Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Тульский государственный университет»

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

БАЗОВЫЕ МЕТОДЫ ИССЛЕДОВАНИЯ УЯЗВИМОСТИ БАЗ ДАННЫХ

отчет о

лабораторной работе №7

по дисциплине

ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Выполнила: ст. гр. 230711 Павлова В.С.
Проверил: асс. каф. ИБ Греков М.М.

Тула, 2023 г.

ЦЕЛЬ РАБОТЫ

Цель: ознакомиться с основными методами поиска уязвимостей присутствующих в базах данных WEB приложений, при помощи специализированных программных средств.

ЗАДАНИЕ НА РАБОТУ

1. Установить DVWA и проведите его настройку.
2. Установить Metasploitable 2 в комплекте с платформой DVWA.
3. Установить уровень Low на платформе DVWA и выполнить следующие действий, получить список таблиц БД, получить список полей таблицы пользователей СУБД. Получить имена пользователей и хеши паролей пользователей. Расшифровать пароль администратора при помощи JhonTheRipper, или HashCat и представить скриншот каждого этапа. По аналогии сделать для medium и height.
4. Установить платформу bWApp и выполнить атаку на раздел, содержащий SQL Injection на основе следующего руководства https://hackware.ru/?p=1956 и передоставить запрос, приведший к получению администратора и его хеша пароля и скриншот окна, содержащий подтверждение его получения.

ХОД РАБОТЫ

1. Установка DVWA и его настройка (рисунок 1):

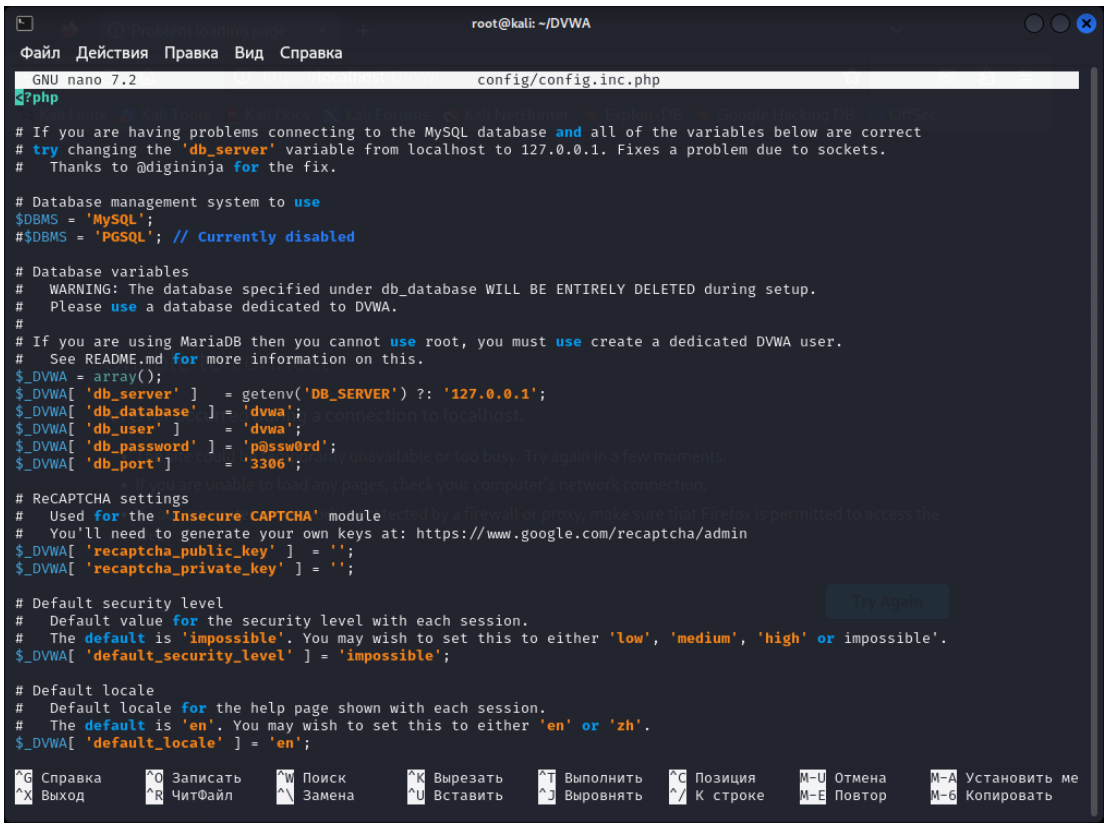

Рисунок 1 – Установка DVWA

2. Получение имён пользователей и хешей их паролей на трёх уровнях (рисунки 2-4 соответственно):

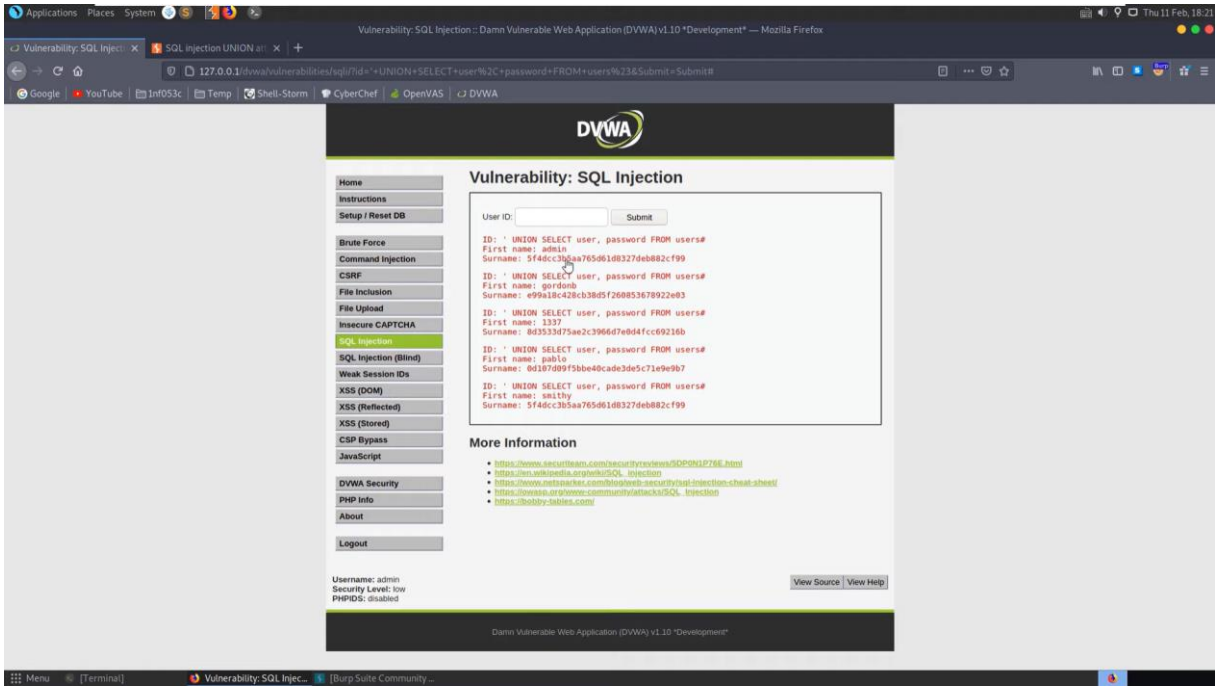

Рисунок 2 – Получение имен пользователей и паролей на уровне low

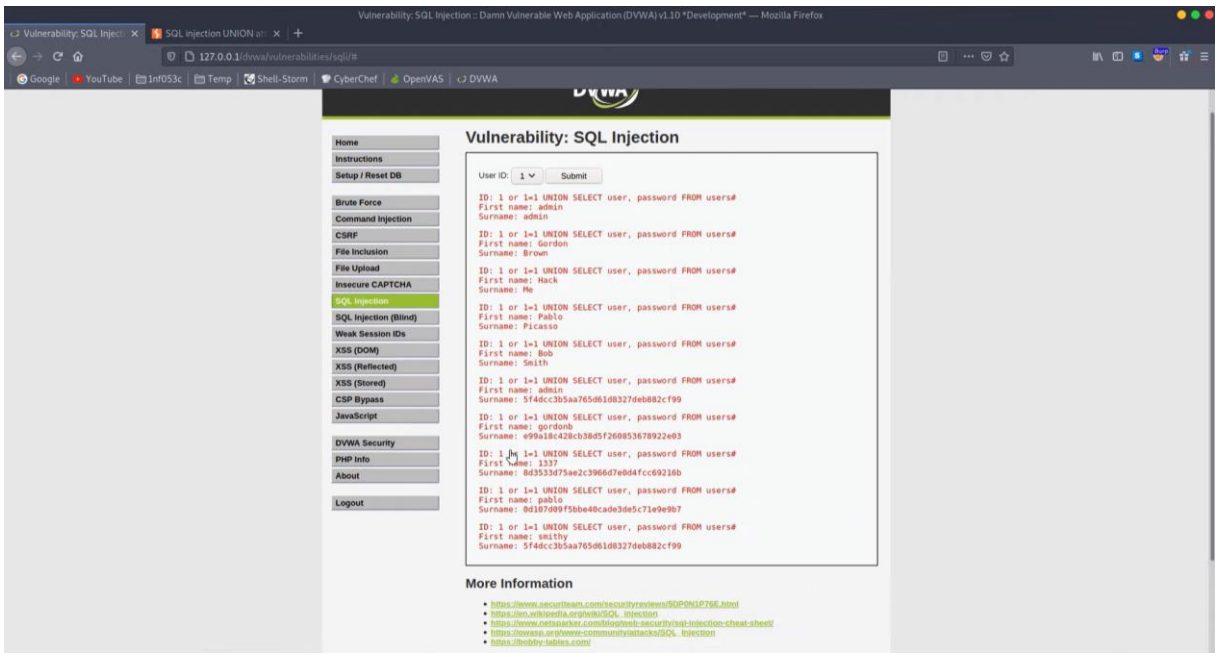

Рисунок 3 – Получение имен пользователей и паролей на уровне medium

