Avoid Hard-coded or In-comment Passwords in Code

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|passwort|watchtwoord|adgangskode|"+

"has\u0142o|parol|parool|parola\\s+d'ordine|mot\\s+de\\s+passe|\u043F\u0430
\u0440\u043E\u043B\u044C|heslo|"+

"\u03C0\u03B1\u03C1\u03B1\u03C3\u03CD\u03BD\u03B8\u03B7\u03BC\u03B1|\u015Fi
fre|\u5BC6\u7801|\u5BC6\u78BC|"+

"\u30D1\u30B9\u30EF\u30FC\u30C9|\uC554\uD638|lozinka|\u043B\u043E\u0437\u04
38\u043D\u043A\u0430|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