FB.MSF\_MUTABLE\_SERVLET\_FIELD

Веб-сервер обычно создает только один экземпляр сервлета или класса JSP (т. е. рассматривает класс как синглтон) и будет иметь несколько потоков, вызывающих методы в этом экземпляре для обслуживания нескольких одновременных запросов. Таким образом, наличие изменяемого поля экземпляра обычно создает условия гонки.

Таблица №1 – Основные характеристики детектора FB.MSF\_MUTABLE\_SERVLET\_FIELD

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Web Application Security Vulnerability |
| CWE | --- |
| CVE | --- |
| Возможные последствия | Race conditions в многопоточной серверной среде; утечка данных между пользовательскими сессиями; непредсказуемое поведение сервлета; возможность атак типа "Time-of-check to time-of-use" (TOCTOU). |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static class UserProfileServletIncorrect extends HttpServlet {  private String currentUser; // Опасное изменяемое поле    @Override  protected void doGet(HttpServletRequest req, HttpServletResponse resp)  throws IOException {  currentUser = req.getParameter("username");  resp.getWriter().write("Profile for: " + currentUser);  }  } | public static class UserProfileServletCorrect extends HttpServlet {  @Override  protected void doGet(HttpServletRequest req, HttpServletResponse resp)  throws IOException {  String currentUser = req.getParameter("username"); // Локальная переменная  resp.getWriter().write("Profile for: " + currentUser);  }  } |