FB.HRS\_REQUEST\_PARAMETER\_TO\_HTTP\_HEADER

Этот код напрямую записывает параметр HTTP в заголовок HTTP, что допускает уязвимость разделения ответа HTTP.

Таблица №1 – Основные характеристики детектора FB.HRS\_REQUEST\_PARAMETER\_TO\_HTTP\_HEADER

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Security Vulnerability (Header Injection) |
| CWE | CWE113 |
| CVE | --- |
| Возможные последствия | HTTP Response Splitting атаки; Кэш-отравление (Cache Poisoning); Межсайтовый скриптинг (XSS); Подмена заголовков ответа |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest(HttpServletRequest request, HttpServletResponse response) {  // Некорректно: прямое использование параметра запроса в заголовке  if (request != null && response != null) {  String lang = request.getParameter("lang");  response.setHeader("Content-Language", lang); // Без валидации  System.out.println("Header set without validation (INSECURE)");  }  } | public static void correctTest(HttpServletRequest request, HttpServletResponse response) {  // Корректно: валидация и фильтрация входных данных  if (request != null && response != null) {  String lang = request.getParameter("lang");  String sanitized = sanitizeLanguageHeader(lang);    if (isValidLanguage(sanitized)) {  response.setHeader("Content-Language", sanitized);  System.out.println("Secure header set with validation");  } else {  response.setHeader("Content-Language", "en"); // Значение по умолчанию  System.out.println("Invalid input, using default header");  }  }  } |