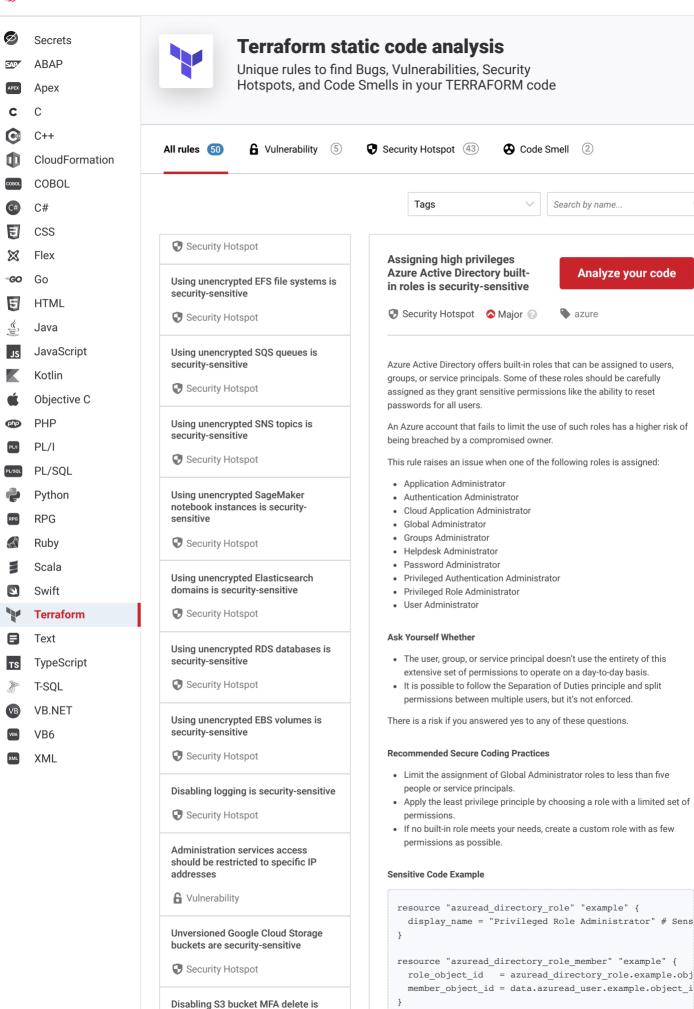


Products ∨



security-sensitive

Terraform static code analysis: Assigning high privileges Azure Active Directory built-in roles is security-sensitive

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

Compliant Solution

```
resource "azuread_directory_role" "example" {
 display_name = "Usage Summary Reports Reader"
resource "azuread_directory_role_member" "example" {
  role_object_id = azuread_directory_role.example.obj
 member_object_id = data.azuread_user.example.object_i
```

See

- OWASP Top 10 2021 Category A1 Broken Access Control
- OWASP Top 10 2021 Category A4 Insecure Design
- OWASP Top 10 2017 Category A5 Broken Access Control
- MITRE, CWE-266 Incorrect Privilege Assignment
- Azure AD Documentation Azure AD built-in roles
- Azure AD Documentation Best practices for Azure AD roles

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