

Индивидуальный проект 2

Информационная безопасность

Волчок Кристина Александровна НПМбд-02-21

Содержание

1	Цель работы	3
2	Задание	4
3	Теоретическое введение	5
4	Выполнение лабораторной работы	7
5	Выводы	12

1 Цель работы

Установить Damn Vulnerable Web Application (DVWA) в гостевую систему Kali Linux для изучения и практики в области безопасности веб-приложений.

2 Задание

- Установить DVWA в гостевую систему Kali Linux.
- Использовать репозиторий: <https://github.com/digininja/DVWA>.
- Ознакомиться с основными уязвимостями, которые содержит DVWA.
- Понять различия между уровнями безопасности, предлагаемыми DVWA.

3 Теоретическое введение

Теоретическое введение

DVWA (Damn Vulnerable Web Application) — это уязвимое веб-приложение, специально созданное для обучения и практики в области веб-безопасности. Оно содержит преднамеренные уязвимости для отработки техник их обнаружения и эксплуатации.

Основные уязвимости DVWA:

- **Брутфорс:** атака методом перебора паролей через форму входа.
- **Исполнение команд:** возможность выполнять команды операционной системы через веб-интерфейс.
- **CSRF (Межсайтовая подделка запроса):** позволяет изменить пароль администратора без его ведома.
- **Внедрение файлов:** подключение удаленных или локальных файлов в приложение.
- **SQL-инъекция:** внедрение SQL-запросов через поля ввода.
- **Небезопасная загрузка файлов:** загрузка вредоносных файлов на сервер.
- **XSS (Межсайтовый скриптинг):** внедрение скриптов в приложение или базу данных.
- **Пасхальные яйца:** скрытые уязвимости, такие как раскрытие полных путей и обход аутентификации.

Уровни безопасности DVWA:

- **Низкий:** полностью уязвимый уровень без какой-либо защиты.

- **Средний:** попытки защитить приложение, которые оказались неэффективными.
- **Высокий:** уязвимости есть, но их эксплуатация затруднена.
- **Невозможный:** все уязвимости устранены; используется для сравнения с уязвимыми уровнями.

