USING CAT.NET INSIDE THE O2 PLATFORM

Cat.Net - Consuming its engine

Install Cat.NET (by downloading MSI from MS and extracting it into _ToolsOrAPIs folder)

```
"CatNet.cs".local().executeFirstMethod();
```

Consuming Cat.NET Exe

```
return "CatNet_1.1/SourceDir/CATNetCmd.exe".assembly();
//_O2Ref:CatNet_1.1/SourceDir/CATNetCmd.exe
```
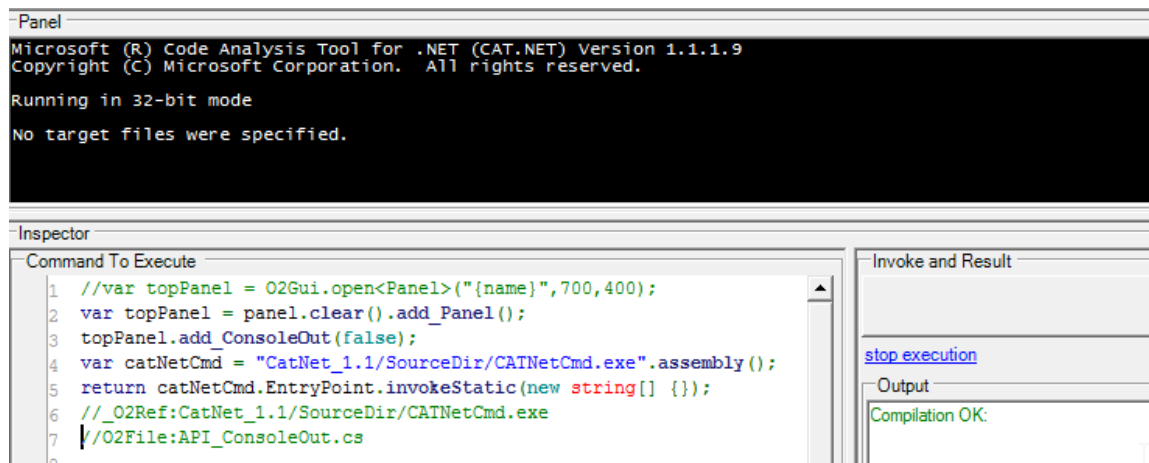
Main Method (exe extry point)

```
var catNetCmd = "CatNet_1.1/SourceDir/CATNetCmd.exe".assembly();
return catNetCmd.EntryPoint;
```

Invoking Main using Reflection

```
var catNetCmd = "CatNet_1.1/SourceDir/CATNetCmd.exe".assembly();
return catNetCmd.EntryPoint.invokeStatic(new string[] {});
```

Invoking Main and seeing its console out message

Refactoring code into scan method

```
Action<string[]> scan =
        (arguments)=>{
                        var catNetCmd = "CatNet_1.1/SourceDir/CATNetCmd.exe".assembly();
                        catNetCmd.EntryPoint.invokeStatic(arguments);
                };
scan(new string[] {} );
```

Scanning a dll

```
//var topPanel = O2Gui.open<Panel>("{name}",700,400);
var topPanel = panel.clear().add_Panel();
topPanel.add_ConsoleOut(false);
Action<string[]> scan =
        (arguments)=>{
                        var catNetCmd = "CatNet_1.1/SourceDir/CATNetCmd.exe".assembly();
                        catNetCmd.Location.info();
                        catNetCmd.EntryPoint.invokeStatic(arguments);
                };
```

```csharp
var testFile = "SuperSecureBank.dll".local();

//testFile = "";
scan(new string[] { "/file:" + testFile } );
//_O2Ref:CatNet_1.1/SourceDir/CATNetCmd.exe
//O2File:API_ConsoleOut.cs

//O2Tag_DontAddExtraO2Files
```

```
Panel
Microsoft (R) Code Analysis Tool for .NET (CAT.NET) Version 1.1.1.9
Copyright (C) Microsoft Corporation.  All rights reserved.

Running in 32-bit mode

6/6/2012 3:07:11 AM:Info : Starting analysis [1 modules]
6/6/2012 3:07:11 AM:Info : Analyzing module SuperSecureBank...
6/6/2012 3:07:15 AM:Info : 1 File Canonicalization issues found.
6/6/2012 3:07:15 AM:Info : 41 SQL Injection issues found.
6/6/2012 3:07:15 AM:Info : 6 Redirection to User Controlled Site issues found.
6/6/2012 3:07:15 AM:Info : 7 Cross-Site Scripting issues found.
6/6/2012 3:07:16 AM:Info : Analysis completed.
```

