Отчёт по этапу проекта №2

Уткина Алина Дмитриевна

Содержание

Список иллюстраций

1 Цель работы

Целью данной работы является установка DVWA в гостевую систему к Kali Linux.

2 Теоретическое введение

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 (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.

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.

3 Выполнение лабораторной работы

Установить программу можно с репозитория https://github.com/digininja/DVWA. При переходе по ссылке мы видим инструкцию по установке.

Для начала скачиваем скрипт (рис. 3.1). Затем устанавливаем права доступа на исполнение файла (рис. 3.2). Затем запускаем этот файл и таким образом получаем установленный пакет (рис. 3.3).

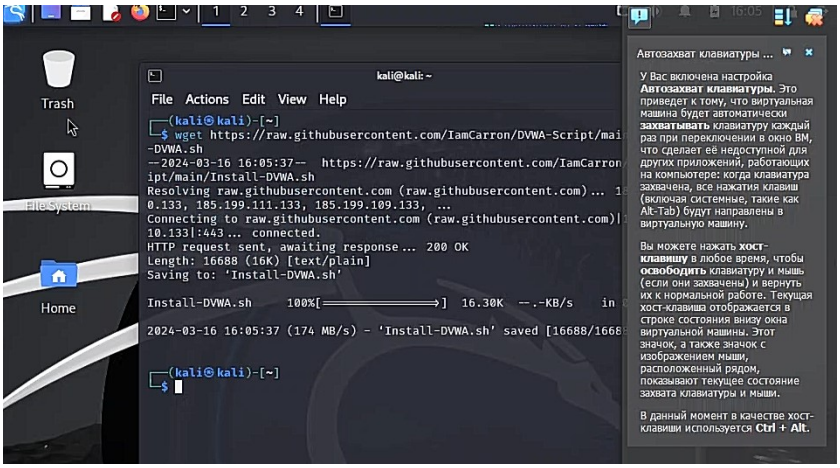

Рис. 3.1: Скачивание скрипта

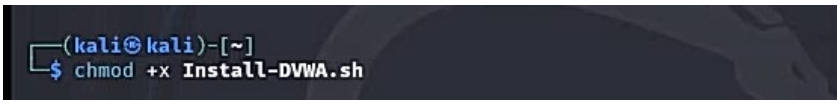

Рис. 3.2: Изменение праав доступа

Рис. 3.3: Завершение установки DVWA

4 Выводы

В ходе данной работы мы установили пакет DVWA и изучили некоторую информацию о нем