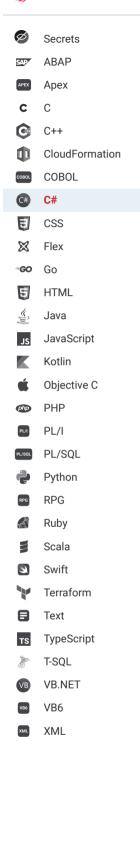
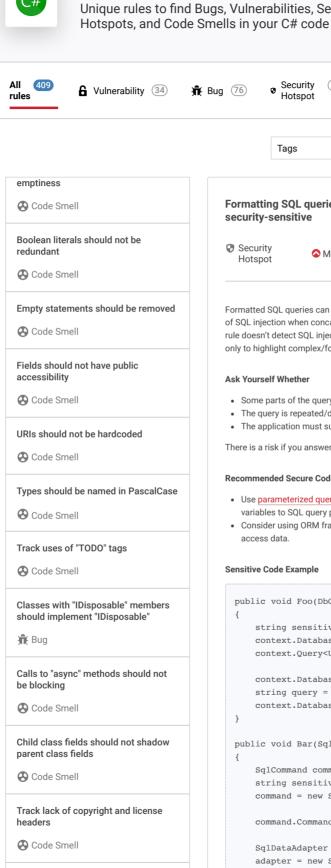
Analyze your code

we owasp sans-top25

bad-practice sql





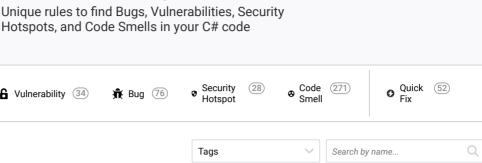


Exit methods should not be called

Classes should "Dispose" of members from the classes' own "Dispose'

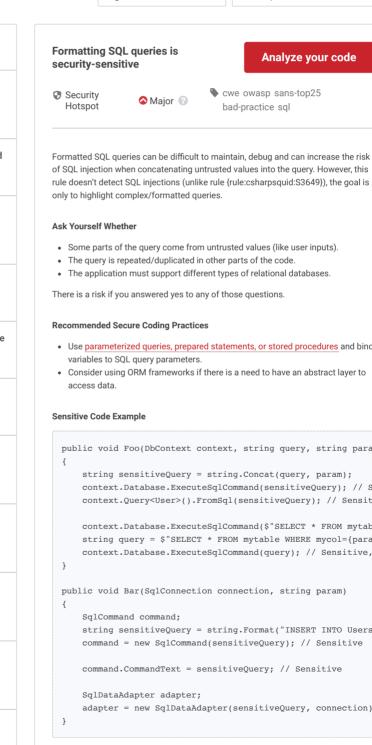
Code Smell

methods

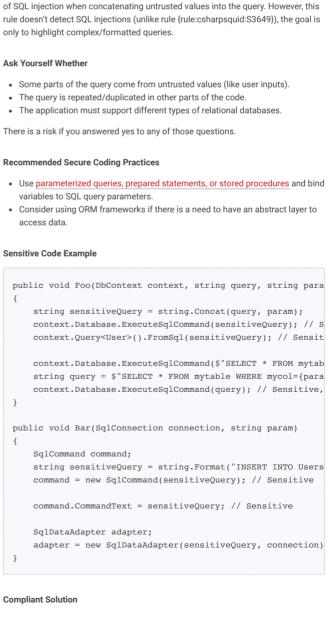


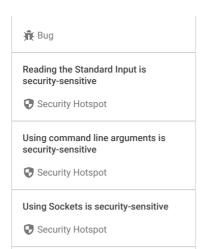
Major

Hotspot



C# static code analysis





Encrypting data is security-sensitive

Security Hotspot

```
public void Foo(DbContext context, string query, string para
{
    context.Database.ExecuteSqlCommand("SELECT * FROM mytabl
}
```

See

- OWASP Top 10 2021 Category A3 Injection
- OWASP Top 10 2017 Category A1 Injection
- MITRE, CWE-89 Improper Neutralization of Special Elements used in an SQL Command
- MITRE, CWE-564 SQL Injection: Hibernate
- MITRE, CWE-20 Improper Input Validation
- <u>MITRE, CWE-943</u> Improper Neutralization of Special Elements in Data Query Logic
- SANS Top 25 Insecure Interaction Between Components
- Derived from FindSecBugs rules Potential SQL/JPQL Injection (JPA), Potential SQL/JDQQL Injection (JDO), Potential SQL/HQL Injection (Hibernate)

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