



PLATFORM

PRESENTED BY DINIS CRUZ

LONDON UK – THURSDAY, SEPTEMBER 3 2009

before we start

# my dedication to OWASP :)

I returned 3 days earlier from Portugal to participate on London Chapter event

... kids were not impressed (photo before boarding plane 5 hours ago) ...



# OBJECTIVE OF TODAY'S SESSION

---

-  O2 developer
-  senior consultant
-  security consultant
-  analyst
-  manager

GEEK-O-METER

## WHAT AM I DOING HERE?

---

- I'm making the business case for you to:

**focus,**

**invest time & resources,**

**use,**

**contribute** and maybe even

**sponsor**

the ***OWASP O2 Platform*** project



# WHAT IS O2?

and the OWASP O2 PLATFORM

---

-  O2 developer
-  senior consultant
-  security consultant
-  analyst
-  manager

GEEK-O-METER



is an:

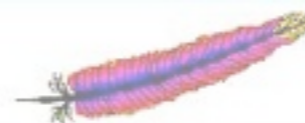


# OPEN PLATFORM.



## License Agreement

Please read the following license agreement carefully.



Apache License  
Version 2.0, January 2004  
<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

I accept the terms in the license agreement



for  
**AUTOMATING.**

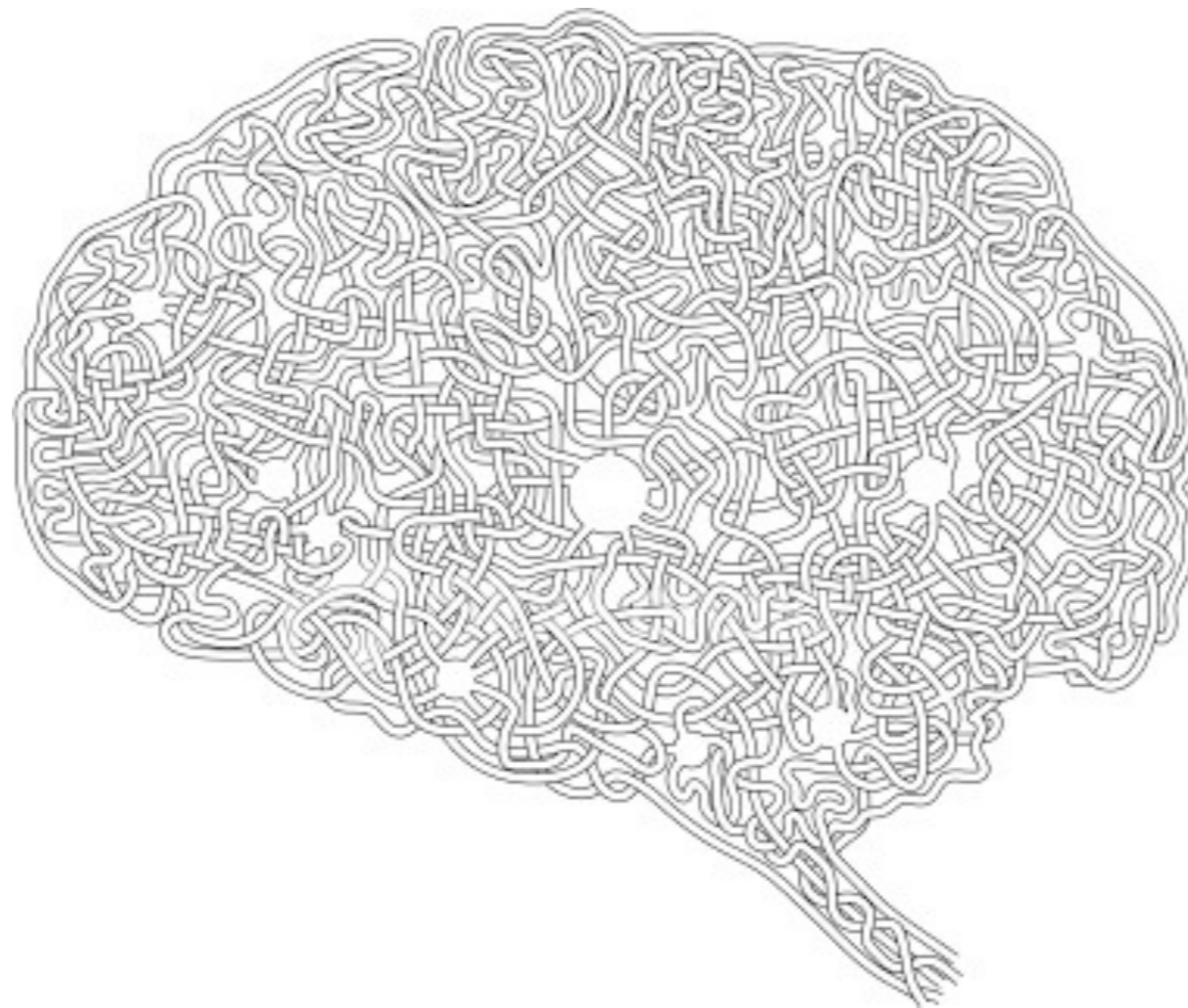


# APPLICATION SECURITY.





# KNOWLEDGE.



# and WORKFLOWS.

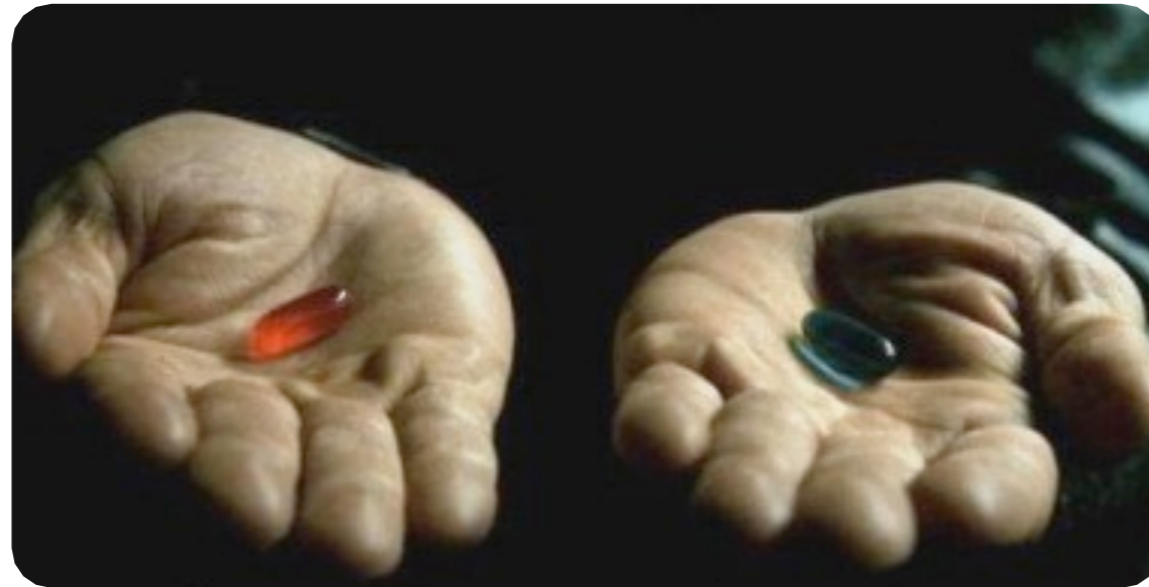


 is an:



**OPEN PLATFORM**  
**for**  
**AUTOMATING**  
**APPLICATION SECURITY**  
**KNOWLEDGE**  
**and**  
**WORKFLOWS**

... and when you start using it ...



... you will be able to do impossible things ...





and your clients will love you



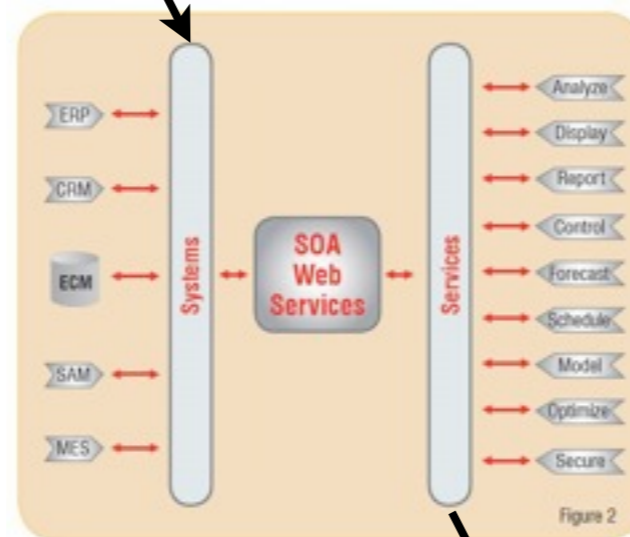
<http://007.dn.ru>



# 'Joined trace' example (before):

```

[-] HacmeBank_v2_Website.ascx.AccountTransfer.Page_Load(object;System.EventArgs):void
  [-] System.Web.UI.UserControl.get_Session():System.Web.SessionState.HttpSessionState
    [-] System.Web.SessionState.HttpSessionState.get_Item(string):object
      [-] System.Object.ToString():string
        [-] HacmeBank_v2_Website.Gui.populateDropDownListWithListOfUserAccounts(System.Web.UI.WebControls.DropDownList;string):void
          [-] HacmeBank_v2_Website.AccountManagement.WS_GetUserAccounts_using_UserID(string;string):object[]
            [-] HacmeBank_v2_Website.WS_AccountManagement.WS_AccountManagement.GetUserAccounts_using_UserID(string;string):object[]
              [-] System.Web.Services.Protocols.SoapHttpClientProtocol.Invoke(string;object[]):object[]
  
```



Example of two separate  
Traces of an  
HacmeBank  
Web Service call  
(vulnerable to SQL Injection)

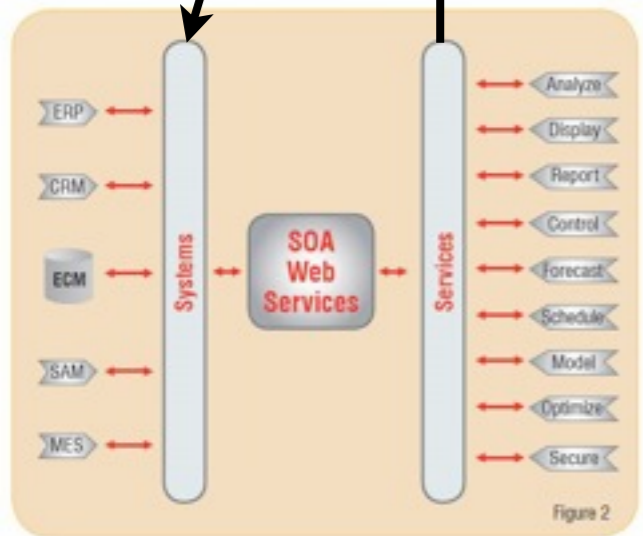
```

[-] HacmeBank_v2_WS.WS_AccountManagement.GetUserAccounts_using_UserID(string;string):System.Collections.ArrayList
  [-] HacmeBank_v2_WS.DataFactory.GetUserAccounts_using_userID(string):System.Collections.ArrayList
    [-] System.String.Concat(string;string):string
      [-] HacmeBank_v2_WS.SqlServerEngine.returnArrayListFromSQLQuery_containing_FirstFieldFromAllRows(string):System.Collections.ArrayLis
        [-] HacmeBank_v2_WS.SqlServerEngine.executeSqlCommand_returnSqlDataReader(string):System.Data.SqlClient.SqlDataReader
          [-] System.Data.SqlClient.SqlCommand.SqlCommand(string;System.Data.SqlClient.SqlConnection):void
            System.Data.SqlClient.SqlCommand.ExecuteReader():System.Data.SqlClient.SqlDataReader
  
```

# 'Joined trace' example (after):

```

[-] HacmeBank_v2_Website.ascx.AccountTransfer.Page_Load(object;System.EventArgs):void
  [-] System.Web.UI.UserControl.get_Session():System.Web.SessionState.HttpSessionState
    [-] System.Web.SessionState.HttpSessionState.get_Item(string):object
      [-] System.Object.ToString():string
        [-] HacmeBank_v2_Website.Gui.populateDropDownListWithListOfUserAccounts(System.Web.UI.WebControls.DropDownList:string):void
          [-] HacmeBank_v2_Website.AccountManagement.WS_GetUserAccounts_using_UserID(string:string):object[]
            [-] HacmeBank_v2_Website.WS_AccountManagement.WS_AccountManagement.GetUserAccounts_using_UserID(string:string):object[]
              [-] System.Web.Services.Protocols.SoapHttpClientProtocol.Invoke(string;object[]):object[]
                [-] HacmeBank_v2_WS.WS_AccountManagement.GetUserAccounts_using_UserID(string:string):System.Collections.ArrayList
                  [-] HacmeBank_v2_WS.DataFactory.GetUserAccounts_using_userID(string):System.Collections.ArrayList
                    [-] System.String.Concat(string:string):string
                      [-] HacmeBank_v2_WS.SqlServerEngine.returnArrayListFromSQLQuery_containing_FirstFieldFromAllRows(string):System.Collections.ArrayList
                        [-] HacmeBank_v2_WS.SqlServerEngine.executeSqlCommand_returnSqlDataReader(string):System.Data.SqlClient.SqlDataReader
                          [-] System.Data.SqlClient.SqlCommand.SqlCommand(string;System.Data.SqlClient.SqlConnection):void
                            ..... System.Data.SqlClient.SqlCommand.ExecuteReader():System.Data.SqlClient.SqlDataReader
  
```



Example of a single  
 'Joined Trace' of the same  
 HacmeBank  
 Web Service call  
 (vulnerable to SQL Injection)



# TECHNOLOGIES SUPPORTED by O2

---

-  O2 developer
-  senior consultant
-  security consultant
-  analyst
-  manager

GEEK-O-METER

## Supported Technologies

---

- **Ounce Labs Scanner:** (FULL Support): scanning, CIR consumption, rules creation, open & save findings format). Languages: .NET, Java, C/C++, ASP Classic, VB 6.0
- **IBM AppScan Developer Edition:** open findings format. Language: Java
- **Microsoft CAT.NET scanner:** scanning, open findings format. Language: .NET (C#, VB.net, Iron Phyton, etc...)
- **FindBugs scanner:** open findings format. Language: Java
- **OWASP CodeCrawler:** open findings format. Language: .NET
- **Fortify (very early stages) :** open findings format (FVDL). Language: .NET, Java, C/C++, etc..
- **.NET** - create CIR, create call flow traces, create run-time traces
- **Java** - create CIR, create call flow traces
- **Spring MVC 'Annotation Based Controllers'** - Model controllers behavior, drive BlackBox tests

## So what can O2 do for Advanced Users

---

- This is for users who know what they (technically) want do
- These are the users that ALL/MOST tool vendors don't cater for today (since they are not a big enough market)
- The following (are some of the) problems that O2 has solutions for:
  - Advanced findings filtering (for example query 50M to 500Mb assessment files)
  - Visualizing traces
  - Mass rule creation & management
  - “Rules Driven Scans”
  - Creating ALL Traces
  - Joining and Manipulating Traces
  - Scripting questions and workflows (on top of rich objects like CirData, Findings or Rules)
  - Gain visibility into Frameworks
  - Understand and exploit Spring MVC apps
  - Integrate complex workflows with SDLs
  - Do Virtual Patching
  - Quickly Write PoCs and exploits using O2's .NET's power Debugger
  - Create “Run-time traces”
  - Write Unit Tests for PoCs
  - Find (via instrumenting and automating the security consultant's brain) all sorts of application security issues (like to ones in the OWASP Top 10)
  - Start venturing into Source-Code-Fixing for vulnerabilities found
  - Start venturing into auto-writing WAF rules for vulnerabilities found





# O2 MODULES

---

-  O2 developer
-  senior consultant
-  security consultant
-  analyst
-  manager

GEEK-O-METER

## O2 MODULES - DEVELOPMENT STATE

---

### ACTIVE

- O2 Tool - Findings Viewer
- O2 Tool - CirViewer
- O2 Tool - Rules Manager
- O2 Cmd - Findings Filter
- O2 Cmd - Spring MVC
- O2 Tool - Join Traces
- O2 Debugger Mdbg
- O2 Tool - CSharpScripts
- O2 Scanner - MsCatNet
- O2 Tool - Host Local Website
- O2 Tool - Java Execution
- O2 Tool - O2 Scripts
- O2 Tool - Python
- O2 Tool - Search Engine

### LEGACY

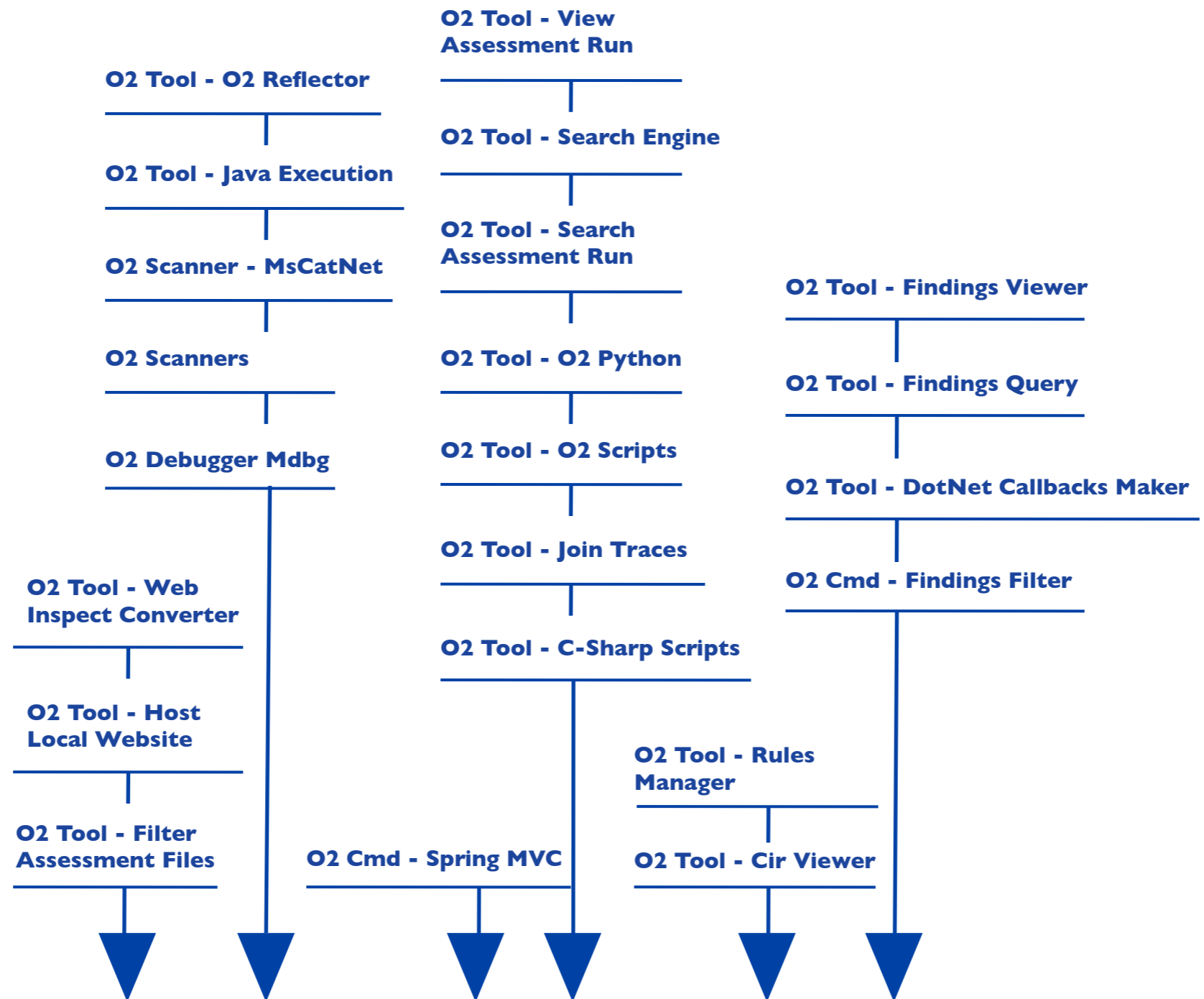
- O2 Scanners
- O2 Tool - DotNet Callbacks Maker
- O2 Tool - Findings Query
- O2 Tool - Search Assessment Run
- O2 Tool - View Assessment Run
- O2 Tool - WebInspect Converter

Vaporware

- O2 Tool - Filter Assessment Files
- O2 Tool - O2 Reflector



# O2 MODULES - MATURITY



**UNSOLVED  
PROBLEM**

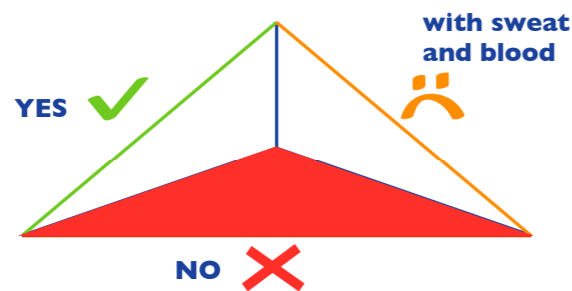
**SOLVED**

**PROTOTYPE**

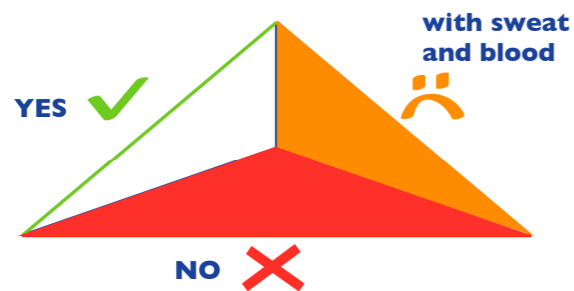
**VERSION 1.0**

## O2 MODULES - FEATURE COMPARISON WITH OSA

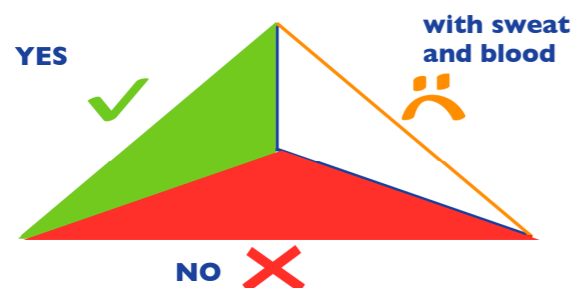
- This graph maps the module's features to the current version of Ounce's 6.x OSA (Ounce Security Analyst)



- O2 Tool - Rules Manager
- O2 Tool - CirViewer
- O2 Cmd - Spring MVC
- O2 Debugger Mdbg
- O2 Tool - CSharpScripts
- O2 Scanner - MsCatNet
- O2 Tool - Host Local Website
- O2 Tool - Java Execution
- O2 Tool - Join Traces
- O2 Tool - O2 Reflector
- O2 Tool - O2 Scripts
- O2 Tool - Python
- O2 Tool - WebInspect Converter



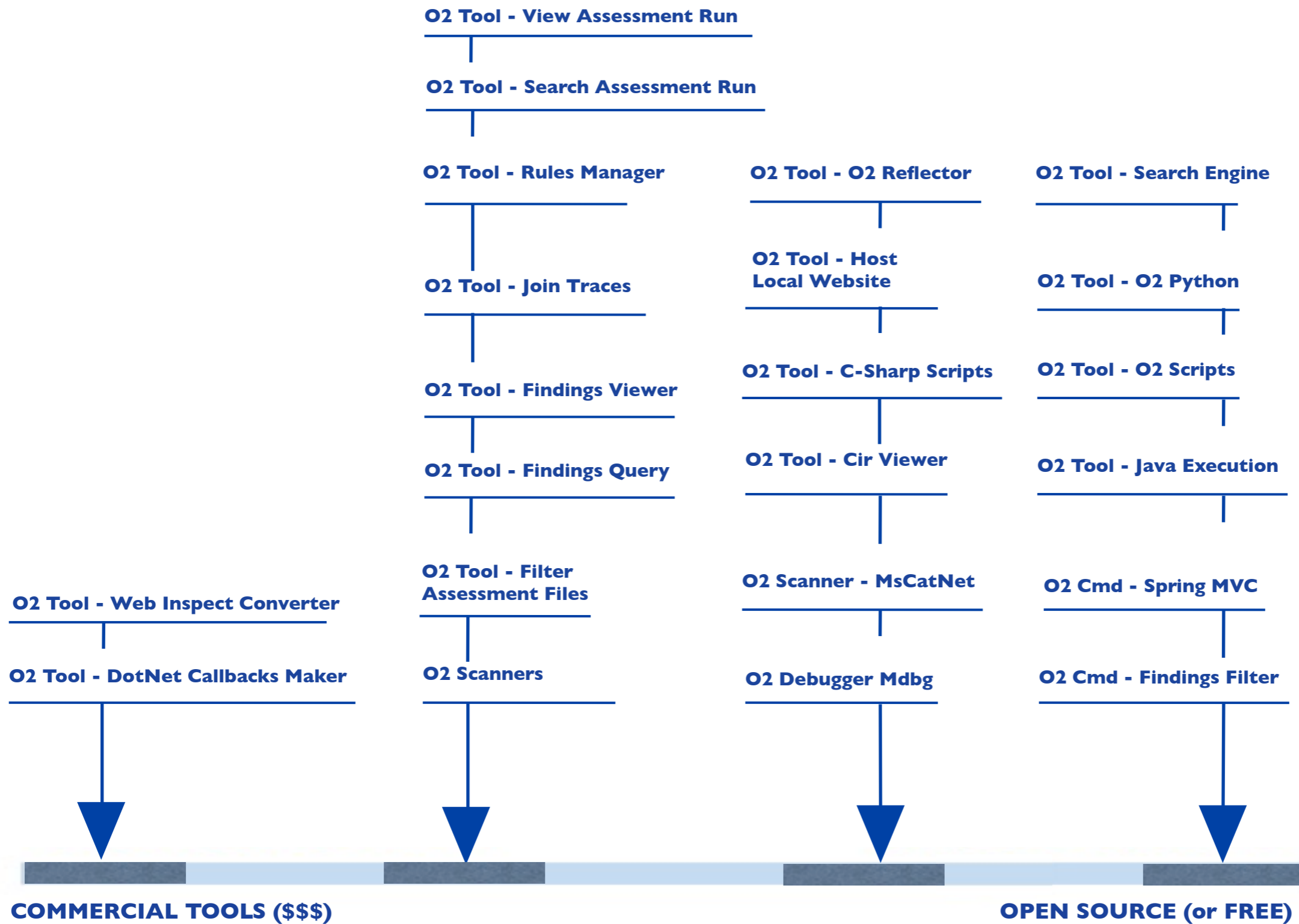
- O2 Tool - Findings Viewer
- O2 Cmd - Findings Filter
- O2 Tool - Findings Query
- O2 Tool - DotNet Callbacks Maker
- O2 Tool - Filter Assessment Files
- O2 Tool - Search Engine
- O2 Tool - Search Assessment Run
- O2 Tool - View Assessment Run



- O2 Scanners



# O2 MODULES - COMMERCIAL SOFTWARE DEPENDENCIES







# O2 MODULES DETAILS

---

-  O2 developer
-  senior consultant
-  security consultant
-  analyst
-  manager

GEEK-O-METER

## ACTIVE O2 MODULES (6X)

---

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>

for individual slides with O2 Modules details

# ACTIVE O2 MODULES (6X)

ACTIVE
MODULE:

### O2 Cmd - Findings Filter

**DESCRIPTION**  
 This O2 module shows how command line tools can be easily created to provide specific functionality (based on business requirements) which can then be easily integrated on an SDL.  
 This module takes advantage of the highly flexible O2 Findings Object model. A GUI is provided to execute and customize the implemented filters

**KEY / UNIQUE FEATURES**

- Filters implemented: `onlyTraces`, `noTraces`, `allFindings`, `onlyHighs`, `onlyVulnerabilities`, `oneFilePerConfidence`, `uniqueTraces`
- Ability to create assessments files that can be published
- Ability to dynamically compile and execute custom filters

**USE CASES**

- SDL Integration
- Custom Findings Filtering

**PRODUCTIZATION READINESS**

UNRESOLVED PROBLEM   SOLVED   PROTOTYPE

▲

**CAN OSA DO THIS?**

YES ✓   NO ✗

with oosa and blood

**COMMERCIAL SOFTWARE DEPENDENCIES:**  
 Consumes `o2asm` files created by Ounce (& others)

IBM / COMMERCIAL TOOLS (BEE)      OPEN SOURCE (FREE)

**ROADMAP: NEXT DEVELOPMENT**

- Add support for the other 'O2 Supported' Scripting languages (`IronPython`, `Python`, `Java`)
- Add more sample scripts
- Document functionality and O2's command line tools architecture
- Fix bug with Unique Traces filter (as reported by Eduardo)
- Run on Mono (& Linux and Mac)

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>

for individual slides with O2 Modules details

# ACTIVE O2 MODULES (6X)

**ACTIVE**

MAIN GUI

**MODULE: O2 Cmd - Findings Filter**

**DESCRIPTION**  
This O2 module shows how command line tools can be easily created to resemble

**ACTIVE**

MAIN GUI

**MODULE: O2 Cmd - Spring MVC**

**DESCRIPTION**  
Specifically targeted at the Java Spring MVC framework, this module is able to analyze an application written under this framework and extract its attack surface and exposed internal objects. In addition to powerful visualization tools for the data collected, this module also contains a simple 'analysis engine' which creates Spring MVC related Findings

**KEY / UNIQUE FEATURES**

- Supports and understand Spring MVC's Java Annotations: @Controller, @ModelAttribute, @RequestParam
- Creates complete representations of Spring MVC binded objects
- Creates finding with references to controller's source code
- Loads \*.class, \*.jar and \*.war files

**USE CASES**

- Security review of Spring MVC Application

**GEEK-O-METER**

03	developer
02	senior consultant
01	security consultant
00	analyst
00	manager

**PRODUCTIZATION READINESS**

UNSOLVED PROBLEM	SOLVED	PROTOTYPE
------------------	--------	-----------

**CAN OSA DO THIS?**

**COMMERCIAL SOFTWARE DEPENDENCIES:**

NON / COMMERCIAL TOOLS (\$\$\$)	OPEN SOURCE (FREE)
---------------------------------	--------------------

**ROADMAP: NEXT DEVELOPMENT**

- Add support for other Spring MVC binding
- Export URL mappings for consumption by other tools (AppScan, O2 JoinTraces)
- Map current controllers mappings into joined findings
- Add support for auto unit test creation & execution

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>  
for individual slides with O2 Modules details

# ACTIVE O2 MODULES (6X)

**ACTIVE MODULE: O2 Cmd - Findings Filter**

**DESCRIPTION**  
This O2 module shows how command line tools can be easily created to resolve

**ACTIVE MODULE: O2 Cmd - Spring MVC**

**DESCRIPTION**  
Specifically targeted at the Java Spring MVC framework, this module is able to

**ACTIVE MODULE: O2 Debugger Mdbg**

**DESCRIPTION**  
Managed wrapper on top of Microsoft's managed debugger. This module allows the easy debugging of .NET applications (started or hooked into processes). The power of this module lies on the wrapping of the 'command line' Managed debugger interface into a GUI & a scriptable environment.

**KEY / UNIQUE FEATURES**

- Ability to 'Animate Tracing' (StepInto, StepOver, StepOut)
- Record traces, Modify values on breakpoints, view object model (via reflection) of running processes
- Mass break breakpoint creation
- Allows easy exploit creation and auto-patching of vulnerabilities

**USE CASES**

- .NET framework debugging
- Vulnerability exploit writing

**PRODUCTION READINESS**

UNRESOLVED PROBLEM → SOLVED → PROTOTYPE

**CAN OSA DO THIS!**

YES ✓ (with sweat and blood) / NO ✗

**COMMERCIAL SOFTWARE DEPENDENCIES:**

Free Microsoft Managed Debugger demo application

OWN / COMMERCIAL TOOLS (\$\$\$) | OPEN SOURCE (FREE)

**ROADMAP: NEXT DEVELOPMENT**

- Implement the same capabilities for Java and Python
- Add ability to trace into unmanaged traces
- Improve trace creation process and data collection
- Improve patching & hooking workflow

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>  
for individual slides with O2 Modules details

# ACTIVE O2 MODULES (6X)

## O2 Cmd - Findings Filter

**DESCRIPTION**  
This O2 module shows how command line tools can be easily created to resolve

## O2 Cmd - Spring MVC

**DESCRIPTION**  
Specifically targeted at the Java Spring MVC framework, this module is able to

## O2 Debugger Mdbg

**DESCRIPTION**  
Managed wrapper on top of Microsoft's manager debugger

## O2 Scanner - MsCatNet

**DESCRIPTION**  
Module that allows the scanning of .NET applications using the freely available Microsoft's CATNET Scanner with the results being converted into the O2 Findings Format (o2asmf compatible)  
This module allows CATNET users to benefit from O2's powerful findings filtering and manipulation

**KEY / UNIQUE FEATURES**

- Ability to scan (recursively) entire directories
- Ability to convert CATNET results into O2 Findings Schema
- Uses the Firefox Engine to render the webpages shown when the user is asked to install CATNET

**USE CASES**

- Scan of .NET projects by users with no access to Ounce 6.x

**GEEK-O-METER**

- OO developer
- senior consultant
- security consultant
- analyst
- manager

**PRODUCTIZATION READINESS**

UNRESOLVED PROBLEMS SOLVED PROTOTYPE

**CAN OSA DO THIS?**

YES ✓ with sweat and blood  
NO ✗

**COMMERCIAL SOFTWARE DEPENDENCIES:**

Uses Microsoft's free CATNET software

OPEN / COMMERCIAL TOOLS (FREE) OPEN SOURCE (FREE)

**ROADMAP: NEXT DEVELOPMENT**

- Map O2 rules format into CATNET (with both import and export capabilities)
- Add support to compile .NET solutions files from the GUI (this capability already exists in O2)
- Add more links to related Microsoft and CATNET documentation
- Add visualization of for CATNET created traces representation

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>  
for individual slides with O2 Modules details



# ACTIVE O2 MODULES (6X)

**ACTIVE MODULE: O2 Cmd - Findings Filter**

**DESCRIPTION**  
This O2 module shows how command line tools can be easily created to resolve

**ACTIVE MODULE: O2 Cmd - Spring MVC**

**DESCRIPTION**  
Specifically targeted at the Java Spring MVC framework, this module is able to

**ACTIVE MODULE: O2 Debugger Mdbg**

**DESCRIPTION**  
Managed wrapper on top of Microsoft's manager debugger

**ACTIVE MODULE: O2 Scanner - MsCatNet**

**DESCRIPTION**  
Module that allows the scanning of .NET applications using the freely available

**ACTIVE MODULE: O2 Tool - Cir Viewer**

**DESCRIPTION**  
This module allows the the creation (.NET) and visualization (all Ounce supported languages) of CIR (O2's version of Ounce's Common Intermediate Representation) By exposing the CIR object model in a powerful GUI (and programmatically object model), this module allows O2 users to gain a much wider understanding of the application under analysis. It is also possible to create O2 Findings from CIR data.

**KEY / UNIQUE FEATURES**

- Ability to consume CIR created from all languages supported by the Ounce 6.x engine
- Ability to create CIR from .NET (and very soon) Java class files
- Recursive mapping of function callers, Function Callee's and SuperClasses/Interfaces

**USE CASES**

- Visualize an application object model
- Create call-flow traces (i.e. findings) from CIR

**GEEK-O-METER**

02 developer
senior consultant
security consultant
analyst
manager

**PRODUCTIZATION READINESS**

UNSOLVED PROBLEM	SOLVED	PROTOTYPE
------------------	--------	-----------

**CAN OSA DO THIS?**

YES ✓ (with sweat and blood)

NO ✗

**COMMERCIAL SOFTWARE DEPENDENCIES:**

Uses Ounce's created CIR.

02 / COMMERCIAL TOOLS (0%)	OPEN SOURCE (100%)
----------------------------	--------------------

**ROADMAP: NEXT DEVELOPMENT**

- Convert O2 CirData representation into the (under development) OIR (Open Intermediate Representation) Schema
- Add support for CirData creation for Java class files (functionality already available in the O2 Spring MVC module)

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>  
for individual slides with O2 Modules details

# ACTIVE O2 MODULES (6X)

**ACTIVE MODULE: O2 Cmd - Findings Filter**

**DESCRIPTION**  
This O2 module shows how command line tools can be easily created to resolve

**ACTIVE MODULE: O2 Cmd - Spring MVC**

**DESCRIPTION**  
Specifically targeted at the Java Spring MVC framework, this module is able to

**ACTIVE MODULE: O2 Debugger Mdbg**

**DESCRIPTION**  
Managed wrapper on top of Microsoft's managed debugger

**ACTIVE MODULE: O2 Scanner - MsCatNet**

**DESCRIPTION**  
Module that allows the scanning of .NET applications using the freely available

**ACTIVE MODULE: O2 Tool - Cir Viewer**

**DESCRIPTION**  
This module allows the the creation (.NET) and visualization (all Ounce supported)

**ACTIVE MODULE: O2 Tool - C-Sharp Scripts**

**DESCRIPTION**  
This module is designed to help writing O2 modules in O2. It provides a full compilation and debugging environment (using the same modules as the O2 Debugger (Mdbg) module) and allows advanced users to write powerful scripts on top of the O2 Object model

**KEY / UNIQUE FEATURES**

- Write analysis scripts (i.e. custom modules) on a managed language (C#)
- Ability to hook and control the debugging engine (which is how the O2 virtual patching occurs)

**USE CASES**

- Advanced debugging of .NET & ASP.NET applications
- Exploit development and Virtual patching

**PRODUCTIZATION READINESS**

UNSOLVED PROBLEM | SOLVED | PROTOTYPE

**CAN OSA DO THIS?**

YES ✓ | NO ✗

**COMMERCIAL SOFTWARE DEPENDENCIES:**

Free Microsoft Managed Debugger demo application

IBM / COMMERCIAL TOOLS (O2) | OPEN SOURCE (FREE)

**ROADMAP: NEXT DEVELOPMENT**

- Integrate with the O2 Scripts module in order to create a single scripting environment for O2
- Lazy load required scripting and debugging engines

O2 logo

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>  
for individual slides with O2 Modules details

## ACTIVE O2 MODULES (6X)

---

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>

for individual slides with O2 Modules details

# ACTIVE O2 MODULES (6X)

ACTIVE
MODULE:

### O2 Tool - Java Execution

**DESCRIPTION**  
Module that allows users to access the rich O2 object model from Java. Although the code written in Java will seem to have FULL access to the O2 Object model, under the hood Java [bytecode] is converted (using IKVM) into .NET byte code, who is then able to access and consume directly the O2 modules used (IKVM has a built in tool that creates jar stubs from .NET assemblies)

**KEY / UNIQUE FEATURES**

- Wraps IKVM and allows the easy creation of the dependencies required to write O2 Modules in Java (making it easy to script O2 from Eclipse)
- Adds to O2 Scripting module the ability to write and execute Java code

**USE CASES**

- Write custom scripts in Java that access or manipulate data stored in O2 Objects

**PRODUCTIZATION READINESS**

UNSOLVED PROBLEM    SOLVED    PROTOTYPE

**CAN OSA DO THIS?**

YES ✓    NO ✗

with sweat and blood

**COMMERCIAL SOFTWARE DEPENDENCIES:**

IBM / COMMERCIAL TOOLS (OVC)    OPEN SOURCE (FREE)

**ROADMAP: NEXT DEVELOPMENT**

- Further automate the process of using IKVM in O2
- Auto configure Eclipse so that developers can use it (Eclipse) to write and execute their (written) Java code

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>  
for individual slides with O2 Modules details

# ACTIVE O2 MODULES (6X)

**ACTIVE**

MAIN GUI

**MODULE: O2 Tool - Java Execution**

**DESCRIPTION**  
Module that allows users to access the rich O2 object model from Java. Although...

**ACTIVE & LEGACY**

MAIN GUI

**MODULE: O2 Tool - Join Traces**

**DESCRIPTION**  
This module provides a PoC (Proof of Concept) for how traces can be joined together based on simple string mappings ("join traces when the Sink on trace A matches the Source on trace B") or web services mappings ("join traces when the sink from trace from the web layer scan matches the source of the web services layer")

**KEY / UNIQUE FEATURES**

- Join separate traces based on a simple string criteria
- Automatically handle the joining of .NET web services

**USE CASES**

- Create traces that cross multiple logical or physical boundaries and create highly-actionable findings

**PRODUCTIZATION READINESS**

**CAN OSA DO THIS?**

**COMMERCIAL SOFTWARE DEPENDENCIES:**  
Joins traces created by Ounce and others

**ROADMAP: NEXT DEVELOPMENT**

- Convert Join algorithm in new O2 Findings Format
- Add support for more automatic Traces joins (getters & setters, `SetAttribute`, `MatchTags`, etc.)

**GEEK-O-METER**

- OO developer
- senior consultant
- security consultant
- analyst
- manager

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>  
for individual slides with O2 Modules details



# ACTIVE O2 MODULES (6X)

**ACTIVE**

MAIN GUI

**MODULE: O2 Tool - Java Execution**

**DESCRIPTION**  
Module that allows users to access the rich O2 object model from Java. Although

**ACTIVE & LEGACY**

MAIN GUI

**MODULE: O2 Tool - Join Traces**

**DESCRIPTION**  
This module provides a PoC (Proof of Concept) for how traces can be joined

**ACTIVE**

MAIN GUI

**MODULE: O2 Tool - O2 Scripts**

**DESCRIPTION**  
Lightweight O2 scripting environment that supports scripting in .NET, Java, Python and Iron Python

**KEY / UNIQUE FEATURES**

- Supports multiple engines
- Exposes O2 Object model

**USE CASES**

- Quickly write Python scripts that consume the O2 engines and access Java Jars or .NET assemblies

**PRODUCTIZATION READINESS**

UNSOLVED PROBLEM SOLVED PROTOTYPE

**CAN OSA DO THIS?**

YES ✓ NO ✗

with sweat and blood

**COMMERCIAL SOFTWARE DEPENDENCIES:**

IBM / COMMERCIAL TOOLS (€€€) OPEN SOURCE (FREE)

**ROADMAP: NEXT DEVELOPMENT**

- Add Intellisense to C# editing environment
- Add support for unit test creation and execution

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>  
for individual slides with O2 Modules details

Saturday, 5 September 2009

# ACTIVE O2 MODULES (6X)

**ACTIVE**

MAIN GUI

**MODULE: O2 Tool - Java Execution**

**DESCRIPTION**  
Module that allows users to access the rich O2 object model from Java. Although

**ACTIVE & LEGACY**

MAIN GUI

**MODULE: O2 Tool - Join Traces**

**DESCRIPTION**  
This module provides a PoC (Proof of Concept) for how traces can be joined

**ACTIVE**

MAIN GUI

**MODULE: O2 Tool - O2 Scripts**

**DESCRIPTION**  
Lightweight O2 scripting environment that supports scripting in .NET, Java, IronPython

**ACTIVE**

MAIN GUI

**MODULE: O2 Tool - Python**

**DESCRIPTION**  
O2 module that allows the quick creation and execution of Python scripts in IronPython (.NET) or CPython (C). An interactive Shell is also provided for IronPython and Jython.

