# Fuzzy Logic-based SQL injection Detection

# How To Detect Potential SQL Injection with Fuzzy Logic ?

A SQL Injection is the alteration of an existing SQL. Therefore it’s a SQL statement that should have some kind of likeness with an existing one.

Fuzzy Logic computes a score of likeness between 0 and 100.

There are 2 main ways, the standard and the partial one. Partial seems to be more effective at detecting likeness when the alteration is not at the start of the SQL statement which is most likely to be the case in case of SQL Injection.

# Demo

# Outline

0 - Environment : Linux + PostGresql + Python

1 - Basic check

2 - Creation of the Data structure

3 - Presentation of the program

- Module
- Main
- Thread

4 - Run

5 - Read results

6 - Alert

# Module Available on GitHub

We can download this module and test by yourself

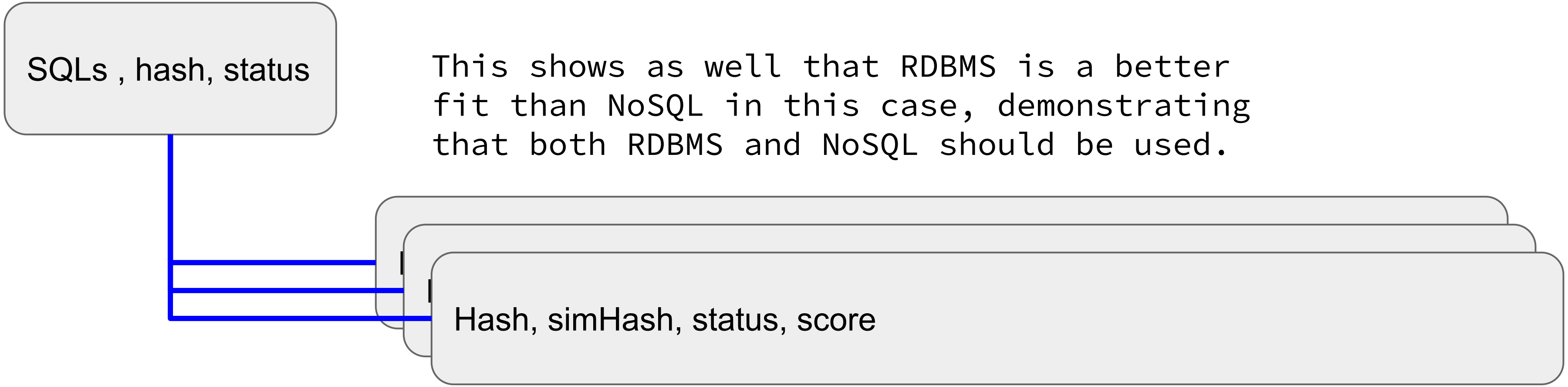
You need :

- postgreSql database
- sql_creation.sql
- Python + fuzzywuzzy module
- Ekfuzzy.py
- Main.py
- You may have to change the credentials hardcoded in the py scripts to access your postgres instance

# Data Architecture

Each check computers a score. We record all checks above a certain score threshold, for example above 40. We record the new SQL in the reference list and it is used in the next test.

Therefore, the resulting Data Architecture  we have a 1 to n relationship between a SQL being checked and the existing SQLs, as follows:



This shows as well that RDBMS is a better fit than NoSQL in this case, demonstrating that both RDBMS and NoSQL should be used.

# Software Architecture

1 Module containing 1 Class

Main instantiates the Class and runs the object as a thread.

The goal is to integrate the check within the Enriched ETL.

The Enriched ETL is a RT process that can be used to verify SQL statements. The SQL Injection check could be done at that time. This integration will be performed later in Context22 OpenSource project

# Next Steps

- Misc : parameterize the posgresql credentials
- Cloud version : to allow users to test and try without having to deploy the posgresql DB
- Integration with the CT22 Enriched ETL

# A New Approach in SQL Injection Detection on Databases

Author : Frederic Petit - Context 22 -
info@context22.com