O2 Platform

Automating Security Knowledge through Unit Tests

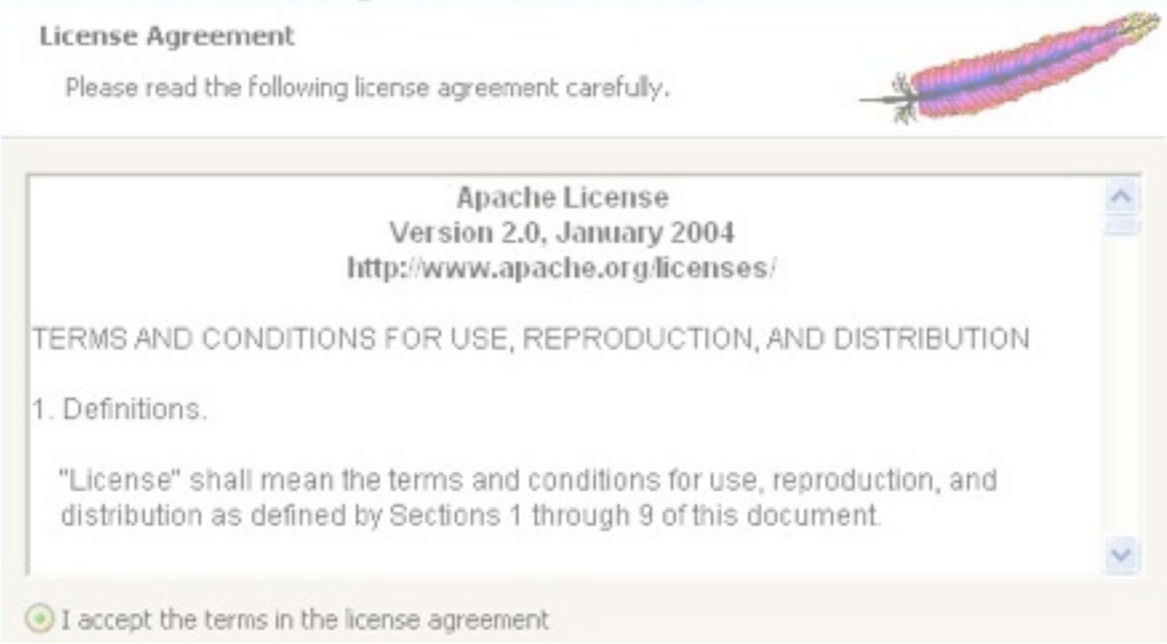
WHAT IS ② ?

and the OWASP O2 PLATFORM

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

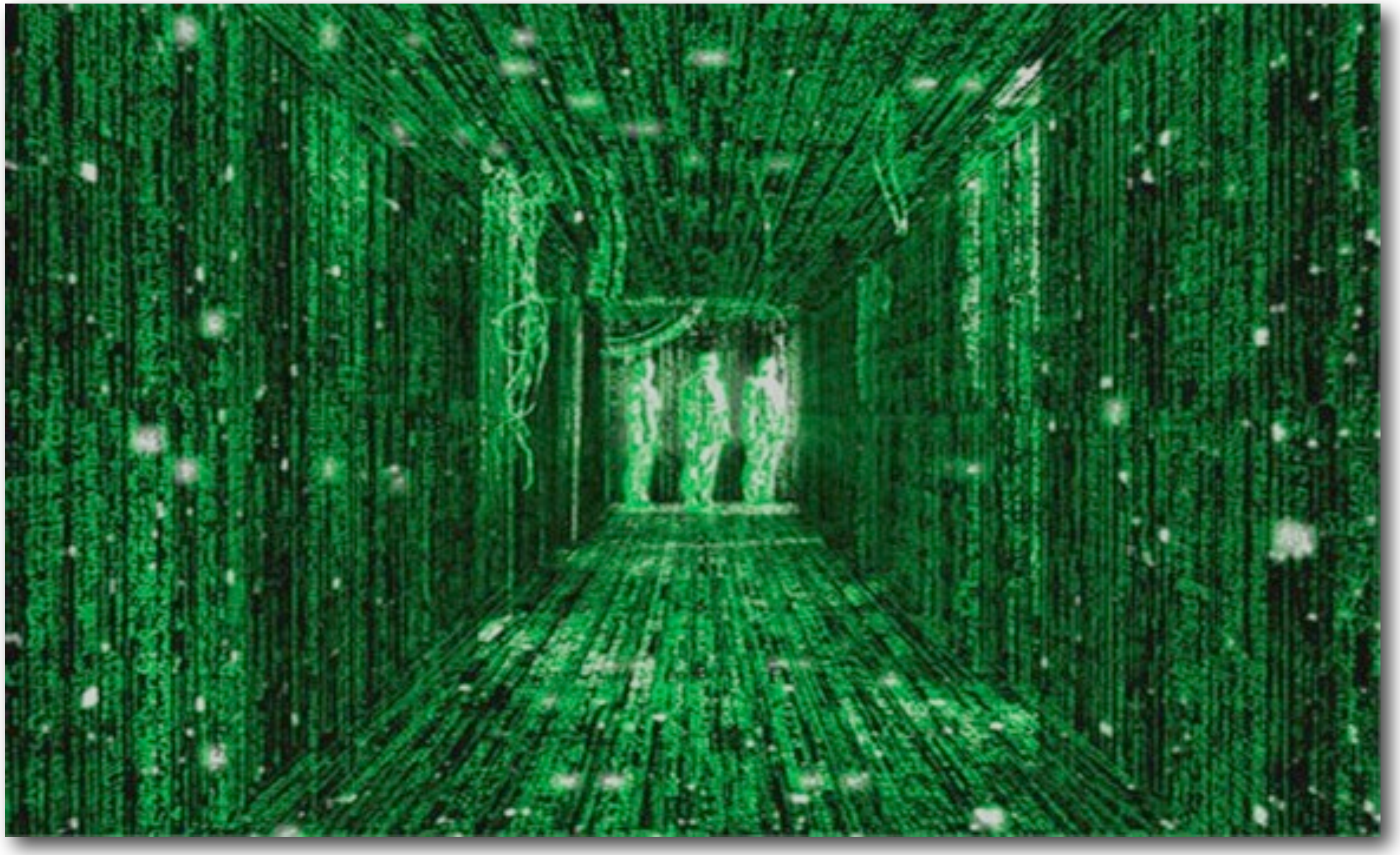
1. Definitions.