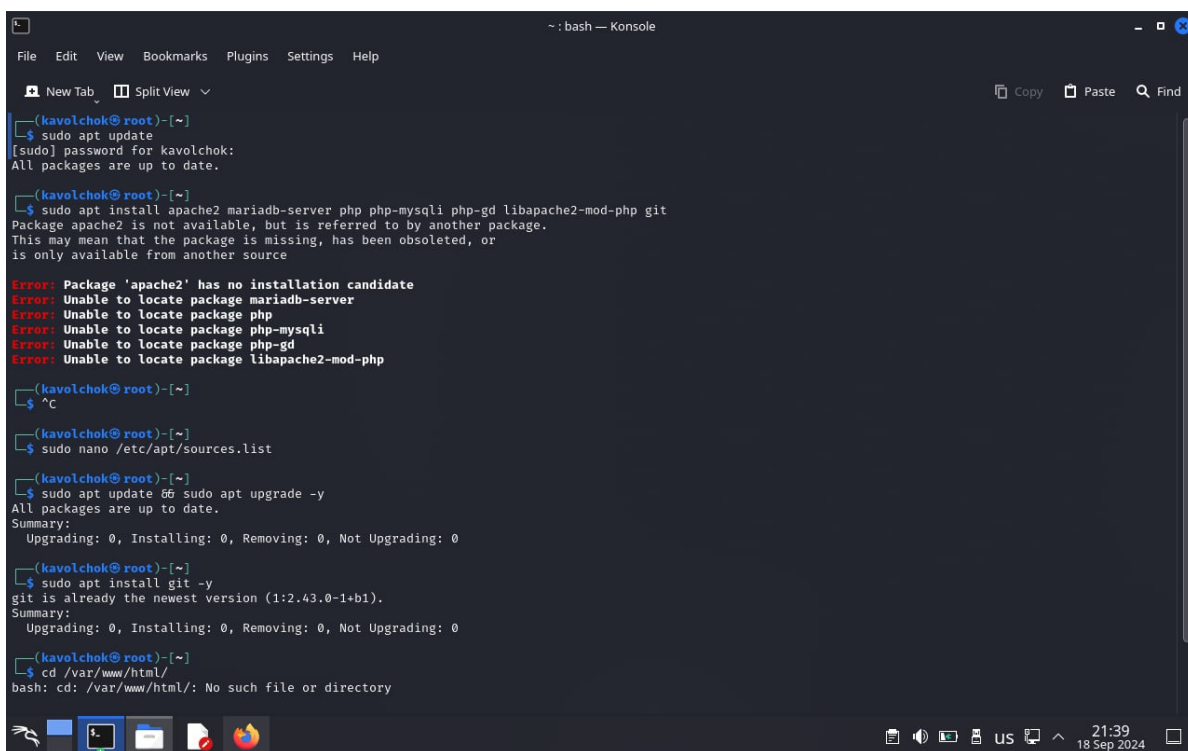
4 Выполнение лабораторной работы

Процесс установки DVWA

Обновление системы:

Для начала я обновляю систему с помощью следующей команды:

```
(sudo apt update && sudo apt upgrade -y)
```



```
~: bash — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
(kavolchok@root)~$ sudo apt update
[sudo] password for kavolchok:
All packages are up to date.

(kavolchok@root)~$ sudo apt install apache2 mariadb-server php php-mysql php-gd libapache2-mod-php git
Package apache2 is not available, but is referred to by another package.
This may mean that the package is missing, has been obsoleted, or
is only available from another source

Error: Package 'apache2' has no installation candidate
Error: Unable to locate package mariadb-server
Error: Unable to locate package php
Error: Unable to locate package php-mysql
Error: Unable to locate package php-gd
Error: Unable to locate package libapache2-mod-php

(kavolchok@root)~$ ^C

(kavolchok@root)~$ sudo nano /etc/apt/sources.list

(kavolchok@root)~$ sudo apt update && sudo apt upgrade -y
All packages are up to date.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

(kavolchok@root)~$ sudo apt install git -y
git is already the newest version (1:2.43.0-1+b1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

(kavolchok@root)~$ cd /var/www/html/
bash: cd: /var/www/html/: No such file or directory
```

Рис. 4.1: Установка DVWA

Установка необходимых пакетов:

После обновления системы я устанавливаю необходимые пакеты:

```
personal project : bash — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View Copy Paste Find
(kavolchok@root) - [~/personal project]
$ sudo git clone https://github.com/digininja/DVWA.git
[sudo] password for kavolchok:
Cloning into 'DVWA' ...
remote: Enumerating objects: 4758, done.
remote: Counting objects: 100% (308/308), done.
remote: Compressing objects: 100% (180/180), done.
remote: Total 4758 (delta 167), reused 241 (delta 122), pack-reused 4450 (from 1)
Receiving objects: 100% (4758/4758), 2.39 MiB | 5.73 MiB/s, done.
Resolving deltas: 100% (2262/2262), done.
(kavolchok@root) - [~/personal project]
$ ls -la DVWA/
total 460
drwxr-xr-x 12 root root 4096 Sep 18 21:37 .
drwxrwxr-x 3 kavolchok kavolchok 4096 Sep 18 21:37 ..
-rw-r--r-- 1 root root 77 Sep 18 21:37 .dockerignore
drwxr-xr-x 8 root root 4096 Sep 18 21:37 .git
-rw-r--r-- 1 root root 474 Sep 18 21:37 .gitattributes
drwxr-xr-x 4 root root 4096 Sep 18 21:37 .github
-rw-r--r-- 1 root root 273 Sep 18 21:37 .gitignore
-rw-r--r-- 1 root root 7134 Sep 18 21:37 CHANGELOG.md
-rw-r--r-- 1 root root 32485 Sep 18 21:37 COPYING.txt
-rw-r--r-- 1 root root 807 Sep 18 21:37 Dockerfile
-rw-r--r-- 1 root root 25027 Sep 18 21:37 README.ar.md
-rw-r--r-- 1 root root 21777 Sep 18 21:37 README.es.md
-rw-r--r-- 1 root root 30612 Sep 18 21:37 README.fa.md
-rw-r--r-- 1 root root 20674 Sep 18 21:37 README.fr.md
-rw-r--r-- 1 root root 26188 Sep 18 21:37 README.id.md
-rw-r--r-- 1 root root 32492 Sep 18 21:37 README.ko.md
-rw-r--r-- 1 root root 29310 Sep 18 21:37 README.md
-rw-r--r-- 1 root root 21239 Sep 18 21:37 README.pt.md
-rw-r--r-- 1 root root 19838 Sep 18 21:37 README.tr.md
-rw-r--r-- 1 root root 34865 Sep 18 21:37 README.vi.md
-rw-r--r-- 1 root root 17394 Sep 18 21:37 README.zh.md
-rw-r--r-- 1 root root 151 Sep 18 21:37 SECURITY.md
-rw-r--r-- 1 root root 2883 Sep 18 21:37 about.php
-rw-r--r-- 1 root root 629 Sep 18 21:37 compose.yml
drwxr-xr-x 2 root root 4096 Sep 18 21:37 config
drwxr-xr-x 2 root root 4096 Sep 18 21:37 database
```

