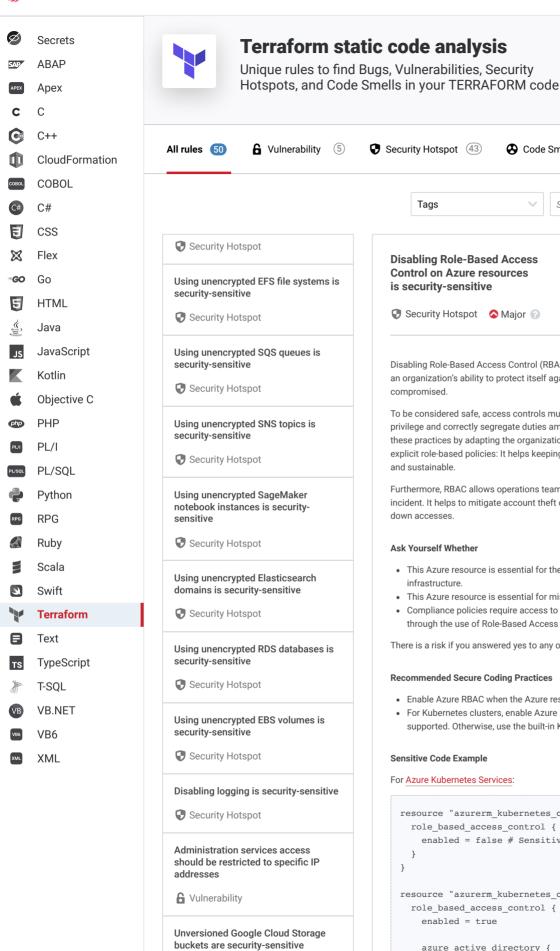
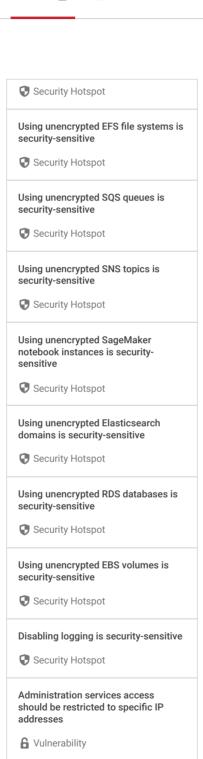
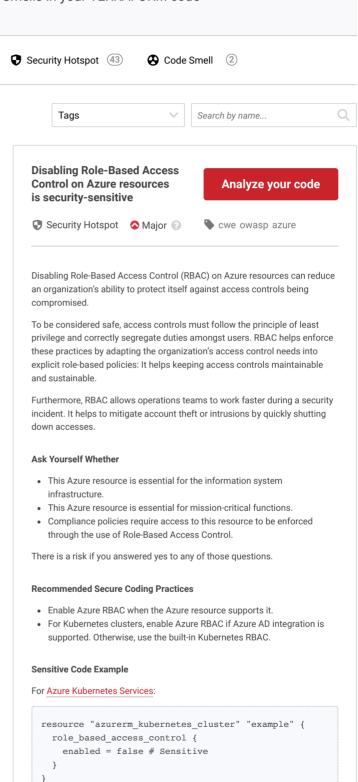


Products ∨







resource "azurerm_kubernetes_cluster" "example2" {

azure_rbac_enabled = false # Sensitive

role based access control {

azure_active_directory { managed = true

enabled = true

Security Hotspot

security-sensitive

Disabling S3 bucket MFA delete is

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

For Key Vaults:

```
resource "azurerm_key_vault" "example" {
  enable_rbac_authorization = false # Sensitive
```

Compliant Solution

For Azure Kubernetes Services:

```
resource "azurerm_kubernetes_cluster" "example" {
  role_based_access_control {
   enabled = true
}
resource "azurerm_kubernetes_cluster" "example" {
 role based access control {
   enabled = true
   azure_active_directory {
     managed = true
     azure rbac enabled = true
 }
}
```

For Key Vaults:

```
resource "azurerm_key_vault" "example" {
  enable rbac authorization = true
```

- OWASP Top 10 2021 Category A1 Boken Access Control
- OWASP Top 10 2017 Category A5 Broken Access Control
- MITRE, CWE-668 Exposure of Resource to Wrong Sphere

Available In:

sonarcloud <equation-block> 🗆 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