Inspector

Command To Execute

```csharp
1  //var topPanel = O2Gui.open<Panel>("{name}",700,400);
2  var topPanel = panel.clear().add_Panel();
3  topPanel.add_ConsoleOut(false);
4  Action<string[]> scan =
5      (arguments)=>{
6                  var catNetCmd = "CatNet_1.1/SourceDir/CATNetCmd.exe".assembly();
7                  catNetCmd.Location.info();
8                  catNetCmd.EntryPoint.invokeStatic(arguments);
9              };
10
11 var testFile = "SuperSecureBank.dll".local();
12
13 scan(new string[] { "/file:" + testFile } );
14 //_O2Ref:CatNet_1.1/SourceDir/CATNetCmd.exe
15 //O2File:API_ConsoleOut.cs
```
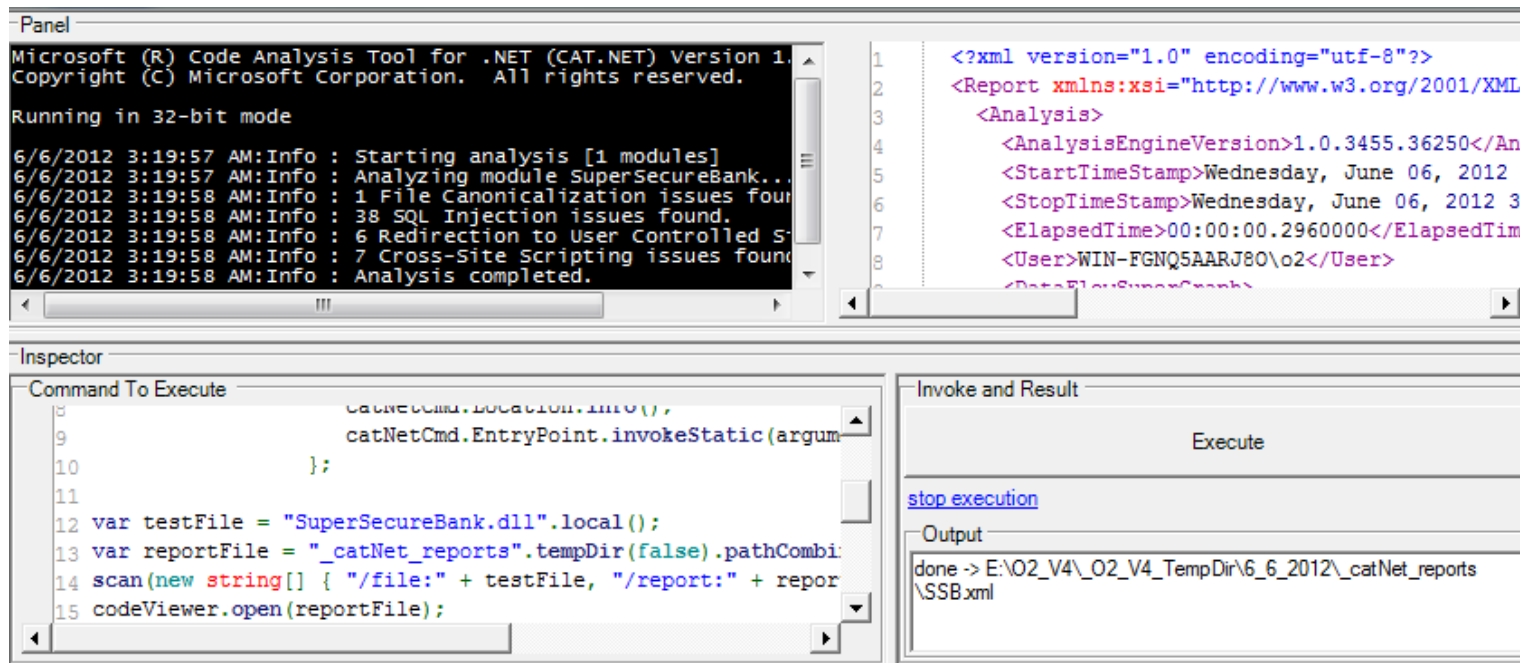
Scanning file, saving +showing report file

```csharp
//var topPanel = O2Gui.open<Panel>("{name}",700,400);
var topPanel = panel.clear().add_Panel();
var codeViewer = topPanel.insert_Right().add_SourceCodeViewer();
topPanel.add_ConsoleOut(false);
Action<string[]> scan =
      (arguments)=>{
                  var catNetCmd = "CatNet_1.1/SourceDir/CATNetCmd.exe".assembly();
                  catNetCmd.Location.info();
                  catNetCmd.EntryPoint.invokeStatic(arguments);
              };

var testFile = "SuperSecureBank.dll".local();
var reportFile = "_catNet_reports".tempDir(false).pathCombine("SSB.xml");
scan(new string[] { "/file:" + testFile, "/report:" + reportFile } );
codeViewer.open(reportFile);
return "done -> {0}".format(reportFile);
//_O2Ref:CatNet_1.1/SourceDir/CATNetCmd.exe
//O2File:API_ConsoleOut.cs
```
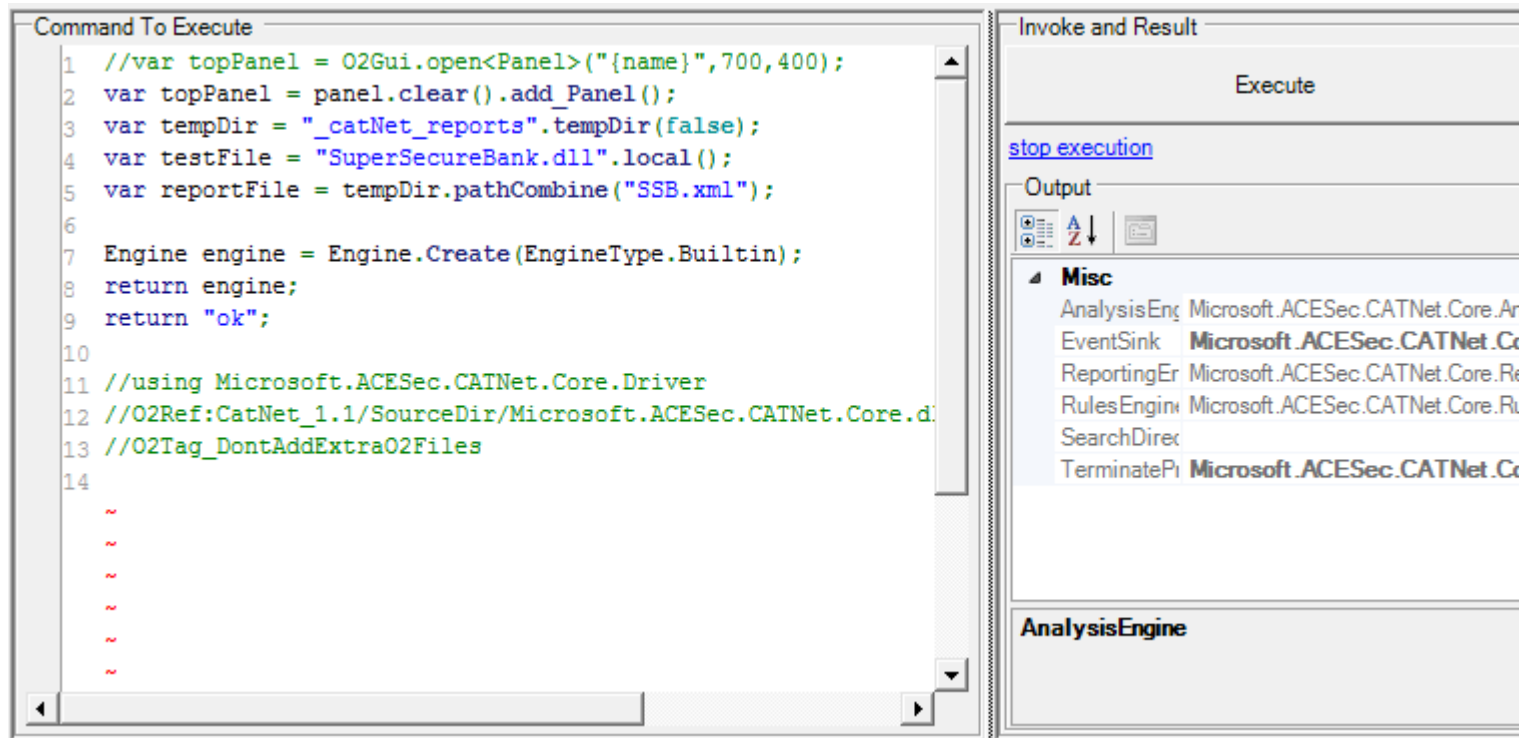
Inspector

Command To Execute

```
8                CatNetCmd.Location.info();
9                catNetCmd.EntryPoint.invokeStatic(argum
10              };
11
12   var testFile = "SuperSecureBank.dll".local();
13   var reportFile = "_catNet_reports".tempDir(false).pathCombi
14   scan(new string[] { "/file:" + testFile, "/report:" + repor
15   codeViewer.open(reportFile);
```

Invoke and Result

Execute

stop execution

Output

done -> E:\O2_V4_O2_V4_TempDir\6_6_2012_catNet_reports
\SSB.xml

Scanning file, generating scanning stats and creating a graphml graph

```csharp
//var topPanel = O2Gui.open<Panel>("{name}",700,400);
var topPanel = panel.clear().add_Panel();
var codeViewer = topPanel.insert_Right().add_SourceCodeViewer();
topPanel.add_ConsoleOut(false);
Action<string[]> scan =
    (arguments)=>{
                    var catNetCmd = "CatNet_1.1/SourceDir/CATNetCmd.exe".assembly();
                    catNetCmd.Location.info();
                    catNetCmd.EntryPoint.invokeStatic(arguments);
                };
var tempDir = "_catNet_reports".tempDir(false);
var testFile = "SuperSecureBank.dll".local();
var reportFile = tempDir.pathCombine("SSB.xml");
var dfGraph = tempDir.pathCombine("SSB.graphml");
scan(new string[] { "/file:" + testFile,
                    "/report:" + reportFile,
                    "/dfgraph:" + dfGraph,
                    "/profile" }
                    );
codeViewer.open(reportFile);
return "done -> {0}".format(reportFile);
//_O2Ref:CatNet_1.1/SourceDir/CATNetCmd.exe
//O2File:API_ConsoleOut.cs
```

DIRECTLY using the CAT.NET Engine
(from Microsoft.ACESec.CATNet.Core.dll)

Creating an Engine Object

```
1  //var topPanel = O2Gui.open<Panel>("{name}",700,400);
2  var topPanel = panel.clear().add_Panel();
3  var tempDir = "_catNet_reports".tempDir(false);
4  var testFile = "SuperSecureBank.dll".local();
5  var reportFile = tempDir.pathCombine("SSB.xml");
6
7  Engine engine = Engine.Create(EngineType.Builtin);
8  return engine;
9  return "ok";
10
11 //using Microsoft.ACESec.CATNet.Core.Driver
12 //O2Ref:CatNet_1.1/SourceDir/Microsoft.ACESec.CATNet.Core.d]
13 //O2Tag_DontAddExtraO2Files
14
    ~
    ~
    ~
    ~
    ~
    ~
```

Command To Execute

Invoke and Result

Execute

stop execution

Output

▲ Misc
- AnalysisEng Microsoft.ACESec.CATNet.Core.An
- EventSink   **Microsoft.ACESec.CATNet.Co**
- ReportingEr Microsoft.ACESec.CATNet.Core.Re
- RulesEngin   Microsoft.ACESec.CATNet.Core.Ru
- SearchDirec
- TerminatePi **Microsoft.ACESec.CATNet.Co**

