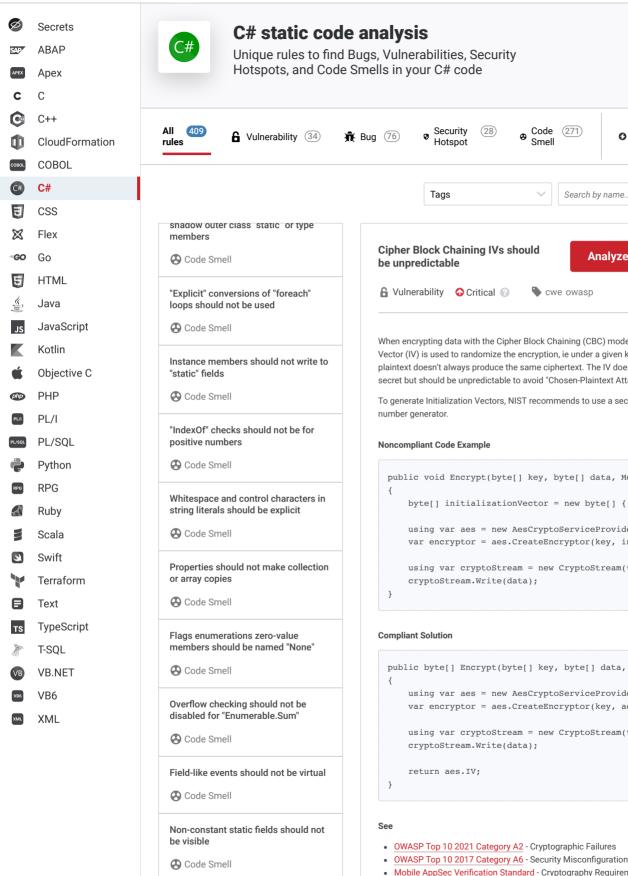
Quick 52 Fix





Inappropriate casts should not be

Constructors should only call non-

Available In:

Code Smell

Code Smell

overridable methods

Analyze your code cwe owasp When encrypting data with the Cipher Block Chaining (CBC) mode an Initialization Vector (IV) is used to randomize the encryption, ie under a given key the same plaintext doesn't always produce the same ciphertext. The IV doesn't need to be secret but should be unpredictable to avoid "Chosen-Plaintext Attack". To generate Initialization Vectors, NIST recommends to use a secure random public void Encrypt(byte[] key, byte[] data, MemoryStream ta byte[] initializationVector = new byte[] { 1, 2, 3, 4, 5 using var aes = new AesCryptoServiceProvider(); var encryptor = aes.CreateEncryptor(key, initializationV using var cryptoStream = new CryptoStream(target, encryp public byte[] Encrypt(byte[] key, byte[] data, MemoryStream using var aes = new AesCryptoServiceProvider(); var encryptor = aes.CreateEncryptor(key, aes.IV); // aes using var cryptoStream = new CryptoStream(target, encryp • OWASP Top 10 2021 Category A2 - Cryptographic Failures OWASP Top 10 2017 Category A6 - Security Misconfiguration Mobile AppSec Verification Standard - Cryptography Requirements OWASP Mobile Top 10 2016 Category M5 - Insufficient Cryptography • MITRE, CWE-329 - Not Using an Unpredictable IV with CBC Mode MITRE, CWE-330 - Use of Insufficiently Random Values • MITRE, CWE-340 - Generation of Predictable Numbers or Identifiers MITRE, CWE-1204 - Generation of Weak Initialization Vector (IV) • NIST, SP-800-38A - Recommendation for Block Cipher Modes of Operation

"GC.Collect" should not be called

② Code Smell

Methods should not be empty
③ Code Smell

Exceptions should not be thrown in finally blocks
③ Code Smell

Method overrides should not change parameter defaults
③ Code Smell

sonarlint ⊖ | 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