


-  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




C++ static code analysis


Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your C++ code


All rules 578

 Vulnerability 13

 Bug 111

 Security Hotspot 18

 Code Smell 436

 Quick Fix 68

Tags

Search by name...

"memset" should not be used to delete sensitive data

 Vulnerability

POSIX functions should not be called with arguments that trigger buffer overflows

 Vulnerability

XML parsers should not be vulnerable to XXE attacks

 Vulnerability

Function-like macros should not be invoked without all of their arguments

 Bug

The address of an automatic object should not be assigned to another object that may persist after the first object has ceased to exist

 Bug

Assigning to an optional should directly target the optional

 Bug

Result of the standard remove algorithms should not be ignored

 Bug

"std::scoped_lock" should be created with constructor arguments

 Bug

Objects should not be sliced

 Bug

Immediately dangling references should not be created

 Bug

"pthread_mutex_t" should be unlocked in the reverse order they were locked

 Bug

"pthread_mutex_t" should be properly initialized and destroyed

 Bug

"pthread_mutex_t" should not be consecutively locked or unlocked twice

Standard outputs should not be used directly to log anything

Analyze your code

 Code Smell  Major  bad-practice cert owasp

When logging a message there are several important requirements which must be fulfilled:

- The user must be able to easily retrieve the logs
- The format of all logged message must be uniform to allow the user to easily read the log
- Logged data must actually be recorded
- Sensitive data must only be logged securely

If a program directly writes to the standard outputs, there is absolutely no way to comply with those requirements. That's why defining and using a dedicated logger is highly recommended.

Noncompliant Code Example

```
std::cout << "My Message"; // Noncompliant
std::cerr << "My Message"; // Noncompliant
printf("My Message"); // Noncompliant
```

Compliant Solution

```
Log().Get(logINFO) << "My Message";
```

See

- [OWASP Top 10 2021 Category A9](#) - Security Logging and Monitoring Failures
- [OWASP Top 10 2017 Category A3](#) - Sensitive Data Exposure

Available In:

sonarlint

| sonarcloud

| sonarqube

Developer Edition

 Bug
<p>"std::move" and "std::forward" should not be confused</p>  Bug
<p>A call to "wait()" on a "std::condition_variable" should have a condition</p>  Bug
<p>A pointer to a virtual base class shall only be cast to a pointer to a derived class by means of dynamic_cast</p>  Bug
<p>Functions with "noreturn" attribute should not return</p>  Bug
<p>RAII objects should not be temporary</p>  Bug
<p>"memcmp" should only be called with pointers to trivially copyable types with no padding</p>  Bug
<p>"memcpy", "memmove", and "memset" should only be called with pointers to trivially copyable types</p>  Bug
<p>"std::auto_ptr" should not be used</p>  Bug
<p>Destructors should be "noexcept"</p>  Bug