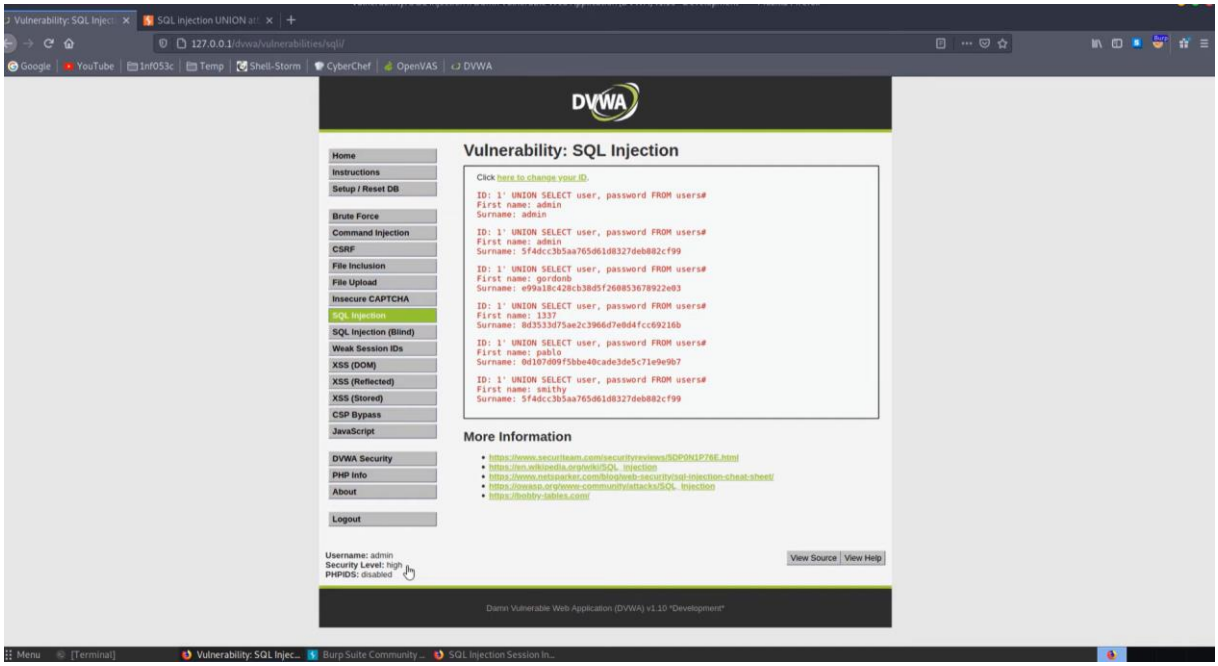

Рисунок 4 – Получение имен пользователей и паролей на уровне height

3. Расшифровка полученных хешей с помощью ресурса crackstation (рисунок 5):

