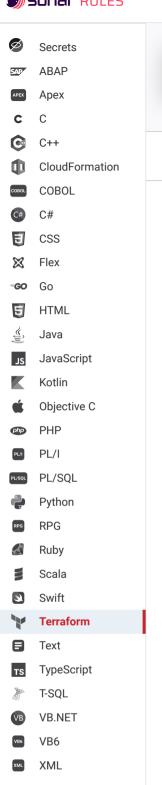
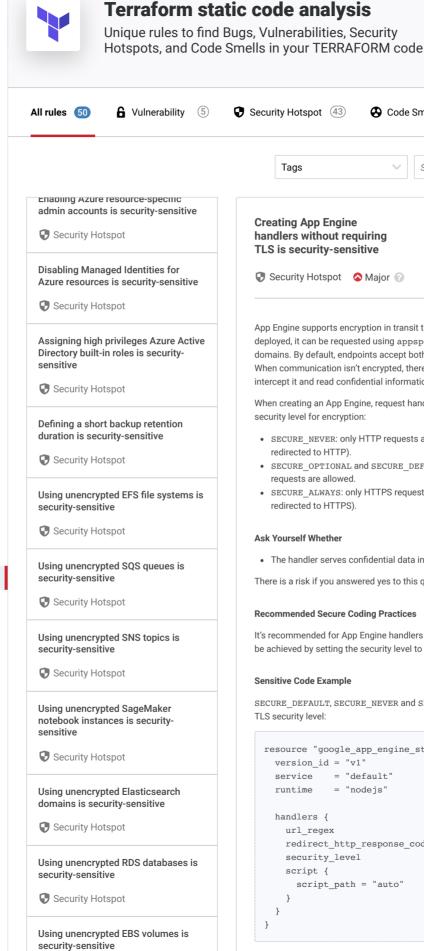
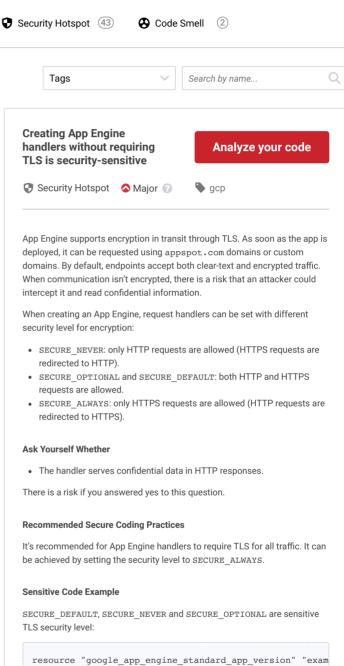


Products >







Compliant Solution

} }

version_id = "v1"

= "default"

= "nodejs"

security_level

script_path = "auto"

= ".*"

= "SECURE_OPTIONAL" # S

redirect_http_response_code = "REDIRECT_HTTP_RESPON

service

runtime

handlers {

url regex

script {

Security Hotspot

Disabling logging is security-sensitive

Security Hotspot

Administration services access

Administration services access should be restricted to specific IP addresses

읍 Vulnerability

Unversioned Google Cloud Storage buckets are security-sensitive

Security Hotspot

Disabling S3 bucket MFA delete is security-sensitive

Security Hotspot

Disabling versioning of S3 buckets is

Force the use of TLS for the handler by setting the security level on SECURE_ALWAYS:

```
resource "google_app_engine_standard_app_version" "exam
  version_id = "v1"
  service = "default"
  runtime = "nodejs"

  handlers {
    url_regex = ".*"
    redirect_http_response_code = "REDIRECT_HTTP_RESPON
    security_level = "SECURE_ALWAYS"
    script {
        script_path = "auto"
      }
   }
}
```

See

- OWASP Top 10 2021 Category A2 Cryptographic Failures
- OWASP Top 10 2017 Category A3 Sensitive Data Exposure
- OWASP Top 10 2017 Category A6 Security Misconfiguration
- <u>MITRE, CWE-200</u> Exposure of Sensitive Information to an Unauthorized Actor
- MITRE, CWE-319 Cleartext Transmission of Sensitive Information
- GCP Documentation Overview of App Security

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