**KEY / UNIQUE FEATURES**

- GUI based interactive shell for IronPython and Jython
- Opens external shells and supports dynamic scripting and execution for IronPython, Jython and CPython

**USE CASES**

- Quickly write scripts that consume the O2 engines in Python

**PRODUCTIZATION READINESS**

UNSOLVED PROBLEM | SOLVED | PROTOTYPE

**CAN OSA DO THIS!**

YES ✓ | NO ✗

with sweat and blood

**COMMERCIAL SOFTWARE DEPENDENCIES:**

100% / COMMERCIAL TOOLS (100%) | OPEN SOURCE (FREE)

**ROADMAP: NEXT DEVELOPMENT**

- Integrate with a better Python editor
- Add Python debugging

**GEEN-O-METER**

O2 Developer  
Senior Consultant  
Security Consultant  
Analyst  
Manager

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>  
for individual slides with O2 Modules details

Saturday, 5 September 2009

# ACTIVE O2 MODULES (6X)

**ACTIVE MODULE: O2 Tool - Java Execution**

**DESCRIPTION**  
Module that allows users to access the rich O2 object model from Java. Although

**ACTIVE & LEGACY MODULE: O2 Tool - Join Traces**

**DESCRIPTION**  
This module provides a PoC (Proof of Concept) for how traces can be joined

**ACTIVE MODULE: O2 Tool - O2 Scripts**

**DESCRIPTION**  
Lightweight O2 scripting environment that supports scripting in .NET, Java, Python

**ACTIVE MODULE: O2 Tool - Python**

**DESCRIPTION**  
O2 module that allows the quick creation and execution of Python scripts in

**ACTIVE MODULE: O2 Tool - Rules Manager**

**DESCRIPTION**  
Very powerful O2 Module that allows the quick visualization, creation and editing of Ounce rules. The module supports the O2 Rule Pack format which can be used to import or export rules between different O2 or Ounce computers. This module supports the following common work flow: Scan application, create CIR, create rules from CIR, rescan application, create rules from scan findings

**KEY / UNIQUE FEATURES**

- Import rules from Ounce's MySQL database; powerful filtering; create or modify rules; commit changed rules to MySQL database; map CirData and Findings to existing rules; automatically create rules from CirData; Apply rules to findings without requiring rescan

**USE CASES**

- Advanced use of the Ounce Engine
- Use of O2's mini Call-Flow Analysis Engine

**KEY / UNIQUE FEATURES**

- O2 developer
- senior consultant
- security consultant
- analyst
- manager

GECK-O-METER

**PRODUCTIZATION READINESS**

UNSOLVED PROBLEM SOLVED PROTOTYPE

**CAN OSA DO THIS?**

YES ✓ NO ✗

with sweat and blood

**COMMERCIAL SOFTWARE DEPENDENCIES:**

Ounce MySQL rules database and Ounce Scanner

IBM / COMMERCIAL TOOLS (???) OPEN SOURCE (FREE)

**ROADMAP: NEXT DEVELOPMENT**

- Add support for rules diff (between O2 RulePacks or Ounce live databases)
- Simplify mature workflows by creating new simple GUIs with only 1 or 2 moving parts
- Move rules format into the (under development) ORDF (Open Rules Definition Language) Schema
- Add Oracle support (Ounce)

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>  
for individual slides with O2 Modules details

# ACTIVE O2 MODULES (6X)

**MODULE: O2 Tool - Java Execution**

**DESCRIPTION**  
Module that allows users to access the rich O2 object model from Java. Although...

**MODULE: O2 Tool - Join Traces**

**DESCRIPTION**  
This module provides a PoC (Proof of Concept) for how traces can be joined.

**MODULE: O2 Tool - O2 Scripts**

**DESCRIPTION**  
Lightweight O2 scripting environment that supports scripting in .NET, Java, Python.

**MODULE: O2 Tool - Python**

**DESCRIPTION**  
O2 module that allows the quick creation and execution of Python scripts in...

**MODULE: O2 Tool - Rules Manager**

**DESCRIPTION**  
Very powerful O2 Module that allows the quick visualization, creation and editing...

**MODULE: O2 Tool - Search Engine**

**DESCRIPTION**  
Simple tool to allow the quick `Regex` search of source files (source code, xml config files, etc...)  
During a normal engagement, this tool tends to be used very regularly (from helping to quickly find a particular text string to validating a source code finding)

**KEY / UNIQUE FEATURES**

- Ability to recursively import files from a drag and dropped directly (with quick filtering on file type and display of files size)
- Ability to run multiple searches and to quickly see its source code reference

**USE CASES**

- Text search of provided source code artifacts during security engagement

**PRODUCTIZATION READINESS**

UNSOLVED PROBLEM | SOLVED | PROTOTYPE

**CAN OSA DO THIS?**

YES ✓ | NO ✗

**COMMERCIAL SOFTWARE DEPENDENCIES:**

100% / COMMERCIAL TOOLS (YES) | OPEN SOURCE (FREE)

**ROADMAP: NEXT DEVELOPMENT**

- Create findings from Search results
- Save Search Criteria `Regex` as a Rule (create rule save format first)
- Allow boolean logic on
- Add 'Search by Proximity' feature

**GEEN-O-METER**

- 00 Developer
- Senior consultant
- Security consultant
- Analyst
- Manager

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>  
for individual slides with O2 Modules details



## LEGACY O2 MODULES (6X)

---

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>

for individual slides with O2 Modules details



# LEGACY O2 MODULES (6X)

LEGACY
MODULE:

MAIN GUI

### O2 Scanners

**DESCRIPTION**  
 O2 module that allows the easy triggering of scans using the Ounce CLI (Command Line Interface) or the Microsoft's CATNET Scanner. This module also contains an earlier version of the O2's Cir creation process and a special scanning mode (now discontinued) that aimed at generating ALL possible traces.

**KEY / UNIQUE FEATURES**

- Standard interface to trigger scans
- Drag & Drop scanning environment
- Ability to run a multi-pass scan (on the Ounce 6.x) engine that generates ALL possible traces
- Ability to manually control the CIR creation process

**USE CASES**

- Advanced O2 users that want to generate all traces or control the CIR creation process

**PRODUCTIZATION READINESS**

**CAN OSA DO THIS?**

**COMMERCIAL SOFTWARE DEPENDENCIES:**  
 Uses Ounce's and Microsoft's CATNET scanning engine

**ROADMAP: NEXT DEVELOPMENT**

- This module has been made redundant by the new version of Rules Manager and standalone CATNET scanning module

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>  
 for individual slides with O2 Modules details

# LEGACY O2 MODULES (6X)

**LEGACY**

MAIN GUI

**MODULE: O2 Scanners**

**DESCRIPTION**  
O2 module that allows the easy triggering of scans using the Ounce CLI

---

**MODULE: O2 Tool - DotNet Callbacks Maker**

**DESCRIPTION**  
Allow the automatic generation of Ounce 6.x rules (of type 'callback') for web services and public methods  
This module parses the provided .NET dlls (directly or by recursively searching a directory) and uses .NET reflection to identify public methods or methods marked with the [WebMethod] attribute (i.e. Web Services methods)

**KEY / UNIQUE FEATURES**

- Quickly identify public or web services methods
- Quickly create Ounce 6.0 rules for the identified methods

**USE CASES**

- Scanning .NET applications with .NET Web Services

**PRODUCTIZATION READINESS**

UNSOLVED PROBLEM   SOLVED   PROTOTYPE

**CAN OSA DO THIS!**

YES ✓   NO ✗

with sweat and blood

**COMMERCIAL SOFTWARE DEPENDENCIES:**

Connects to Ounce Rules Database

IBM / COMMERCIAL TOOLS (YES)   OPEN SOURCE (FREE)

**ROADMAP: NEXT DEVELOPMENT**

- This module has been made redundant by the new version of Rules Manager and standalone CATNET scanning module

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>

for individual slides with O2 Modules details

# LEGACY O2 MODULES (6X)

**LEGACY MODULE: O2 Scanners**

**DESCRIPTION**  
O2 module that allows the easy triggering of scans using the Ounce CLI

**LEGACY MODULE: O2 Tool - DotNet Callbacks Maker**

**DESCRIPTION**  
Allow the automatic generation of Ounce 6.x rules (of type 'callback') for web

**LEGACY MODULE: O2 Tool - Findings Query**

**DESCRIPTION**  
This module provides advanced findings filtering capabilities via a LAMDA like query. For example the user can use the following query to list all findings marked as vulnerabilities:  
`From O2Finding finding in O2Findings where finding.confidence == 1 select finding`

**KEY / UNIQUE FEATURES**

- Ability to write filters in a dynamically constructed LAMDA query
- High performance filtering engine allows quick analysis and (saving) of 100Mb+ assessment files

**USE CASES**

- Filtering large \*.o2assmt files
- Creating smaller o2assmt files based on LAMDA query results

**PRODUCTIZATION READINESS**

UNSOLVED PROBLEM   SOLVED   PROTOTYPE

**CAN OSA DO THIS?**

YES ✓   NO ✗

with sweat and blood

**COMMERCIAL SOFTWARE DEPENDENCIES:**

Consumes o2assmt files created by Ounce (& others)

OPEN / COMMERCIAL TOOLS (20%)   OPEN SOURCE (FREE)

**ROADMAP: NEXT DEVELOPMENT**

- This module was made redundant by the O2 Findings Viewer Module


see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>  
for individual slides with O2 Modules details

# LEGACY O2 MODULES (6X)

LEGACY

MAIN GUI

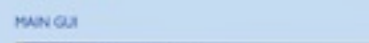


**MODULE: O2 Scanners**

**DESCRIPTION**  
O2 module that allows the easy triggering of scans using the Ounce CLI

LEGACY

MAIN GUI

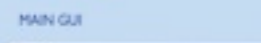


**MODULE: O2 Tool - DotNet Callbacks Maker**

**DESCRIPTION**  
Allow the automatic generation of Ounce 6.x rules (of type 'callback') for web

LEGACY

MAIN GUI

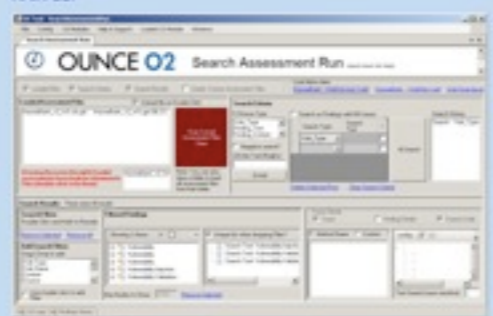


**MODULE: O2 Tool - Findings Query**

**DESCRIPTION**  
This module provides advanced findings filtering capabilities via a LAMDA like

LEGACY

MAIN GUI



**MODULE: O2 Tool - Search Assessment Run**

**DESCRIPTION**  
This was the first O2 module that fully supported the loading of multiple assessment files with powerful filtering capabilities (with support to save the filter results)  
This module (using the same engine as the O2 Tool - View Assessment Run) also provides a very powerful visualization tool which is able to visualize multiple traces at the same time (and visually identify common vulnerable code patterns)

**KEY / UNIQUE FEATURES**

- Load multiple assessment files
- Run multiple filter criteria and save the results in separate files
- Visualize multiple traces

**USE CASES**

- Analysis of *Qzasm* files

**PRODUCTIZATION READINESS**

UNSOLVED PROBLEM   SOLVED   PROTOTYPE

**CAN OSA DO THIS?**

YES ✓   NO ✗

with sweat and blood

**COMMERCIAL SOFTWARE DEPENDENCIES:**

Consumes *Qzasm* files created by Ounce (& others)

IBM / COMMERCIAL TOOLS (31%)   OPEN SOURCE (69%)

**ROADMAP: NEXT DEVELOPMENT**

- This module was made redundant by the O2 Findings Viewer Module

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>  
for individual slides with O2 Modules details

Saturday, 5 September 2009



# LEGACY O2 MODULES (6X)

**LEGACY MODULE: O2 Scanners**

**DESCRIPTION**  
O2 module that allows the easy triggering of scans using the Ounce CLI

**LEGACY MODULE: O2 Tool - DotNet Callbacks Maker**

**DESCRIPTION**  
Allow the automatic generation of Ounce 6.x rules (of type 'callback') for web

**LEGACY MODULE: O2 Tool - Findings Query**

**DESCRIPTION**  
This module provides advanced findings filtering capabilities via a LAMDA like

**LEGACY MODULE: O2 Tool - Search Assessment Run**

**DESCRIPTION**  
This was the first O2 module that fully supported the loading of multiple assessment

**LEGACY MODULE: O2 Tool - View Assessment Run**

**DESCRIPTION**  
This was the first module to provide a simple view into the unique lists of Sources, Sinks and Lost sinks of O2assmt files  
This module is a simpler version of the O2 Tool - Search Assessment Run and its main use today is to provide an easier interface into the trace visualization of multiple traces

**KEY / UNIQUE FEATURES**

- Visualization of O2 Traces
- View Finding and Trace information
- Unique set of filters for O2assmt files

**USE CASES**

- Analysis of O2assmt files

**GEK-O-METER**

02 developer
senior consultant
security consultant
analyst
manager

**PRODUCTIZATION READINESS**

UNSOLVED PROBLEM   SOLVED   PROTOTYPE

**CAN OSA DO THIS?**

YES ✓   NO ✗

with sweat and blood

**COMMERCIAL SOFTWARE DEPENDENCIES:**

Consumes o2assmt files created by Ounce (& others)

BAR / COMMERCIAL TOOLS (RED)   OPEN SOURCE (FREE)

**ROADMAP: NEXT DEVELOPMENT**

- This module was made redundant by the O2 Findings Viewer Module

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>  
for individual slides with O2 Modules details





# LEGACY O2 MODULES (6X)

	<b>LEGACY MODULE:</b> <b>O2 Scanners</b> <b>DESCRIPTION</b> O2 module that allows the easy triggering of scans using the Ounce CLI
	<b>LEGACY MODULE:</b> <b>O2 Tool - DotNet Callbacks Maker</b> <b>DESCRIPTION</b> Allow the automatic generation of Ounce 6.x rules (of type 'callback') for web
	<b>LEGACY MODULE:</b> <b>O2 Tool - Findings Query</b> <b>DESCRIPTION</b> This module provides advanced findings filtering capabilities via a LAMDA like
	<b>LEGACY MODULE:</b> <b>O2 Tool - Search Assessment Run</b> <b>DESCRIPTION</b> This was the first O2 module that fully supported the loading of multiple assessment
	<b>LEGACY MODULE:</b> <b>O2 Tool - View Assessment Run</b> <b>DESCRIPTION</b> This was the first module to provide a simple view into the unique lists of
	<b>LEGACY MODULE:</b> <b>O2 Tool - WebInspect Converter</b> <b>DESCRIPTION</b> PoC of the integration of an Black Box scanning engine (HP's Web Inspect) with a White Box scanning engine (Ounce Labs 6.0)

**KEY / UNIQUE FEATURES**

- Show how the integration between White Box and Black Box can be implemented

**USE CASES**

- Create consolidated findings between multiple scan engines

**PRODUCTIZATION READINESS**

UNSOLVED PROBLEM → SOLVED → PROTOTYPE

**CAN OSA DO THIS!**

YES ✓ (with sweat and blood) / NO ✗

**COMMERCIAL SOFTWARE DEPENDENCIES:**

Matches Ounce's with WebInspect's results

100% / COMMERCIAL TOOLS (YES) — OPEN SOURCE (FREE)

**ROADMAP: NEXT DEVELOPMENT**

- Add support for other Black Box scanners
- Improve the GUI to allow the visual mapping of both set of results
- Create command line version so that this process can be automated into a build process

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>  
 for individual slides with O2 Modules details

# STABLE O2 MODULES (IX)

**STABLE**

MAIN GUI

**MODULE:**

## O2 Tool - Host Local Website

**DESCRIPTION**  
 Allows the drag and drop of a local folder which will become exposed as a locally executed web server.  
 This module is usually used in conjunction with the O2 Debugger **M0bg** since once the web server has started it can be remotely hooked and instrumented.

**KEY / UNIQUE FEATURES**

- Easy creation of locally running web servers on arbitrary folders

**USE CASES**

- Debug .NET applications
- Write exploits for .NET application

**PRODUCTIZATION READINESS**

UNSOLVED PROBLEM | SOLVED | PROTOTYPE

**CAN OSA DO THIS!**

YES ✓ | NO ✗

**COMMERCIAL SOFTWARE DEPENDENCIES:**  
 Uses Microsoft's test **webserver** included with Visual Studio

IBM / COMMERCIAL TOOLS (EXP) | OPEN SOURCE (FREE)

**ROADMAP: NEXT DEVELOPMENT**

- Add creation of 'slices of websites' based on dynamic creation of unit tests

GEEK-O-METER

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>  
 for individual slides with O2 Modules details



## VAPORWARE O2 MODULES (2X)

---

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>

for individual slides with O2 Modules details

# VAPORWARE O2 MODULES (2X)

## O2 Tool - Filter Assessment Files

**DESCRIPTION**  
 This module was originally written as a PoC (Proof of Concept) to deal with a number of commonly asked feature requests by Ounce users. The objective was to create a GUI that allowed the easy processing and filtering of large assessment files (for example by extracting only the findings marked with a confidence = Vulnerability and a severity = High). The technology required is already in O2.

**KEY / UNIQUE FEATURES**

- (if implemented) Provides easy GUI-Driven filtering of O2assmt files

**USE CASES**

- Filtering large O2assmt findings files

**PRODUCTIZATION READINESS**

UNSOLVED PROBLEM
SOLVED
PROTOTYPE

**CAN OSA DO THIS!**

YES ✓

NO ✗

with sweat and blood

**COMMERCIAL SOFTWARE DEPENDENCIES:**  
 Consumes o2assmt files created by Ounce (& others)

IBM / COMMERCIAL TOOLS (EXP) OPEN SOURCE (FREE)

**ROADMAP: NEXT DEVELOPMENT**

- This module was made redundant by the O2 Findings Viewer Module
- This module is currently not complete, and unless there are further requests there are no extra development planned.

see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>  
 for individual slides with O2 Modules details

# VAPORWARE O2 MODULES (2X)

**Vaporware** MODULE:

MAIN GUI

## O2 Tool - Filter Assessment Files

### DESCRIPTION

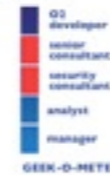
This module was originally written as a PoC (Proof of Concept) to deal with a number of commonly asked feature requests by Ounce users. The objective was to create a GUI that allowed the easy processing and filtering of large assessment files (for example by extracting only the findings marked with a confidence = Vulnerability and a severity = High). The technology required is already in O2.

### KEY / UNIQUE FEATURES

- (if implemented) Provides easy GUI-Driven filtering of *Ozasmr* files

### USE CASES

- Filtering large *Ozasmr* findings files



### PRODUCTIZATION READINESS



### CAN OSA DO THIS!

with sweat and blood

### COMMERCIAL SOFTWARE DEPENDENCIES:

Consumes *ozasmr* files created by Ounce

IBM / COMMERCIAL TOOLS (EXP)

### ROADMAP: NEXT DEVELOPMENT

- This module was made redundant
- This module is currently not com there are no extra development

**Vaporware** MODULE:

MAIN GUI

## O2 Tool - O2 Reflector

### DESCRIPTION

This module aims to create a single point of decompilation/creation and visualization of .NET assemblies and Java class files. The objective is to support the multiple Byte Code analysis engines and provide a single environment to quickly manually analyze compiled .NET, Java or *CirData* files.

### KEY / UNIQUE FEATURES

- Supports visualization of classes and methods for .NET assemblies (using .NET Reflection and Mono Cecil) and for *CirData* files
- Uses MonoCecil Decompiler to convert .NET ByteCode to C#

### USE CASES

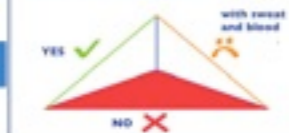
- Visualize .NET assemblies, Java classes or *CirData* files



### PRODUCTIZATION READINESS



### CAN OSA DO THIS!



### COMMERCIAL SOFTWARE DEPENDENCIES:

Consumes *CirData* files created by Ounce

IBM / COMMERCIAL TOOLS (EXP)

OPEN SOURCE (FREE)

### ROADMAP: NEXT DEVELOPMENT

- Add support for the latest O2 *Cir* data creation and visualization capabilities
- Add support for .NET code decompilation (using MonoCecil decompiler or Reflector) and Java (using JAD)



see presentation

<http://www.o2-ounceopen.com/files-binaries-source-and-demo/old-documents-and-presentations/O2%20Modules%20Presentation%20V1.0.pdf>  
for individual slides with O2 Modules details





-  **O2 developer**
  -  **senior consultant**
  -  **security consultant**
  -  **analyst**
  -  **manager**
- GEEK-O-METER**

# O2 is now an OWASP Project "OWASP O2 PLATFORM"



page discussion view source history

## OWASP O2 Platform

This is the future home of O2 (Ounce Open) which is currently hosted at <http://www.o2-ounceopen.com/>

## OWASP Projects that O2 will immediately start to integrate with and add value:

### Category:OWASP Orion Project

About Goals Discussion group Join the project Project Identification

Download The blog FAQ News Contributors/Users

The quest for secure code is what all developers want to achieve (at least we hope so). Software must be reliable. Software must be strong. Software must be secure. How secure does my software have to be? The correct answer is hard to find. But security is a problem that even a development team must consider.

Should skilled developers also be security gurus? Not necessarily, but it is important to provide security tools that will augment their development skills. And so our quest for secure code begins...

The OWASP Orion project was created with the aim of providing a common ground for safe coding and code review methodologies to be applied to software. The project is approaching its first major release and it will be able to be used in a production environment in the near future.

Orion must give thanks to Findbugs, the OWASP LAMPSE Project, RATS, and Flawfinder for ideas and inspiration.

### Category:OWASP Code Review Project

This project has produced a book that can be downloaded or purchased. Feel free to browse the full catalog of available OWASP books.

Project Name	OWASP Code Review Guide V1.1
Short Project Description	The code review guide is currently at release version 1.1 and the second best selling OWASP book in 2006. Many positive comments have been feedback regarding this initial version and believe it's a key enabler for the OWASP fight against software insecurity. It has even inspired individuals to build tools based on its information. The combination of a book on secure code review and tools to support such an activity is very powerful as it gives the developer community a place to start regarding secure application development. Going forward I hope to further integrate with the ASVS and other guides such as the testing and ASQR guides shall be performed for version 2.0
Project key information	Project Leader: <a href="#">Erik</a>   Project Contributors: <a href="#">See here</a>   Mailing List: <a href="#">Subscribe here</a>   License: <a href="#">Creative Commons Attribution</a>   Project Type: <a href="#">Documentation</a>   Sponsor: <a href="#">OWASP</a>

### Category:OWASP .NET Project

[.NET Project Overview](#) [Resources](#) [Project Tracker](#) [Project Identification](#)

**Purpose**

The purpose of the OWASP .NET Project is to provide a central repository of information and tools for software professionals that use the Microsoft .NET Framework for web applications and services. The project will try to include resources from Microsoft and from the Open Source community, the ASP.NET community and other related security resources.

Please review the [vulnerabilities](#) section at OWASP for the grand list of web vulnerabilities, many apply to .NET software. This section has a Quick Reference table for OWASP projects that you can use for your security projects now. For .NET related content throughout the site, look for the [.NET category](#). There is plenty of work to be done, so feel free to join the OWASP .NET Project (See [Joining the project](#) below). Contribute work or join our mailing list, many voices are better than one, so join today!

### Category:OWASP Enterprise Security API

About FAQ Java EE .NET Classic ASP PHP ColdFusion/CFML

Python Haskell News Contributors/Users

OWASP Tools Project

**Enterprise Security API (ESAPI)**

OWASP Enterprise Security API Toolkit help software developers guard against security-related design and implementation flaws. Just as web applications and web services can be Public Key Infrastructure (PKI) enabled (PKI enabled) to perform for example certificate-based authentication, applications and services can be ESAPI-enabled (ES-enabled) to enable applications and services to protect themselves from attackers. Further development ESAPI occurs through mailing list discussions and occasional workshops, and suggestions I improvement are welcome. For more information, please [contact us](#).

**ESAPI Toolkits**

- Java EE
- .NET
- Classic ASP
- PHP
- ColdFusion
- Python

### Category:OWASP Testing Project

This project has produced a book that can be downloaded or purchased. Feel free to browse the full catalog of available OWASP books.

Project Name	OWASP Testing Guide V1.4 Project
Short Project Description	The OWASP Testing Guide includes a "best practice" penetration testing framework which users can implement in their own organizations and a "low level" penetration testing guide that describes techniques for testing most common web application and web service security issues. OWASP Testing Guide v3 is a 349 page book, we have split the set of active tests in 9 sub-categories for a total of 98 controls to test during the Web Application Testing activity.
Key Project Information	Project Leader: <a href="#">Muhim</a>   Project Contributors: <a href="#">See here</a>   Mailing List: <a href="#">Subscribe here</a>   License: <a href="#">Creative Commons Attribution</a>   Project Type: <a href="#">Documentation</a>   Sponsor: <a href="#">OWASP</a>

### Category:OWASP Java Project

About [\[edit\]](#)

The OWASP Java Project's goal is to enable Java and J2EE developers to build secure applications efficiently. See the [OWASP Java Project Roadmap](#) for more information on our plans.

[Joining the Project](#) [\[edit\]](#)

Rohit Belani is the project lead. The project's high level roadmap can be found at the [OWASP Java Project Roadmap](#)

- Please submit your ideas for individual articles to the [Java Project Article Wishlist](#).
- If you'd like to contribute:
  - visit the [Tutorial](#),
  - join the [mailing list](#)
  - and pick a topic from the [OWASP Java Table of Contents](#), or suggest a new topic.

Remember to add the tag: `[[Category:OWASP Java Project]]` to the end of new articles so that they're properly categorised.

### Category:OWASP Live CD Project

Overview [\[edit\]](#)

The OWASP Live CD project was originally started to update the previous OWASP Live CD 2007. The project met the September 19th, 2008 deadline for the OWASP Summer of Code (SoC) and produced its first release - the SoC release. Since the completion of the SoC, the project has made the following releases:

- the Portugal release (Dec 12, 2008)
- the Austin/Texas release (Feb 10, 2009)
- the AppSec EU release (May, 2009)

In addition to creating these releases of the OWASP Live CD, the maintainer has created a series of forums and tutorials for support and documentation in an effort to help the Application Security

### ORG (OWASP Report Generator)

The ORG (OWASP Report Generator) is a tool for Security Consultants that supports the documentation and reporting of security vulnerabilities discovered during security audits.

Currently the [Mark Rosberry](#) leads this project. Formerly the project leader was [Diris Chou](#) with strong contributions from [Mika de Lencastre](#). Mika was sponsored under an OWASP Autumn of Code 2006 sponsored to work on ORG.

**Downloads**

The latest release of ORG's installer can be found at [Updated on 5/15/2007 Report Generator Installer](#). The source code for latest stable version can be downloaded from [here](#) (updated on 11/4/2006) [Report Generator Source](#).

This project is in active development and the latest version can be obtained from [Google SVN](#).

**Instructions for using the zip file**

- Unzip the files
- Run `regAuthenticPlugin.bat` to register the AuthenticPlugin
- Open the solution in VS.Net 2005. You can use any version of VS but the primary version used for development is the express edition.
- More than likely you need to modify the references area to use the local files for `(\bin\authentic\bin) XSLSPYU2005`.
- Then try and compile and you should be good to go. If not contact Mike and we will work with you

### Category:OWASP Source Code Review OWASP Projects Project

PROJECT IDENTIFICATION						
Project Name	OWASP Source Code Review OWASP-Projects Project					
Short Project Description	The objectives of this project are: 1. Develop and document a workflow for FLOSS projects to incorporate static analysis into the Software Development Life Cycle (SDLC); 2. Apply the above workflow as a required step for OWASP projects; 3. Aid in auditing select FLOSS projects to create a baseline for comparing security amongst FLOSS projects.					
Project key information	Project Leader: <a href="#">Dan Cornell</a> SoC's Project Leader	Project Contributors: <a href="#">Justin Derry</a> <a href="#">Maureen Doyle</a> <a href="#">Michael</a>	Mailing list: <a href="#">Subscribe here</a> <a href="#">Use here</a>	License: <a href="#">Creative Commons Attribution</a> <a href="#">Share Alike 3.0</a>	Project Type: <a href="#">Documentation</a>	Sponsor: <a href="#">OWASP SoC 06</a> <a href="#">Fortify</a>

## (EXAMPLE OF THE MANY) O2 CONTRIBUTIONS TO Open Standards: ICirData, ICirClass, ICirFunction, ICir\*

```
public interface ICirData
{
    Dictionary<string, ICirClass> dClasses_bySignature ( get; set; )
    Dictionary<string, ICirFunction> dFunctions_bySignature ( get; set; )
}
```

```
public interface ICirClass
{
    Dictionary<string, ICirFunction> dFunctions ( get; set; )
    Dictionary<string, ICirClass> dIsSuperClassedBy ( get; set; )
    Dictionary<string, ICirClass> dSuperClasses ( get; set; )

    string Signature ( get; set; )
    string Module ( get; set; )
    string Name ( get; set; )
    string FullName ( get; set; )
    string Namespace ( get; set; )

    // Reference to file location (or the source code in most case)
    string File ( get; set; )
    string FileLine ( get; set; )
}
```

```
public interface ICirFunction
{
    List<ICirFunction> FunctionsCalledUniqueList ( get; set; )
    List<ICirFunctionCall> FunctionsCalled ( get; set; )

    List<ICirFunctionCall> FunctionIsCalledBy ( get; set; )
    List<ICirFunctionParameter> FunctionParameters ( get; set; )

    ICirClass ParentClass ( get; set; )

    string FunctionSignature ( get; set; )
    string ReturnType ( get; set; )
    string FunctionNameAndParameters ( get; set; )
    string ClassNameFunctionNameAndParameters ( get; set; )
    string FunctionName ( get; set; )
    string ParentClassFullName ( get; set; )
    string ParentClassName ( get; set; )
    string Module ( get; set; )
}
```

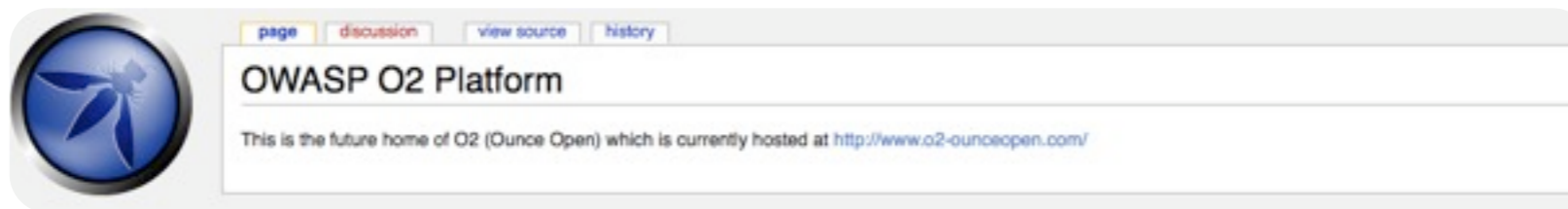
```
public interface ICirFunctionCall
{
    ICirFunction cirFunction ( get; set; )
    int lineNumber ( get; set; )
    string fileName ( get; set; )
    int sequenceNumber ( get; set; )
    String sourceCodeText ( get; set; )
}
```

```
public interface ICirFunctionParameter
{
    string ParameterName ( get; set; )
    string ParameterType ( get; set; )
    string Constant ( get; set; )
    bool HasConstant ( get; set; )
    bool HasDefault ( get; set; )
    string Method ( get; set; )
    bool IsTainted ( get; set; )
}
```



## TWO O2 WEBSITES

- Like OWASP's SAMM (& others), in the short term, O2 will be hosted in two separate websites:
  - **Official** 'stable' versions will be hosted using OWASP's WIKI engine at: [http://www.owasp.org/index.php/OWASP O2 Platform](http://www.owasp.org/index.php/OWASP_O2_Platform)



- **Development** versions & Community features will be hosted using SquareSpace web engine at: <http://www.o2-ounceopen.com>



### Traffic Overview

Statistical data gathered from your website usage logs. Search engine crawls and other specially identified hits are not factored in to your unique visitor counts. **This information is updated every minute.**



Traffic Summary	
Page Views	4,454
Page Views / Week (Avg)	337
Unique Visitors	1,419
Unique Visitors / Week (Avg)	107
Robot Hits	5,713
Robot Hits / Week (Avg)	425

Traffic Details			
	(Views)	(Unique)	(Robots)
Week of Aug 23	70	25	185
Week of Aug 16	573	164	668
Week of Aug 9	482	125	578
Week of Aug 2	339	87	550
Week of Jul 26	413	177	546
Week of Jul 19	355	81	514
Week of Jul 12	300	91	475
Week of Jul 5	475	135	403

## BTW, SOMEBODY should sponsor an OWASP 'Application Security Summit' :)

- Which would be a world wide gathering of security experts with the objective to figure out how to use the current resources (People, Process and Technology) to help customers to fix security vulnerabilities in their applications
- This Summit could be organized by OWASP using the same model used on the last OWASP Summit in Portugal