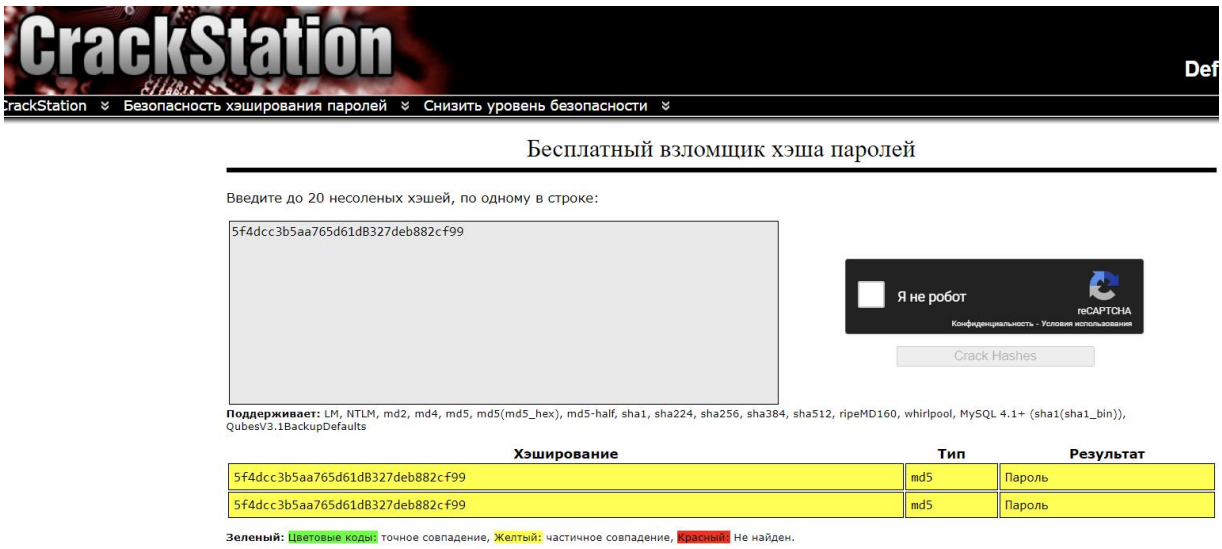

Рисунок 5 – Результат расшифровка хэша

4. Получение хеша пароля и логина администратора в bWApp с помощью атаки на раздел, содержащий SQL Injection (рисунок 6):

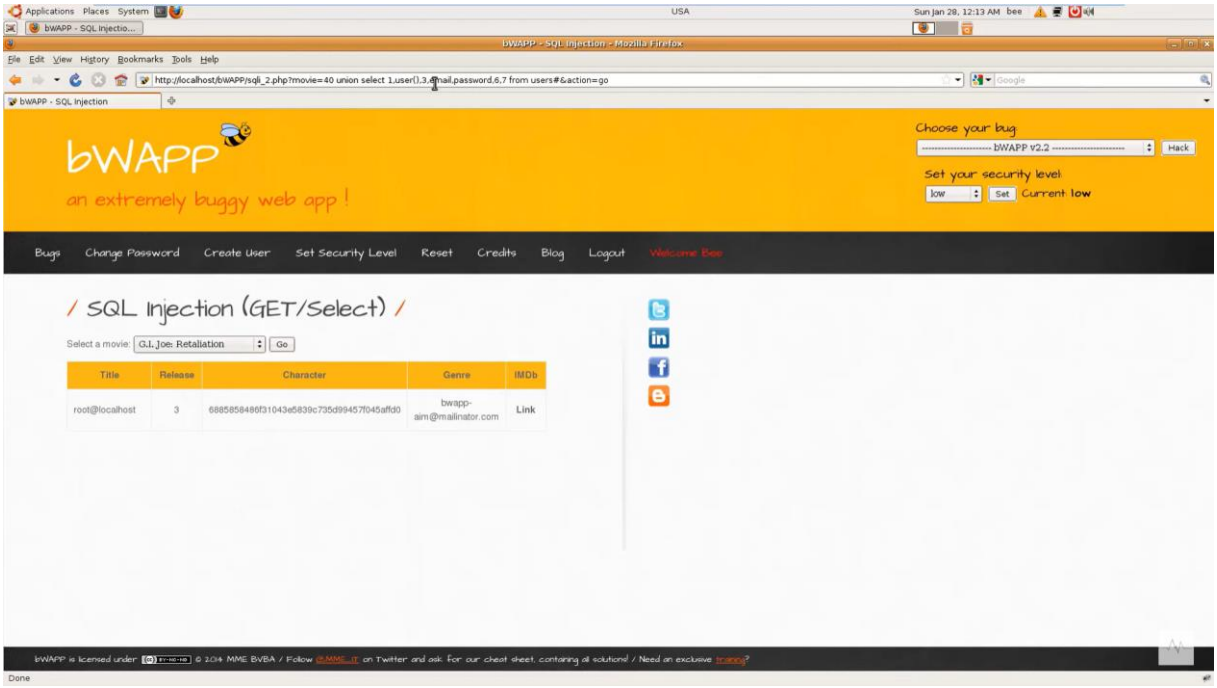

Рисунок 6 – Результат получения хэша

ВЫВОД

В ходе выполнения данной лабораторной работы я ознакомилась с дополнительными методами эксплуатации уязвимостей на объекте защиты информации.