

# **Индивидуальный проект - этап 2**

**Установка DVWA**

Плагин Никита

# Содержание

1	Цель работы	4
2	Введение	5
3	Выполнение лабораторной работы	7
4	Вывод	9

# List of Figures

3.1	Запуск скрипта . . . . .	7
3.2	Окончание установки . . . . .	8
3.3	Страница DVWA в браузере . . . . .	8

# 1 Цель работы

Целью данной работы является изучение задач приложения DVWA и его установка в систему Kali Linux.

## 2 Введение

**Damn Vulnerable Web Application (DVWA)** — это веб-приложение на PHP/MySQL, которое чертовски уязвимо. Его главная цель — помочь профессионалам по безопасности протестировать их навыки и инструменты в легальном окружении, помочь веб-разработчикам лучше понять процесс безопасности веб-приложений и помочь и студентам и учителям в изучении безопасности веб-приложений в контролируемом окружении аудитории.

Цель DVWA попрактиковаться в некоторых самых распространённых веб-уязвимостях, с различными уровнями сложности, с простым прямолинейным интерфейсом. Обратите внимание, что имеются как задокументированные, так и незадокументированные уязвимости в этом программном обеспечении. Это сделано специально. Вам предлагается попробовать и обнаружить так много уязвимостей, как сможете.

Некоторые из уязвимостей веб-приложений, который содержит DVWA;

- **Брут-форс:** Брут-форс 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.

### 3 Выполнение лабораторной работы

Для установки приложения на Debian системы можно воспользоваться командой в одну строку.

```
sudo bash -c "$(curl --fail --show-error --silent --location https://raw.githubusercontent.com/IamCarron/DVWA-Script/main/install-dvwa.sh)"
```

Или же скопировать из репозитория установочный скрипт и запустить его.

Также существует полностью ручной способ установки, но рассматривать его мы не будем.



Figure 3.1: Запуск скрипта

```
Processing triggers for libapache2-mod-php8.2 (8.2.27-1) ...
libapache2-mod-php is installed!
git is installed!
Downloading DVWA from GitHub...
Cloning into '/var/www/html/DVWA' ...
remote: Enumerating objects: 5077, done.
remote: Counting objects: 100% (54/54), done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 5077 (delta 44), reused 35 (delta 35), pack-reused 5023 (from 2)
Receiving objects: 100% (5077/5077), 2.48 MiB | 6.51 MiB/s, done.
Resolving deltas: 100% (2480/2480), done.
Enabling MariaDB...
Starting MariaDB...

Default credentials:
Username: root

Password: [No password just hit Enter]
Enter SQL user:
Enter SQL password (press Enter for no password):
Enter password:
SQL commands executed successfully.
Configuring DVWA...
Configuring permissions...
Configuring PHP...
Enabling Apache...
Restarting Apache...
DVWA has been installed successfully. Access http://localhost/DVWA to get started.
Credentials:
Username: admin
Password: password

With ♡ by IamCarron

(user@nsplugin)-[~]
$
```

Figure 3.2: Окончание установки

Далее DVWA работает как локальный сервер и доступно через браузер.

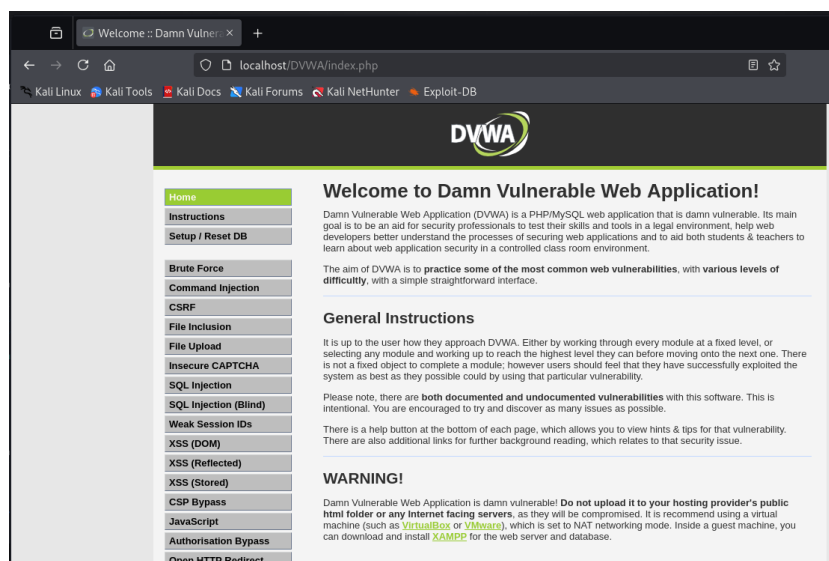


Figure 3.3: Страница DVWA в браузере



## **4 Вывод**

Мы приобрели знания о приложении DVWA и установили его в ОС.