FB.SQL\_BAD\_PREPARED\_STATEMENT\_ACCESS

Детектор определяет ошибку, в ходе которой был выполнен вызов метода setXXX подготовленного оператора, где индекс параметра равен 0. Поскольку индексы параметров начинаются с индекса 1, это всегда является ошибкой.

Таблица №1 – Основные характеристики детектора

|  |  |
| --- | --- |
| Категория критичности | MAJOR |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Ошибка разработчика |
| CWE | — |
| CVE | — |
| Возможные последствия | Попытка установить значение параметра с индексом 0 приведёт к исключению SQLException. Это может привести к сбою выполнения SQL-запроса и, как следствие, к некорректной работе приложения. |
| Комментарий | Необходимо проверить индексы параметров в подготовленном операторе. Индексация начинается с 1, поэтому необходимо использовать корректные значения индексов. |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Некорректное написание | Корректное написание |
| public static void incorrectTest(PreparedStatement preparedStatement) throws SQLException {  preparedStatement.setInt(0, 1);  // ...  } | public static void correctTest(PreparedStatement preparedStatement) throws SQLException {  preparedStatement.setInt(1, 1);  // ...  } |

Методы устранения уязвимости при срабатывании детектора:

1. Найдите все вызовы методов setXXX у объектов PreparedStatement, где индекс параметра равен 0.
2. Измените индекс параметра на корректное значение, начиная с 1. Индекс должен соответствовать позиции знака вопроса (?) в SQL-запросе. Если в запросе несколько параметров, они нумеруются слева направо, начиная с 1.
3. Проверьте SQL-запрос, связанный с PreparedStatement, чтобы определить правильное количество и порядок параметров. Убедитесь, что индексы, используемые в методах setXXX, соответствуют этим параметрам.
4. Если вы динамически строите SQL-запрос и добавляете параметры, убедитесь, что логика установки параметров также корректно управляет индексами, начиная с 1 и последовательно увеличивая их.
5. Протестируйте код, выполняющий SQL-запросы с подготовленными операторами, чтобы убедиться, что исключение SQLException больше не возникает из-за некорректных индексов параметров.
6. Используйте константы или перечисления для представления индексов параметров, если это улучшает читаемость и предотвращает ошибки, связанные с "магическими числами".