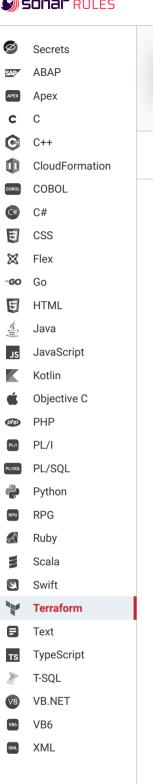
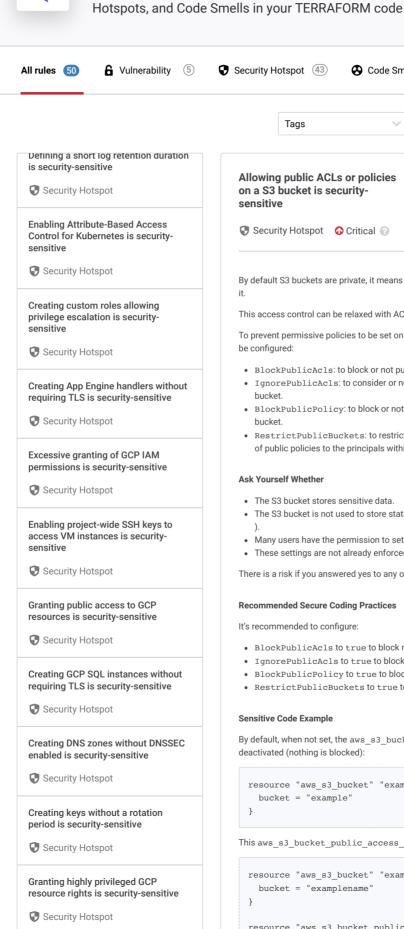
Terraform static code analysis

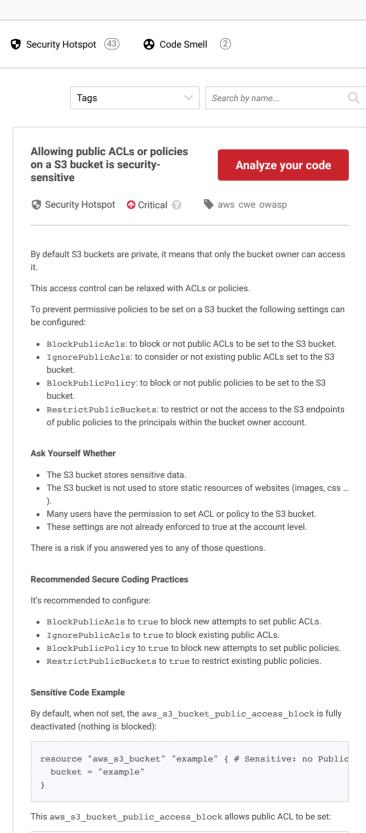
Unique rules to find Bugs, Vulnerabilities, Security



Products >







resource "aws s3 bucket" "example" { # Sensitive

resource "aws_s3_bucket_public_access_block" "example-publi

bucket = "examplename"

Using unencrypted cloud storages is security-sensitive

Security Hotspot

Azure role assignments that grant access to all resources of a subscription are security-sensitive

Security Hotspot

Disabling Role-Based Access Control on Azure resources is securitysensitive

Security Hotspot

Disabling certificate-based authentication is security-sensitive

Coourity Hotopot

```
bucket = aws_s3_bucket.example.id
block_public_acls
                      = false # should be true
                   = true
block public policy
ignore public acls
restrict_public_buckets = true
```

Compliant Solution

This aws_s3_bucket_public_access_block blocks public ACLs and policies, ignores existing public ACLs and restricts existing public policies:

```
resource "aws_s3_bucket" "example" {
  bucket = "example"
resource "aws_s3_bucket_public_access_block" "example-publi
  bucket = aws_s3_bucket.example.id
  block_public_acls
                            = true
  block_public_policy = true
ignore_public_acls = true
  restrict_public_buckets = true
}
```

See

- OWASP Top 10 2021 Category A1 Broken Access Control
- OWASP Top 10 2021 Category A5 Security Misconfiguration
- AWS Documentation Blocking public access to your Amazon S3 storage
- 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