FB.XPATH\_INJECTION

Ошибка "The use of XPath.evaluate() is vulnerable to XPath injection" указывает на потенциальную уязвимость в коде, связанную с использованием метода XPath.evaluate() при обработке пользовательского ввода, что может привести к атаке XPath Injection.

XPath (XML Path Language) используется для навигации и запросов в XML-документах. Атака XPath Injection возникает, когда злоумышленник вводит данные в поле запроса (например, форма на веб-сайте), и эти данные непосредственно внедряются в XPath-запрос, что может привести к несанкционированному доступу к данным или выполнению нежелательных действий.

Таблица №1 – Основные характеристики детектора FB.XPATH\_INJECTION

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | XPath Injection |
| CWE | CWE643 |
| CVE | --- |
| Возможные последствия | Обход аутентификации, несанкционированный доступ к данным, раскрытие конфиденциальной информации через XML-базы данных |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest() throws FileNotFoundException {  FileInputStream fis = new FileInputStream("missing.txt"); // Может выбросить исключение  System.out.println("Файл открыт (но мы этого не увидим при ошибке)");  } | public static void correctTest() {  try {  FileInputStream fis = new FileInputStream("missing.txt");  System.out.println("Файл открыт");  } catch (FileNotFoundException e) {  System.err.println("Ошибка: Файл не найден");  // Логирование или обработка ошибки  } finally {  System.out.println("Блок finally выполнен");  }  } |