Второй этап индивидуального проекта

Установка DVWA

Беличева Дарья Михайловна

Содержание

Список иллюстраций

1 Цель работы

Установить и настроить DVWA в гостевую систему к Kali Linux.

2 Теоретическое 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 контролируем окружении аудитории [1].

Цель DVWA попрактиковаться в некоторых самых распространённых веб-уязвимостях, с различными уровнями сложности, с простым прямолинейном 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 (инклуд) 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

3.1 Установка DVWA

Поскольку мы будем настраивать DVWA на нашем локальном хостинге, запустим терминал и перейдем в /var/www/html каталог. Это место, где хранятся файлы localhost. Далее мы клонируем репозиторий DVWA с GitHub в директорию /html (рис. 3.1).

Рис. 3.1: Скачивание DVWA: клонирование репозитория

3.2 Настройка DVWA

После успешного клонирования репозитория запустим команду `ls`, чтобы подтвердить, что DVWA был успешно клонирован. Теперь нам нужно назначить этой папке разрешения на чтение, запись и выполнение (777). Чтобы настроить DVWA, нам нужно будет перейти в каталог /dvwa/config. Запустим команду `ls`, чтобы просмотреть содержимое каталога конфигурации. Увидим

файл с именем config.inc.php.dist. Этот файл содержит конфигурации DVWA по умолчанию. Создадим копию этого файла с именем config.inc.php, который мы будем использовать для настройки DVWA (рис. 3.2).

Рис. 3.2: Каталог конфигурации

Теперь откроем config.inc.php файл с помощью nano редактора, чтобы произвести необходимые настройки. Прокрутим вниз до того места, где находятся такие параметры, как db_database, db_user, db_password и т.д. Отредактируем эти значения (рис. 3.3).

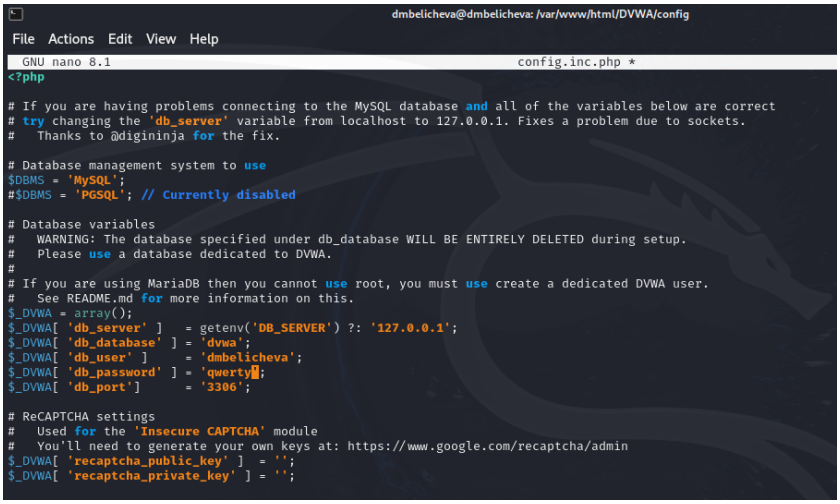

Рис. 3.3: Редактирование файла конфигурации

3.3 Настройка базы данных

По умолчанию Kali Linux поставляется с системой управления реляционными базами данных MariaDB. Следовательно,не нужно устанавливать никаких пакетов. Сначала запустим службу mysql.

Рис. 3.4: Запуск службы mysql

Войдем в базу данных. Создадим нового пользователя, используя учетные данные, которые мы установили в config.inc.php файле в каталоге DVWA.

Рис. 3.5: Вход в базу данных, создание пользователя

3.4 Настройка сервера Apache

Веб-сервер Apache по умолчанию установлен в Kali Linux. Следовательно, нам не нужно устанавливать никаких дополнительных пакетов.

Чтобы приступить к настройке Apache2, запустим терминал и перейдем в /etc/php/7.4/apache2 каталог. При выполнении команды `ls` увидим файл с именем php.ini.

