FB.XSS\_REQUEST\_PARAMETER\_TO\_JSP\_WRITER

Этот код напрямую записывает параметр HTTP в выходные данные JSP, что допускает возможность межсайтового скриптинга.

Таблица №1 – Основные характеристики детектора FB.XSS\_REQUEST\_PARAMETER\_TO\_JSP\_WRITER

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Security Vulnerability (Cross-Site Scripting) |
| CWE | CWE79 |
| CVE | --- |
| Возможные последствия | Межсайтовый скриптинг (XSS); кража сессий и cookies; подмена содержимого страницы |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest(HttpServletRequest request, JspWriter out) {  // Некорректно: прямой вывод пользовательского ввода  if (request != null && out != null) {  try {  String userInput = request.getParameter("comment");  out.print(userInput); // Уязвимость XSS!  System.out.println("Content printed (INSECURE)");  } catch (Exception e) {  e.printStackTrace();  }  }  } | public static void correctTest(HttpServletRequest request, JspWriter out) {  // Корректно: экранирование HTML-сущностей  if (request != null && out != null) {  try {  String userInput = request.getParameter("comment");  String safeOutput = escapeHtml(userInput);  out.print(safeOutput);  System.out.println("Content printed securely");  } catch (Exception e) {  e.printStackTrace();  }  }  } |