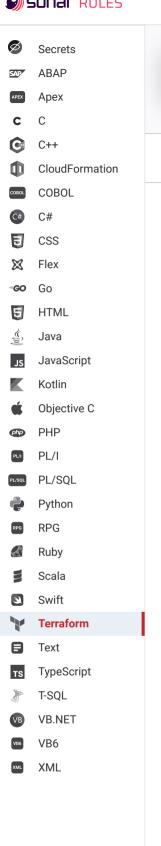
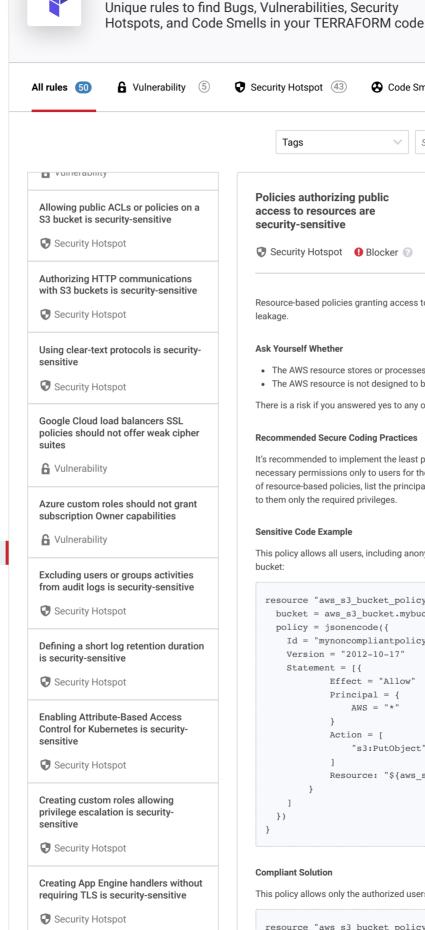
Terraform static code analysis

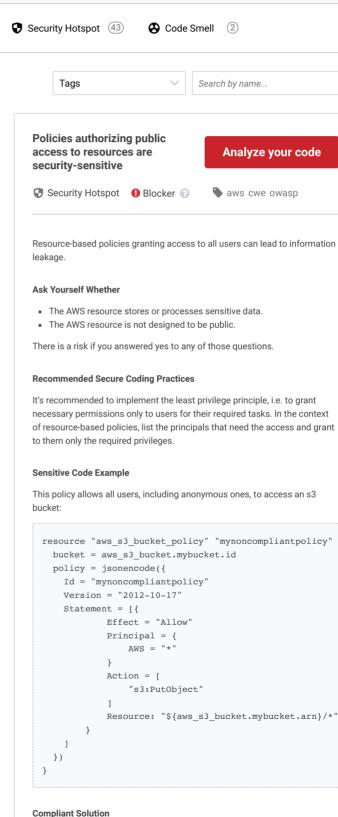


Products ∨





Excessive granting of GCP IAM



This policy allows only the authorized users:

bucket = aws_s3_bucket.mybucket.id

resource "aws_s3_bucket_policy" "mycompliantpolicy" {

permissions is security-sensitive

Security Hotspot

Enabling project-wide SSH keys to access VM instances is securitysensitive

Security Hotspot

Granting public access to GCP resources is security-sensitive

Security Hotspot

Creating GCP SQL instances without requiring TLS is security-sensitive

Security Hotspot

Creating DNS zones without DNSSEC enabled is security-sensitive

See

- OWASP Top 10 2021 Category A1 Broken Access Control
- AWS Documentation Grant least privilege
- MITRE, CWE-732 Incorrect Permission Assignment for Critical Resource
- MITRE, CWE-284 Improper Access Control
- OWASP Top 10 2017 Category A5 Broken Access Control

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