AnalysisEngine

Addding an event (backed by API_CatNet.cs class)

```
var reportFile = tempDir.pathCombine("SSB.xml");
var engine = Engine.Create(EngineType.Builtin);
engine.EventSink = new CatNetEvents();
return engine;
return "ok";

//using Microsoft.ACESec.CATNet.Core.Driver
 //O2File:API_CatNet.cs
//O2Ref:CatNet_1.1/SourceDir/Microsoft.ACESec.CATNet.Core.dll



namespace O2.XRules.Database.APIs
{
        public class API_CatNet
        {

                public API_CatNet()
                {

                }
        }

        public class CatNetEvents  : EventSink
        {
                public override void AssemblyLoadFailure(string path)
                {
                        "[CatNetEvents] AssemblyLoadFailure: {0}".error(path);
                }

                public override void Output(EventSink.OutputType type, string format, params object[] p)
                {
                        "[CatNetEvents] {0} : {1}".info(type, format.format(p));
                }
        }}
```

Running a scan with no rules

```
//var topPanel = O2Gui.open<Panel>("{name}",700,400);
var topPanel = panel.clear().add_Panel();
var tempDir = "_catNet_reports".tempDir(false);
var testFile = "SuperSecureBank.dll".local();

var reportFile = tempDir.pathCombine("SSB.xml");
var engine = Engine.Create(EngineType.Builtin);
engine.EventSink = new CatNetEvents();
engine.Analyze(testFile);
```
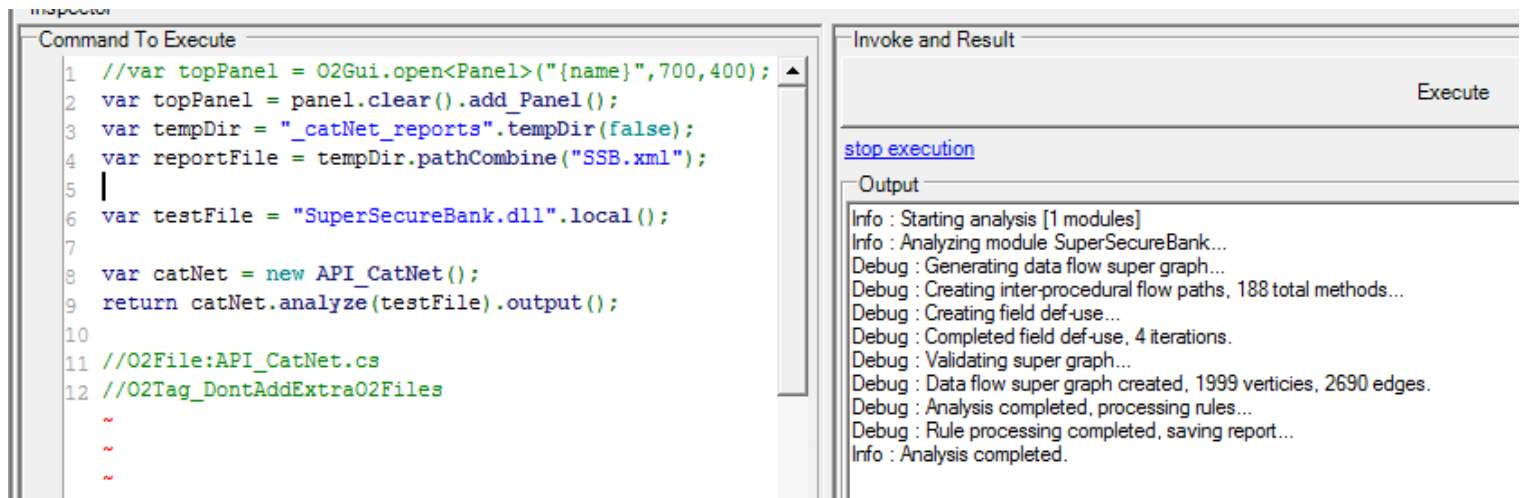
```
return engine;

//using Microsoft.ACESec.CATNet.Core.Driver
//O2File:API_CatNet.cs
//O2Ref:CatNet_1.1/SourceDir/Microsoft.ACESec.CATNet.Core.dll
//O2Tag_DontAddExtraO2Files
```
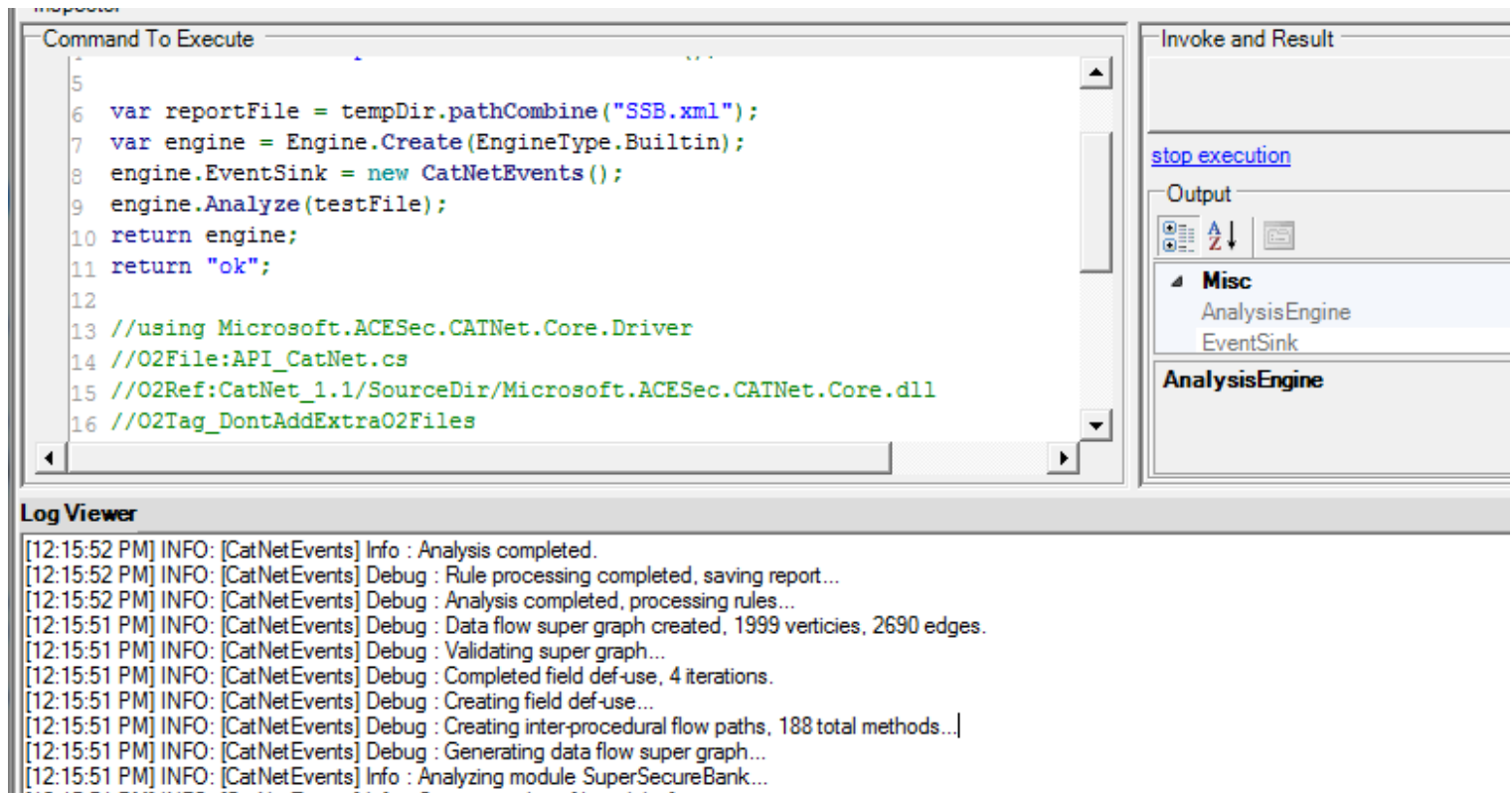

Running scan via API:

```
var testFile = "SuperSecureBank.dll".local();

var catNet = new API_CatNet();
return catNet.analyze(testFile).output();

//O2File:API_CatNet.cs
```


