Assignment - SQL Injection & Password cracking

In this assignment, initially you will do SQL injection using DVWA(Damn Vulnerable Web Application). Lastly, you are expected to crack some password. All details given below.

1 SQL Injection

You are expected to complete SQL injection tutorial at High security level on DVWA web application.

1.1 Requirements

You will need to setup DVWA. Step by step installation guide for Ubuntu can be found in `https://avesis.yildiz.edu.tr/fuato/dokumanlar`. You are free to use any operating system. For more detailed installation guide, please read documentation given in `https://github.com/digininja/DVWA`

1.2 Details

After you installed DVWA, you should set security level to high. Then you are expected to inject your SQL to expose user passwords from default "USERS" table. You are not restricted to use any specific method, you are free. However, you are expected to record a video that shows how you do it.

2 Password Cracking

You are expected to crack MD5 crypted password.

2.1 Requirements

You will need to setup password cracking tool called **John the Ripper(JtR)**. It is highly recommended to use Kali Linux that allows you to use pre-installed JtR. However, you are free to use any kind of operating system:

- For Windows, you can download JtR from its homepage: `http://www.openwall.com/john/`
- For macOS, you can use **brew** package manager. For more information visit `https://brew.sh/`. Once you've installed Homebrew, you can instlal JtR using the command :

```
brew install john--jumbo
```

You will also need to download `https://www.scrapmaker.com/download/data/wordlists/dictionaries/rockyou.txt` word list.

2.2 Details

Imagine you have hacked into a database with SQL injection. You have found that database stores many **MD5** encrypted passwords. And finally, assume that all those hashed passwords are generated from the words can be found in **rockyou.txt** file.

You are expected to decrypt hashed password that corresponds to your student ID from the given **"BSG_assignment"** excel file. Please note that you do not have to decrypt entire all hashes in the file, so it is recommended to decrypt only your own password.

3 Deliverables

- Deadline: 27 December 2021
- A video(3 minutes max.) that illustrates how you do Sql Injection(High).
- A video(3 minutes max.) that illustrates how you use JtR on command line and show password.
- A short report(2 page max.) where your explanations, screenshoots must take place.