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

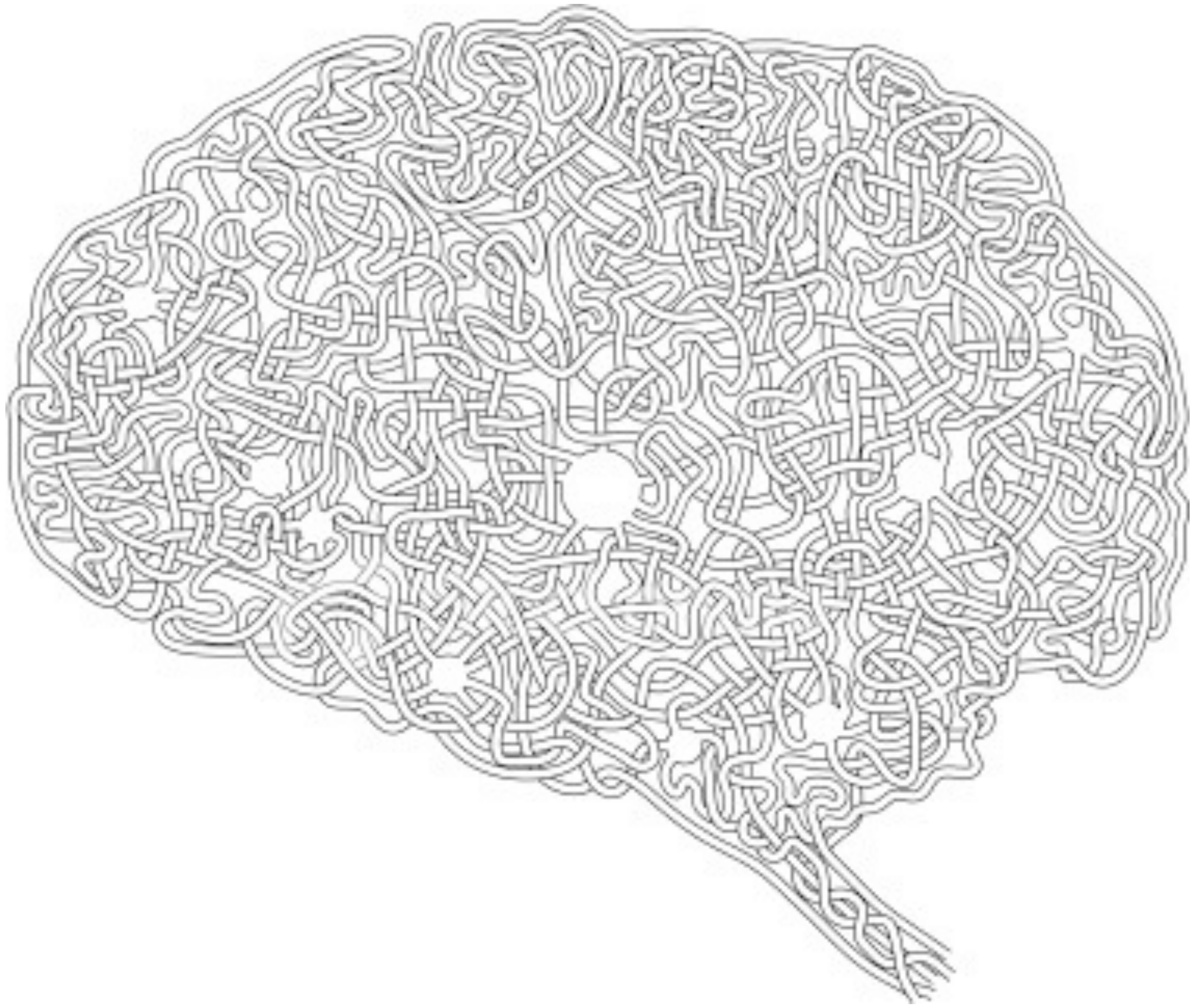
○ I accept the terms in the license agreement for

AUTOMATING.

APPLICATION SECURITY.



KNOWLEDGE.



and

WORKFLOWS.

Anyone has gum, tabasco, a bag of fertilizer, two pints of Guinness, and a croissant?
After building a missile out of his broken moped, MacGyver realizes he needs to make the warhead

② is an:

O2 is an:

OPEN PLATFORM

for

AUTOMATING

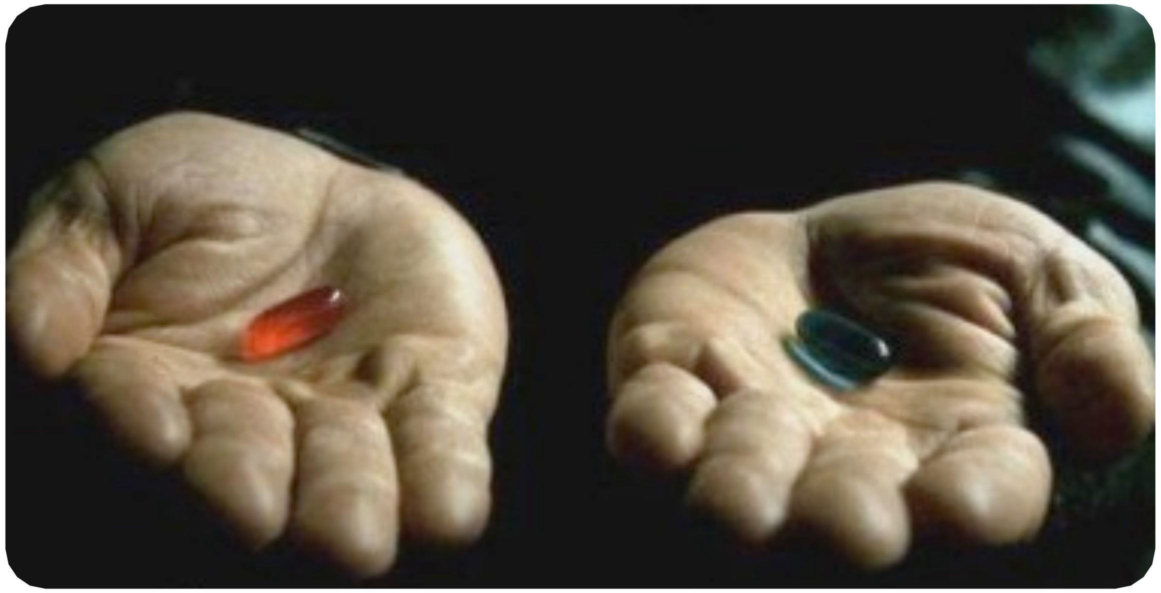
APPLICATION SECURITY

KNOWLEDGE

and

WORKFLOWS

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



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

and your clients will love you

O2 Quote, by David Campbell

O2 Quote, by David Campbell

" Earlier this year I gave a presentation about how the 'future of penetration testing' is all greybox. We now get source for almost every assessment we do, and so the blackbox toolset we traditionally used had to evolve.

O2 Quote, by David Campbell

" Earlier this year I gave a presentation about how the 'future of penetration testing' is all greybox. We now get source for almost every assessment we do, and so the blackbox toolset we traditionally used had to evolve.

The O2 framework provides a very flexible set of tools for performing greybox testing. The concept of 'MethodStreams' makes it radically simpler to get all of the source for a single method in one place to easily 'follow the taint'. O2 also provides a set of blackbox tools to quickly verify your static analysis findings and rapidly develop POC exploits.

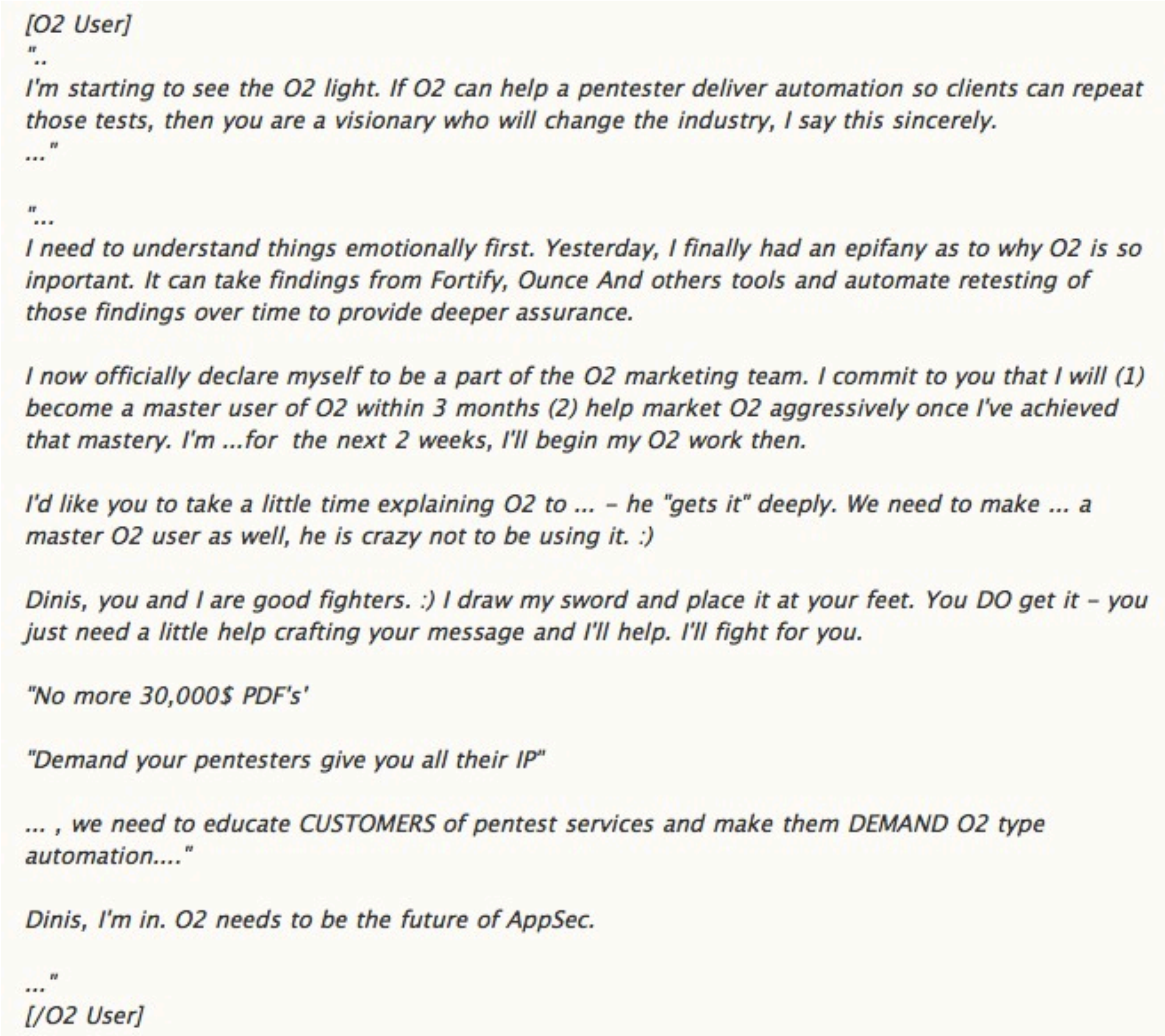
O2 Quote, by David Campbell

" Earlier this year I gave a presentation about how the 'future of penetration testing' is all greybox. We now get source for almost every assessment we do, and so the blackbox toolset we traditionally used had to evolve.

The O2 framework provides a very flexible set of tools for performing greybox testing. The concept of 'MethodStreams' makes it radically simpler to get all of the source for a single method in one place to easily 'follow the taint'. O2 also provides a set of blackbox tools to quickly verify your static analysis findings and rapidly develop POC exploits.

In a nutshell, the pentesting game has changed, and the O2 is the swiss army knife you need to carry. "

AN O2 USER'S Epiphany



[O2 User]

"..