Run scan and create GraphML and Xml Report (note that there are no findings because we have not loaded up the rules)

```
var testFile = "SuperSecureBank.dll".local();
var reportFile = tempDir.pathCombine("SSB.xml");
var graphMl = tempDir.pathCombine("SSB.graphml");
var catNet = new API_CatNet();
catNet.Engine.Configuration.ReportFile = reportFile;
```

```
catNet.Engine.Configuration.DataFlowGraphFile = graphMl;

return catNet.analyze(testFile).output();
```
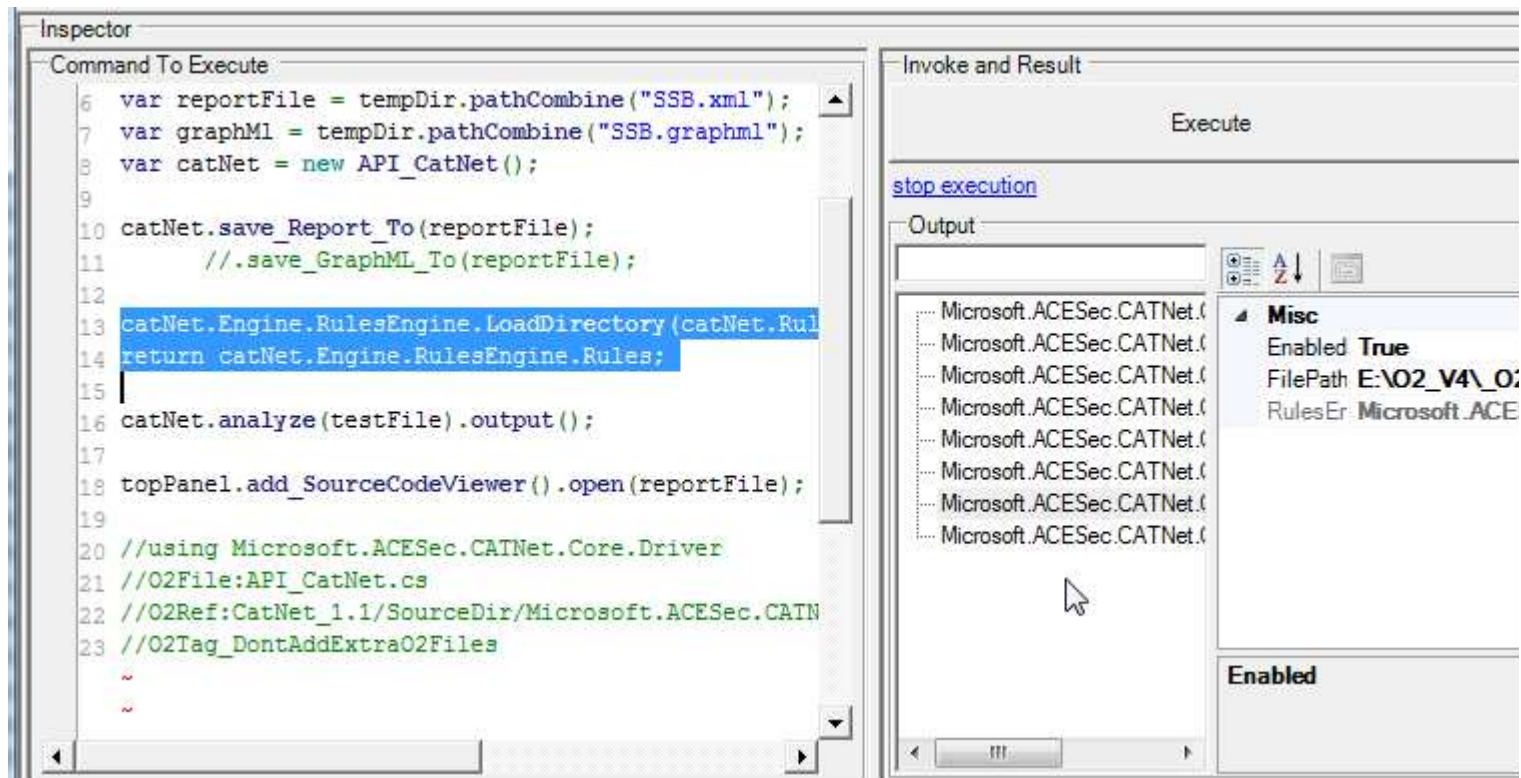
Scan and view result xml file

```
//var topPanel = O2Gui.open<Panel>("{name}",700,400);
var topPanel = panel.clear().add_Panel();
var tempDir = "_catNet_reports".tempDir(false);

var testFile = "SuperSecureBank.dll".local();
var reportFile = tempDir.pathCombine("SSB.xml");
var graphMl = tempDir.pathCombine("SSB.graphml");
var catNet = new API_CatNet();

catNet.save_Report_To(reportFile);
        //.save_GraphML_To(reportFile);

catNet.analyze(testFile).output();

topPanel.add_SourceCodeViewer().open(reportFile);

//using Microsoft.ACESec.CATNet.Core.Driver
 //O2File:API_CatNet.cs
//O2Ref:CatNet_1.1/SourceDir/Microsoft.ACESec.CATNet.Core.dll
//O2Tag_DontAddExtraO2Files
```
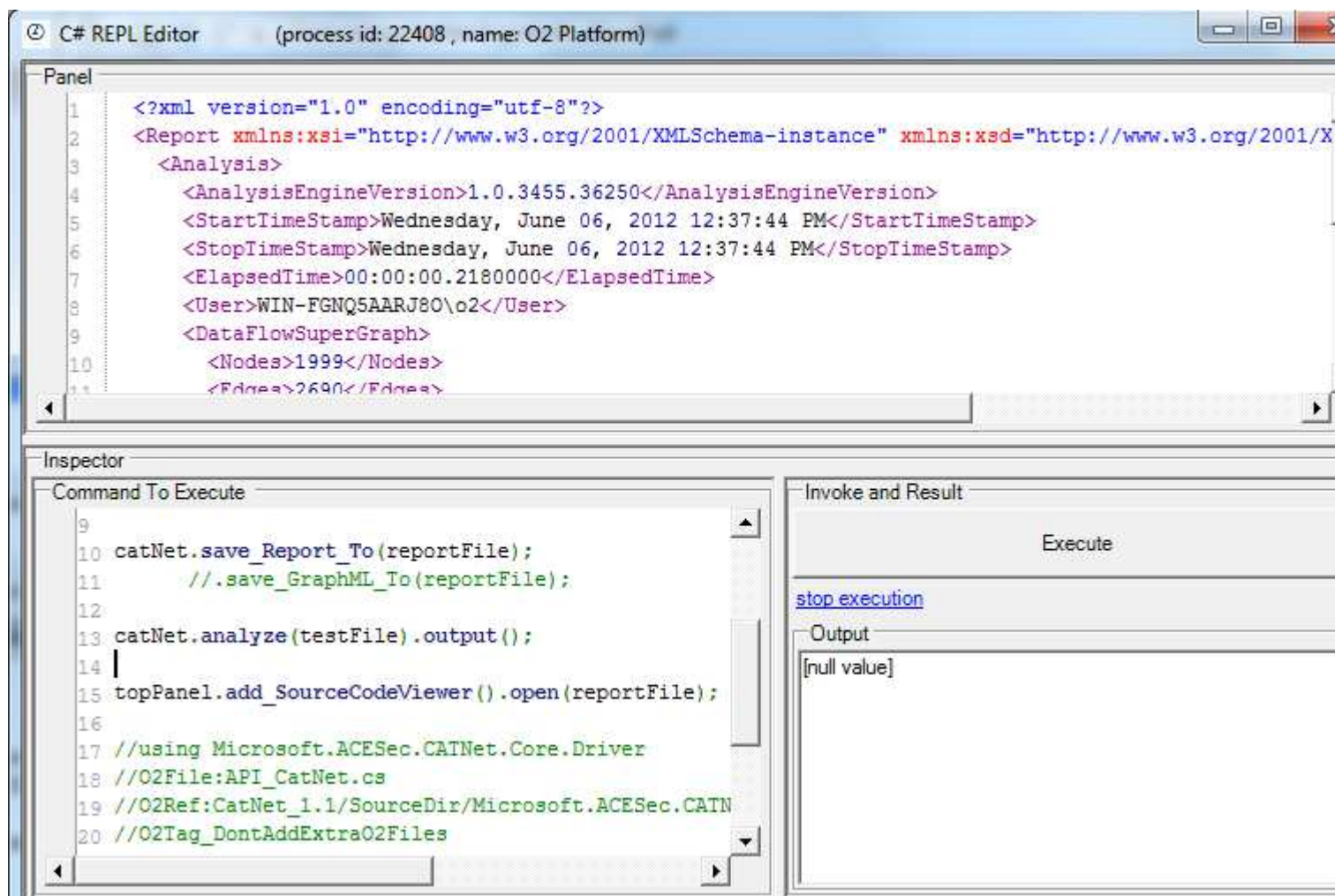

