sonar RULES

Products

- Secrets
- ABAP
- Apex
- C
- C++
- CloudFormation
- COBOL
- C#
- CSS
- Flex
- Go
- HTML
- Java
- JavaScript
- Kotlin
- Objective C
- PHP
- PL/I
- PL/SQL
- Python
- RPG
- Ruby
- Scala
- Swift
- Terraform
- Text
- TypeScript
- T-SQL
- VB.NET
- VB6
- XML

Terraform static code analysis

Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your TERRAFORM code

All rules 50 Vulnerability 5 Security Hotspot 43 Code Smell 2

Tags

Search by name...

Security Hotspot

Using unencrypted EFS file systems is security-sensitive

Security Hotspot

Using unencrypted SQS queues is security-sensitive

Security Hotspot

Using unencrypted SNS topics is security-sensitive

Security Hotspot

Using unencrypted SageMaker notebook instances is security-sensitive

Security Hotspot

Using unencrypted Elasticsearch domains is security-sensitive

Security Hotspot

Using unencrypted RDS databases is security-sensitive

Security Hotspot

Using unencrypted EBS volumes is security-sensitive

Security Hotspot

Disabling logging is security-sensitive

Security Hotspot

Administration services access should be restricted to specific IP addresses

Vulnerability

Unversioned Google Cloud Storage buckets are security-sensitive

Security Hotspot

Disabling S3 bucket MFA delete is security-sensitive

Terraform parsing failure

Analyze your code

Code Smell Major suspicious

When the HCL-Terraform parser fails, it is possible to record the failure as a violation on the file. This way, not only it is possible to track the number of files that do not parse but also to easily find out why they do not parse.

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

Security Hotspot

Disabling versioning of S3 buckets is security-sensitive

Security Hotspot

Disabling server-side encryption of S3 buckets is security-sensitive

Security Hotspot

AWS tag keys should comply with a naming convention

Code Smell

Terraform parsing failure

Code Smell