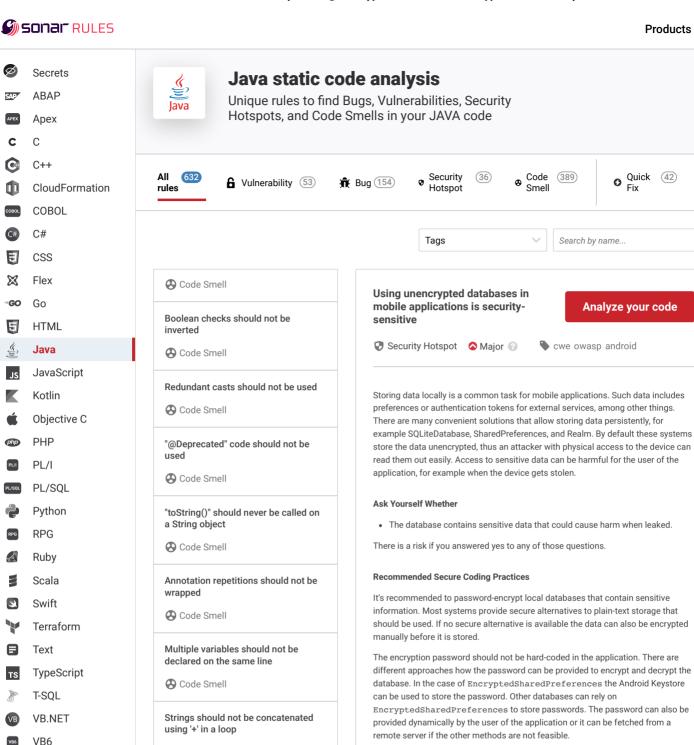


Products ✓

O Quick 42 Fix



different approaches how the password can be provided to encrypt and decrypt the database. In the case of EncryptedSharedPreferences the Android Keystore can be used to store the password. Other databases can rely on

EncryptedSharedPreferences to store passwords. The password can also be provided dynamically by the user of the application or it can be fetched from a

Sensitive Code Example

For SQLiteDatabase:

SOLiteDatabase db = activity.openOrCreateDatabase("test.db",

For SharedPreferences:

SharedPreferences pref = activity.getPreferences(Context.MOD

For Realm:

RealmConfiguration config = new RealmConfiguration.Builder() Realm realm = Realm.getInstance(config); // Sensitive

Compliant Solution

Instead of SQLiteDatabase you can use $\underline{\hbox{SQLCipher:}}$

Code Smell

Maps with keys that are enum values

XML

Lambdas containing only one statement should not nest this statement in a block

Code Smell

"Collections.EMPTY_LIST",
"EMPTY_MAP", and "EMPTY_SET"
should not be used

Code Smell

Local variables should not be declared and then immediately returned or thrown

Code Smell

SQLiteDatabase db = SQLiteDatabase.openOrCreateDatabase("tes

Instead of SharedPreferences you can use EncryptedSharedPreferences:

```
String masterKeyAlias = new MasterKeys.getOrCreate(MasterKey
EncryptedSharedPreferences.create(
    "secret",
    masterKeyAlias,
    context,
    EncryptedSharedPreferences.PrefKeyEncryptionScheme.AES25
    EncryptedSharedPreferences.PrefValueEncryptionScheme.AES
);
```

For Realm an encryption key can be specified in the config:

```
RealmConfiguration config = new RealmConfiguration.Builder()
    .encryptionKey(getKey())
    .build();
Realm realm = Realm.getInstance(config);
```

See

- OWASP Top 10 2021 Category A2 Cryptographic Failures
- OWASP Top 10 2021 Category A4 Insecure Design
- OWASP Top 10 2021 Category A5 Security Misconfiguration
- Mobile AppSec Verification Standard Data Storage and Privacy Requirements
- OWASP Mobile Top 10 2016 Category M2 Insecure Data Storage
- OWASP Top 10 2017 Category A3 Sensitive Data Exposure
- OWASP Top 10 2017 Category A6 Security Misconfiguration
- MITRE, CWE-311 Missing Encryption of Sensitive Data

Available In:

sonarcloud 🔂 | sonarqube

© 2008-2022 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE and SONARCLOUD are trademarks of SonarSource S.A. All other trademarks and copyrights are the property of their respective owners. All rights are expressly reserved.

Privacy Policy