Рис. 4.2: Установка необходимых пакетов

Запуск и настройка служб:

Затем я запускаю и настраиваю службы Apache и MariaDB для их автоматического запуска при старте системы:

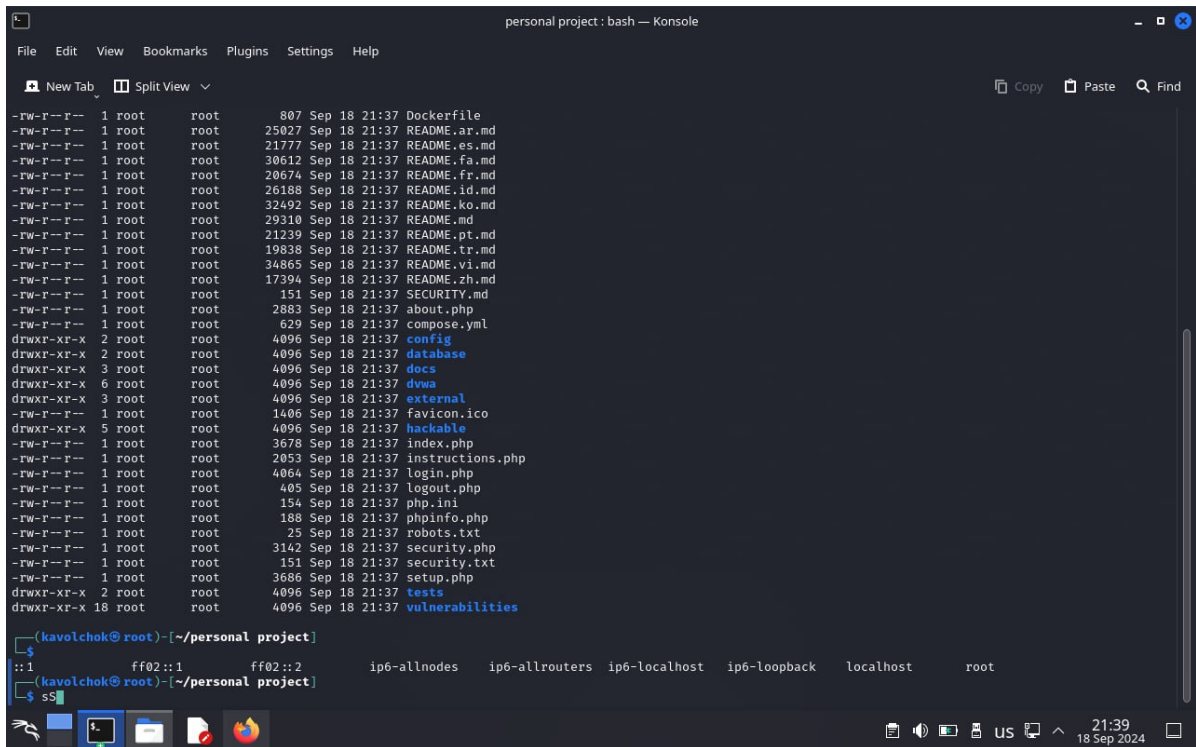


Рис. 4.3: Запуск и настройка служб

Настройка базы данных:

После того как службы запущены, я перехожу к настройке базы данных:

```
(sudo mysql_secure_installation)
```

```
(sudo mysql -u root -p)
```

В MySQL я ввожу следующие команды для создания базы данных и пользователя:

```
“sql CREATE DATABASE dvwa; CREATE USER ‘dvwauser’@‘localhost’ IDENTIFIED BY ‘password’; GRANT ALL PRIVILEGES ON dvwa.* TO ‘dvwauser’@‘localhost’; FLUSH PRIVILEGES; EXIT;
```

