Отчет 3 этапу индивидуального проекта

Использование Hydra

Гисматуллин Артём Вадимович НПИбд-01-22

Содержание

[1 Цель работы 1](#__RefHeading___Toc190_447188492)

[2 Задание 1](#__RefHeading___Toc192_447188492)

[3 Выполнение лабораторной работы 1](#__RefHeading___Toc194_447188492)

[4 Выводы 5](#__RefHeading___Toc196_447188492)

# 1 Цель работы

Получение практических навыков работы с Hydra и подбором паролей.

# 2 Задание

Последовательно выполнять все пункты, занося ответы и замечания в отчет.

# 3 Выполнение лабораторной работы

1.Первым делом перейдем в раздел DVWA Security и поставим низкий уровень безопасности (рис. 1)

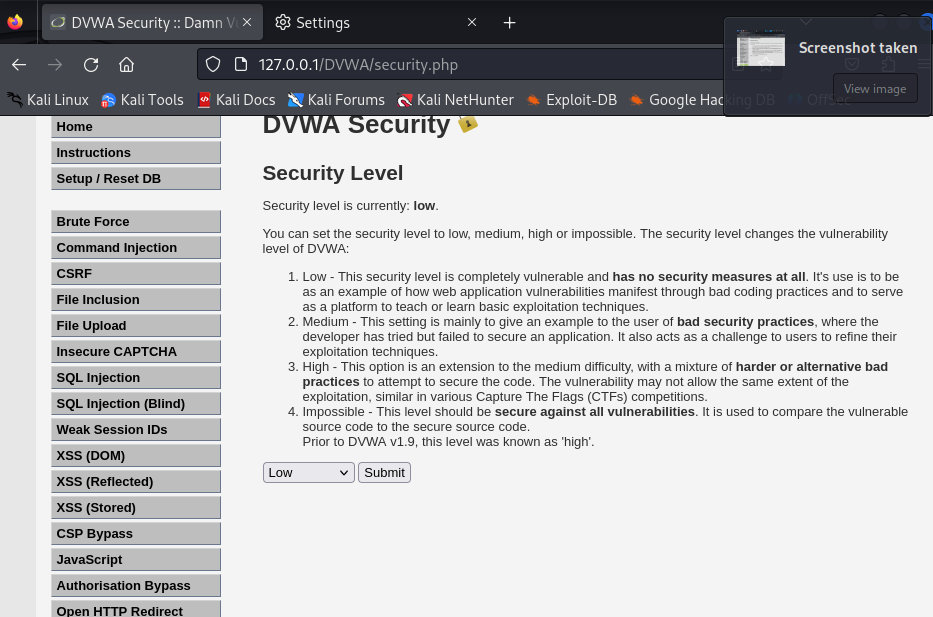


Рис. 1: Установка низкого уровня безопасности

1. После этого создадим файл password.txt, куда поместим примерные “простые” пароли, которые могут подойти к аккаунту пользователя-жертвы атаки (рис. 2)

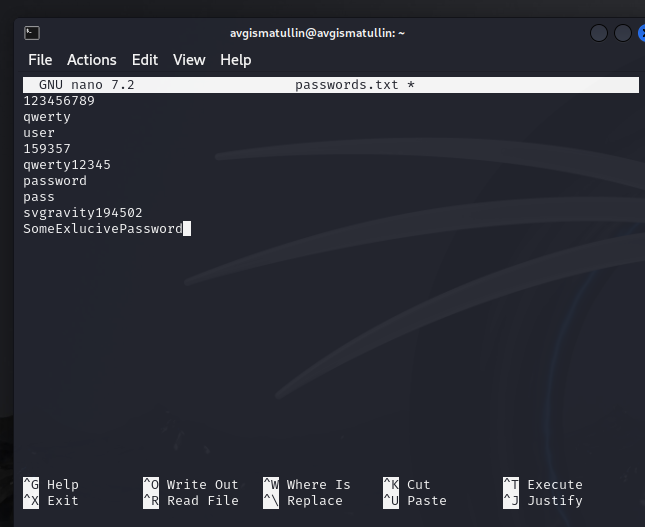


Рис. 2: Заполнение файла с паролями

1. Открываем затем на сайте Brute Force раздел и попытаемся подобрать имя и пароль пользователя. После неудачной попытки откроем исходный код страницы и проверим метод отправки данных формы (метод GET) (рис. 3)

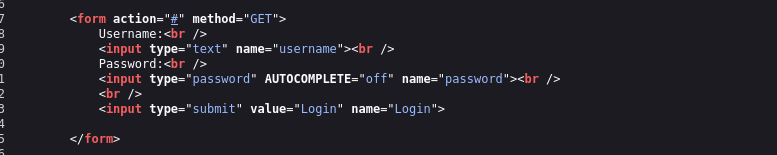


Рис. 3: Поиск метода отправки данных

1. Далее для формирования запроса к Hydra нам потребуется информация о PHPSEESID. Для этого во вкладке Inspect страницы найдем в Storage графу об этом (рис. 4)