Loading Rules

```
catNet.Engine.RulesEngine.LoadDirectory(catNet.Rules_Folder);
return catNet.Engine.RulesEngine.Rules;
```

Scanning with rules and finding vulnerabilities:

```
//var topPanel = O2Gui.open<Panel>("{name}",700,400);
var topPanel = panel.clear().add_Panel();
var tempDir = "_catNet_reports".tempDir(false);

var testFile = "SuperSecureBank.dll".local();
var reportFile = tempDir.pathCombine("SSB.xml");
var graphMl = tempDir.pathCombine("SSB.graphml");
var catNet = new API_CatNet();

catNet.save_Report_To(reportFile)
        //.save_GraphML_To(reportFile);
        .loadRules();


catNet.analyze(testFile).output();

topPanel.add_SourceCodeViewer().open(reportFile);
return   catNet.output();
//using Microsoft.ACESec.CATNet.Core.Driver
 //O2File:API_CatNet.cs
//O2Ref:CatNet_1.1/SourceDir/Microsoft.ACESec.CATNet.Core.dll
//O2Tag_DontAddExtraO2Files
```
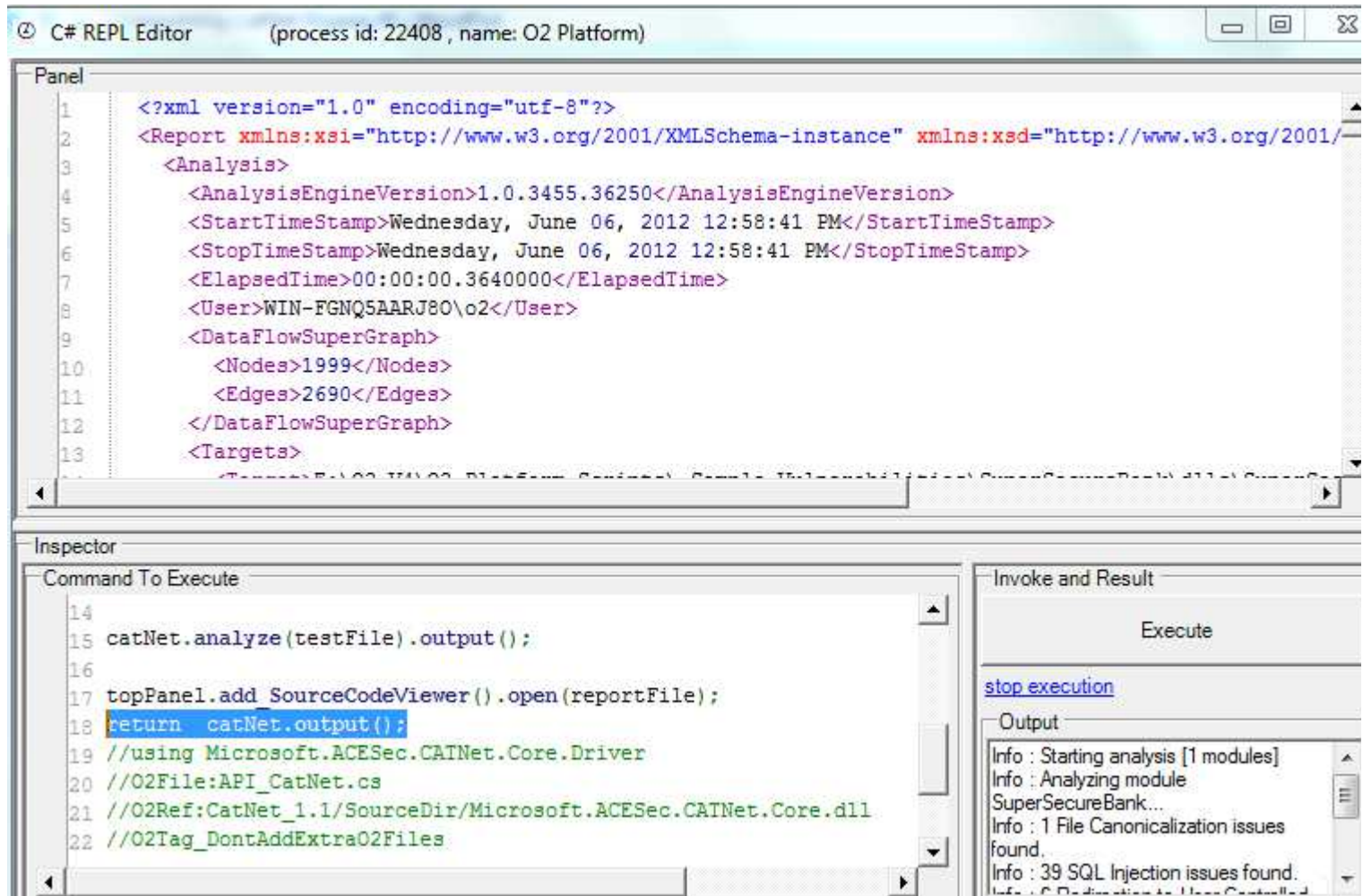
Scanning O2_Fluent_Sharp_CoreLib.dll

```
//var topPanel = O2Gui.open<Panel>("{name}",700,400);
var topPanel = panel.clear().add_Panel();
var tempDir = "_catNet_reports".tempDir(false);


var testFile = "SuperSecureBank.dll".local();
testFile = "O2_FluentSharp_CoreLib.dll".assembly_Location();
var reportFile = tempDir.pathCombine("SSB.xml");
var graphMl = tempDir.pathCombine("SSB.graphml");
var catNet = new API_CatNet();
catNet.EventsLog.ShowDebugEvents = true;
catNet.save_Report_To(reportFile)
        //.save_GraphML_To(reportFile);
        .loadRules();


catNet.analyze(testFile).output();

topPanel.add_SourceCodeViewer().open(reportFile);
return  catNet.output();
//using Microsoft.ACESec.CATNet.Core.Driver
 //O2File:API_CatNet.cs
//O2Ref:CatNet_1.1/SourceDir/Microsoft.ACESec.CATNet.Core.dll
//O2Tag_DontAddExtraO2Files
```
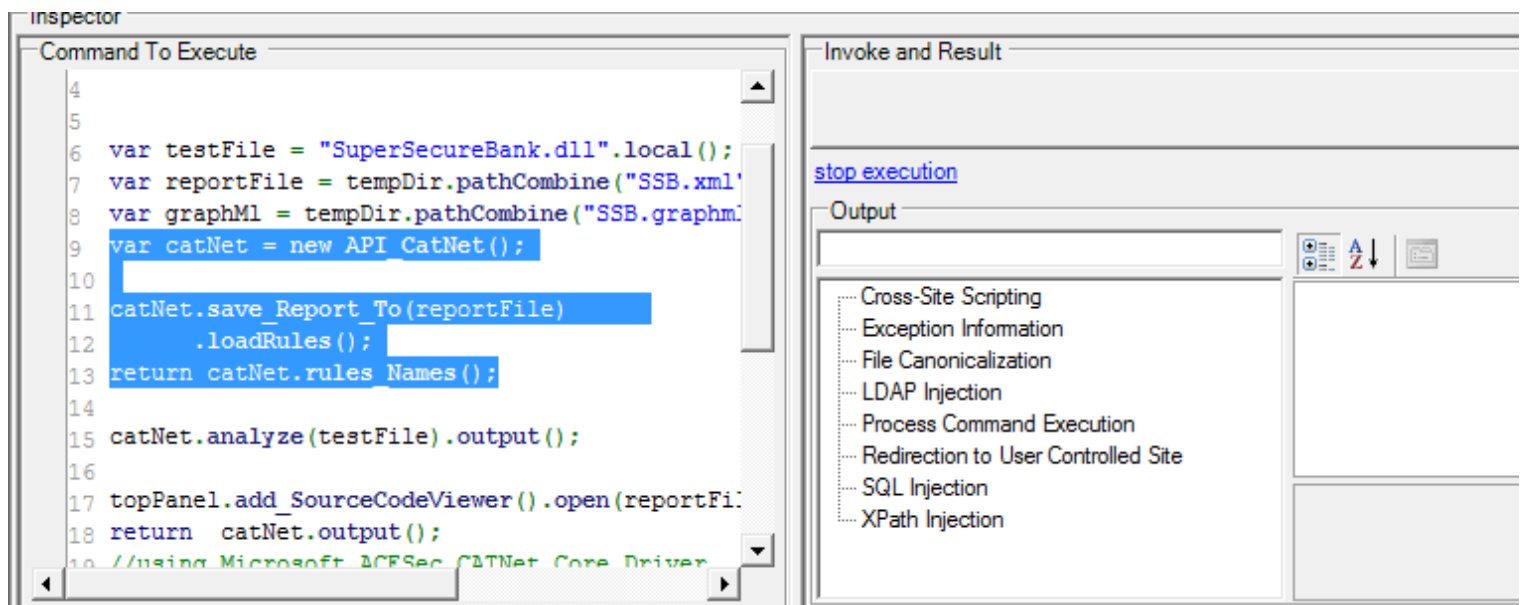
Getting loaded rules names:

```
var catNet = new API_CatNet();

catNet.save_Report_To(reportFile)
        .loadRules();
return catNet.rules_Names();
```

