

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 провести его настройку.
2. Установить Metasploitable 2 в комплекте с платформой DVWA.
3. Установить уровень Low на платформе DVWA и выполнить следующие действия, 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 high.
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):

```
root@kali: ~/DVWA
Файл Действия Правка Вид Справка
GNU nano 7.2 config/config.inc.php
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
# Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
# $DBMS = 'PGSQL'; // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
# See README.md for more information on this.
$_DVWA = array();
$_DVWA['db_server'] = getenv('DB_SERVER') ? '127.0.0.1';
$_DVWA['db_database'] = 'dvwa'; // connection to localhost
$_DVWA['db_user'] = 'dvwa';
$_DVWA['db_password'] = 'p@ssw0rd';
$_DVWA['db_port'] = '3306'; // unavailable or too busy. Try again in a few moments.
// Unable to load any pages, check your computer's network connection.

# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module, need to have a key or proxy, make sure that Firefox is permitted to access the
# You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA['recaptcha_public_key'] = '';
$_DVWA['recaptcha_private_key'] = '';

# Default security level
# Default value for the security level with each session.
# The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or impossible'.
$_DVWA['default_security_level'] = 'impossible';

# Default locale
# Default locale for the help page shown with each session.
# The default is 'en'. You may wish to set this to either 'en' or 'zh'.
$_DVWA['default_locale'] = 'en';

[Ctrl]G Справка [Ctrl]O Записать [Ctrl]W Поиск [Ctrl]K Вырезать [Ctrl]T Выполнить [Ctrl]C Позиция [M-U] Отмена [M-A] Установить ме
[Ctrl]X Выход [Ctrl]R ЧитФайл [Ctrl]N Замена [Ctrl]U Вставить [Ctrl]J Выровнять [Ctrl]G К строке [M-E] Повтор [M-B] Копировать
```

Рисунок 1 – Установка DVWA

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

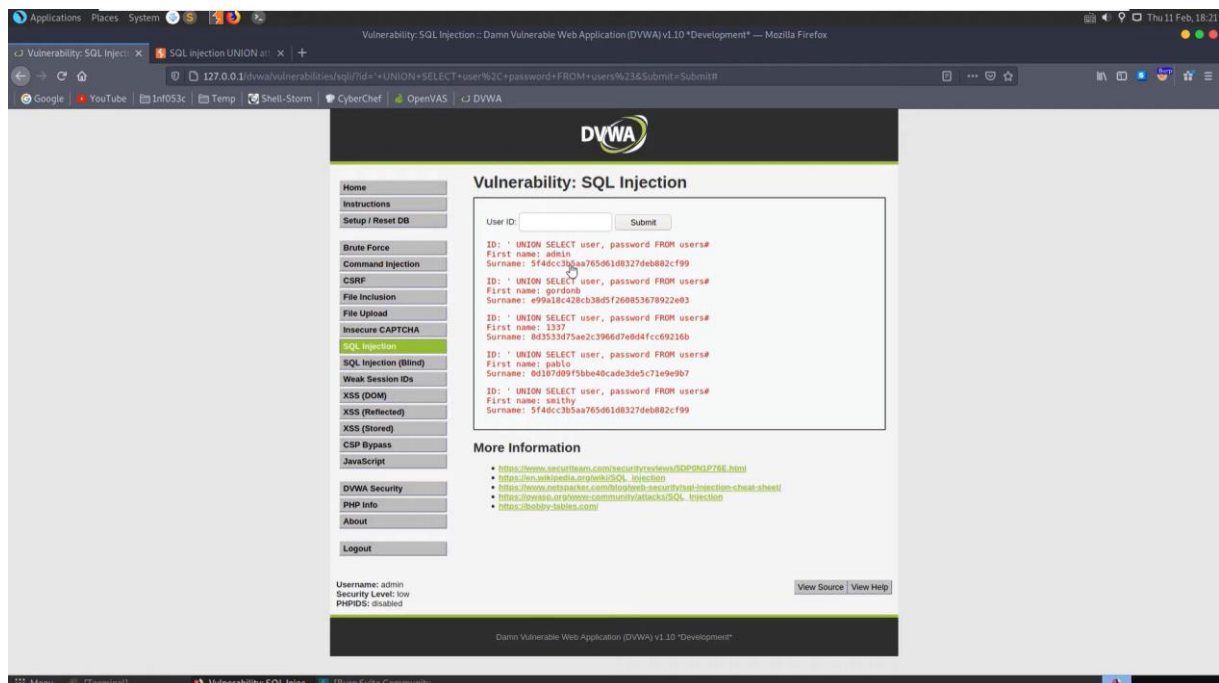


Рисунок 2 – Получение имен пользователей и паролей на уровне low

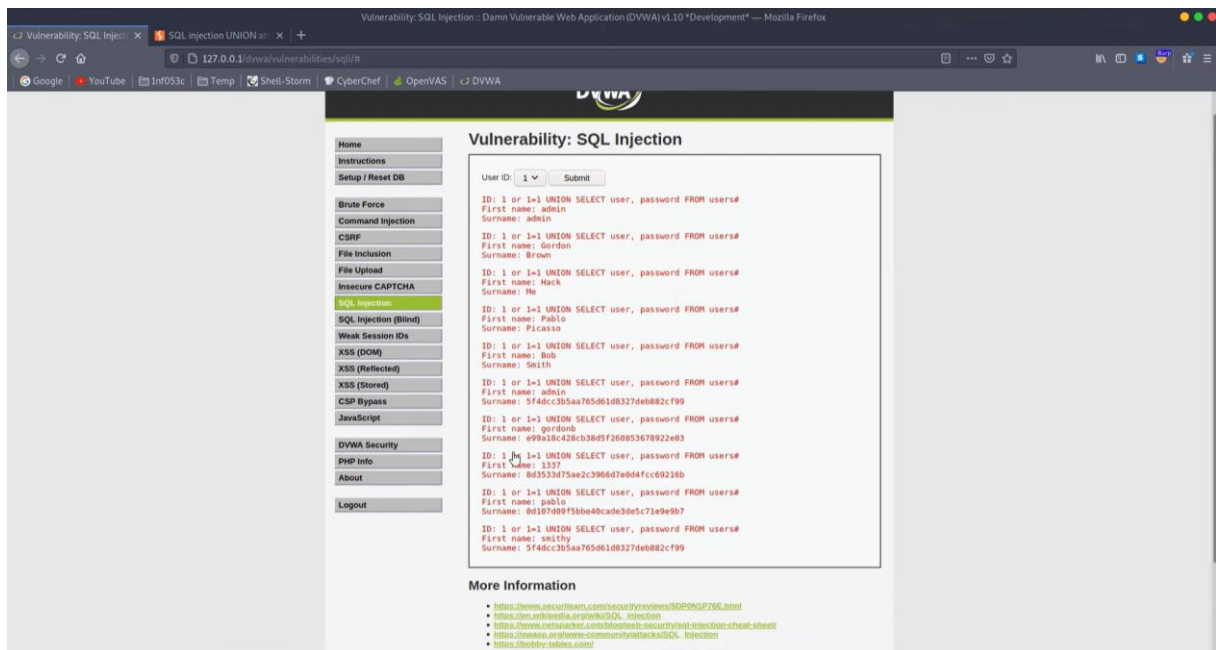


Рисунок 3 – Получение имен пользователей и паролей на уровне medium

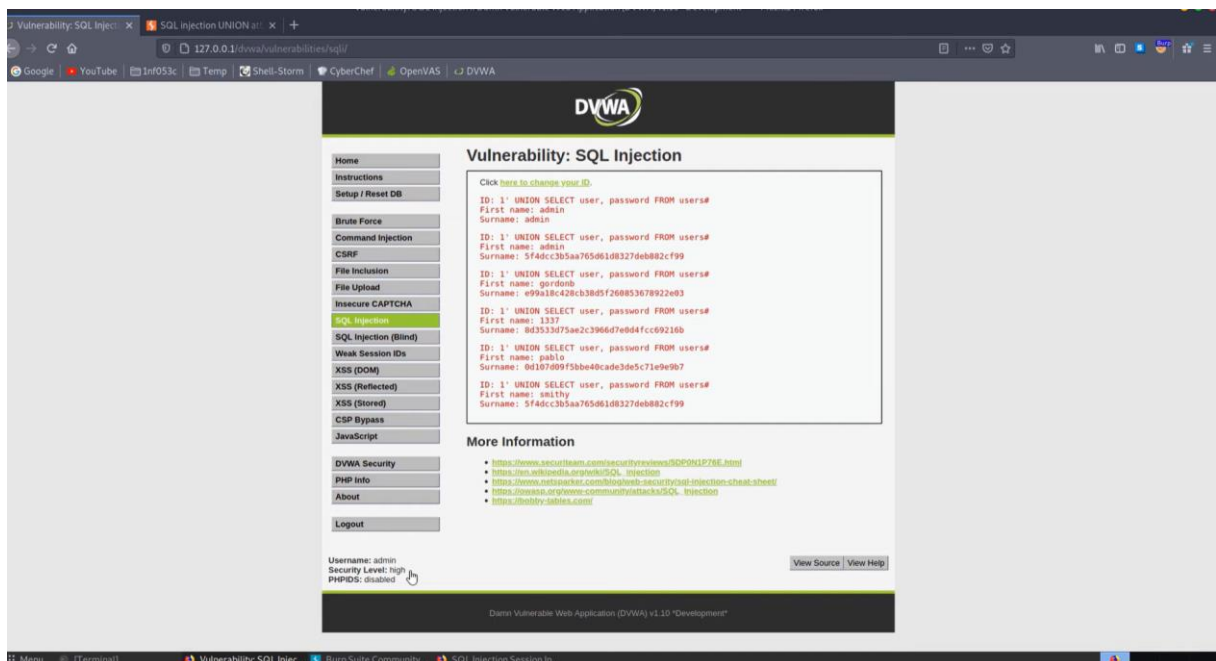


