

# Security Enhancements - Excel Tools Plugin

---

## Overview

This document outlines the security improvements implemented in the Excel Tools Plugin to address potential vulnerabilities and enhance overall security posture.

## Security Improvements

### SQL Injection Prevention

- **Enhanced input validation** for all database identifiers (table names, column names)
- **Proper quote escaping** to handle quote characters safely
- **System table access blocking** to prevent unauthorized access to database metadata
- **Table existence validation** to prevent information disclosure through error messages
- **Column/Table Name Length Limits** to prevent buffer overflow attacks

### Key Security Features

- All SQL identifiers are properly quoted and escaped
- System tables (information\_schema, mysql\_user, etc.) are blocked from access
- Input validation includes length limits and security checks
- Generic error messages prevent information leakage
- Support for international/special characters while maintaining security

### Database Compatibility

- Multi-database support with proper security handling for:
  - MySQL/MariaDB
  - PostgreSQL
  - Oracle
  - SQL Server
  - DB2

### JNDI Security

- Validation of JNDI datasource names
- Blocking of potentially dangerous protocols
- Restricted to legitimate JDBC datasource patterns

## Benefits

- **Prevents SQL injection attacks** through comprehensive input validation
- **Protects sensitive database information** from unauthorized access
- **Maintains functionality** while enhancing security
- **Supports international use cases** with proper character handling
- **Provides clear audit trail** through validation logging

## Usage Guidelines

### Automatic Database Quoting

The plugin automatically applies database-specific identifier quoting to table/column names to protect against SQL injection:

- MySQL/MariaDB: Backticks( ``table name`` )
- SQL Server: Brackets( `[table name]` )
- Oracle: Double quotes( `"table name"` )

#### IMPORTANT:

- Remove quotes that were manually added for SQL safety (e.g., change `"my table"` to `my table` )- The plugin applies the appropriate delimiters automatically based on your database type.
- Keep quotes that are part of actual identifier names (e.g., if your table is literally named `my'table` , keep the quote as part of the name)
- Update any code accessing system tables (`information_schema`, `mysql_user`, etc.) as these are now blocked