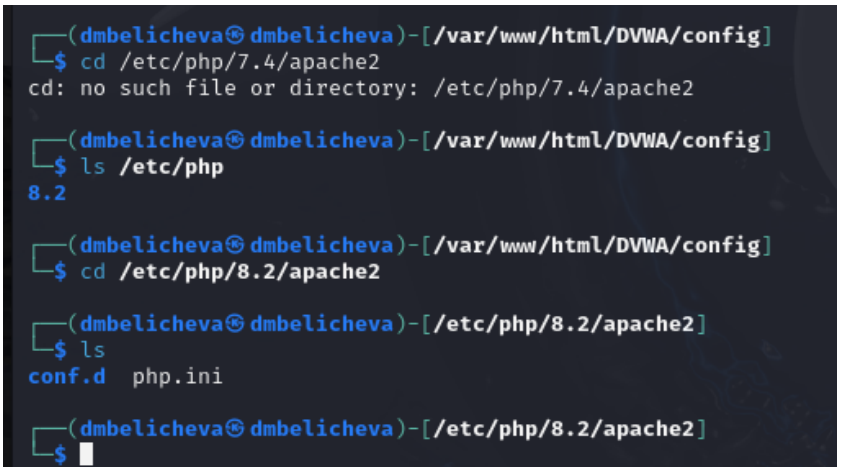

Рис. 3.6: Переход в нужную директории

Откроем файл на редактирование. Прокрутим и найдем строки allow_url_fopen и allow_url_include, убедитесь, что для обеих установлено значение On.

Рис. 3.7: Редактирование файла php.ini

Перейдем к запуску службы веб-сервера apache. Можно проверить, запущена ли служба, выполнив команду `status`.

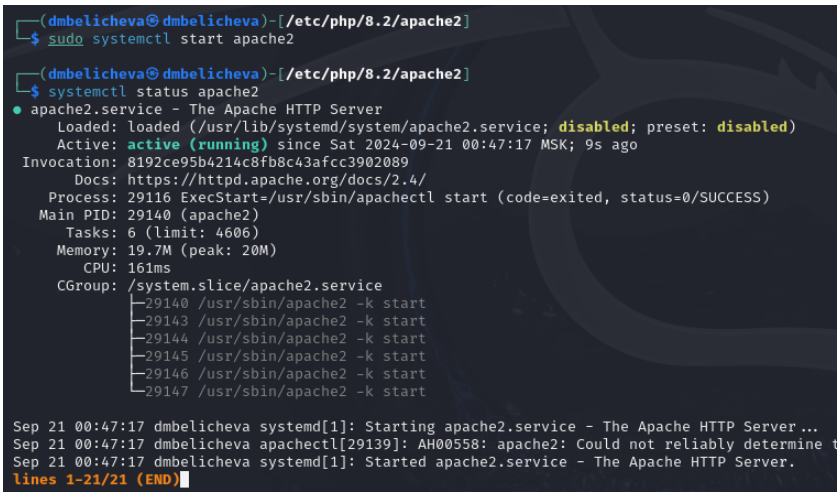

Рис. 3.8: Запуск службы веб-сервера apache

3.5 Открытие DVWA в веб-браузере

На данный момент мы настроили DVWA, базу данных и веб-сервер Apache.

Теперь мы можем приступить к запуску приложения DVWA. Запустим свой веб-браузер и введем URL-адрес.

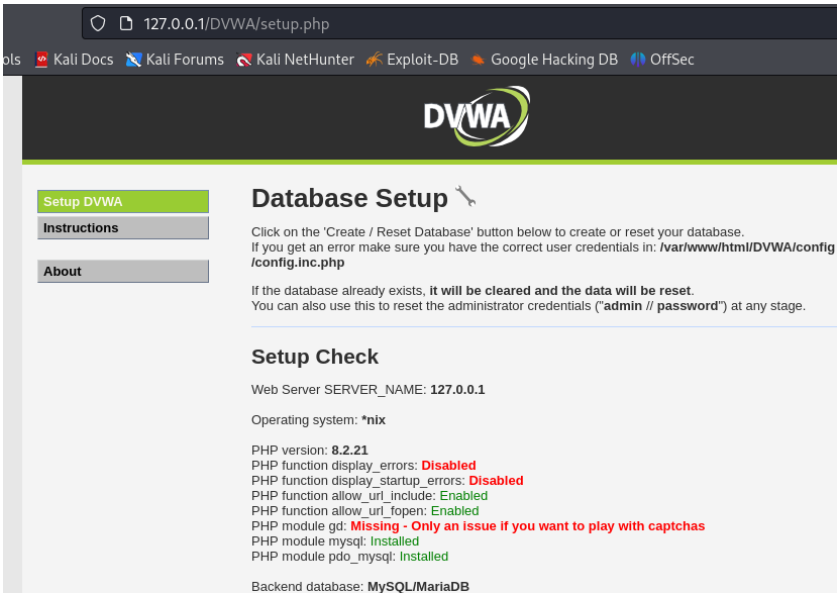

Рис. 3.9: Запуск приложения DVWA в веб-браузере

Нажмем кнопку Создать / Сбросить базу данных в конце страницы. Это создаст и настроит базу данных DVWA. Через несколько секунд мы будем перенаправлены на страницу входа в DVWA.