# THE CHALLENGE

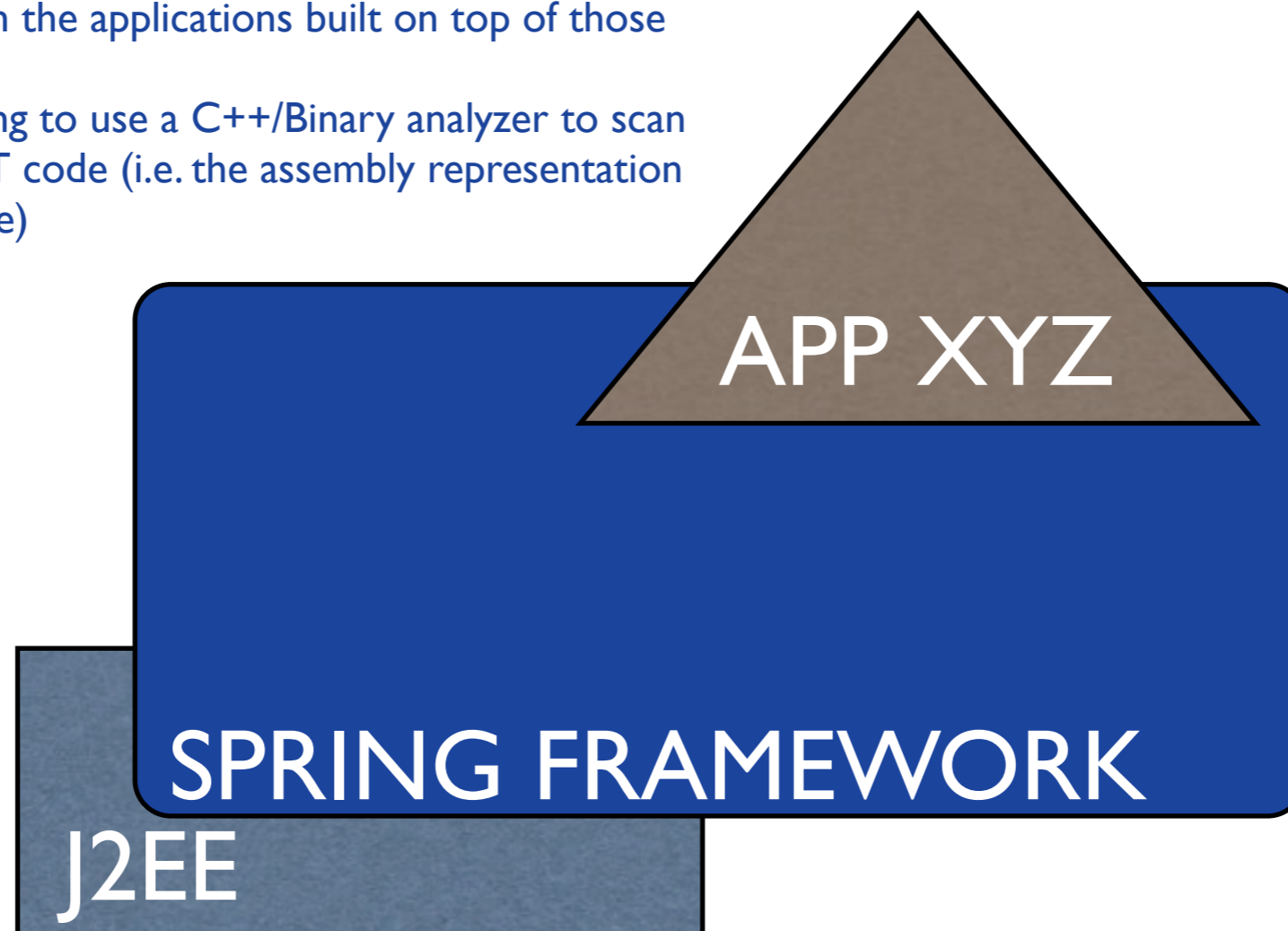
---

-  O2 developer
-  senior consultant
-  security consultant
-  analyst
-  manager

**GEEK-O-METER**

## THE PROBLEM WITH FRAMEWORKS

- For this discussion a 'Framework' is an environment which augments the capabilities of the core language implementations (.NET Framework or J2EE). Examples of what I call a Frameworks are: Spring, Struts, Microsoft Enterprise Library, SharePoint, WebSphere Portal, Salesforce API,
- Each Framework creates its own 'reality' almost like a VM (Virtual Machine), where they (for example Spring MVC) create an abstraction layer between the core language (i.e. Java) and the target application.
- So, if the scanning engines (Black Box, White Box, Human Brain) don't explicitly support frameworks, they will NOT understand how they work they and will NOT be able to find security issues in the applications built on top of those frameworks.
  - It is like trying to use a C++/Binary analyzer to scan JITTED .NET code (i.e. the assembly representation of .NET code)



## SOME TECHNOLOGICAL SOLUTIONS THAT STILL NEED TO BE SOLVED

---



- All current (Commercial and Open Source) Static Source Code Analysis tools have most (if not all) of the problems below (some have minor/basic coverage of it)
- ANALYSIS ENGINES - Part I
  - Attributes, Collections & other type of objects that receive taint in A and output it in B
  - Global Variables
  - Proper Taint Propagation across strings and between data types
  - Reflection (which creates 'Hyper Jumps' between code paths)
  - Events
  - Rules based on assemblies/jars versions and not on signatures
  - Taint Typing (also applied to business logic)
- ANALYSIS ENGINES - Part II
  - Rules Management (user-friendly process to mass create, edit, modify, import and export)
  - Join Traces (between application layers or interfaces or 'Hyper Jumps')
  - Read (and understand) configuration files (who have major impact on the attack surface and exploitability)
  - Auto Attack Surface Markup
  - Expose Control Flow
  - Understand Framework behavior
- GlassBox
  - Integration with WB & BB (driving one tool from the other)
  - Common Reporting
- **Note:** *this (list above)*  
*IS A VERY **SMALL** & LIMITED LIST of the **technologies** / **techniques** that **need to be supported** when running (manual or automatic, Black or White) scans.*  
*These capabilities (either when **used by non-expert users** or by expert security consultants) allows the security engagement to be **accurate, effective, consumable and actionable***

# WHERE WE ARE TODAY and WHERE WE NEED TO BE ASAP

• Here is the evolution of technologies and where the current level of support is:

• **1996-2000:** MainFrames, Web Servers, Java, ASP Classic

• **2000-2004:** C/C++, .NET Framework, J2EE, PHP

• **2004-2006:** Struts, Spring Framework, Ajax, Flash, Hibernate, Microsoft Enterprise Library

• **2006-2009:** lots of web innovation going on, here is a small list:

**Languages & Technologies:** Aspect, Web Services, REST, Widgets/Gadgets, AIR, Silverlight, Groovy & Grails, Python, Ruby & Ruby on Rails, JSP EL, Velocity, JSF (Faces),

**Application Platforms / Frameworks:** ASP.NET MVC, SharePoint, IBM WebSphere Portal, WebSphere Application Portal, SAP (web stuff), iPhone & Apple iStore

**Online Applications:** Salesforce, Amazon Web Services, MySpace/Facebook/Twitter

**OWASP 'standards/APIs/frameworks':** ESAPI, SAMM, ASVF, etc...

And let's not forget that most enterprise applications have their OWN frameworks and APIs (and sometimes even VMs)

• **2010-....** : Chrome, cloud computing (vSphere (VMWare's cloud), Azure (Microsoft's cloud)), Web 3.0 and next generation of all of the above :)

'Out of the box' capabilities is here

O2 is here

We need to be here ASAP

# TO SCALE WE NEED TARGETED SOLUTIONS

---

-  O2 developer
-  senior consultant
-  security consultant
-  analyst
-  manager



## HOW TO SCALE: AUTOMATE SECURITY KNOWLEDGE

---

- The only way we will be able to scale (and have these solutions used by a wide audience (from developer's upwards), is if we are able to **'capture + automate' the knowledge, workflow and wisdom of security consultants**. And we need to do this in such a way that repeated analysis by non-technical staff will have the same result as the analysis created by an security expert

- In a nutshell ... what we need is to do,

**is to automate the security expert's brain ...**

so that we are able to independently use it in a repeatable and consistently way,

and once we have done that (automating their brain) ... we can work on making it

**very simple to use by non-security experts**

And due to the complexity of each targeted application / framework ...

... this 'one button' solution is only possible if ....

### **WE CREATE TARGETED SOLUTIONS & PRODUCT**

(see next 4 slides for an example of what this could look like)

Note that today an 'Application Security Analysis' engagement is a very: complex, non-repeatable, non-scalable, non-measurable, and very opaque (from the client point of view) process. It is also very hard to calculate its ROI

# SPRING FRAMEWORK : SECURITY ANALYSIS PLATFORM

- Due to the complexity and 'realities' created by the Spring Framework, the only way to deal to analyze/expose its behavior is to create fine-tune 'packages' of the available technology

**MAIN GUI**

## SECURITY ANALYSIS PLATFORM

**DESCRIPTION**

Specifically targeted at the Java Spring MVC framework, this module is able to analyze an application written under this framework and extract its attack surface and exposed internal objects. In addition to powerful visualization tools for the data collected, this module also contains a simple 'analysis engine' which creates Spring MVC related Findings

**MATURITY**

UNSOLVED PROBLEM

SOLVED

PROTOTYPE

COMMERCIAL TOOLS (\$\$\$)

OPEN SOURCE (FREE)

Blah Blah, Yadda, Yadda, Blah Blah, Yadda, Yadda, Blah Blah, Yadda, Yadda.

## SHAREPOINT (MOSS) : SECURITY ANALYSIS PLATFORM

- Same think for frameworks & development environments like Microsoft Office Sharepoint Server (MOSS). Unless we have a customized engine & technology that understands Sharepoint, it is very hard (if not impossible) to (for example) write secure web parts.

The image is a composite of two parts. On the left is a 3D ring diagram representing the architecture of Microsoft Office SharePoint Server (MOSS). The central core is labeled 'Platform Services'. Surrounding this core are several layers of services: 'Topology', 'Security', 'Storage', 'Workspaces', and 'Site Web'. The outer ring is divided into six segments: 'Business Intelligence', 'Collaboration', 'Portal', 'Search', 'Content Management', and 'Business Processes'. Below this diagram is the Microsoft Office logo.

On the right is the cover of the 'SECURITY ANALYSIS PLATFORM' for Microsoft Office SharePoint Server 2007. The cover features the Microsoft Office SharePoint Server 2007 logo at the top. Below it, the title 'SECURITY ANALYSIS PLATFORM' is written in large, bold, blue letters. At the bottom, there is a photograph of a globe with the text: 'Security Analysis Platform specifically customized for Microsoft's Office Sharepoint Server (MOSS)'. A small circular icon with the number '2' is visible on the left side of the cover.



# SHAREWORKZ SECURITY ANALYSIS PLATFORM

- .... and the same thing applies for for applications built on top MOSS (which also create their own reality and unique class of vulnerabilities (before & after customization)
  - quote from [www.shareworkz.com](http://www.shareworkz.com): "... ShareWorkz helps you get the most from Microsoft SharePoint – quickly! Built in SharePoint Server 2007 Standard Edition, ShareWorkz reduces the time to build and deploy a best practice, enterprise class SharePoint 2007 Solution to 1 month or less..."

The graphic illustrates the ShareWorkz Security Analysis Platform architecture. On the left, a cylindrical stack represents the technology layers, from bottom to top: Microsoft Windows Server, Microsoft SQL Server, Windows Sharepoint S..., ShareWorkz Core Components, ShareWorkz Template Libraries, and ShareWorkz Unified User Interface. Various components are shown as markers protruding from the stack, including BizTalk Server, Office System, SharePoint Portal Server, and MS CRM. To the right, the text 'ShareWorkz SECURITY ANALYSIS PLATFORM' is displayed above a blue background with a water ripple effect. Below this, a circular diagram shows the 'ShareWorkz CORE' at the center, surrounded by concentric layers of 'Intranet' and 'Extranet' collaboration types. A legend on the right lists the specific collaboration types for each layer.

**ShareWorkz CORE**

- Intranet** – Information Collaboration  
Content Management  
Document Management  
Information Dashboards
- Intranet** – Project Collaboration
- Intranet** – Process Collaboration
- Intranet** – Community Collaboration
- Extranet** – Information Collaboration
- Extranet** – Project Collaboration
- Extranet** – Process Collaboration
- Extranet** – Community Collaboration
- Extranet** – Complex Multi-party Collaboration

# OPEN SOURCE SECURITY ANALYSIS PLATFORM

- The Open Source community also needs a generic platform made up of only Open Source or free tools.
- This is a very CRITICAL piece of the puzzle, since this is what will enable the wide use of these techniques across the Open Source and Commercial Software development world (it will also allow the Framework developers to be responsible for creating their markups (after all, who better than the Spring developers to help with the development of the “Spring Framework : Security Analysis Platform”)



## 2 PLATFORM



## OPEN SOURCE SECURITY ANALYSIS PLATFORM





Blah Blah, Yadda, Yadda, Blah Blah, Yadda, Yadda, Blah Blah, Yadda, Yadda,





Thank you ....