

Отчёт по 2 этапу индивидуального проекта

Дисциплина: Информационная безопасность

Андрианова Марина Георгиевна

Содержание

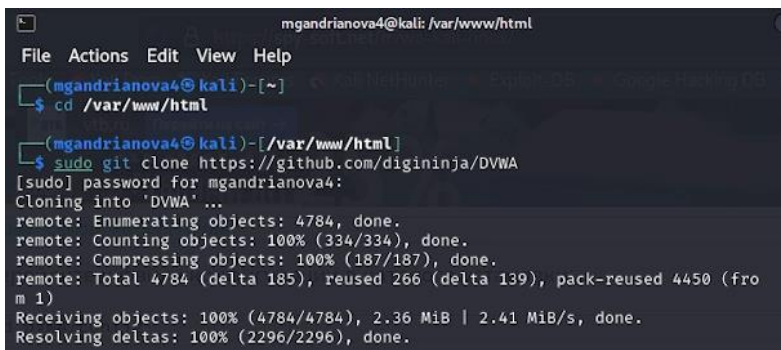
Цель работы	1
Выполнение 2-го этапа индивидуального проекта.....	1
Выводы.....	6

Цель работы

Установить DVWA на дистрибутив Kali Linux.

Выполнение 2-го этапа индивидуального проекта

Переходим в каталог html, введя команду “cd /var/www/html”. Клонировем репозиторий git командой “sudo git clone https://github.com/digininja/DVWA” (рис.1).



```
mgandrianova4@kali: /var/www/html
File Actions Edit View Help
(mgandrianova4@kali)-[~]
$ cd /var/www/html
(mgandrianova4@kali)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA
[sudo] password for mgandrianova4:
Cloning into 'DVWA'...
remote: Enumerating objects: 4784, done.
remote: Counting objects: 100% (334/334), done.
remote: Compressing objects: 100% (187/187), done.
remote: Total 4784 (delta 185), reused 266 (delta 139), pack-reused 4450 (from 1)
Receiving objects: 100% (4784/4784), 2.36 MiB | 2.41 MiB/s, done.
Resolving deltas: 100% (2296/2296), done.
```

Рис.1:Переход в каталог и клонирование репозитория

Проверяем, что файлы скопировались правильно и изменяем права доступа к папке установки(рис.2).

```
(mgandrianova4@kali)-[/var/www/html]
$ ls
DVWA index.html index.nginx-debian.html

(mgandrianova4@kali)-[/var/www/html]
$ sudo chmod -R 777 DVWA
```

Рис.2:Изменение прав доступа

Переходим к файлу конфигурации в каталоге установки: /dvwa/config. Проверяем содержимое каталога (рис.3).

```
(mgandrianova4@kali)-[/var/www/html]
$ cd DVWA/config

(mgandrianova4@kali)-[/var/www/html/DVWA/config]
$ ls
config.inc.php.dist
```

Рис.3:Переход к файлу конфигурации

Копируем файл конфигурации (config.inc.php.dist) и переименовываем его на config.inc.php (рис.4).

```
(mgandrianova4@kali)-[/var/www/html/DVWA/config]
$ sudo cp config.inc.php.dist config.inc.php

(mgandrianova4@kali)-[/var/www/html/DVWA/config]
$ ls
config.inc.php config.inc.php.dist
```

Рис.4:Копирование и переименование файла

Открываем файл настроек (рис.5) и изменяем пароль на что-то более простое для ввода (я изменю пароль на toor20) (рис.6).

```
(mgandrianova4@kali)-[/var/www/html/DVWA/config]
$ sudo nano config.inc.php
```

Рис.5:Открытие файла настроек


```
MariaDB [(none)]> create user 'mgdvwa'@'127.0.0.1' identified by 'toor20';
Query OK, 0 rows affected (0.012 sec)

MariaDB [(none)]> grant all privileges on dwwa.* to 'mgdvwa'@'127.0.0.1' identified by 'toor20';
Query OK, 0 rows affected (0.006 sec)

MariaDB [(none)]> exit
Bye
```

Puc.9: MariaDB

Для настройки сервера apache2 переходим в соответствующую директорию (рис.10).

```
(mgandrianova4@kali)-[/var/www/html/DVWA/config]
$ cd /etc/php/8.2/apache2
```

Рис.10:Переход в каталог arache2

Открываем для редактирования файл `php.ini` (с помощью команды `“sudo nano php.ini”`) (рис.11), чтобы включить следующие параметры: `allow_url_fopen` и `allow_url_include`.

```
(mgandrianova4@kali)-[/etc/php/8.2/apache2]
$ sudo nano php.ini
```

Рис.11:Редактирование файла

Файл большой, поэтому нам потребовалось прокрутить до середины файла, чтобы добраться до `foren` и изменить значения “off” на ‘on’ (рис.12).

```

; 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

