SQL Injection Detection Using Anomaly-Based Model

Rahnema College Internship Project Proposal

By Fatemeh Shiri

Under Mentorship of Mahjoubeh Chavoshi

1.Introduction

In this project, we were asked to develop a system being able to recognize anomalous http requests from client side in web servers using a time series dataset which is driven from logs of a web server. I have chosen to work on Sql injection attack and build a model which is able to detect requests containing this attack. Sql Injection occurs when untrusted data is sent to an interpreter as part of a query, tricking it to execute unintended commands or to access unauthorized data.

2.Overview of Implementation Workflow

The project is going to be developed in proactive manner and if possible, be updated to active manner.

1- Model Creation:
   - Feature Extraction (based on http logs)
   - Feature Engineering and Data Pre-Processing
   - Finding Association Rules and Patterns in Normal requests
   - Anomaly Detection (Unsupervised Case)
   - Labeling Anomalous Requests as ‘Abnormal’ (Bring the Problem to One-Class Classification Problem)
2- Optimize Model
3- Develop the Model-Based Application (Proactive)
4- Use and Test the Application in an Active manner