

Отчет по третьему этапу проекта

Основы информационной безопасности

Ищенко Ирина НПИбд-02-22

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	10
	Список литературы	11

Список иллюстраций

2.1	Изменение уровня безопасности	6
2.2	Вход в Brute Force	7
2.3	Настройки конфигурации	7
2.4	Файл с паролем	8
2.5	hydra	8

Список таблиц

1 Цель работы

Научиться использовать hydra для подбора логина и пароля[1].

2 Выполнение лабораторной работы

Заходим в DVWA сервис. Устанавливаем низкий уровень безопасности (рис. 2.1).

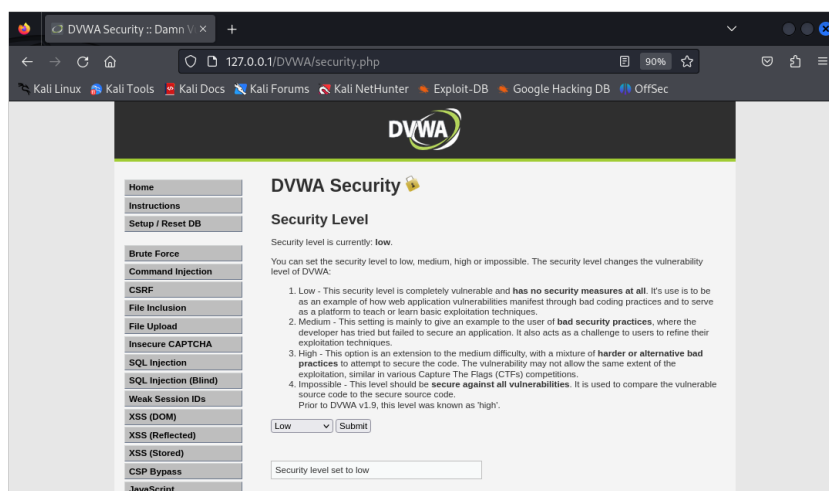


Рис. 2.1: Изменение уровня безопасности

Входим в Brute Force (рис. 2.2).

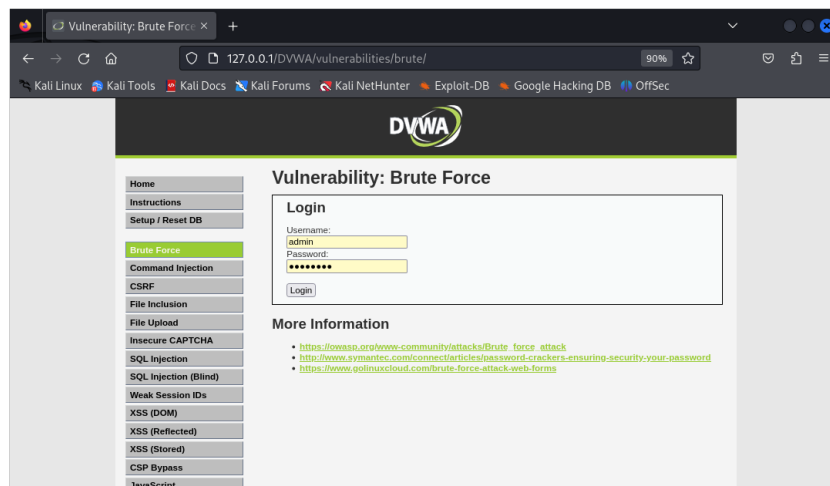


Рис. 2.2: Вход в Brute Force

В настройках браузера меняем вручную настройки конфигурации, указываем IP (рис. 2.3).

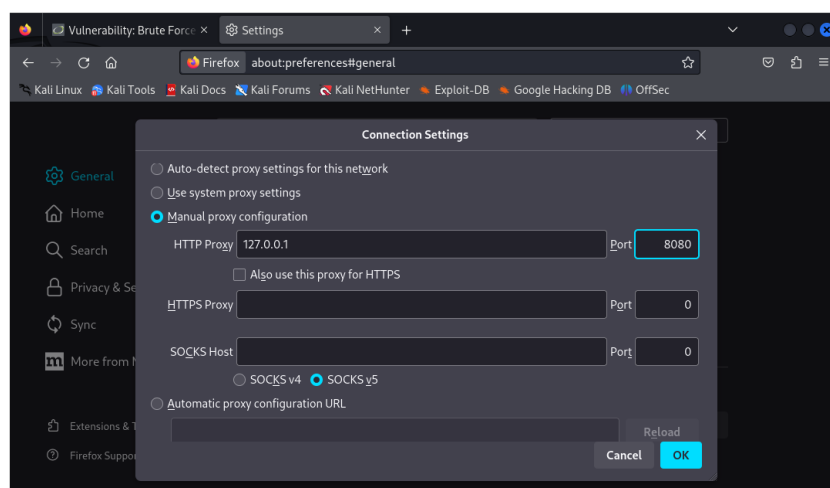


Рис. 2.3: Настройки конфигурации

Создаем файл и заполняем его возможными паролями (рис. 2.4).

