Microsoft

SonarQube

Crystal Tenn
Crystal.Tenn@microsoft.com

SonarQube

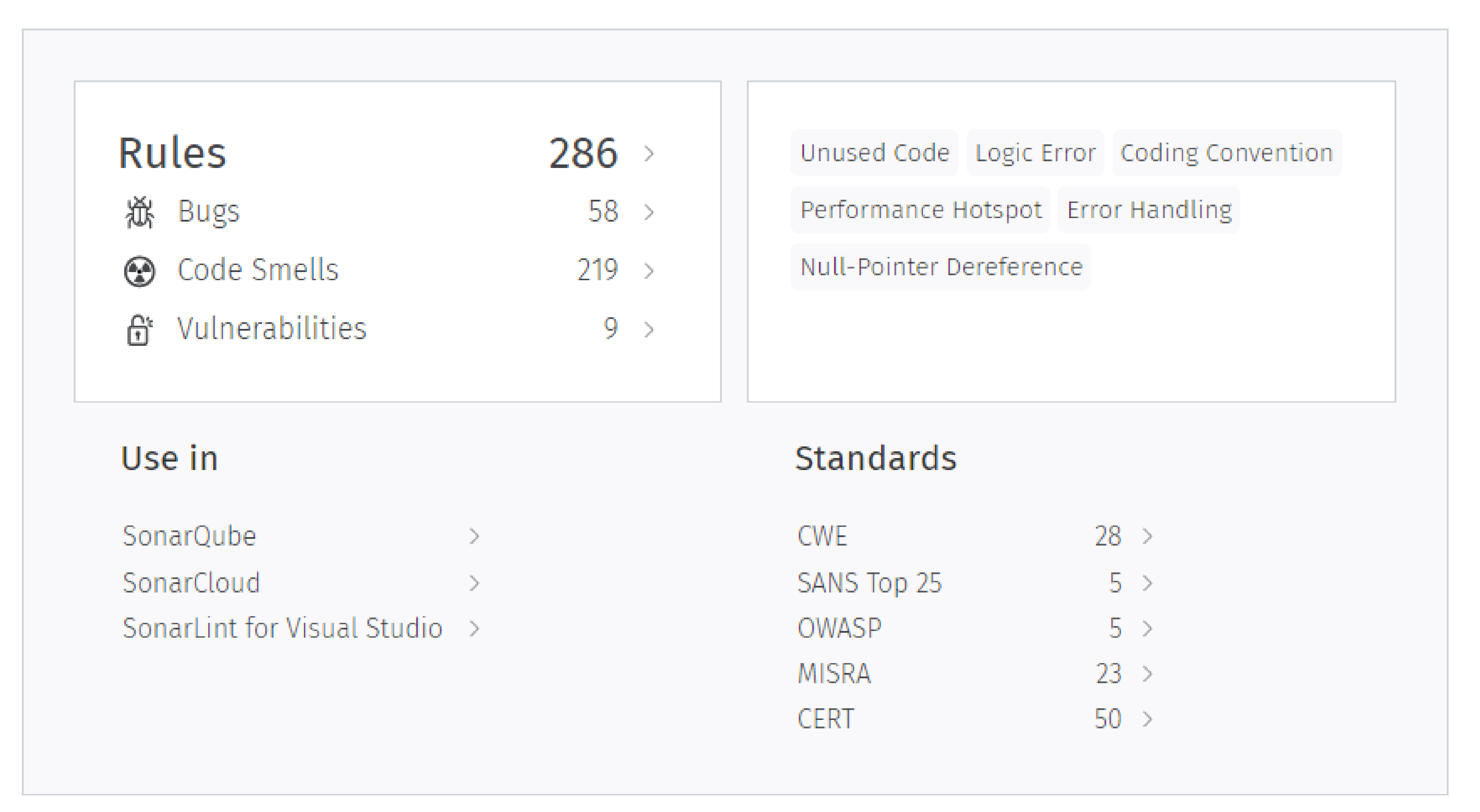
- SonarSource delivers what is probably the best static code analyzer you can find on the market for C#. Based on Microsoft Roslyn compiler front-end, it uses the most advanced techniques (pattern matching, dataflow analysis) to analyze code and find code smells, bugs and security vulnerabilities. As for any product we develop at SonarSource, it was built on the following principles: depth, accuracy and speed.
- SonarC# has a great coverage of well-established quality standards. The SonarC# capability is available in Visual Studio for developers (SonarLint) as well as throughout the development chain for automated code review with on-premise SonarQube or on-line SonarCloud.

