PROJECT REPORT

SQL Injection Playground with Detection Engine

- Introduction
  The aim of the project is to develop a training project to detect sql injection in a web page
  The project is divided in to 2 parts
  1. To have a web page containing username / password which allows you to login
  2. Python file detecting the sql injection in the webpage

- Tools Used:
  OS: Linux
  Languages: Python3, Flask, SQL, Html, Css
  Database: SqlLite3

- Steps Involved in Building the Project
  Python is an interpreted language, does not require any building
  The python file **a.py** can be executed directly executed by typing at command prompt using python3 a.py

- Conclusion
  1. There are multiple ways sql injection can be injected in a wed page.
  2. I have demonstrated comment & conditions based sql injection
  3. When any condition is given in the sql statement, if no parameterized query is used by the developer, then we can use the sql injection to by pass the query to directly fetch the required data from the database.
  4. The concepts are taken from the below given references for this project:
     - SQL injection – Wikipedia
     - SQL Injection (With Examples)
     - What Is SQL Injection? Risks, Examples & How to Prevent It | DataCamp
     - SQL Injection - GeeksforGeeks