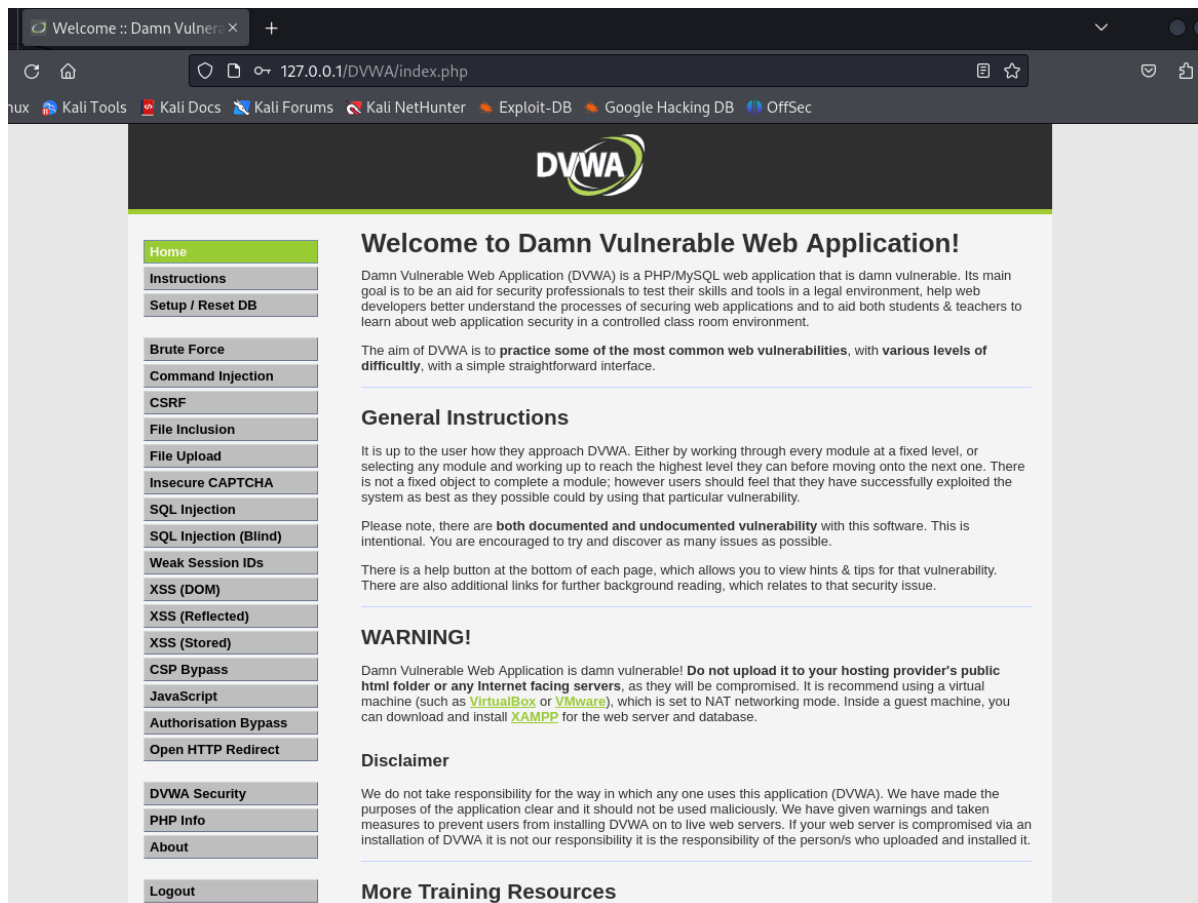


Рис. 1.4: Результат

2 Выводы

Я смогла установить DVWA.

Список литературы