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...

Creating public APIs is security-sensitive
Security Hotspot

Allowing public network access to cloud resources is security-sensitive
Security Hotspot

Having AWS policies that grant access to all resources of an account is security-sensitive
Security Hotspot

Having policies that grant all privileges is security-sensitive
Security Hotspot

Policies authorizing public access to resources are security-sensitive
Security Hotspot

Granting access to S3 buckets to all or authenticated users is security-sensitive
Security Hotspot

AWS IAM policies should not allow privilege escalation
Vulnerability

Weak SSL/TLS protocols should not be used
Vulnerability

Allowing public ACLs or policies on a S3 bucket is security-sensitive
Security Hotspot

Authorizing HTTP communications with S3 buckets is security-sensitive
Security Hotspot

Using clear-text protocols is security-sensitive

Creating public APIs is security-sensitive

Analyze your code

Security Hotspot Blocker aws cwe owasp

A public API, which can be requested by any authenticated or unauthenticated identities, can lead to unauthorized actions and information disclosures.

Ask Yourself Whether

The public API:

- exposes sensitive data like personal information.
- can be used to perform sensitive operations.

There is a risk if you answered yes to any of those questions.

Recommended Secure Coding Practices

It's recommended to restrict API access to authorized entities, unless the API offers a non-sensitive service designed to be public.

Noncompliant Code Example

A public API that doesn't have access control implemented:

```
resource "aws_api_gateway_method" "noncompliantapi" {
  authorization = "NONE" # Sensitive
  http_method   = "GET"
}
```

Compliant Solution

An API that implements AWS IAM permissions:

```
resource "aws_api_gateway_method" "compliantapi" {
  authorization = "AWS_IAM"
  http_method   = "GET"
}
```

See

- OWASP Top 10 2021 Category A1 - Broken Access Control
- AWS Documentation - Controlling and managing access to a REST API in API Gateway
- MITRE, CWE-284 - Improper Access Control
- OWASP Top 10 2017 Category A5 - Broken Access Control

Available In:

sonarcloud sonarqube

Security Hotspot

Google Cloud load balancers SSL policies should not offer weak cipher suites

Vulnerability

Azure custom roles should not grant subscription Owner capabilities

Vulnerability

Excluding users or groups activities from audit logs is security-sensitive

Security Hotspot

Defining a short log retention duration is security-sensitive

Security Hotspot