

Avoid Hard-coded or In-comment Passwords in Code

- [Problem](#)
- [Solution](#)
- [Related articles](#)

Problem

The Javascript rule "Avoid hard-coded or in-comment passwords in code" (rule code OPT.JAVASCRIPT.PasswordInComments) searches for hard-coded passwords in source code.

This rule checks if there are comments in the code that contain expressions that match with a **predefined regexp pattern**, so it can lead to several false positives and/or false negatives.

Solution

This rule contains the **parameter "passwordPattern"** that you can **edit to change the default pattern if you are finding too many false positives**.

The default regexp pattern is :

```
public static final String _PASSWORD_TOKEN =
    "password|passwd|contrase..?a|kontrazeinu|pasahitza|contra-
    senha|senha|password|watchwoord|adgangskode|" +

    "has\u00142o|parol|parool|parola\\s+d'ordine|mot\\s+de\\s+passe|\u0043F\u00430
    \u00440\u0043E\u0043B\u0044C|heslo|" +

    "\u003C0\u003B1\u003C1\u003B1\u003C3\u003CD\u003BD\u003B8\u003B7\u003BC\u003B1|\u0015Fi
    fre|\u005BC6\u007801|\u005BC6\u0078BC|" +

    "\u003D1\u0030B9\u0030EF\u0030FC\u0030C9|\u00C554\u00D638|lozinka|\u0043B\u0043E\u00437\u004
    38\u0043D\u0043A\u00430|paasavard";
/**
 * Common regex pattern for detecting a password encoded in comments.
 * Matches a 'password' token in common languages, optionally followed by
 * at most 7 plain words,
 * with optional whitespace followed by a separator/quoting char.
 */
public static final String PASSWORD_IN_COMMENT_PATTERN = "(\\b|_)(?:"
+ _PASSWORD_TOKEN+" )(?::\\s+[\\p{L}]{0,7}\\s*[=\\:\\\\-'\"]";
```

Related articles

- [SSO - Form-based authentication fails](#)
- [SSO - HTTP authentication fails](#)
- [SSO - WIA is not working](#)
- [SSO - Cannot authenticate with credentials](#)
- [Basic Authentication Error when Exporting Action Plan to Atlassian JIRA](#)