SQL Injection Detection System - Deployment Report

Developer Information

Name: Musharraf Perwez

Internship Domain: Cloud Computing

Organization: CodeAlpha

Project Summary

Project Name: SQL Injection Detection System

Description:

This project is a Flask-based web application designed to detect and mitigate SQL injection attempts.

It inspects incoming user inputs and filters malicious SQL patterns using basic detection logic.

The app stores registered user data securely and uses AES encryption for password storage.

Technology Stack:

- Backend: Python (Flask)
- Frontend: HTML (Jinja2 templates)
- Database: SQLite
- Encryption: cryptography (AES)
- Deployment: AWS EC2 (Ubuntu 22.04)
- Version Control: Git & GitHub

Deployment Details

Hosted On: AWS EC2 Instance (Ubuntu 22.04)

Public IP: http://13.60.252.61

Access: Application running on port 5000

Project Repository:

https://github.com/MusharrafPerwez-sam/CodeAlpha_SQL_InjectionDetectionSystem

SQL Injection Detection System - Deployment Report

Directory Structure:

- app.py
- config.py
- encryption/
- access/
- templates/
- users.db
- requirements.txt

Features Implemented

- User Registration and Login with capability token
- AES-encrypted password storage
- SQL Injection detection via simple keyword scanning
- Secure session handling with Flask
- Hosted and accessible from AWS EC2 instance

Security Measures

- AES encryption for password storage
- Session-based login with token
- Basic SQL injection prevention with keyword checks
- HTTPS: Not enabled (runs on HTTP)
- Authentication: Implemented via login system