```

Puc.12:Fopen wrappers

Запускаем сервер Apache и проверяем, запущена ли служба(рис.13).

```
(mgandrianova4@kali)-[/etc/php/8.2/apache2]
$ sudo systemctl start apache2

(mgandrianova4@kali)-[/etc/php/8.2/apache2]
$ systemctl status start apache2
Unit start.service could not be found.
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Fri 2024-09-20 22:26:01 MSK; 21s ago
  Invocation: 613646354449468c8b179a0e2cc08736
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 15347 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 15371 (apache2)
    Tasks: 6 (limit: 4549)
   Memory: 21.7M (peak: 22.1M)
      CPU: 497ms
   CGroup: /system.slice/apache2.service
           └─15371 /usr/sbin/apache2 -k start
             └─15374 /usr/sbin/apache2 -k start
               └─15375 /usr/sbin/apache2 -k start
                 └─15376 /usr/sbin/apache2 -k start
                   └─15377 /usr/sbin/apache2 -k start
                     └─15378 /usr/sbin/apache2 -k start

Sep 20 22:26:00 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...
```

Рис.13:Запуск сервера Apache

Пробуем открыть DVWA в браузере, введя в адресной строке следующее: “127.0.0.1/DVWA/”. Перед нами открылась страница настройки, это означает, что мы успешно установили DVWA на Kali Linux(рис.14).

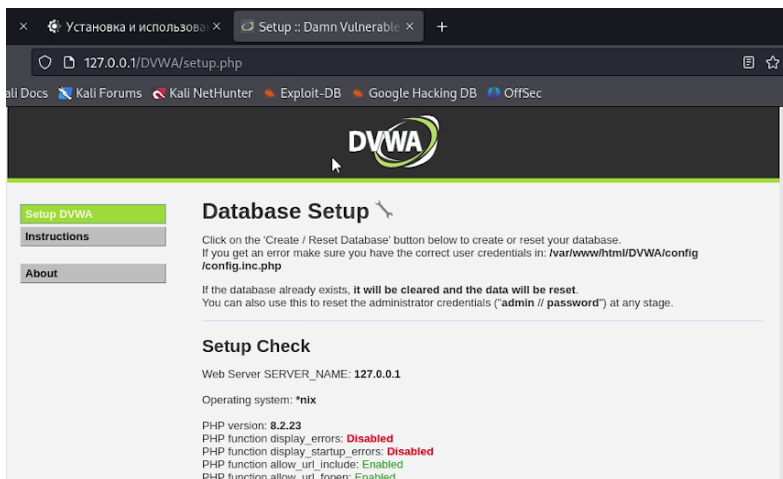


Рис.14:Запуск DVWA в браузере

Прокручиваем вниз и нажимаем “Create / Reset Database” (Создать / сбросить базу данных) (рис.15).

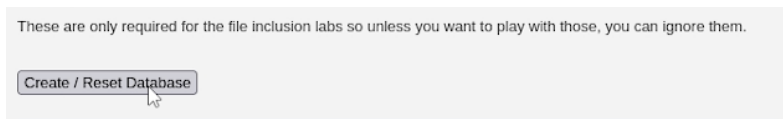



Рис.15:Создание базы данных

И через несколько секунд нас перенаправили на страницу входа в DVWA. Авторизуемся с помощью предложенных по умолчанию данных (рис.16).



Username

admin

Password

••••••••

Login

Рис.16:Авторизация

Оказываемся на домашней странице веб-приложения. Можем заметить, что существует множество интересных уязвимостей, которые мы можем протестировать, например, брутфорс, SQL-инъекция и другие (рис.17). На этом установка окончена.

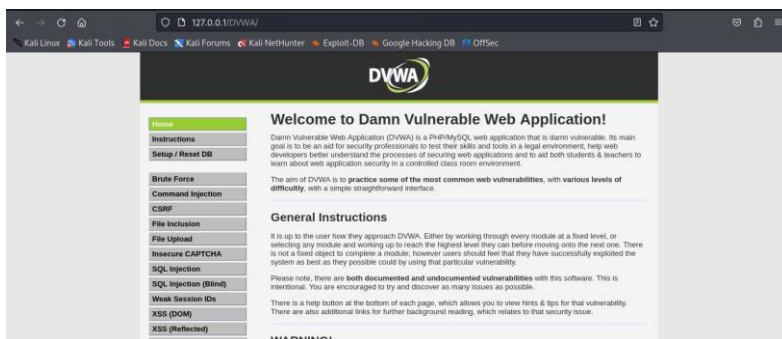


Рис.17:Домашняя страница DVWA

Выводы

Установила веб-приложение DVWA на дистрибутив Kali Linux.