Рисунок 4 – Получение имен пользователей и паролей на уровне height

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

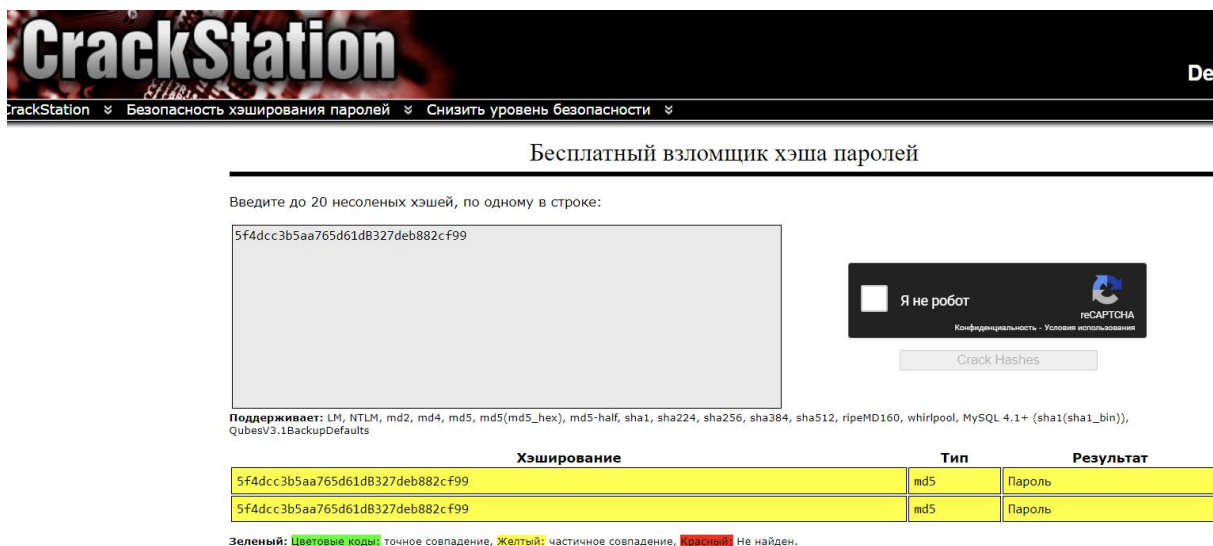


Рисунок 5 – Результат расшифровка хэша

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

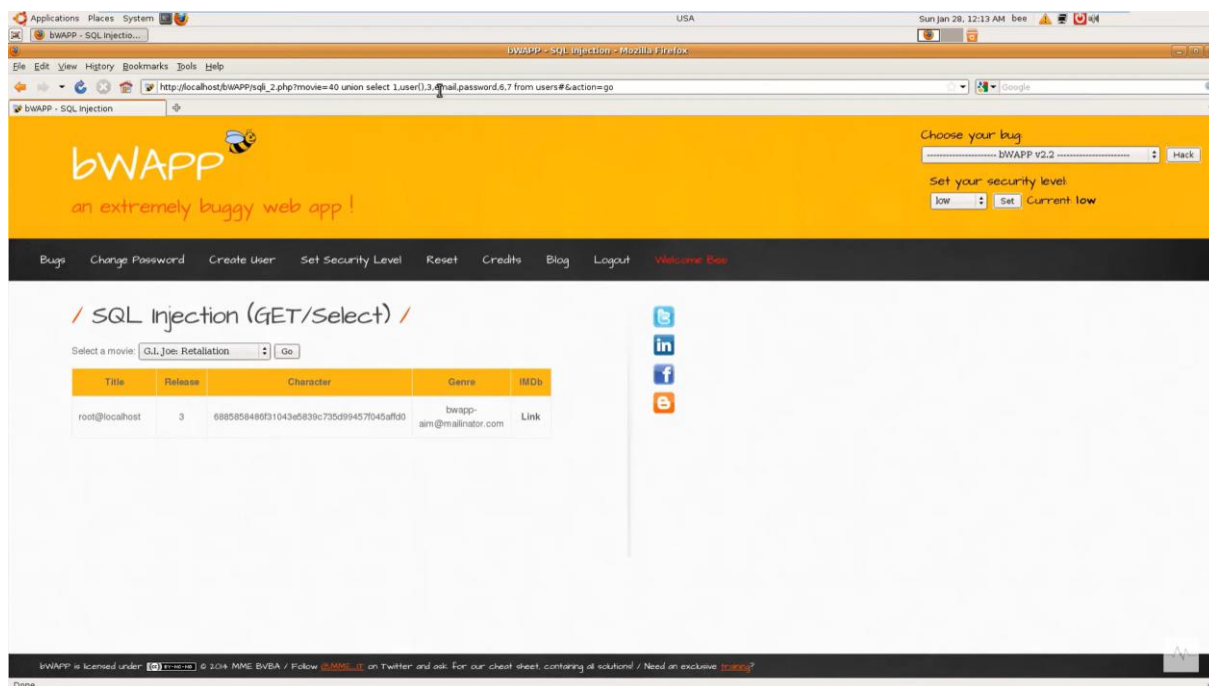


Рисунок 6 – Результат получения хэша

ВЫВОД

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