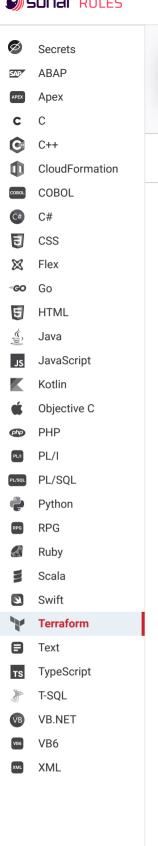
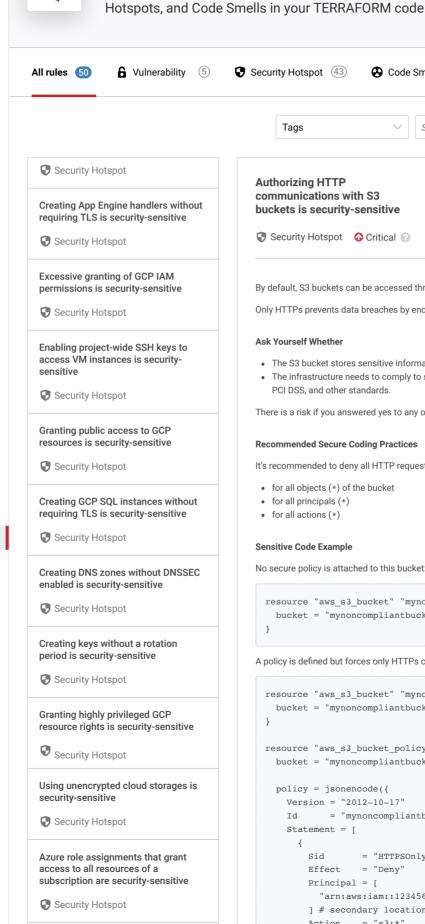
Terraform static code analysis

Unique rules to find Bugs, Vulnerabilities, Security

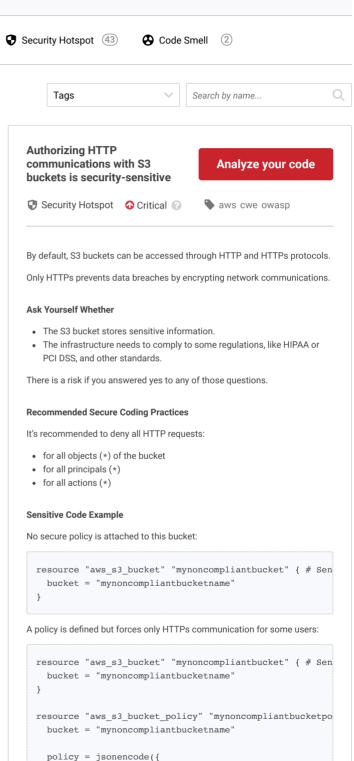


Products ∨





Disabling Role-Based Access Control



Version = "2012-10-17"

Statement = [

Effect

Principal = [

{

= "mynoncompliantbucketpolicy"

= "HTTPSOnly"

"arn:aws:iam::123456789123:root"

] # secondary location: only one principal is f

= "Deny"

on Azure resources is securitysensitive

Security Hotspot

Disabling certificate-based authentication is security-sensitive

Security Hotspot

Assigning high privileges Azure Resource Manager built-in roles is security-sensitive

Security Hotspot

Authorizing anonymous access to Azure resources is security-sensitive

Security Hotspot

Enabling Azure resource-specific

```
Resource = [
    aws_s3_bucket.mynoncompliantbucketpolicy.arn,
    "${aws_s3_bucket.mynoncompliantbucketpolicy.a}

]
    Condition = {
     Bool = {
        "aws:SecureTransport" = "false"
     }
    }
},
```

Compliant Solution

A secure policy that denies all HTTP requests is used:

```
resource "aws_s3_bucket" "mycompliantbucket" {
 bucket = "mycompliantbucketname"
}
resource "aws_s3_bucket_policy" "mycompliantpolicy" {
 bucket = "mycompliantbucketname"
  policy = jsonencode({
    Version = "2012-10-17"
    Id = "mycompliantpolicy"
    Statement = [
      {
                 = "HTTPSOnly"
       Sid
        Effect
                 = "Deny"
       Principal = "*"
       Action = "s3:*"
        Resource = [
          aws s3 bucket.mycompliantbucket.arn,
          "${aws s3 bucket.mycompliantbucket.arn}/*",
        Condition = {
          Bool = {
            "aws:SecureTransport" = "false"
     },
   ]
 })
}
```

See

- OWASP Top 10 2021 Category A2 Cryptographic Failures
- OWASP Top 10 2021 Category A5 Security Misconfiguration
- AWS documentation Enforce encryption of data in transit
- MITRE, CWE-319 Cleartext Transmission of Sensitive Information
- OWASP Top 10 2017 Category A3 Sensitive Data Exposure
- OWASP Top 10 2017 Category A6 Security Misconfiguration

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