Getting specific Rule

```
var catNet = new API_CatNet();

catNet.save_Report_To(reportFile)
        .loadRules();
return catNet.rule("Cross-Site Scripting");
```


Running a report with a couple rules disabled:
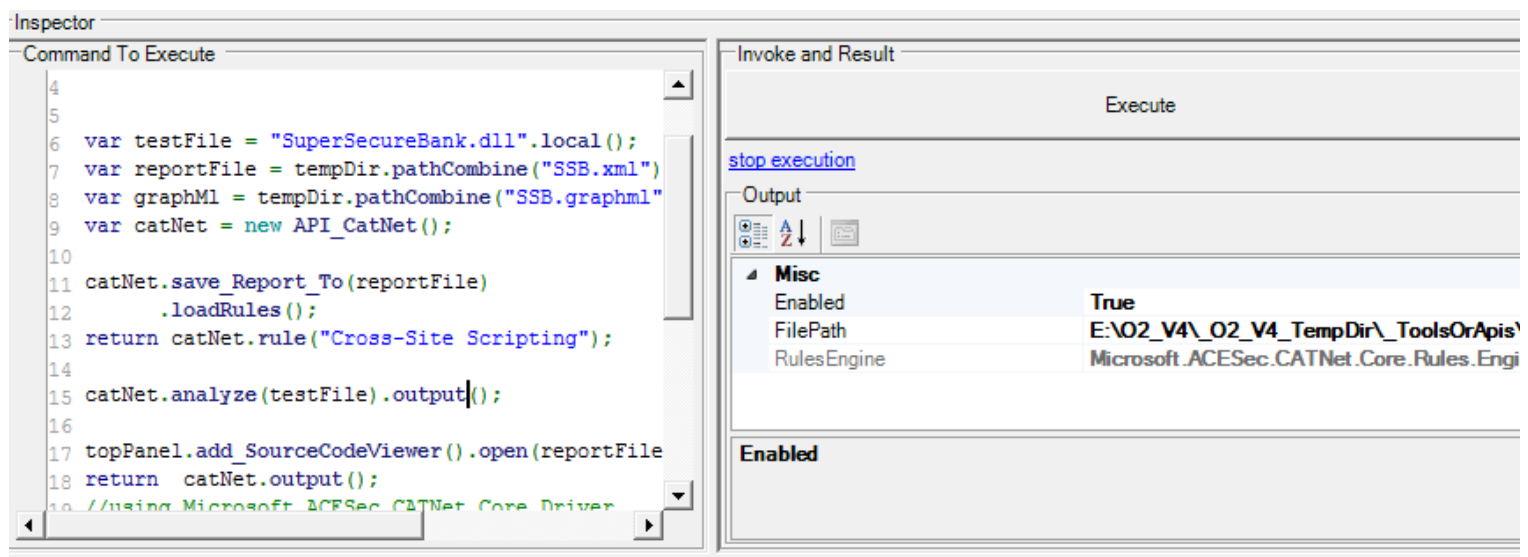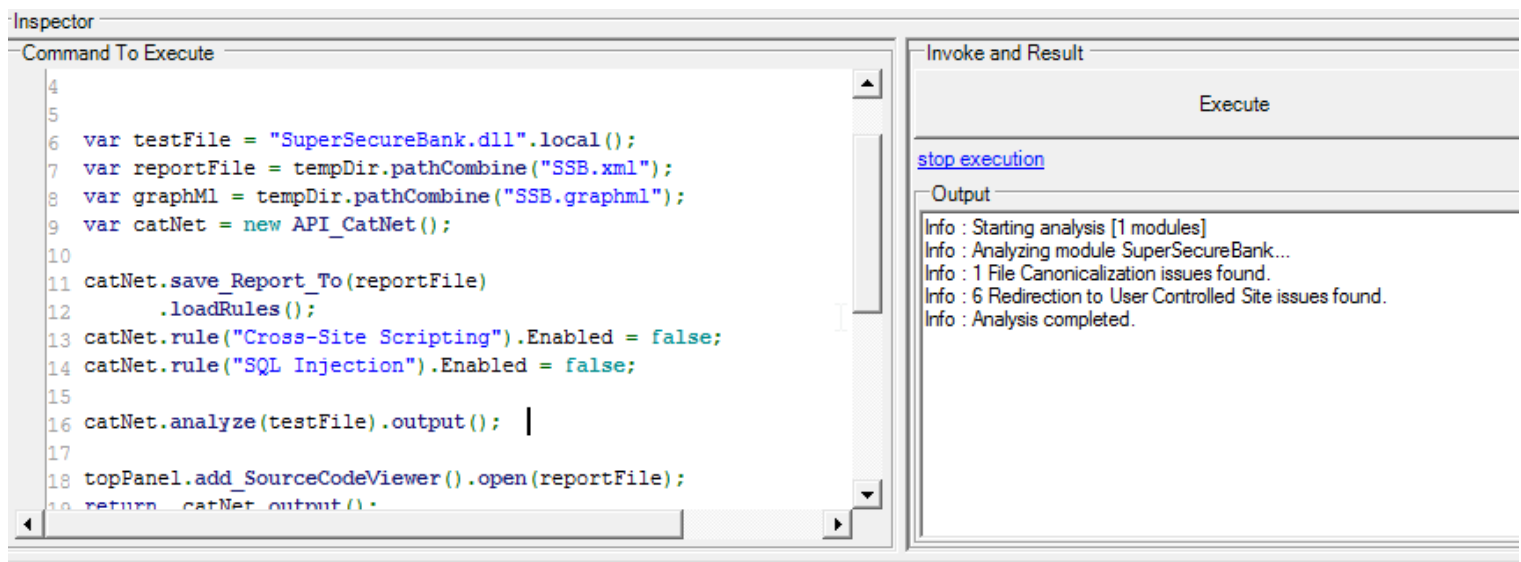
```
var catNet = new API_CatNet();

catNet.save_Report_To(reportFile)
        .loadRules();
catNet.rule("Cross-Site Scripting").Enabled = false;
catNet.rule("SQL Injection").Enabled = false;

catNet.analyze(testFile).output();
```

Command To Execute

```
 4
 5
 6   var testFile = "SuperSecureBank.dll".local();
 7   var reportFile = tempDir.pathCombine("SSB.xml");
 8   var graphMl = tempDir.pathCombine("SSB.graphml");
 9   var catNet = new API_CatNet();
10
11   catNet.save_Report_To(reportFile)
12        .loadRules();
13   catNet.rule("Cross-Site Scripting").Enabled = false;
14   catNet.rule("SQL Injection").Enabled = false;
15
16   catNet.analyze(testFile).output();   |
17
18   topPanel.add_SourceCodeViewer().open(reportFile);
19   return  catNet output();
```