SonarQube

- Easy analysis of any existing Visual Studio Solution or MSBuild project
- Native integration with any existing build in TFS or VSTS

- Code coverage by tests: SonarC# supports the import of Microsoft Visual Studio, dotCover, OpenCover, and NCover 3 test coverage reports.

Main Dashboard



Rules	286
Bugs	58
Code Smells	219
Vulnerabilities	9

Unused Code Logic Error Coding Convention Performance Hotspot Error Handling Null-Pointer Dereference

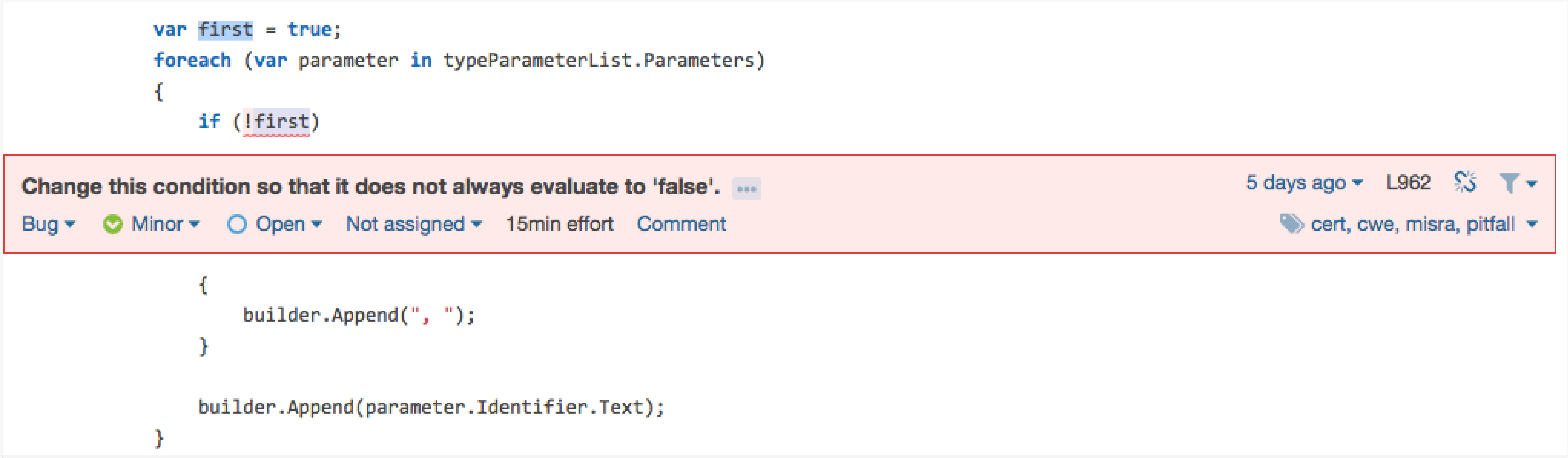
Use in

- SonarQube
- SonarCloud
- SonarLint for Visual Studio

Standards

CWE	28
SANS Top 25	5
OWASP	5
MISRA	23
CERT	50

Sample of Code Cleanup Suggestions



```
var first = true;
foreach (var parameter in typeParameterList.Parameters)
{
    if (!first)
```

Change this condition so that it does not always evaluate to 'false'. ···

5 days ago ▾ L962

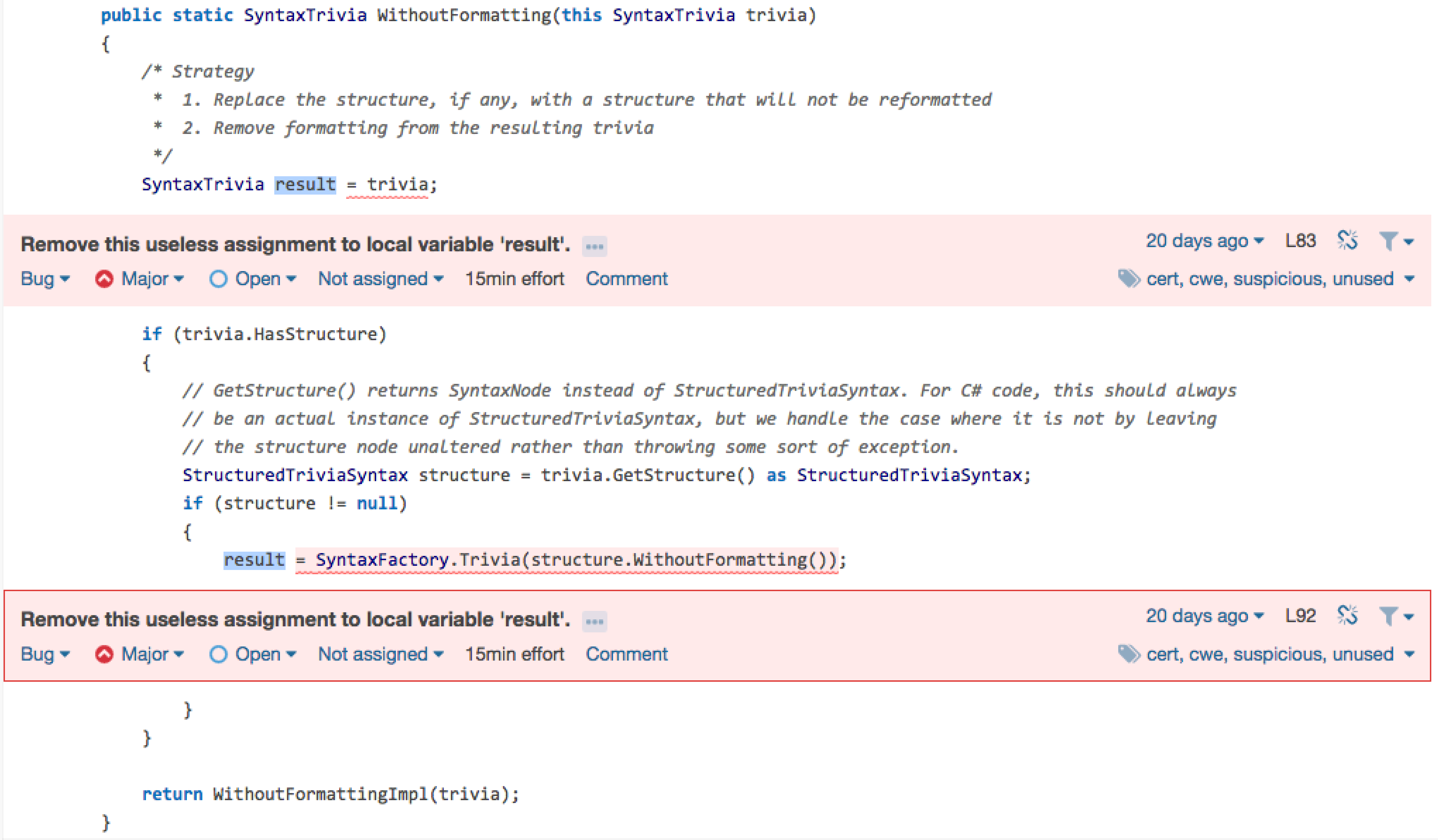
Bug ▾ Minor ▾ ○ Open ▾ Not assigned ▾ 15min effort Comment

cert, cwe, misra, pitfall ▾

```
    {
        builder.Append(", ");
    }

    builder.Append(parameter.Identifier.Text);
}
```

Sample of Code Cleanup Suggestions



```
public static SyntaxTrivia WithoutFormatting(this SyntaxTrivia trivia)
{
    /* Strategy
     *  1. Replace the structure, if any, with a structure that will not be reformatted
     *  2. Remove formatting from the resulting trivia
     */
    SyntaxTrivia result = trivia;
```

Remove this useless assignment to local variable 'result'. ···

20 days ago ▾ L83

Bug ▾ Major ▾ ○ Open ▾ Not assigned ▾ 15min effort Comment

cert, cwe, suspicious, unused ▾

```
    if (trivia.HasStructure)
    {
        // GetStructure() returns SyntaxNode instead of StructuredTriviaSyntax. For C# code, this should always
        // be an actual instance of StructuredTriviaSyntax, but we handle the case where it is not by leaving
        // the structure node unaltered rather than throwing some sort of exception.
        StructuredTriviaSyntax structure = trivia.GetStructure() as StructuredTriviaSyntax;
        if (structure != null)
        {
            result = SyntaxFactory.Trivia(structure.WithoutFormatting());
```