I'm starting to see the O2 light. If O2 can help a pentester deliver automation so clients can repeat those tests, then you are a visionary who will change the industry, I say this sincerely.

..."

"...

I need to understand things emotionally first. Yesterday, I finally had an epifany as to why O2 is so inportant. It can take findings from Fortify, Ounce And others tools and automate retesting of those findings over time to provide deeper assurance.

I now officially declare myself to be a part of the O2 marketing team. I commit to you that I will (1) become a master user of O2 within 3 months (2) help market O2 aggressively once I've achieved that mastery. I'm ...for the next 2 weeks, I'll begin my O2 work then.

I'd like you to take a little time explaining O2 to ... – he "gets it" deeply. We need to make ... a master O2 user as well, he is crazy not to be using it. :)

Dinis, you and I are good fighters. :) I draw my sword and place it at your feet. You DO get it – you just need a little help crafting your message and I'll help. I'll fight for you.

"No more 30,000$ PDF's'

"Demand your pentesters give you all their IP"

... , we need to educate CUSTOMERS of pentest services and make them DEMAND O2 type automation...."

Dinis, I'm in. O2 needs to be the future of AppSec.

..."

[/O2 User]

Key message of this presentation

Key message of this presentation

NO
MORE

PDF

WITH
SECURITY FINDINGS

Other types of PDF's

Other types of PDF’s

- As bad as delivering a PDF, is delivering Automated Tools results (Static Code Analysis, Website Scanners) which deliver tons of results/findings but have little context or actionable actions.

Other types of PDF's

- As bad as delivering a PDF, is delivering Automated Tools results (Static Code Analysis, Website Scanners) which deliver tons of results/findings but have little context or actionable actions.

- Any client's deliverable that is not easily consumed by the end user (from developers to managers) is what I'm calling a 'PDF'

SPEAKING DEVS LANGUAGE

SPEAKING DEVS LANGUAGE

- Delivering security knowledge inside a PDF is a massively inefficient workflow

SPEAKING DEVS LANGUAGE

- Delivering security knowledge inside a PDF is a massively inefficient workflow

- The Client is going to spend more money trying to figure out what the PDF says and how to deal with it, than they spent in creating it (the PDF)

SPEAKING DEVS LANGUAGE

- Delivering security knowledge inside a PDF is a massively inefficient workflow
- The Client is going to spend more money trying to figure out what the PDF says and how to deal with it, than they spent in creating it (the PDF)
- The developers will struggle to reproduce the findings and in most cases fix the vulnerabilities by making the exploit not work

SPEAKING DEVS LANGUAGE

- Delivering security knowledge inside a PDF is a massively inefficient workflow

- The Client is going to spend more money trying to figure out what the PDF says and how to deal with it, than they spent in creating it (the PDF)

- The developers will struggle to reproduce the findings and in most cases fix the vulnerabilities by making the exploit not work

- We need to speak the developer's language, leverage their knowledge and create two-way communication channels

We need UnitTests

We need UnitTests

- UnitTest are the only ‘language’ we can speak that the developers will understand

We need UnitTests

- UnitTest are the only ‘language’ we can speak that the developers will understand
- Security-Driven Unit tests will allow the developers to:

We need UnitTests

- UnitTest are the only ‘language’ we can speak that the developers will understand
- Security-Driven Unit tests will allow the developers to:
  - Reproduce Security Findings

We need UnitTests

- UnitTest are the only ‘language’ we can speak that the developers will understand
- Security-Driven Unit tests will allow the developers to:
  - Reproduce Security Findings
  - Debug Security Exploits

We need UnitTests

- UnitTest are the only 'language' we can speak that the developers will understand
- Security-Driven Unit tests will allow the developers to:
  - Reproduce Security Findings
  - Debug Security Exploits
  - Write Fixes and Confirm its non-exploitability

We need UnitTests

- UnitTest are the only 'language' we can speak that the developers will understand
- Security-Driven Unit tests will allow the developers to:
  - Reproduce Security Findings
  - Debug Security Exploits
  - Write Fixes and Confirm its non-exploitability
  - Use as part of normal app QA/Testing

We need UnitTests

- UnitTest are the only 'language' we can speak that the developers will understand
- Security-Driven Unit tests will allow the developers to:
  - Reproduce Security Findings
  - Debug Security Exploits
  - Write Fixes and Confirm its non-exploitability
  - Use as part of normal app QA/Testing
  - Ensure vulnerabilities are not re-introduced at a later stage

We need UnitTests

- UnitTest are the only 'language' we can speak that the developers will understand
- Security-Driven Unit tests will allow the developers to:
  - Reproduce Security Findings
  - Debug Security Exploits
  - Write Fixes and Confirm its non-exploitability
  - Use as part of normal app QA/Testing
  - Ensure vulnerabilities are not re-introduced at a later stage

- There are lots of other advantages: better management reports, WAF rules, etc...

SECURITY BY DESIGN & DEFAULT

SECURITY BY DESIGN & DEFAULT

DELIVERING

SECURITY BY DESIGN & DEFAULT

DELIVERING

SECURITY UNIT TESTS

SECURITY BY DESIGN & DEFAULT

DELIVERING

SECURITY UNIT TESTS

WILL ALLOW US TO

SECURITY BY DESIGN & DEFAULT

DELIVERING

SECURITY UNIT TESTS

WILL ALLOW US TO

MAKE SECURITY

SECURITY BY DESIGN & DEFAULT

DELIVERING

SECURITY UNIT TESTS

WILL ALLOW US TO

MAKE SECURITY

INVISIBLE/TRANSPARENT

SECURITY BY DESIGN & DEFAULT

DELIVERING

SECURITY UNIT TESTS

WILL ALLOW US TO

MAKE SECURITY

INVISIBLE/TRANSPARENT

TO DEVELOPERS

Living in an O2 world

WHAT DOES IT LOOK LIKE?

WHAT DOES IT LOOK LIKE?

- By now (hopefully) you agree that the concept of creating Security-Driven-UnitTest vs PDFs is a good one

WHAT DOES IT LOOK LIKE?

- By now (hopefully) you agree that the concept of creating Security-Driven-UnitTest vs PDFs is a good one

- But how does it work in practice?

WHAT DOES IT LOOK LIKE?

- By now (hopefully) you agree that the concept of creating Security-Driven-UnitTest vs PDFs is a good one

- But how does it work in practice?

- What type of Unit Tests can be created?

WHAT DOES IT LOOK LIKE?

- By now (hopefully) you agree that the concept of creating Security-Driven-UnitTest vs PDFs is a good one
- But how does it work in practice?
- What type of Unit Tests can be created?
- Don't the current tools in the market (including O2) suck at automating security consultant's knowledge, workflows and exploits?

WHAT DOES IT LOOK LIKE?

- By now (hopefully) you agree that the concept of creating Security-Driven-UnitTest vs PDFs is a good one
- But how does it work in practice?
- What type of Unit Tests can be created?
- Don't the current tools in the market (including O2) suck at automating security consultant's knowledge, workflows and exploits?
- To answer this, lets look at a number of case studies of what O2 can do in the hands of an O2 Power User (i.e in my hands)

Recapping: OWASP O2 PLATFORM

PLATFORM

Recapping: OWASP O2 PLATFORM

PLATFORM

The O2 platform represents a new paradigm for how to perform, document and distribute Web Application security reviews.

O2 is designed to ***Automate Security Consultants Knowledge and Workflows***

and to

Allow non-security experts to access and consume Security Knowledge and Unit Tests

SO WHAT IS O2?

SO WHAT IS O2?

- Scripting Engine and development environment

SO WHAT IS O2?

- Scripting Engine and development environment
  - I write "O2 in O2" using its "C#, Python-like, reflection-on-steroids, dynamically-compiled-extension-methods" environment

SO WHAT IS O2?

- Scripting Engine and development environment
  - I write "O2 in O2" using its "C#, Python-like, reflection-on-steroids, dynamically-compiled-extension-methods" environment
- Black-Box/Browser-automation environment

SO WHAT IS O2?

- Scripting Engine and development environment
    - I write "O2 in O2" using its "C#, Python-like, reflection-on-steroids, dynamically-compiled-extension-methods" environment

- Black-Box/Browser-automation environment

- Source Code analysis environment:

SO WHAT IS O2?

- Scripting Engine and development environment
  - I write "O2 in O2" using its "C#, Python-like, reflection-on-steroids, dynamically-compiled-extension-methods" environment
- Black-Box/Browser-automation environment
- Source Code analysis environment:
  - It's own .NET Static Analysis engine (with taint-flow analysis)

SO WHAT IS O2?

- Scripting Engine and development environment
  - I write "O2 in O2" using its "C#, Python-like, reflection-on-steroids, dynamically-compiled-extension-methods" environment
- Black-Box/Browser-automation environment
- Source Code analysis environment:
  - It's own .NET Static Analysis engine (with taint-flow analysis)
  - Supports Java ByteCode/classes call-flow analysis (and source code mappings)

SO WHAT IS O2?

- Scripting Engine and development environment
  - I write "O2 in O2" using its "C#, Python-like, reflection-on-steroids, dynamically-compiled-extension-methods" environment
- Black-Box/Browser-automation environment
- Source Code analysis environment:
  - It's own .NET Static Analysis engine (with taint-flow analysis)
  - Supports Java ByteCode/classes call-flow analysis (and source code mappings)
  - Multiple visualizers for Development Frameworks (Spring MVC, Struts, ASP.NET MVC)

SO WHAT IS O2?

- Scripting Engine and development environment
  - I write "O2 in O2" using its "C#, Python-like, reflection-on-steroids, dynamically-compiled-extension-methods" environment
- Black-Box/Browser-automation environment
- Source Code analysis environment:
  - It's own .NET Static Analysis engine (with taint-flow analysis)
  - Supports Java ByteCode/classes call-flow analysis (and source code mappings)
  - Multiple visualizers for Development Frameworks (Spring MVC, Struts, ASP.NET MVC)
- Data Consumption and API Generation

SO WHAT IS O2?

- Scripting Engine and development environment
  - I write “O2 in O2” using its “C#, Python-like, reflection-on-steroids, dynamically-compiled-extension-methods” environment
- Black-Box/Browser-automation environment
- Source Code analysis environment:
  - It’s own .NET Static Analysis engine (with taint-flow analysis)
  - Supports Java ByteCode/classes call-flow analysis (and source code mappings)
  - Multiple visualizers for Development Frameworks (Spring MVC, Struts, ASP.NET MVC)
- Data Consumption and API Generation
- Powerful search engine, Graphical Engines, multiple APIs for popular tools/websites and tons of utilities

Automating myself

Automating myself

- KEY CONCEPT:

  Today (Nov 2010) when I do a security assessment:

Automating myself

- KEY CONCEPT:

  Today (Nov 2010) when I do a security assessment:

IT IS FASTER FOR ME TO AUTOMATE MYSELF

VIA CUSTOM APIs

THAN IT IS DO KEEP DOING IT BY HAND

IN PRACTICE

IN PRACTICE

- To really understand what this all means, lets look at a number of case studies of where I have successfully used O2 in the real world

IN PRACTICE

- To really understand what this all means, lets look at a number of case studies of where I have successfully used O2 in the real world

- Hopefully this will clear the myth that security consultants still have today that there is no way to automate their workflows and security findings

Real world O2 usage

PROBLEM:

PROBLEM:

Create a scripting environment that:

- allows maximum customisation and extensibility,
- has Intelisense/CodeComplete,
- with full access to rich APIs
- allows to quickly create new APIS and new methods
- allows one-click execution of scripts created

I'm basically looking for: ***Strongly Typed Python***

PROBLEM:

Create a scripting environment that:

- allows maximum customisation and extensibility,
- has Intelisense/CodeComplete,
- with full access to rich APIs
- allows to quickly create new APIS and new methods
- allows one-click execution of scripts created

I'm basically looking for: ***Strongly Typed Python***

SOLUTION:

PROBLEM:

Create a scripting environment that:

- allows maximum customisation and extensibility,
- has Intelisense/CodeComplete,
- with full access to rich APIs
- allows to quickly create new APIS and new methods
- allows one-click execution of scripts created

