The PowerPoint of Clean Code

April 7th, 2022

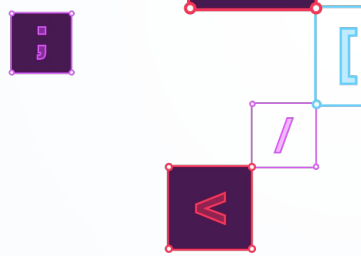
Olivier Gaudin
CEO - SonarSource

Geoffray Adde
PM - SonarSource

sonar

SonarSource

- 300 employees
- Geneva (HQ), Annecy (FR), Bochum (DE), Austin (TX)
- Clean Code for 29 languages
- 350K companies use the solution
- Strong commitment to OSS



The Power of Clean Code

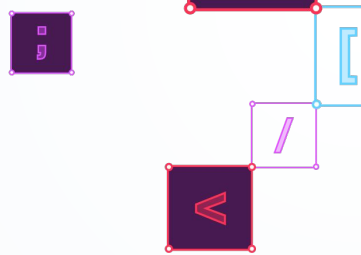
- Source Code is the software asset
- Reduce maintenance and rework
- Better work environment
- Reduce operational and security risks

⇒ do a better job!

sonar

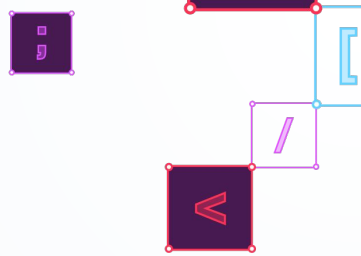
Challenges

- Too late
- Pushback from developers
- Lack of ownership by developers
- Inconsistent requirements
- Quality gate



sonar

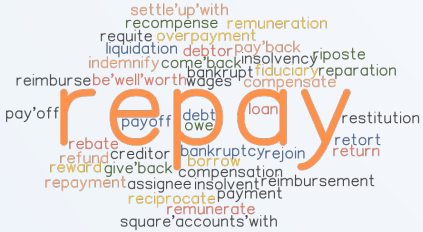
Clean as you Code



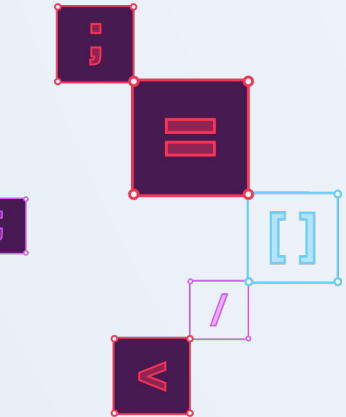
sonar

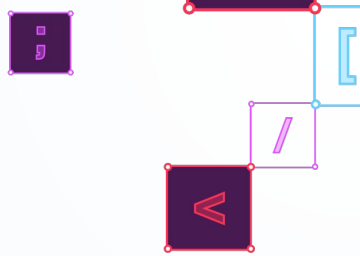
Clean as you Code

- Strict quality gate to promote code
- Based on added and changed code



Demo





sonar

Capture by reference in lambdas used locally

Noncompliant Code Example

```
using Vec = vector<int>;

Vec applyPermutation(const Vec& v, const Vec& permutation) {
    assert(v.size() == permutation.size());

    const auto n = v.size();
    Vec result(n);

    // Noncompliant: this will copy the entire v vector for each iteration, resulting in n^2 operat
    transform(permutation.begin(), permutation.end(), back_inserter(result),
      [v](int position){ return v[position]; });

     return result;
}
```

Can lead to slow downs and increased memory footprint, QuickFixable

Capture by reference in lambdas used locally

Compliant Solution

```
using Vec = vector<int>;

Vec applyPermutation(const Vec& v, const Vec& permutation) {
    assert(v.size() == permutation.size());

    const auto n = v.size();
    Vec result(n);

    // Compliant: this will NOT copy the entire v vector for each iteration, resulting in n operati
    transform(permutation.begin(), permutation.end(), back_inserter(result),
      [&v](int position){ return v[position]; });

     return result;
}
```

