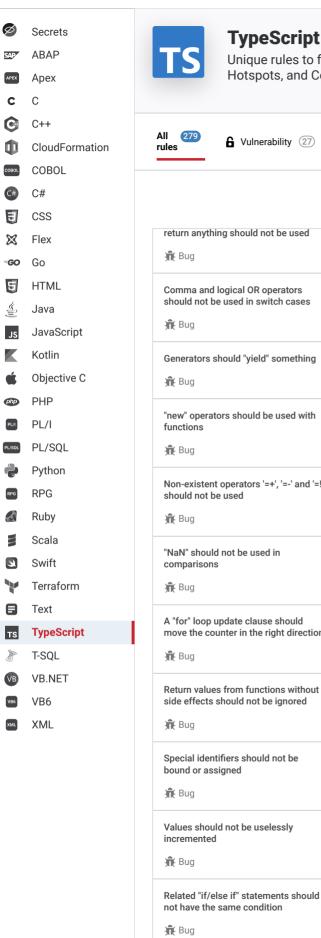
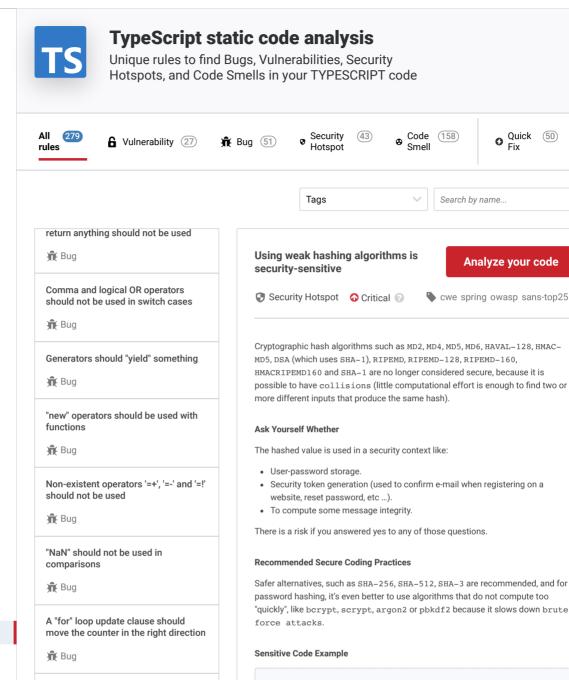


Products >

O Quick 50 Fix

Q





```
const crypto = require("crypto");
const hash = crypto.createHash('shal'); // Sensitive
```

Compliant Solution

```
const crypto = require("crypto");
const hash = crypto.createHash('sha512'); // Compliant
```

See

- OWASP Top 10 2021 Category A2 Cryptographic Failures
- OWASP Top 10 2017 Category A3 Sensitive Data Exposure
- 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-1240 Use of a Risky Cryptographic Primitive
- SANS Top 25 Porous Defenses

Available In:

sonarcloud 🔂 | sonarqube

Objects should not be created to be dropped immediately without being

Bug

Identical expressions should not be used on both sides of a binary operator

\$\hat{\pi}\$ Bug

All code should be reachable

\$\hat{\pi}\$ Bug

Loops with at most one iteration should be refactored

\$\hat{\pi}\$ Bug

Variables should not be self-assigned

\$\hat{\pi}\$ Bug

© 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