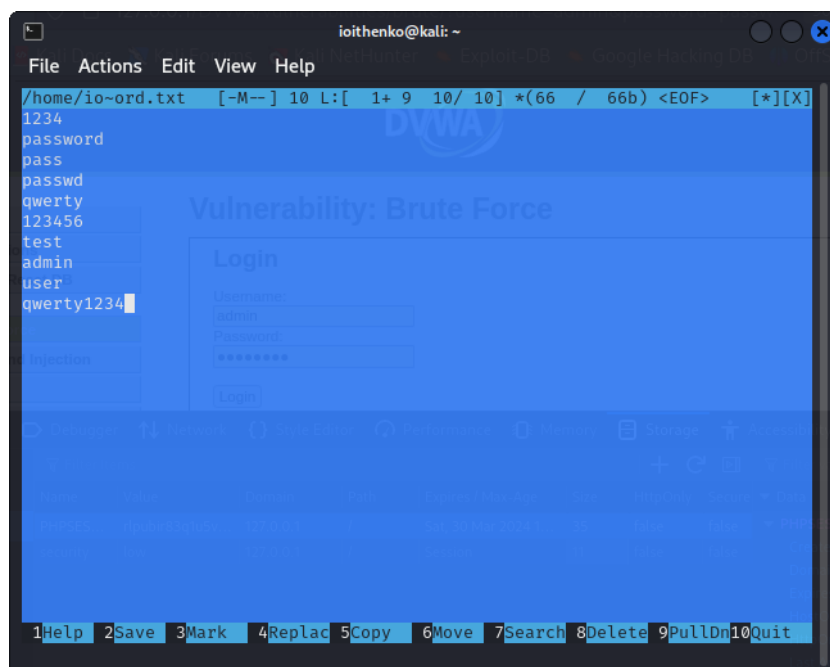


Рис. 2.4: Файл с паролем

Прописываем команду для hydra: указываем IP, логин, файл паролей и путь к форме с указанием PHPSESSID (найден с помощью inspect) (рис. 2.5).

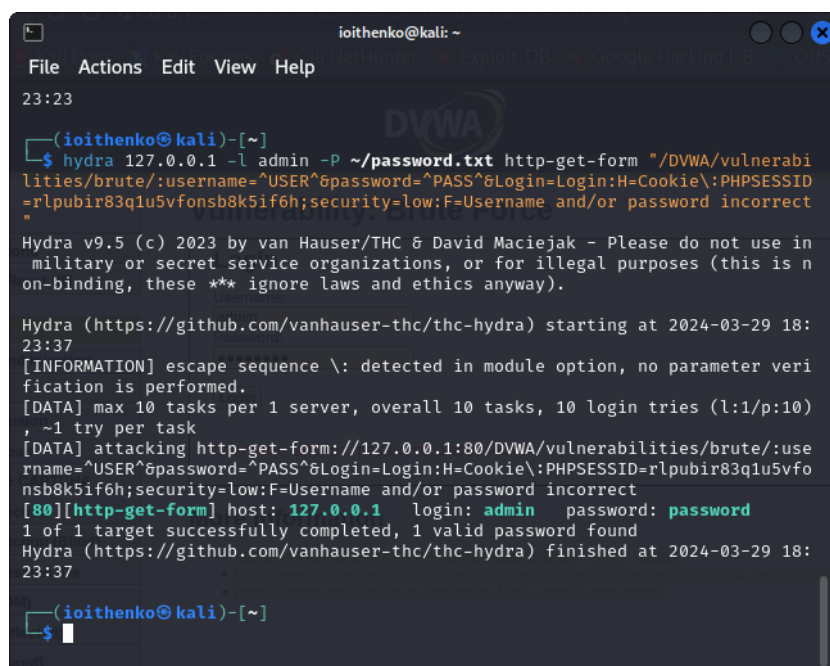


Рис. 2.5: hydra

Команда выполнена верно, пароль подобран.

3 Выводы

В ходе этапа проекта я научилась использовать hydra для подбора логина и пароля.

Список литературы

1. Ш. Парасрам Т.Х. А. Замм. Kali Linux: Тестирование на проникновение и безопасность. 4-е изд. Санкт-Петербург: Питер, 2022. 448 с.