




 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


Using unencrypted EFS file systems is security-sensitive

 Security Hotspot


 Security Hotspot


Using unencrypted SQS queues is security-sensitive

 Security Hotspot


 Security Hotspot


Using unencrypted SNS topics is security-sensitive

 Security Hotspot


 Security Hotspot


Using unencrypted SageMaker notebook instances is security-sensitive

 Security Hotspot


 Security Hotspot

Using unencrypted Elasticsearch domains is security-sensitive

 Security Hotspot

 Security Hotspot

Using unencrypted RDS databases is security-sensitive

 Security Hotspot

 Security Hotspot

Using unencrypted EBS volumes is security-sensitive

 Security Hotspot

 Security Hotspot

Disabling logging is security-sensitive

 Security Hotspot

 Vulnerability

Administration services access should be restricted to specific IP addresses




 Security Hotspot

Unversioned Google Cloud Storage buckets are security-sensitive

 Security Hotspot

Disabling S3 bucket MFA delete is security-sensitive

### Creating GCP SQL instances without requiring TLS is security-sensitive

 Security Hotspot  Major  gcp

By default, GCP SQL instances offer encryption in transit, with support for TLS, but insecure connections are still accepted. On an unsecured network, such as a public network, the risk of traffic being intercepted is high. When the data isn't encrypted, an attacker can intercept it and read confidential information.

When creating a GCP SQL instance, a public IP address is automatically assigned to it and connections to the SQL instance from public networks can be authorized.

TLS is automatically used when connecting to SQL instances through:

- The [Cloud SQL Auth proxy](#).
- The [Java Socket Library](#).
- The built-in mechanisms in the [App Engine](#) environments.

#### Ask Yourself Whether

Connections are not already automatically encrypted by GCP (eg: SQL Auth proxy) and

- Connections to the SQL instance are performed on untrusted networks.
- The data stored in the SQL instance is confidential.

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

#### Recommended Secure Coding Practices






It's recommended to encrypt all connections to the SQL instance, whether using public or private IP addresses. However, since private networks can be considered trusted, requiring TLS in this situation is usually a lower priority task.

#### Sensitive Code Example

```
resource "google_sql_database_instance" "example" { # S
  name           = "noncompliant-master-instance"
  database_version = "POSTGRES_11"
  region         = "us-central1"

  settings {
    tier = "db-f1-micro"
  }
}
```

#### Compliant Solution

 Security Hotspot
<b>Disabling versioning of S3 buckets is security-sensitive</b>  Security Hotspot
<b>Disabling server-side encryption of S3 buckets is security-sensitive</b>  Security Hotspot
<b>AWS tag keys should comply with a naming convention</b>  Code Smell
<b>Terraform parsing failure</b>  Code Smell

```
resource "google_sql_database_instance" "example" {
  name           = "compliant-master-instance"
  database_version = "POSTGRES_11"
  region         = "us-central1"

  settings {
    tier = "db-f1-micro"
    ip_configuration {
      require_ssl = true
      ipv4_enabled = true
    }
  }
}
```

See

- [OWASP Top 10 2021 Category A2](#) - Cryptographic Failures
- [OWASP Top 10 2017 Category A6](#) - Security Misconfiguration
- [MITRE, CWE-311](#) - Missing Encryption of Sensitive Data
- [MITRE, CWE-319](#) - Cleartext Transmission of Sensitive Information
- [GCP Documentation](#) - Cloud SQL: Authorizing with SSL/TLS certificates

Available In:

