People's Democratic Republic of Algeria

Ministery of Higher Education and Scientific Research

Ferhat Abbas University of Setif 1



Faculty of Sciences

Computer Science Department

**THEME**

Detecting SQL injection using Deep Learning

Realizedby: Supervised by:

ZITOUNI AHMED FAOUZI DR. BENZINE MEHDI

SEDJAL MOHAMED AYMEN DHIAEDDINE

**2024/2025**

**Table of contents**

**General introduction** **............................................................................................. 1**

**Chapter 1 SQL injection** **.........................................................................................2**

1.1 introduction **.......................................................................................................3**

**1 SQL Injection**

**1.1Introduction**

Withincreasingly digital living, web applications are at the core of daytoday lifefrommanaging finances and online purchasing to collaborating and communicating. This ease of the virtual world comeswithinherentsecurity challenges. Cyber attackerspersistentlyevolvetheirmethods to exploit weaknesses, therebyendangeringunauthorized data access, downtime of services, and irreparable damage to reputation.

        Instead of goingwith the traditionalenumeration, itis pertinent to talk about these five new categories of risksthatcontemporary web applications have to face:

**Inadequate Input Validation:**

Not validating and sanitizing user-supplied data properly can facilitate a range of attacks, such as injection and cross-site scripting (XSS). Suchneglectpermitsattackers to injectmalicious code into the system, therebyviolating data integrity and application functionality.

**InsufficientAuthentication and Session Management:**

Insufficientmethods of validating user identities or handling active sessions can permit unauthorizedusers to obtainaccess. Adequatecontrolssuch as multi-factor authentication and secure session managementare essential for protecting user accounts and sensitive information.

**Lack of data protection:**

Irrespective of whether the data is at rest or in motion, poorencryption or weak key management practices can lead to exposure of sensitive data. Robustcryptographic standards have to beimplemented, and sensitive data has to bemaintainedconfidentiallyfromits life cycle for successful protection of data.

**DefectiveIntegration&DependencyManagement:**

Contemporary web applications tend to includeexternal services and libraries. Whentheseunderlyingelements are insecure or outdated, they can injectvulnerabilitiesinto the system overall. Diligent monitoring ofdependencies, alongwith routine security audits, isrequired to avertthesethreats.

**Poor error handling and logging:**

Poorlycontrollederror messages and a lack of logging can inadvertentlydisclose system information to prospective attackers or hamper the timelydetection of a security incident. Havingwelldefinederrorhandling routines and utilizingsolid monitoring systems are essential for the timelydetection and containment of maliciousactivity.

One of the mostrisky implications of thesevulnerabilitiesisexposure to SQL injection attacks. Where an application does not sanitize input sufficiently, malicioususers can injectmalicious SQL statements, and these have the potential to result in unauthorized data alteration or even system hijacking. The implication of this type of exploitation can becatastrophicresulting in data loss, system crash, and long-termreputational damage for an organization.

        Through the use of proactive design principles and audits on a regular basis, developers can greatlyminimize the chances of exploitation in today'sintricate digital world.