Remove this useless assignment to local variable 'result'. ···

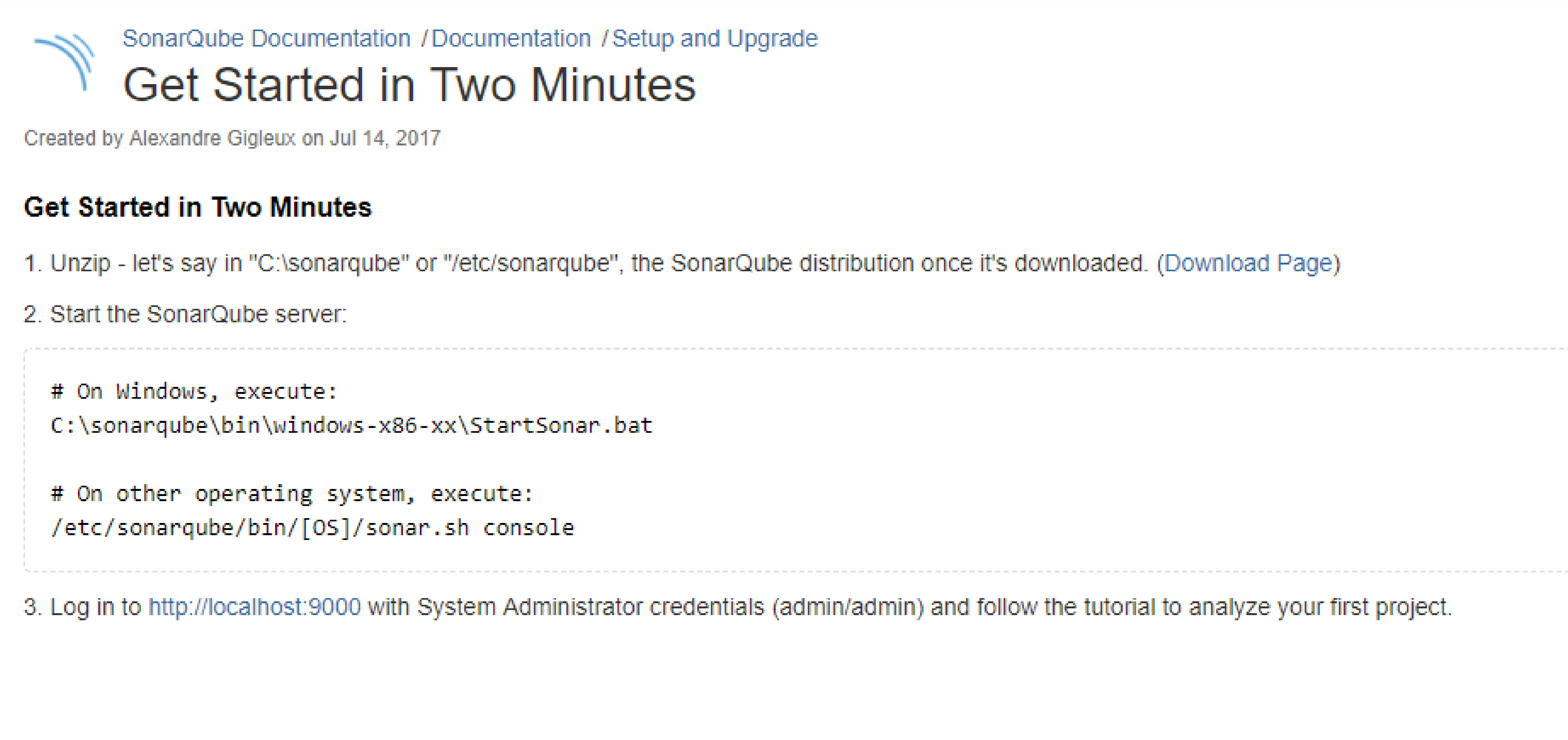
20 days ago ▾ L92

Bug ▾ Major ▾ ○ Open ▾ Not assigned ▾ 15min effort Comment

cert, cwe, suspicious, unused ▾

```
        }
    }

    return WithoutFormattingImpl(trivia);
}
```



SonarQube Documentation / Documentation / Setup and Upgrade

Get Started in Two Minutes

Created by Alexandre Gigleux on Jul 14, 2017

Get Started in Two Minutes

1. Unzip - let's say in "C:\sonarqube" or "/etc/sonarqube", the SonarQube distribution once it's downloaded. (Download Page)

2. Start the SonarQube server:

```
# On Windows, execute:
C:\sonarqube\bin\windows-x86-xx\StartSonar.bat

# On other operating system, execute:
/etc/sonarqube/bin/[OS]/sonar.sh console
```

3. Log in to http://localhost:9000 with System Administrator credentials (admin/admin) and follow the tutorial to analyze your first project.

https://docs.sonarqube.org/display/SONAR/Get+Started+in+Two+Minutes

Full SonarQube Setup Documentation

The only prerequisite for running SonarQube is to have Java (Oracle JRE 8 onwards or OpenJDK 8 onwards) installed on your machine.

The SonarQube server requires at least 2GB of RAM to run efficiently and 1GB of free RAM for the OS.

https://docs.sonarqube.org/pages/viewpage.action?pageId=1441900

Microsoft

Thank you!