Cipher algorithms should be robust

Noncompliant Code Example

OpenSSL

```
#include <openssl/evp.h>

EVP_bf_cbc(); // Noncompliant: 64-bit size block
EVP_cast5_cbc(); // Noncompliant: 64-bit size block
EVP_des_cbc(); // Noncompliant: DES works with 56-bit keys allow attacks via exhaustive search
EVP_idea_cbc(); // Noncompliant: 64-bit size block
EVP_rc4(); // Noncompliant:  has numerous design flaws which make it hard to use correctly
EVP_rc2_cbc(); // Noncompliant: RC2 is vulnerable to a related-key attack
```

Potentially severe security breach. Can put business and reputation at risk.

sonar

Cipher algorithms should be robust

Compliant Solution

OpenSSL

```
#include <openssl/evp.h>

EVP_aes_128_gcm() // Compliant: AES is a good default choice for symmetric encryption
```

Supports *OpenSSL*, *Botan*, *Crypto++*

sonar

"memset" should not be used to delete sensitive data

Noncompliant Code Example

```
void f(char *password, size_t bufferSize) {
  char localToken[256];
  init(localToken, password);
  memset(password, ' ', strlen(password)); // Noncompliant, password is about to be freed
  memset(localToken, ' ', strlen(localBuffer)); // Noncompliant, localToken is about to go out of s
  free(password);
}
```

Misleading. Code seems to address security. Can be missed in review.

sonar

"memset" should not be used to delete sensitive data

Compliant Solution

```
void f(char *password, size_t bufferSize) {
  char localToken[256];
  init(localToken, password);
  memset_s(password, bufferSize, ' ', strlen(password));
  memset_s(localToken, sizeof(localToken), ' ', strlen(localBuffer));
  free(password);
}
```

Arguments evaluation order should not be relied on

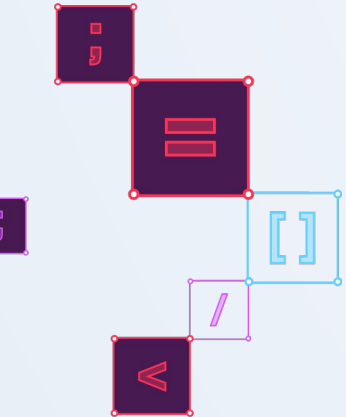
Noncompliant Code Example

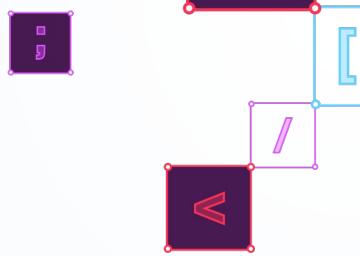
```
void f(int i, int j);

void g() {
  int i = 0;
  f(++i, ++i); // Noncompliant, the call could either be f(1,2) or f(2,1) (since C++17) or undefine
}
```

Standard dependent. Can slip through unit tests.

sonar

Demo

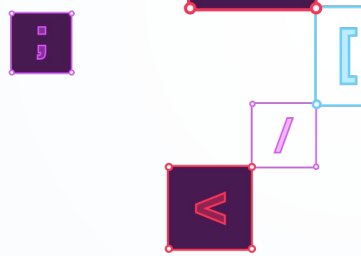




sonar

A glimpse of C++

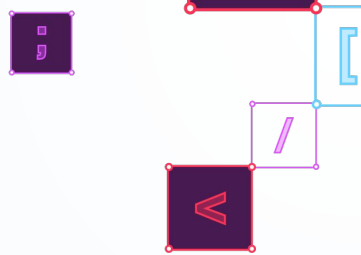
- 574 rules
- 65 quick fixes
- Covers C++ core guidelines, MISRA, CERT, OWASP, CWE
- C++20



sonar

Wrap-up

- The Power of Clean Code
- Clean as you Code
- SonarLint in your favorite IDE



Questions?

@sonarsource

https://sonarsource.com

sonar