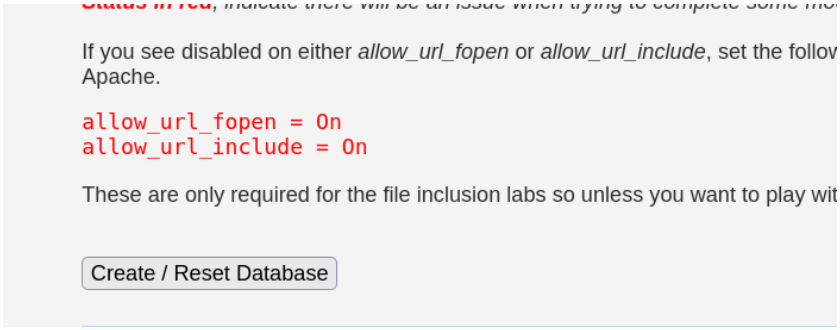

Рис. 3.10: Создание базы данных

Используем приведенные ниже учетные данные по умолчанию для входа в систему.

Имя пользователя: admin

Пароль: пароль

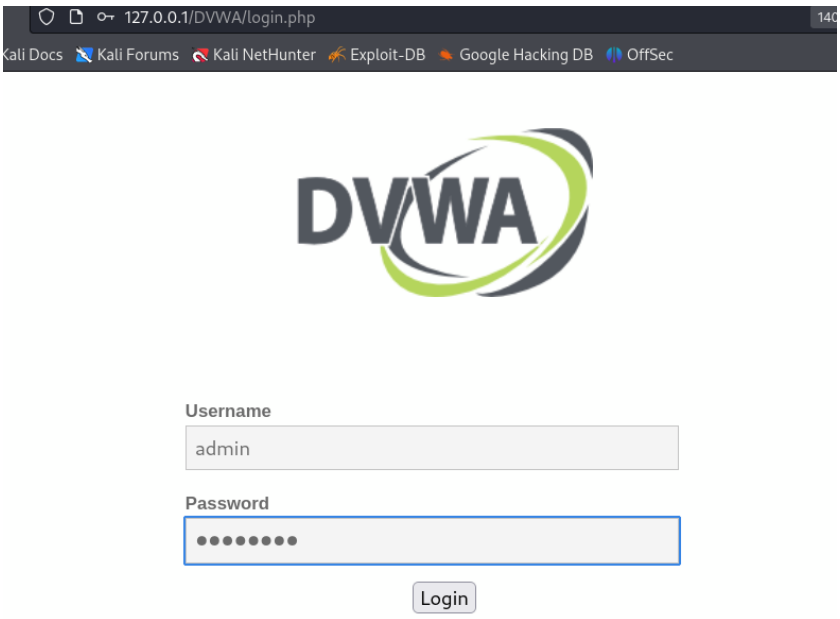

Рис. 3.11: Вход в систему DVWA

После успешного входа в систему увидим домашнюю страницу DVWA. В левой части увидим все доступные уязвимые страницы, которые можно использовать для практики.

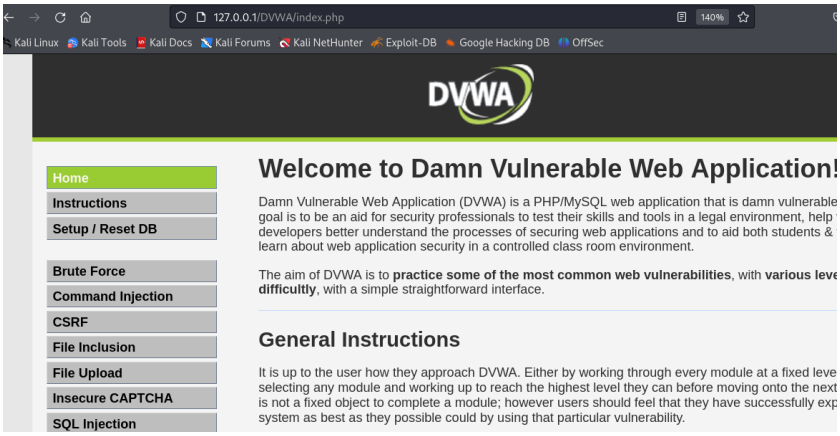

Рис. 3.12: Домашняя страница DVWA

4 Выводы

В результате выполнения данного этапа проекта я установила и настроила DVWA в гостевую систему к Kali Linux.

Список литературы

1. Damn Vulnerable Web Application (DVWA) [Электронный ресурс]. 2024. URL: https://kali.tools/?p=1820.