

































-  **Secrets**
-  ABAP
-  Apex
-  C
-  C++
-  CloudFormation
-  COBOL
-  C#
-  CSS
-  Flex
-  Go
-  HTML
-  Java
-  JavaScript
-  Kotlin
-  Kubernetes
-  Objective C
-  PHP
-  PL/I
-  PL/SQL
-  Python
-  RPG
-  Ruby
-  Scala
-  Swift
-  Terraform
-  Text
-  TypeScript
-  T-SQL
-  VB.NET
-  VB6
-  XML



## Secrets static code analysis

Unique rules to find Vulnerabilities in your source code and language agnostic config files

All rules 7 Vulnerability 7

Amazon Web Services credentials should not be disclosed
Vulnerability
Amazon MWS credentials should not be disclosed
Vulnerability
Google API keys should not be disclosed
Vulnerability
Google Cloud service accounts keys should not be disclosed
Vulnerability
Alibaba Cloud AccessKeys should not be disclosed
Vulnerability
IBM API keys should not be disclosed
Vulnerability
Azure Storage Account Keys should not be disclosed
Vulnerability

Tags ▾

Search by name... 🔍

### Google API keys should not be disclosed

Analyze your code

Vulnerability Blocker SonarSource default severity click to learn more cwe sans-top25-porous owasp-a3

Google API keys are used to authenticate applications that consume Google Cloud APIs. They are especially useful for accessing public data anonymously (like Google Maps), and are used to associate API requests with your project for quota and billing.

API keys are not strictly secret as they are often embedded into client side code or mobile applications that consume Google Cloud APIs. Still,they should be secured and should never be treated as public information.

An unrestricted Google API key being disclosed in a public source code would be used by malicious actors to consume Google APIs on the behalf ofyour application. This will have a financial impact as your organisation will be billed for the data consumed by the malicious actor. If your accounthas enabled quota to cap the API consumption of your application, this quota can be exceeded, leaving your application unable to request the GoogleAPIs it requires to function properly.

#### Recommended Secure Coding Practices

Only administrators should have access to the Google API keys used by your application.

As a consequence, Google API keys should not be stored along with the application code as they could be disclosed to a large audience or could bemade public.

Google API keys should be stored outside of the code in a file that is never committed to your application code repository.

If possible, a better alternative is to use your cloud provider’s service for managing secrets. On Google Cloud this service is called Secret Manager.

When credentials are disclosed in the application code, consider them as compromised and revoke them immediately.

In addition to secure storage, it’s important to apply restrictions to API keys in order to mitigate the impacts whenthey are discovered by malicious actors.

#### See

- [Google Cloud](#) - Using API keys
- [OWASP Top 10 2017 Category A3](#) - Sensitive Data Exposure
- [MITRE, CWE-798](#) - Use of Hard-coded Credentials
- [MITRE, CWE-259](#) - Use of Hard-coded Password
- [CERT, MSC03-J.](#) - Never hard code sensitive information
- [SANS Top 25](#) - Porous Defenses

Available In:

sonarlint