Invoke and Result

Execute

stop execution

Output

```
Info : Starting analysis [1 modules]
Info : Analyzing module SuperSecureBank...
Info : 1 File Canonicalization issues found.
Info : 6 Redirection to User Controlled Site issues found.
Info : Analysis completed.
```

Invoking Scan workflow directly (from assembly or file)

```
var testFile = "SuperSecureBank.dll".local();
var reportFile = tempDir.pathCombine("SSB.xml");
var graphMl = tempDir.pathCombine("SSB.graphml");
var catNet = new API_CatNet();

catNet.save_Report_To(reportFile)
        .loadRules();

var analysisEngine = catNet.Engine.AnalysisEngine;
analysisEngine.BeginAnalysis();

var cci = "CatNet_1.1/SourceDir/Microsoft.Cci.dll".assembly();
var assemblyNode = cci.type("AssemblyNode");
var assemblyToScan = testFile.assembly();
var module = assemblyNode.invokeStatic("GetAssembly", assemblyToScan);
analysisEngine.invoke("AnalyzeModule", module);
analysisEngine.FinalizeState();
catNet.Engine.RulesEngine.Process(analysisEngine);
analysisEngine.EndAnalysis();
catNet.Engine.SaveReport();

analysisEngine.ResetState();
//var module = assemblyNode.invokeStatic("GetAssembly", testFile);
return module;
catNet.analyze(testFile).output();
catNet.Engine.details();

return "ok";
```

Command To Execute

```
14  var analysisEngine = catNet.Engine.AnalysisEngine;
15  analysisEngine.BeginAnalysis();
16
17  var cci = "CatNet_1.1/SourceDir/Microsoft.Cci.dll".assembly();
18  var assemblyNode = cci.type("AssemblyNode");
19  var assemblyToScan = testFile.assembly();
20  var module = assemblyNode.invokeStatic("GetAssembly", assembly?
21  analysisEngine.invoke("AnalyzeModule", module);
22  analysisEngine.FinalizeState();
23  catNet.Engine.RulesEngine.Process(analysisEngine);
24  analysisEngine.EndAnalysis();
25  catNet.Engine.SaveReport();
26
27  analysisEngine.ResetState();
28  //var module = assemblyNode.invokeStatic("GetAssembly", testFi?
```

Invoke and Result

Execute

stop execution

Output

▲ **Misc**
    Attributes   Microsoft.Cci.AttributeList
    ContractAssembly
    Documentation   System.Xml.XmlDocument
    EntryPoint
    ExportedTypes   Microsoft.Cci.TypeNodeList

Attributes

Log Viewer

```
[1:59:15 PM] INFO: [CatNetEvents] Info : 7 Cross-Site Scripting issues found.
[1:59:15 PM] INFO: [CatNetEvents] Info : 6 Redirection to User Controlled Site issues found.
[1:59:15 PM] INFO: [CatNetEvents] Info : 38 SQL Injection issues found.
[1:59:15 PM] INFO: [CatNetEvents] Info : 1 File Canonicalization issues found.
[1:59:15 PM] INFO: [CatNetEvents] Info : Analyzing module SuperSecureBank...
```

Simple API to scan files

```
var catNet = new API_CatNet();
catNet.save_Report_To(reportFile)
        .loadRules();

catNet.analyze(testFile.assembly());
catNet.analyze(testFile);
```

Inspector

Command To Execute

```
8   var graphMl = tempDir.pathCombine("SSB.graphml");
9
10  var catNet = new API_CatNet();
11  catNet.save_Report_To(reportFile)
12          .loadRules();
13
14  catNet.analyze(testFile.assembly());
15  catNet.analyze(testFile);
16
```

Invoke and Result

Execute

stop execution

Output

```
Info : Analyzing module SuperSecureBank...
Info : 1 File Canonicalization issues found.
Info : 37 SQL Injection issues found.
Info : 6 Redirection to User Controlled Site issues found.
Info : 7 Cross-Site Scripting issues found.
Info : Starting analysis [1 modules]
```

Log Viewer

```
[2:05:06 PM] DEBUG: Scanned file in :0s:676ms
[2:05:06 PM] INFO: [CatNetEvents] Info : Analysis completed.
[2:05:06 PM] INFO: [CatNetEvents] Info : 7 Cross-Site Scripting issues found.
[2:05:06 PM] INFO: [CatNetEvents] Info : 6 Redirection to User Controlled Site issues found.
[2:05:06 PM] INFO: [CatNetEvents] Info : 38 SQL Injection issues found.
[2:05:06 PM] INFO: [CatNetEvents] Info : 1 File Canonicalization issues found.
[2:05:06 PM] INFO: [CatNetEvents] Info : Analyzing module SuperSecureBank...
[2:05:06 PM] INFO: [CatNetEvents] Info : Starting analysis [1 modules]
[2:05:06 PM] DEBUG: Scanned assembly in :0s:559ms
[2:05:05 PM] INFO: [CatNetEvents] Info : 7 Cross-Site Scripting issues found.
[2:05:05 PM] INFO: [CatNetEvents] Info : 6 Redirection to User Controlled Site issues found.
[2:05:05 PM] INFO: [CatNetEvents] Info : 37 SQL Injection issues found.
[2:05:05 PM] INFO: [CatNetEvents] Info : 1 File Canonicalization issues found.
[2:05:05 PM] INFO: [CatNetEvents] Info : Analyzing module SuperSecureBank...
```
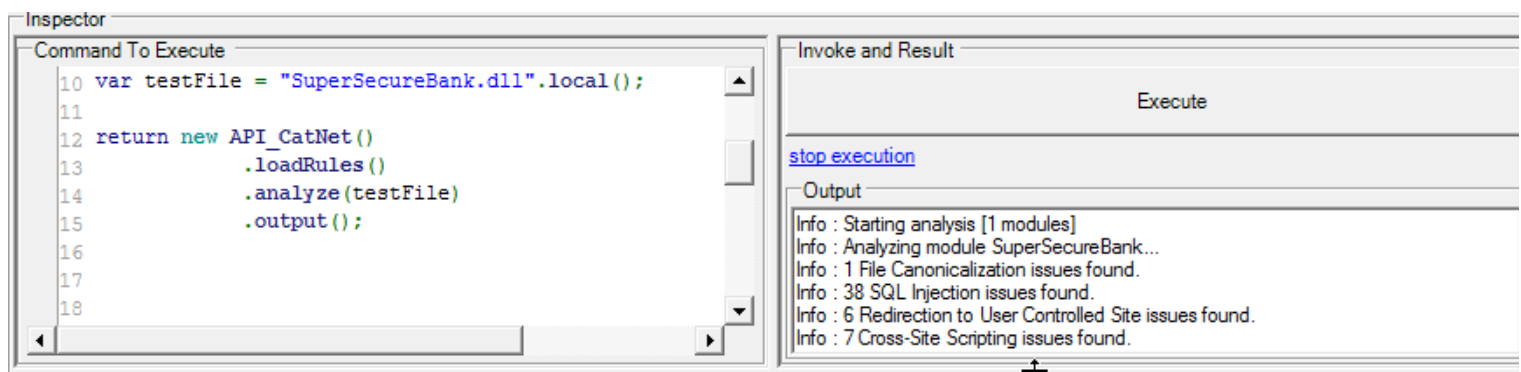
or just

```
var testFile = "SuperSecureBank.dll".local();

return new API_CatNet()
                .loadRules()
                .analyze(testFile)
                .output();
```

Command To Execute

```
10  var testFile = "SuperSecureBank.dll".local();

11

12  return new API_CatNet()
13              .loadRules()
14              .analyze(testFile)
15              .output();

16

17

18
```

Invoke and Result

Execute

stop execution

Output

```
Info : Starting analysis [1 modules]
Info : Analyzing module SuperSecureBank...
Info : 1 File Canonicalization issues found.
Info : 38 SQL Injection issues found.
Info : 6 Redirection to User Controlled Site issues found.
Info : 7 Cross-Site Scripting issues found.
```

Converting into O2Findings format and showing in O2Findings Viewer:

```
//var topPanel = O2Gui.open<Panel>("{name}",700,400);
var topPanel = panel.clear().add_Panel();


var tempDir = "_catNet_reports".tempDir(false);

var reportFile = tempDir.pathCombine("SSB.xml");
var findingsFile  = reportFile + ".findings";
//var testFile = "SuperSecureBank.dll".local();
var testFile = "SuperSecureBankService.dll".local();

new API_CatNet().loadRules()
                          .analyze(testFile);

var catNetConverter = new  CatNetConverter(reportFile);
catNetConverter.convert(findingsFile);

var findingsViewer = topPanel.add_FindingsViewer(true);
findingsViewer.load(findingsFile.loadFindingsFile());

//O2File:Findings_ExtensionMethods.cs
//using O2.XRules.Database.Findings
//using O2.Scanner.MsCatNet.Converter
//O2Ref:_O2_Scanner_MsCatNet.exe




var catNet = new API_CatNet();
catNet.save_Report_To(reportFile)
        .loadRules();

catNet.analyze(testFile);

return catNet.output();

return "ok";

return  catNet.output();
//using Microsoft.ACESec.CATNet.Core.Driver
 //O2File:API_CatNet.cs
//O2Ref:CatNet_1.1/SourceDir/Microsoft.ACESec.CATNet.Core.dll
//_O2Ref:CatNet_1.1/SourceDir/Microsoft.Cci.dll
//_O2Tag_DontAddExtraO2Files
```
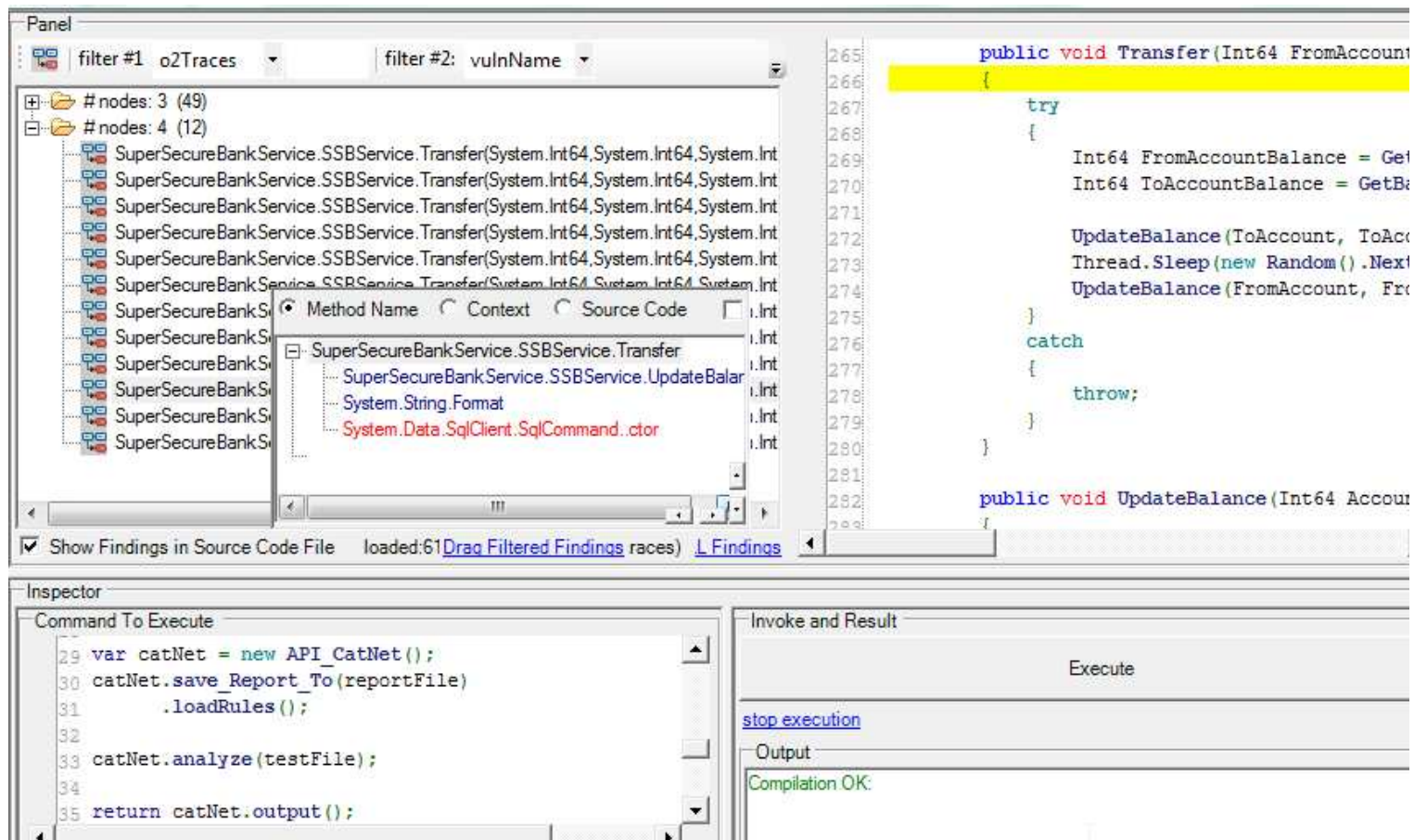
Simpler version to scan and view results

```
//var topPanel = O2Gui.open<Panel>("{name}",700,400);
var topPanel = panel.clear().add_Panel();

var tempDir = "_catNet_reports".tempDir(false);

var reportFile = tempDir.pathCombine("SSB.xml");
var findingsFile  = reportFile + ".findings";
//var testFile = "SuperSecureBank.dll".local();
var testFile = "SuperSecureBankService.dll".local();

new API_CatNet().loadRules()
                        .analyze(testFile);

topPanel.add_CatNet_FindingsViewer(reportFile);
return "ok";
//using Microsoft.ACESec.CATNet.Core.Driver
 //O2File:API_CatNet.cs
//O2Ref:CatNet_1.1/SourceDir/Microsoft.ACESec.CATNet.Core.dll
//_O2Ref:CatNet_1.1/SourceDir/Microsoft.Cci.dll
//_O2Tag_DontAddExtraO2Files
```

or just (this is the complete script)**:**

```
var topPanel = panel.clear().add_Panel();

var tempDir = "_catNet_reports".tempDir(false);

var reportFile = tempDir.pathCombine("SSB.xml");
var findingsFile  = reportFile + ".findings";
var testFile = "SuperSecureBankService.dll".local();

new API_CatNet().loadRules()
                .analyze(testFile)
                .show(topPanel);

return "done";

//O2File:API_CatNet.cs
```

13

Panel

filter #1 vulnType ▾   filter #2: vulnName ▾ drag selected node text

```
☐ 🗁 SQL Injection (58)
      SuperSecureBankService.SSBService.CheckUser(System.String,System.String)
      SuperSecureBankService.SSBService.CheckUser(System.String,System.String)
      SuperSecureBankService.SSBService.CheckUser(System.String,System.String)
      SuperSecureBankService.SSBService.CheckUser(System.String,System.String)
      SuperSe
      SuperSe   ● Method Name  ○ Context  ○ Source Code  ☐ Show Trace in Sour
      SuperSe
      SuperSe   ☐ SuperSecureBankService.SSBService.CheckUser
      SuperSe       System.String.Format
      SuperSe       System.Data.SqlClient.SqlCommand..ctor
```

☐ Show Findings in Source Code File   loaded:58, after te: Drag Filtered Findings Drag ALL Findings ◄

```
72          {
73              userName = reader.GetString(0);
74          }
75      }
76      return userName;
77  }
78
79  public Int64 CheckUser(string username, string passw
80  {
81      Int64 userID = 0;
82
83      string getUserID = "SELECT userID FROM Users WHE
84      using (SqlConnection conn = new SqlConnection(Con
```

Inspector

Command To Execute

```
1  //var topPanel = O2Gui.open<Panel>("{name}",700,400);
2  var topPanel = panel.clear().add_Panel();
3
4  var tempDir = "_catNet_reports".tempDir(false);
5
6  var reportFile = tempDir.pathCombine("SSB.xml");
7  var findingsFile  = reportFile + ".findings";
8  var testFile = "SuperSecureBankService.dll".local();
9
10 new API_CatNet().loadRules()
11                 .analyze(testFile)
12                 .show(topPanel);
13
14 return "done";
15
16 //O2File:API_CatNet.cs
```

Invoke and Result

Execute

stop execution

Output

Compilation OK: