Security Code Scan Overview - static code analyzer for .NET

1. **Introduction:** To scan Vulnerable codes and detect in Microsoft applications (supporting language C# and VB.NET only). Creating a secure way in development, so security code Scan rules silently search for security vulnerabilities and alert you if any are found. Applies for web and window in Visual Studio. Rule categories include Configuration, Cross-Site Scripting, Cryptography, Insecure Deserialization, Injection, Password Management and Validation.
2. **Problem:** During development of any application, the developer is not able to recognized secure way to develop application.
3. **Root Cause:** The code analyzer tool was not able in application to identify security issue during development and fix it instantly. So, the cause of this application leading many security issues examples: Security Misconfiguration, Cross-Site Scripting, Insecure Cryptography, Insecure Deserialization, Injection, Password Management, Validation, Access Control, Secrets Management.
4. **Resolution:** Now two options available in SCS (Security Code Scan) analyzer to resolve these issues. First option, the developer should install SCS extension in their application. Second option, If the developer wants to scan code and fix it after development of application then use suppress and “show potential fixes” option with SCS. It is covering 40%-50% codes only. The SCS is open source so we can customise code as per our needed. We can write set of code to fix Vulnerable codes in web config, As of now it is just detecting issue in web config.
5. **Implementation:**

5A. Installation: First of all, we need to install security code scan (SCS) through NuGet package.

**Option 01:** Download extension and install with your VS (2015 and above) Download link:

<https://marketplace.visualstudio.com/items?itemName=JaroslavLobacevski.SecurityCodeScan&ssr=false#review-details>

**Option 02:** Tools > NuGet Package Manager > Package Manager Console”. Run the command Get-Project -All | Install-Package SecurityCodeScan

**Option 03:** Use “manage NuGet packages for solution”

5B. Configuration: Enable full solution analysis.

5C. To Scan .aspx and web.config Files: Unload project and edit .csproj file and add below line like this.

<!-- Add the line below -->

<AdditionalFileItemNames>$(AdditionalFileItemNames);Content</AdditionalFileItemNames>

After added this line, reload project and re-build solution.

Testing on Process Improvement (sample project in C# 2015 and above): After completion of above steps, build your solution and open error list tab in your VS to get list of warnings.

Suppressing and Fixing the Warnings:

Need to install System.Diagnostics.CodeAnalysis.dll for suppressing and fixing the warning. Once install above DLL, please run Analyse option and ‘Run Code Analysis and Suppress Active Issues’.

Severity: Change severity of info/warn of error list tab.

**Troubleshooting:** If no SCS warnings are displayed, temporarily disable other installed analyzers. A buggy analyzer may [affect results from other analyzers](https://github.com/dotnet/roslyn/issues/23879).