GRAMMATECH

DATASHEET

CodeSonar C#
SAST when Safety and Security Matter

CODESONAR®

Accelerate Application Security

Software teams are under constant pressure to deliver more content with higher complexity, in shorter timeframes, with increased quality and security. Static Application Security Testing is a proven best practice to help software teams deliver the best code in the shortest timeframe. GrammaTech has been a leader in this field for over 15 years with CodeSonar delivering multi-language SAST capabilities for enterprises where software quality and software security matter.

C#

DevSecOps - Speed and Scale

Software developers need rapid feedback on security vulnerabilities in their work artifacts. CodeSonar can be integrated into software development environments, can work unobtrusively to the developer and provide rapid feedback.

Abstract Interpretation

GrammaTech SAST tools use the concept of abstract interpretation to statically examine all the paths through the application and understand the values of variables and how they impact program state. Abstract interpretation gives CodeSonar for C# the highest scores in vulnerability benchmarks.

Security

Broad coverage of security vulnerabilities, including OWASP Top10, SANS/CWE 25. Support for third party applications through byte code analysis.

Quality

Integration into DevSecOps to improve quality of the code and developer efficiency. Find code quality and performance issues at speed.

Privacy

Checkers that detect performance impacts such as unnecessary test for nullness, creation of redundant objects or superfluous memory writes.

Use Cases

Enterprise customers are using C# in their internal applications, either in-house built, or built by a third-party. Static analysis is needed to to improve security and quality to drive business continuity.

Mobile and Client customers are using C# on end-points, sometimes in an internet-of-things deployment, or to provide information to mobile users. Security is critical due to the diverse environment, privacy is top-of-mind as well.

Web Apps drive dynamic content for websites and web-based applications. In a hostile environment tainted data analysis is crucial to assist developers to understand where their applications may be vulnerable.

Frameworks Supported

Currently supported frameworks are listed below. New frameworks are added every release.

Unity, WebForms, WindowsForms, MVC

IDE Support

CodeSonar for C# plugs into, Microsoft Visual Studio and VS Code. Through the IDE you can launch new analyses and review and resolve warnings as you write the code.

U.S. SALES 888-695-2668
INTERNATIONAL SALES +1-607-273-7340

FOR MORE INFORMATION
www.grammatech.com

EMAIL sales@grammatech.com

Checkers

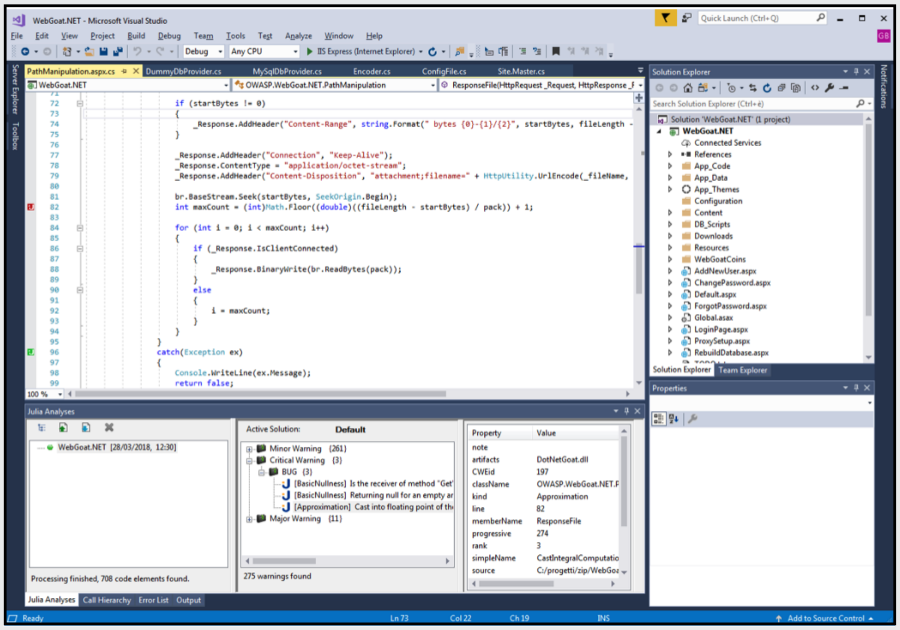
CodeSonar for C# includes a complete range of checkers for security, quality, efficiency and style, some examples:

Security

- Injections
- Cryptography
- XXE
- LDAP
- Cookies
- Passwords

Quality

- Nullness
- Approximation
- CloseResource
- DeadCode
- BadEq
- EqualsHashCode



```
                if (startBytes != 0)
                {
                    _Response.AddHeader("Content-Range", string.Format(" bytes {0}-{1}/{2}", startBytes, fileLength -

                }

                _Response.AddHeader("Connection", "Keep-Alive");
                _Response.ContentType = "application/octet-stream";
                _Response.AddHeader("Content-Disposition", "attachment;filename=" + HttpUtility.UrlEncode(_fileName,

                br.BaseStream.Seek(startBytes, SeekOrigin.Begin);
                int maxCount = (int)Math.Floor((double)((fileLength - startBytes) / pack)) + 1;

                for (int i = 0; i < maxCount; i++)
                {
                    if (_Response.IsClientConnected)
                    {
                        _Response.BinaryWrite(br.ReadBytes(pack));
                    }
                    else
                    {
                        i = maxCount;
                    }
                }
            }
            catch(Exception ex)
            {
                Console.WriteLine(ex.Message);
                return false;
```

WebGoat.NET [28/03/2018, 12:30]

Processing finished, 708 code elements found.

Active Solution: **Default**

```
⊞ Minor Warning   (261)
⊟ Critical Warning   (3)
   ⊟ BUG  (3)
      [BasicNullness]  Is the receiver of method "Get'
      [BasicNullness]  Returning null for an empty ar
      [Approximation]  Cast into floating point of th
⊞ Major Warning   (11)
```

275 warnings found

Property	Value
note	
artifacts	DotNetGoat.dll
CWEid	197
className	OWASP.WebGoat.NET.P
kind	Approximation
line	82
memberName	ResponseFile
progressive	274
rank	3
simpleName	CastIntegralComputatio
source	C:/progetti/zip/WebGoa

Analyze Third Party Code

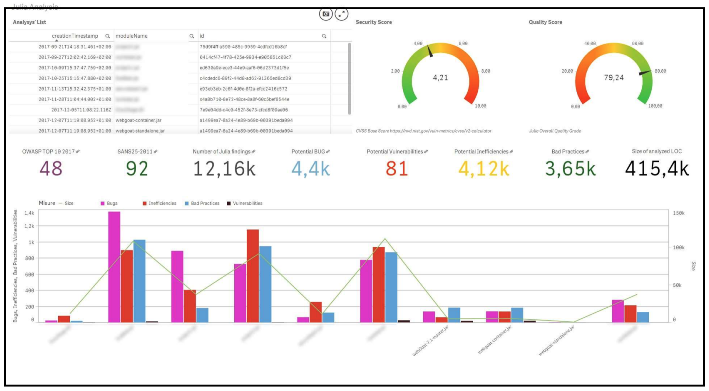
CodeSonar for C# analyzes bytecode and then reflects these warnings back into your source-code. This allows the analysis of both your own code as well as third-party applications where source code may not be available.

Dashboarding

An advanced, interactive dashboard plug-in allows managers and security analysts to understand current status and track progress.

Process Integration

CodeSonar for C# is flexible and can provide output in a variety of different formats such as PDF and XML for easy integration in your process.



creationTimestamp	moduleName	id
2017-09-21T14:18:31.461+02:00	[illegible]	75d9f4ff-a590-485c-9959-4edfcd16b8cf
2017-09-27T12:02:42.169+02:00	[illegible]	0414cf47-4f78-425e-9934-e905851c03c7
2017-10-09T15:37:47.759+02:00	[illegible]	ed630a9e-ece3-44e9-aaf6-06d2373d1f5e
2017-10-25T15:15:47.880+02:00	[illegible]	c4cdedc6-89f2-44d8-ad62-91365ed8cd39
2017-11-13T15:32:42.375+01:00	[illegible]	e93eb3eb-2c6f-4d0e-8f2a-efcc2416c572
2017-11-28T11:04:44.002+01:00	[illegible]	x4a8b710-8e72-48ce-8a8f-60c5bef8544e
2017-12-05T11:08:22.116Z	[illegible]	7e9e04dd-c4c0-452f-8e73-cfcd8f09ae06
2017-12-07T11:19:08.952+01:00	webgoat-container.jar	a1499ea7-8a24-4e89-b69b-00391beda094
2017-12-07T11:19:08.952+01:00	webgoat-standalone.jar	a1499ea7-8a24-4e89-b69b-00391beda094

Free Trial

The best way to try a SAST solution is to run it on your own codebase and review the warnings it issues. Visit **go.grammatech.com** to request a 30-day trial license and learn how GrammaTech technology can rapidly improve your software development capability.

System Requirements

Host: Windows, Linux

Hardware: 2+ Cores, 32+GB of RAM, 20+GB of disk

U.S. SALES 888-695-2668
INTERNATIONAL SALES +1-607-273-7340

FOR MORE INFORMATION
www.grammatech.com

EMAIL sales@grammatech.com