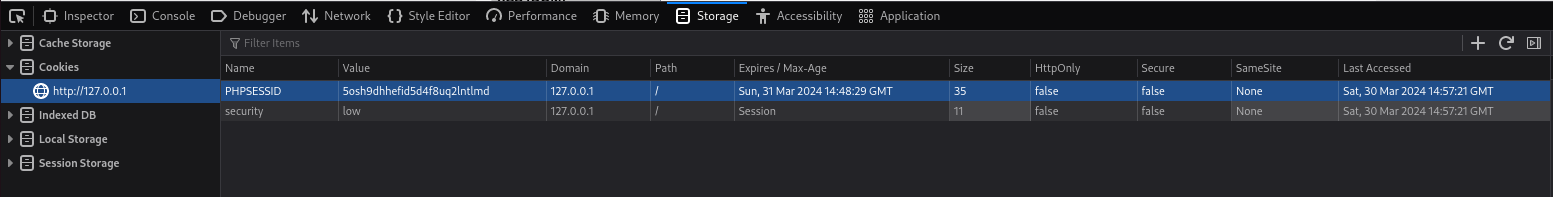


Рис. 4: PHPSEESID

Так как у нас есть все для отправки запроса, формируем его на основе теоретических данных проекта (рис. 5)

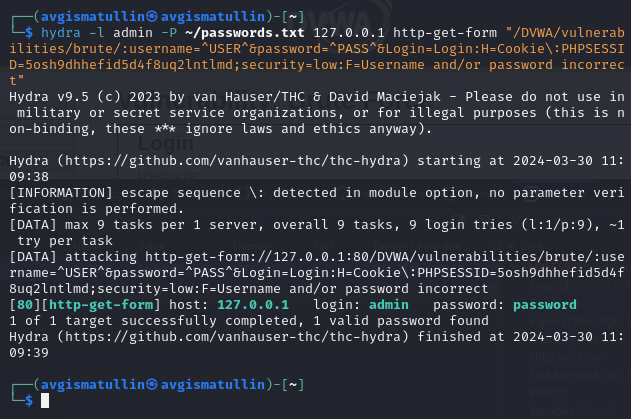


Рис. 5: Формирование запроса к Hydra

Как видим, нам подошли логин admin и пароль password. Попробуем войти под этой учетной записью (рис. 6)

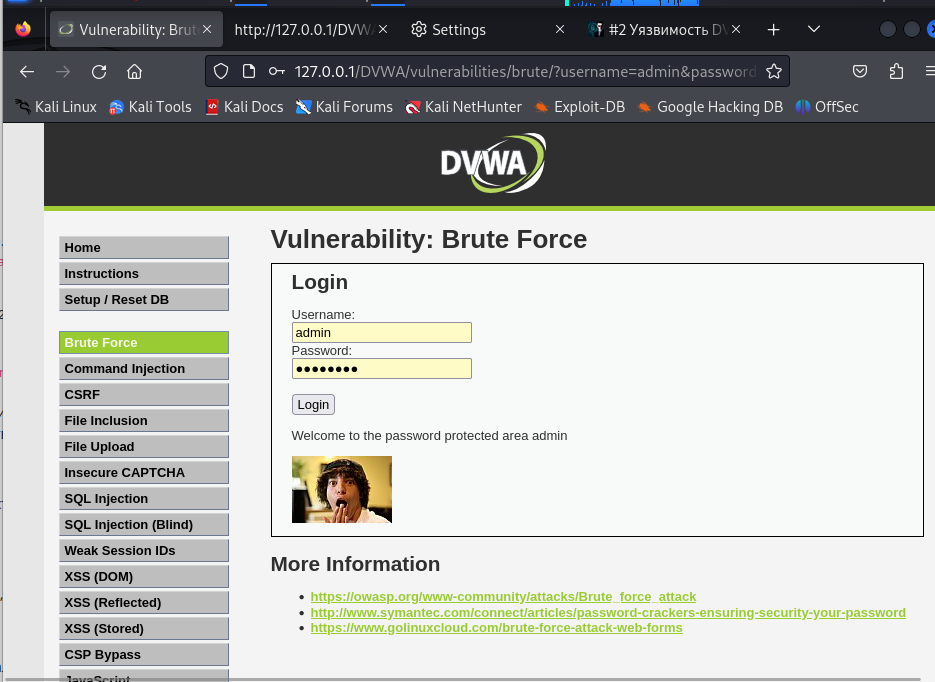


Рис. 6: Проверка данных

Успех!

# 4 Выводы

В ходе выполнения данного этапа были получены практические навыки работы с Hydra и подбора паролей.