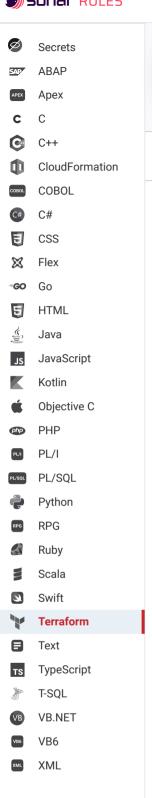
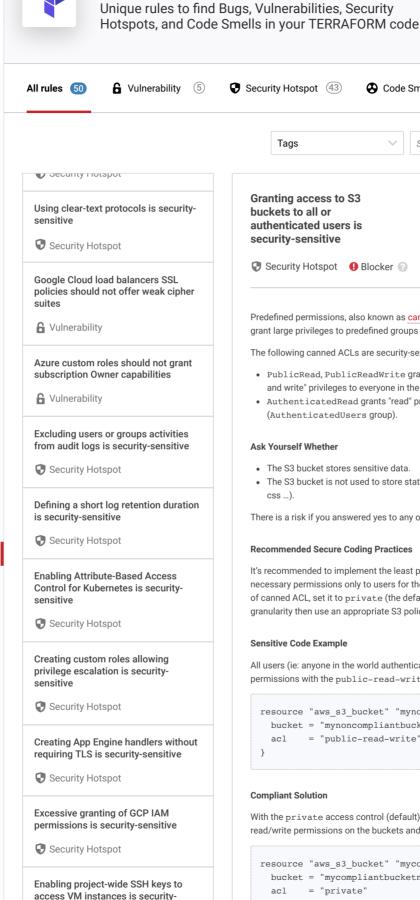
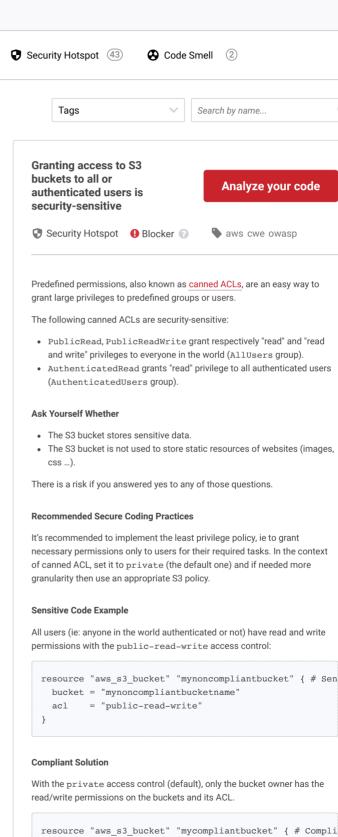
Terraform static code analysis



Products ∨







bucket = "mycompliantbucketname"

= "private"

acl

See

sensitive

Security Hotspot

Terraform static code analysis: Granting access to S3 buckets to all or authenticated users is security-sensitive

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 Security Hotspot Creating keys without a rotation period is security-sensitive Security Hotspot Granting highly privileged GCP

resource rights is security-sensitive

- OWASP Top 10 2021 Category A1 Broken Access Control
- AWS Documentation Access control list (ACL) overview (canned ACLs)
- AWS Documentation Controlling access to a bucket with user policies
- 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 放 | 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