

Vulguard

A framework for evaluating
Database Stored Procedures
against vulnerabilities

Project Requirements

- Design and implement an automated assessment tool for database stored procedures.
- Test all susceptible stored procedures within a database for the potential existence of buffer overflow or SQL injection vulnerabilities.

Vulguard 1.0 Framework

- Vulguard is a generic assessment tool for DB stored Procedures.
- Vulguard tries to find the following kinds of vulnerabilities:
 - Buffer Overflows
 - SQL Injections
- Vulguard runs several tests on the DB specified stored procedures and generates a report describing the results of the stored procedure evaluation.

Vulguard User Interface

- Vulguard is a command line tool.
- The user can control the following parameters:
 - DB name (with optional user/password)
 - The tests to run on the stored procedures
 - A list of stored procedure to evaluate
- While running Vulguard, the user receives indication about the progress of the execution.
- After execution, a full report is generated in XML format, describing which procedures have possible vulnerabilities along with specific information regarding how to reproduce the suspected behavior.

Vulguard is generic

- The framework is cross-platform.
 - We ran Vulguard with no code changes under both MS Windows and Linux Operating Systems.
- Vulguard contains a generic database layer. We can easily implement this layer in for any DB vendor.
 - We implemented it for IBM DB2 database.

Vulguard is generic (2)

- The vulnerability test mechanism is extendible.
 - In order to add a new test to the framework, the user should implement a class that extends `VulTest`.
 - Then, register the new test into `VulTestRegistry` using ***addVulTest*** method.

Vulguard Tests

- String Size
 - Checks the behavior of the stored procedure (SP) with string parameters using variable sized string values (for potential buffer overflows).
- SQL Strings
 - Finds potential SQL injection in SPs using special values of string parameters, which contain SQL code.

Vulguard Tests (2)

- Special Chars

- Checks for various vulnerabilities of SPs caused by invalid parsing of a string parameters (such as “printf” format strings).
- The SPs are challenged with special characters (\$, ‘, “, %, etc) in their string parameters.

- Or SQL Injection

- Finds SQL Injections in SPs by looking for different results when using “a‘OR 1=1” as the string parameter.

Using Vulguard on DB2

- We used Vulguard framework in order to assess the safety level of DB2 stored procedures.
- We ran all our tests on all DB2 stored procedures and found potential vulnerabilities in several stored procedures.

Suspected Procedures

- The following DB2 Stored Procedures have potential vulnerabilities:
 - LIST_COL_LONG_OPTS
 - GET_SWRD_SETTINGS
 - LIST_NN_LONG_OPTS
 - SET_SWRD_SETTINGS
 - GET_WRAP_CFG_C
 - **POLICY_RETRIEVE**
- A more thorough user analysis of POLICY_RETRIEVE procedure comes to the conclusion that this procedure is vulnerable using SQL Injection.