**** Клонирование репозитория DVWA.****

Теперь я клонирую репозиторий DVWA в директорию веб-сервера:

```
(cd /var/www/html/)
```

```
(sudo git clone https://github.com/digininja/DVWA.git)
```

Настройка прав доступа:

Я убеждаюсь, что права доступа к директории настроены корректно:

```
(sudo chown -R www-data:www-data /var/www/html/DVWA/)
```

```
(sudo chmod -R 755 /var/www/html/DVWA/)
```

После этого я перехожу в папку конфигурации и настраиваю файл:

```
(cd /var/www/html/DVWA/config/)
```

```
(sudo cp config.inc.php.dist config.inc.php)
```

```
(sudo nano config.inc.php)
```

Завершение установки через браузер:

Я открываю браузер и перехожу по адресу:

<http://localhost/DVWA/setup.php>

Нажимаю кнопку "Create / Reset Database".

Вход в DVWA:

Перехожу на страницу входа:

<http://localhost/DVWA/login.php>

Ввожу следующие данные для входа:

- Имя пользователя: admin
- Пароль: password

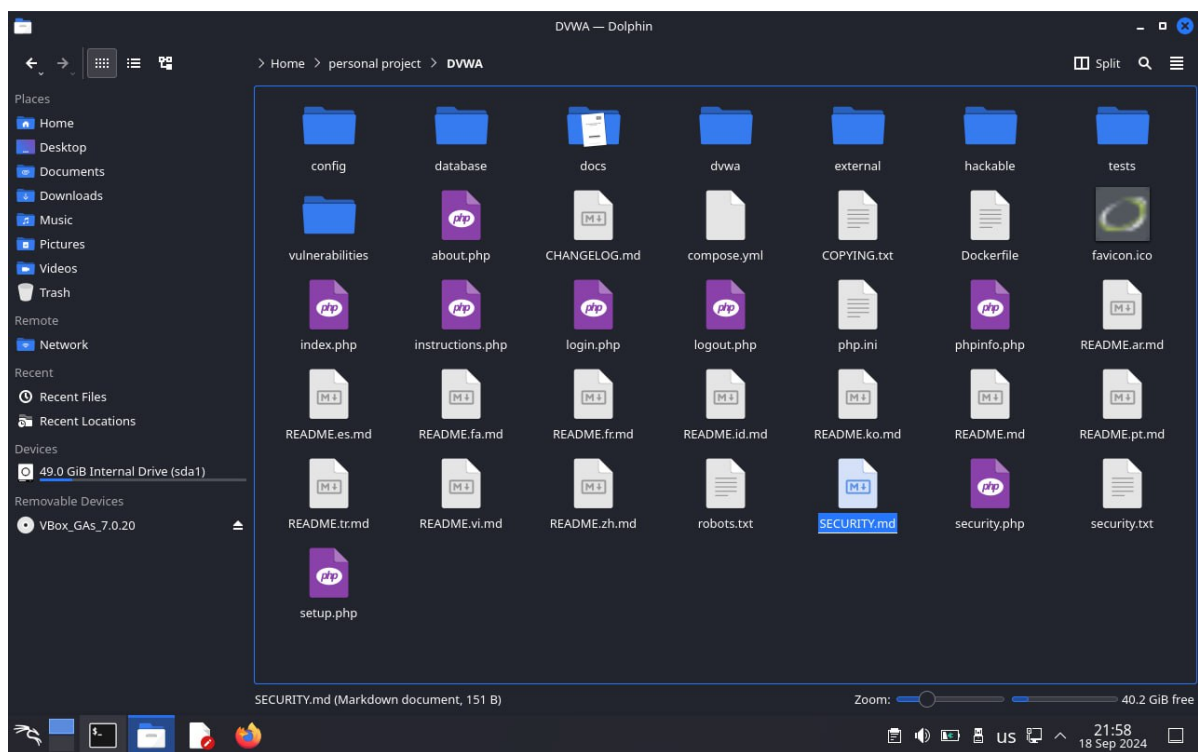


Рис. 4.4: Настроенная DVWA

5 Выводы

В результате выполнения задания была успешно установлена DVWA в гостевую систему Kali Linux. Это позволяет получить практический опыт в области веб-безопасности, изучая и эксплуатируя различные уязвимости. Работа с DVWA способствует повышению квалификации и пониманию методов защиты веб-приложений.