I’m basically looking for: ***Strongly Typed Python***

SOLUTION:

O2 Scripting environment based on C# ExtensionMethods, code refactoring and dynamic compilation of script (and supporting C# files)

PROBLEM:

PROBLEM:

Analyse Source Code Findings (Created by OunceLabs tool) and:

- list unique sources and sinks
- filter findings based on complex criteria
- join and visualise similar findings and identify patterns
- join traces (getters and setters, interfaces, reflection calls, etc...)
- mass create rules based on analysis targets
- dump Ounce's Intermediate Representation (i.e. the analysed code as an Object Model)
- Handle 1+ Million Findings and 300Mb+ Findings file

PROBLEM:

Analyse Source Code Findings (Created by OunceLabs tool) and:

- list unique sources and sinks
- filter findings based on complex criteria
- join and visualise similar findings and identify patterns
- join traces (getters and setters, interfaces, reflection calls, etc...)
- mass create rules based on analysis targets
- dump Ounce's Intermediate Representation (i.e. the analysed code as an Object Model)
- Handle 1+ Million Findings and 300Mb+ Findings file

SOLUTION:

PROBLEM:

Analyse Source Code Findings (Created by OunceLabs tool) and:

- list unique sources and sinks
- filter findings based on complex criteria
- join and visualise similar findings and identify patterns
- join traces (getters and setters, interfaces, reflection calls, etc...)
- mass create rules based on analysis targets
- dump Ounce's Intermediate Representation (i.e. the analysed code as an Object Model)
- Handle 1+ Million Findings and 300Mb+ Findings file

SOLUTION:

Created a bunch of O2 modules that solved these and many more problems

PROBLEM:

PROBLEM:

Source Code: Handle the lack-of-visibility that static analysis engines have (in this case AppScan/OunceLabs engine) with identifying web services (i.e.

PROBLEM:

Source Code: Handle the lack-of-visibility that static analysis engines have (in this case AppScan/OunceLabs engine) with identifying web services (i.e.

SOLUTION:

PROBLEM:

Source Code: Handle the lack-of-visibility that static analysis engines have (in this case AppScan/OunceLabs engine) with identifying web services (i.e.

SOLUTION:

Parse the source code to find the 'formula' that defines the Web Services in the Frameworks used, and mass-create rules that allow its effective scanning

PROBLEM:

PROBLEM:

Analyse an **Spring MVC** application (from both a BlackBox and WhiteBox point of view)

PROBLEM:

Analyse an **Spring MVC** application (from both a BlackBox and WhiteBox point of view)

SOLUTION:

PROBLEM:

Analyse an **Spring MVC** application (from both a BlackBox and WhiteBox point of view)

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

Analyse an **Struts with Java Faces** application (from both a BlackBox and WhiteBox point of view)

PROBLEM:

Analyse an **Struts with Java Faces** application (from both a BlackBox and WhiteBox point of view)

SOLUTION:

PROBLEM:

Analyse an **Struts with Java Faces** application (from both a BlackBox and WhiteBox point of view)

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

Analyse an **ASP.NET MVC** application (from both a BlackBox and WhiteBox point of view)

PROBLEM:

Analyse an **ASP.NET MVC** application (from both a BlackBox and WhiteBox point of view)

SOLUTION:

PROBLEM:

Analyse an **ASP.NET MVC** application (from both a BlackBox and WhiteBox point of view)

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

Automating Browser actions: list fields, enter data, click on buttons, manipulate html/javascript, etc...

PROBLEM:

Automating Browser actions: list fields, enter data, click on buttons, manipulate html/ javascript, etc...

SOLUTION:

PROBLEM:

Automating Browser actions: list fields, enter data, click on buttons, manipulate html/ javascript, etc...

SOLUTION:

Found a great C# Browser Automation API (WatiN) and wrote a large API that simplifies WatiN's behaviour (using extension methods)

PROBLEM:

PROBLEM:

BlackBox: Deploy payloads in post login pages

PROBLEM:

BlackBox: Deploy payloads in post login pages

SOLUTION:

PROBLEM:

BlackBox: Deploy payloads in post login pages

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

BlackBox: Test for reflected vulnerabilities, for example XSS where there are two unique (and complex) web-browsing paths: one to put the payload and one to confirm exploitability

PROBLEM:

BlackBox: Test for reflected vulnerabilities, for example XSS where there are two unique (and complex) web-browsing paths: one to put the payload and one to confirm exploitability

SOLUTION:

PROBLEM:

BlackBox: Test for reflected vulnerabilities, for example XSS where there are two unique (and complex) web-browsing paths: one to put the payload and one to confirm exploitability

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

BlackBox: Easily create XSS PoCs that are specific to the application and are much more than the ALERT pop-up box that nobody outside the WebAppSecurity space understand's it implication

PROBLEM:

BlackBox: Easily create XSS PoCs that are specific to the application and are much more than the ALERT pop-up box that nobody outside the WebAppSecurity space understand's it implication

SOLUTION:

PROBLEM:

BlackBox: Easily create XSS PoCs that are specific to the application and are much more than the ALERT pop-up box that nobody outside the WebAppSecurity space understand’s it implication

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

BlackBox: Create exploit that leverages data inside ASP.NET Viewstate

PROBLEM:

BlackBox: Create exploit that leverages data inside ASP.NET Viewstate

SOLUTION:

PROBLEM:

BlackBox: Create exploit that leverages data inside ASP.NET Viewstate

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

BlackBox: Confirm that an XSS vulnerability has been fixed, by retesting the original payload (with its automation) using the FuzzDB database

PROBLEM:

BlackBox: Confirm that an XSS vulnerability has been fixed, by retesting the original payload (with its automation) using the FuzzDB database

SOLUTION:

PROBLEM:

BlackBox: Confirm that an XSS vulnerability has been fixed, by retesting the original payload (with its automation) using the FuzzDB database

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

BlackBox: Try to open (in web browser) all files available in the web app's root (i.e. file system), and create authorisation mapping table for multiple users

PROBLEM:

BlackBox: Try to open (in web browser) all files available in the web app's root (i.e. file system), and create authorisation mapping table for multiple users

SOLUTION:

PROBLEM:

BlackBox: Try to open (in web browser) all files available in the web app's root (i.e. file system), and create authorisation mapping table for multiple users

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

BlackBox: Automatically Test/Fuzz WebServices where each request needs to be a valid XML/ SOAP request (or the payloads will never reach the application)

PROBLEM:

BlackBox: Automatically Test/Fuzz WebServices where each request needs to be a valid XML/ SOAP request (or the payloads will never reach the application)

SOLUTION:

PROBLEM:

BlackBox: Automatically Test/Fuzz WebServices where each request needs to be a valid XML/SOAP request (or the payloads will never reach the application)

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

BlackBox: perform brute force authentication (username & password) attacks in multiple forms, each having unique signatures, behaviours and workflows

PROBLEM:

BlackBox: perform brute force authentication (username & password) attacks in multiple forms, each having unique signatures, behaviours and workflows

SOLUTION:

PROBLEM:

BlackBox: perform brute force authentication (username & password) attacks in multiple forms, each having unique signatures, behaviours and workflows

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

BlackBox: Perform multiple requests, where for each request do the following actions:

- take screenshot of page with payload in forms
- submit payload
- take screenshot of resulting page
- save HTML

After completion, visualise and analyse the created data

PROBLEM:

BlackBox: Perform multiple requests, where for each request do the following actions:

- take screenshot of page with payload in forms
- submit payload
- take screenshot of resulting page
- save HTML

After completion, visualise and analyse the created data

SOLUTION:

PROBLEM:

BlackBox: Perform multiple requests, where for each request do the following actions:

- take screenshot of page with payload in forms
- submit payload
- take screenshot of resulting page
- save HTML

After completion, visualise and analyse the created data

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

BlackBox: Give developers the ability to reproduce the security findings

PROBLEM:

BlackBox: Give developers the ability to reproduce the security findings

SOLUTION:

PROBLEM:

BlackBox: Give developers the ability to reproduce the security findings

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

BlackBox: Show developers the multiple ways and variations that a particular vulnerability can be exploited

PROBLEM:

BlackBox: Show developers the multiple ways and variations that a particular vulnerability can be exploited

SOLUTION:

PROBLEM:

BlackBox: Show developers the multiple ways and variations that a particular vulnerability can be exploited

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

Show end-client (and developers) the tests made during the security and its coverage

PROBLEM:

Show end-client (and developers) the tests made during the security and its coverage

SOLUTION:

PROBLEM:

Show end-client (and developers) the tests made during the security and its coverage

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

BlackBox: test for CRSF on complex web applications with multiple workflows and complex state

PROBLEM:

BlackBox: test for CRSF on complex web applications with multiple workflows and complex state

SOLUTION:

PROBLEM:

BlackBox: test for CRSF on complex web applications with multiple workflows and complex state

SOLUTION:

Create an API that exposes the application's behaviour as a set of methods, which can the be invoked in a *foreach(var payload in payloads)* loop which handles the payload submission and data collection (i.e. screenshots and html data returned)

PROBLEM:

PROBLEM:

BlackBox: After during code review, finding some ***‘this CRSF token looks like poor crypto to me’*** vulnerability, correctly identify and exploit it.

PROBLEM:

BlackBox: After during code review, finding some ***'this CRSF token looks like poor crypto to me'*** vulnerability, correctly identify and exploit it.

SOLUTION:

PROBLEM:

BlackBox: After during code review, finding some ***'this CRSF token looks like poor crypto to me'*** vulnerability, correctly identify and exploit it.

SOLUTION:

Isolate the original code into a testable component, which is then used to map its entropy behaviour, confirm vulnerable scenario, write ***"CRSF token generator"*** and write javascript based exploit/PoC to detect Login timings

PROBLEM:

PROBLEM:

Create a PoC for the "Google Wireless MAC Address Location exposure"

As made famous by Sammy's "How I meet your girlfriend" presentation

PROBLEM:

Create a PoC for the “Google Wireless MAC Address Location exposure”

As made famous by Sammy’s “How I meet your girlfriend” presentation

SOLUTION:

PROBLEM:

Create a PoC for the "Google Wireless MAC Address Location exposure"

As made famous by Sammy's "How I meet your girlfriend" presentation

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

GreyBox:

Using WhiteBox findings/data to drive BlackBox Analysis

PROBLEM:

GreyBox:

Using WhiteBox findings/data to drive BlackBox Analysis

SOLUTION:

PROBLEM:

GreyBox:

Using WhiteBox findings/data to drive BlackBox Analysis

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

GreyBox Analysis: After finding an XSS in a Custom ASP.NET Control (using on a number of pages) find all vulnerable properties and map them to all exposed web pages

PROBLEM:

GreyBox Analysis: After finding an XSS in a Custom ASP.NET Control (using on a number of pages) find all vulnerable properties and map them to all exposed web pages

SOLUTION:

PROBLEM:

GreyBox Analysis: After finding an XSS in a Custom ASP.NET Control (using on a number of pages) find all vulnerable properties and map them to all exposed web pages

SOLUTION:

Wrote O2 script that isolated the affected controls (using reflection) and fuzzes each exposed property to find out the vulnerable ones. Once that is known, use MethodStreams to find out which output controlled parameter reaches it

This is a great case study of O2's ability to allow the full analysis and understanding of systemic vulnerabilities

PROBLEM:

PROBLEM:

BlackBox: Automate the test and exploitability complex browser-driven applications, specially ones with tons of dynamic Javascript and AJAX requests

PROBLEM:

BlackBox: Automate the test and exploitability complex browser-driven applications, specially ones with tons of dynamic Javascript and AJAX requests

SOLUTION:

PROBLEM:

BlackBox: Automate the test and exploitability complex browser-driven applications, specially ones with tons of dynamic Javascript and AJAX requests

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

BlackBox: While testing create APIs that allow immediate access to 'payload injection' locations without needing to manually go through the steps required to get there (for example, when testing form fields in the post-login 3rd page of a shopping cart workflow)

PROBLEM:

BlackBox: While testing create APIs that allow immediate access to ‘payload injection’ locations without needing to manually go through the steps required to get there (for example, when testing form fields in the post-login 3rd page of a shopping cart workflow)

