




 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... 

 Security Hotspot


Creating App Engine handlers without requiring TLS is security-sensitive

 Security Hotspot


Excessive granting of GCP IAM permissions is security-sensitive

 Security Hotspot


Enabling project-wide SSH keys to access VM instances is security-sensitive

 Security Hotspot


Granting public access to GCP resources is security-sensitive

 Security Hotspot


Creating GCP SQL instances without requiring TLS is security-sensitive

 Security Hotspot


Creating DNS zones without DNSSEC enabled is security-sensitive

 Security Hotspot


Creating keys without a rotation period is security-sensitive

 Security Hotspot


Granting highly privileged GCP resource rights is security-sensitive

 Security Hotspot

Using unencrypted cloud storages is security-sensitive

 Security Hotspot


Azure role assignments that grant access to all resources of a subscription are security-sensitive


 Security Hotspot


Disabling Role-Based Access Control

Authorizing HTTP communications with S3 buckets is security-sensitive

Analyze your code

 Security Hotspot

 Critical

 aws cwe owasp

By default, S3 buckets can be accessed through HTTP and HTTPs protocols.

Only HTTPs prevents data breaches by encrypting network communications.

Ask Yourself Whether

- The S3 bucket stores sensitive information.
- The infrastructure needs to comply to some regulations, like HIPAA or PCI DSS, and other standards.

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

Recommended Secure Coding Practices

It's recommended to deny all HTTP requests:

- for all objects (*) of the bucket
- for all principals (*)
- for all actions (*)

Sensitive Code Example

No secure policy is attached to this bucket:

```
resource "aws_s3_bucket" "mynoncompliantbucket" { # Sensitive Code Example
  bucket = "mynoncompliantbucketname"
}
```

A policy is defined but forces only HTTPs communication for some users:





```
resource "aws_s3_bucket" "mynoncompliantbucket" { # Sensitive Code Example
  bucket = "mynoncompliantbucketname"
}

resource "aws_s3_bucket_policy" "mynoncompliantbucketpolicy" {
  bucket = "mynoncompliantbucketname"

  policy = jsonencode({
    Version = "2012-10-17"
    Id      = "mynoncompliantbucketpolicy"
    Statement = [
      {
        Sid      = "HTTPOnly"
        Effect   = "Deny"
        Principal = [
          "arn:aws:iam::123456789123:root"
        ] # secondary location: only one principal is f
        Action   = "s3:*"
      }
    ]
  })
}
```

https://rules.sonarsource.com/terraform/RSPEC-6249

1/2

Disabling certificate-based authentication on Azure resources is security-sensitive
 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 = [
      {
        Sid      = "HTTPSOnly"
        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:

