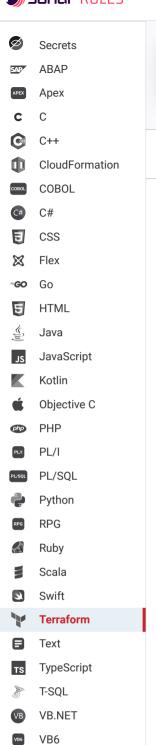
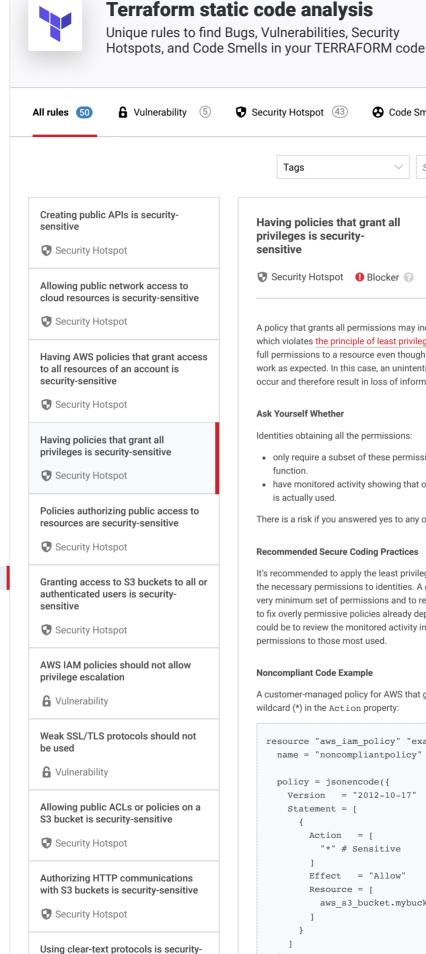
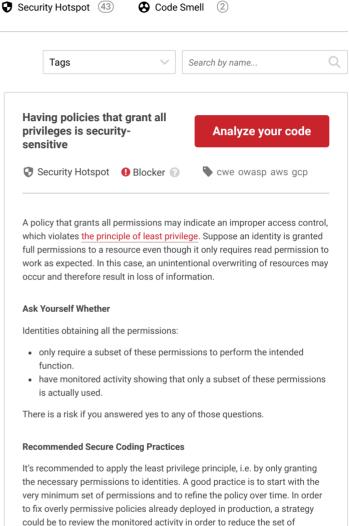


Products >



XML





permissions to those most used.

A customer-managed policy for AWS that grants all permissions by using the wildcard (*) in the Action property:

```
resource "aws_iam_policy" "example" {
 name = "noncompliantpolicy"
 policy = jsonencode({
   Version = "2012-10-17"
   Statement = [
       Action = [
          "*" # Sensitive
        1
       Effect = "Allow"
       Resource = [
         aws_s3_bucket.mybucket.arn
 })
```

sensitive

Security Hotspot

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

6 Vulnerability

Azure custom roles should not grant subscription Owner capabilities

6 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

A customer-managed policy for GCP that grants all permissions by using the actions admin role role property:

```
resource "google_project_iam_binding" "example" {
  project = "example"
  role = "roles/owner" # Sensitive

members = [
    "user:jane@example.com",
  ]
}
```

Compliant Solution

A customer-managed policy for AWS that grants only the required permissions:

A customer-managed policy for GCP that grants restricted permissions by using the actions admin role role property:

```
resource "google_project_iam_binding" "example" {
  project = "example"
  role = "roles/actions.Viewer"

  members = [
    "user:jane@example.com",
  ]
}
```

See

- OWASP Top 10 2021 Category A1 Broken Access Control
- AWS Documentation Grant least privilege
- Google Cloud Documentation Understanding roles
- 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