Презентация по выполнению индивидуального проекта №5

Основы информационной безопасности

Назармамадов У. Дж.

21 сентября 2025

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Назармамадов Умед Джамшедович
- студент группы НКАбд-03-23
- Российский университет дружбы народов

Цель

Научиться использовать Burp Suite.

Выполнение лабораторной работы

Запускаю локальный сервер, на котором открою веб-приложение DVWA для тестирования инструмента Burp Suite

Запуск локального сервера

Рис. 1: Запуск локального сервера

Выполнение лабораторной работы

Запускаю инструмент Burp Suite

Запуск приложения

Рис. 2: Запуск приложения

Выполнение лабораторной работы

Открываю сетевые настройки браузера, для подготовке к работе

Сетевые настройки браузера

Рис. 3: Сетевые настройки браузера

Выполнение лабораторной работы

Изменение настроек сервера для работы с proxy и захватом данных с помощью Burp Suite

Настройки сервера

Рис. 4: Настройки сервера

Выполнение лабораторной работы

Изменяю настройки Proxy инструмента Burp Suite для дальнейшей работы

Настройки Burp Suite

Рис. 5: Настройки Burp Suite

Выполнение лабораторной работы

Во вкладке Proxy устанавливаю “Intercept is on”

Настройки Proxy

Рис. 6: Настройки Proxy

Выполнение лабораторной работы

Чтобы Burp Suite исправно работал с локальным сервером, наобходимо установить параметр `network_allow_hijacking_loacalhost` на `true`

Настройки параметров

Рис. 7: Настройки параметров

Выполнение лабораторной работы

Пытаюсь зайти в браузере на DVWA, тут же во вкладки Proxy появляется захваченный запрос. Нажимаем “Forward”, чтобы загрузить страницу

Получаемые запросы сервера

Рис. 8: Получаемые запросы сервера

Выполнение лабораторной работы

Загрузилась страница авторизации, текст запроса поменялся

Страница авторизации

Рис. 9: Страница авторизации

Выполнение лабораторной работы

История запросов хранится во вкладке Target

История запросов

Рис. 10: История запросов

Выполнение лабораторной работы

Попробуем ввести неправильные, случайные данные в веб-приложении и нажмем `Login`. В запросе увидим строку, в которой отображаются введенные нами данные, то есть поле для ввода

Ввод случайных данных

Рис. 11: Ввод случайных данных

Выполнение лабораторной работы

Этот запрос так же можно найти во вкладке Target, там же жмем правой кнопкой мыши на хост нужного запроса, и далее нажимаем “Send to Intruder”

POST-запрос с вводом пароля и логина

Рис. 12: POST-запрос с вводом пароля и логина

Выполнение лабораторной работы

Попадаем на вкладку Intruder, видим значения по умолчанию у типа атаки и наш запрос

Вкладка Intruder

Рис. 13: Вкладка Intruder

Выполнение лабораторной работы

Изменяем значение типа атаки на Cluster bomb и проставляем специальные символы у тех данных в форме для ввода, которые будем пробивать, то есть у имени пользователя и пароля

Изменение типа атаки

Рис. 14: Изменение типа атаки

Так как мы отметили два параметра для подбора, то нам нужно два списка со значениями для подбора. Заполняем первый список в `Payload setting`

Первый Simple list

Рис. 15: Первый Simple list

Переключаемся на второй список и добавляем значения в него. В строке request count видим нужное количество запросов, чтобы проверить все возможные пары пользователь-пароль

Второй Simple list

Рис. 16: Второй Simple list

Выполнение лабораторной работы

Запускаю атаку и начинаю подбор

Запуск атаки

Рис. 17: Запуск атаки

При открытии результата каждого post-запроса можно увидеть полученный get-запрос, в нем видно, куда нас перенаправило после выполнения ввода пары пользователь-пароль. В представленном случае с подбором пары admin-admin нас перенаправило на login.php, это значит, что пара не подходит

Результат запроса

Рис. 18: Результат запроса

Проверим результат пары admin-password во вкладке Response, теперь нас перенаправляет на страницу index.php, значит пара должна быть верной

Результат запроса

Рис. 19: Результат запроса

Дополнительная проверка с использованием Repeater, нажимаем на нужный нам запрос правой кнопкой мыши и жмем “Send to Repeater”

Дополнительная проверка результата

Рис. 20: Дополнительная проверка результата

Выполнение лабораторной работы

Переходим во вкладку “Repeater”

Вкладка Repeater

Рис. 21: Вкладка Repeater

Нажимаем “send”, получаем в Response в результат перенаправление на index.php

Окно Response

Рис. 22: Окно Response

После нажатия на `Follow redirection`, получим нескомпилированный html код в окне Response

Изменение в окне Response

Рис. 23: Изменение в окне Response

Выполнение лабораторной работы

Далее в подокне Render получим то, как выглядит полученная страница

Полученная страница

Рис. 24: Полученная страница

Вывод

При выполнении лабораторной работы я научился использовать инструмент Burp Suite.

:::