SOLUTION:

PROBLEM:

BlackBox: While testing create APIs that allow immediate access to 'payload injection' locations without needing to manually go through the steps required to get there (for example, when testing form fields in the post-login 3rd page of a shopping cart workflow)

SOLUTION:

O2

PROBLEM:

PROBLEM:

After finding an Header Injection in a WebService method, find all other vulnerable methods, AND, map the vulnerability to the application's source code

PROBLEM:

After finding an Header Injection in a WebService method, find all other vulnerable methods, AND, map the vulnerability to the application's source code

SOLUTION:

PROBLEM:

After finding an Header Injection in a WebService method, find all other vulnerable methods, AND, map the vulnerability to the application's source code

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

Map BlackBox exploits with Source Code traces (i.e.“URLs+Vulnerable-Parameters” to SourceCode’s method+entry-point)

PROBLEM:

Map BlackBox exploits with Source Code traces (i.e."URLs+Vulnerable-Parameters" to SourceCode's method+entry-point)

SOLUTION:

PROBLEM:

Map BlackBox exploits with Source Code traces (i.e. “URLs+Vulnerable-Parameters” to SourceCode’s method+entry-point)

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

Consume data from tools output: FindBugs, OWASP WebScarab, Fiddler, AppScan Standard, AppScan Source Edition, Fortify, CAT.NET, ...

PROBLEM:

Consume data from tools output: FindBugs, OWASP WebScarab, Fiddler, AppScan Standard, AppScan Source Edition, Fortify, CAT.NET, ...

SOLUTION:

PROBLEM:

Consume data from tools output: FindBugs, OWASP WebScarab, Fiddler, AppScan Standard, AppScan Source Edition, Fortify, CAT.NET, ...

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

WhileBox: Review ASP.NET code where all code relevant to a particular method is presented in one location

PROBLEM:

WhileBox: Review ASP.NET code where all code relevant to a particular method is presented in one location

SOLUTION:

PROBLEM:

WhileBox: Review ASP.NET code where all code relevant to a particular method is presented in one location

SOLUTION:

Methods Streams

PROBLEM:

PROBLEM:

WhileBox: Visualise in context (i.e. relevant source code locations) the external validation and code that is executed before or after (for example XSD validation on WebServices or Stored Procedures methods)

PROBLEM:

WhileBox: Visualise in context (i.e. relevant source code locations) the external validation and code that is executed before or after (for example XSD validation on WebServices or Stored Procedures methods)

SOLUTION:

PROBLEM:

WhileBox:Visualise in context (i.e. relevant source code locations) the external validation and code that is executed before or after (for example XSD validation on WebServices or Stored Procedures methods)

SOLUTION:

Methods Streams

PROBLEM:

PROBLEM:

SourceCode: Map ‘stored-procedure-resolution-formula’. in this case: the classes, enums and attributes that map to the stored procedures names

PROBLEM:

SourceCode: Map ‘stored-procedure-resolution-formula’. in this case: the classes, enums and attributes that map to the stored procedures names

SOLUTION:

PROBLEM:

SourceCode: Map ‘stored-procedure-resolution-formula’. in this case: the classes, enums and attributes that map to the stored procedures names

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

WhiteBox: From all available stored procedures, find the ones that are mapped to webservices

PROBLEM:

WhiteBox: From all available stored procedures, find the ones that are mapped to webservices

SOLUTION:

PROBLEM:

WhiteBox: From all available stored procedures, find the ones that are mapped to webservices

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

Mobile Analysis: Grab source code of android app and visualise its dependencies

PROBLEM:

Mobile Analysis: Grab source code of android app and visualise its dependencies

SOLUTION:

PROBLEM:

Mobile Analysis: Grab source code of android app and visualise its dependencies

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

PoCs: Quickly write ASP.NET PoCs for both Exploitation and Security-Fixes (i.e. we need a quick development and test solution that supports the full ASP.NET environment (note: VisualStudio’s workflow is too slow)

PROBLEM:

PoCs: Quickly write ASP.NET PoCs for both Exploitation and Security-Fixes (i.e. we need a quick development and test solution that supports the full ASP.NET environment (note: VisualStudio's workflow is too slow)

SOLUTION:

PROBLEM:

PoCs: Quickly write ASP.NET PoCs for both Exploitation and Security-Fixes (i.e. we need a quick development and test solution that supports the full ASP.NET environment (note: VisualStudio’s workflow is too slow)

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

Create an API for a complex web application like MediaWiki with the ability to:

- Open and edit pages
- Copy and Paste images
- Create an Offline Backup of its content

PROBLEM:

Create an API for a complex web application like MediaWiki with the ability to:

- Open and edit pages
- Copy and Paste images
- Create an Offline Backup of its content

SOLUTION:

PROBLEM:

Create an API for a complex web application like MediaWiki with the ability to:

- Open and edit pages
- Copy and Paste images
- Create an Offline Backup of its content

SOLUTION:

See O2 MediaWIKI API and the O2 MediaWiki Editor

PROBLEM:

PROBLEM:

Easily and programatically handle PGP: Create Keys, Decrypt/Encrypt Text, Decrypt/Encrypt Files

PROBLEM:

Easily and programatically handle PGP: Create Keys, Decrypt/Encrypt Text, Decrypt/Encrypt Files

SOLUTION:

PROBLEM:

Easily and programatically handle PGP: Create Keys, Decrypt/Encrypt Text, Decrypt/Encrypt Files

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

Load and edit Office 2003 files (i.e. OpenXML files)

PROBLEM:

Load and edit Office 2003 files (i.e. OpenXML files)

SOLUTION:

PROBLEM:

Load and edit Office 2003 files (i.e. OpenXML files)

SOLUTION:

Added support for OpenXml via the C# api

PROBLEM:

PROBLEM:

Load and extract data from PDF files

PROBLEM:

Load and extract data from PDF files

SOLUTION:

PROBLEM:

Load and extract data from PDF files

SOLUTION:

O2 :)

PROBLEM:

PROBLEM:

Test an application that can only be accessed via a Client Certificate (that we have) but that is not accepted by IE or Firefox

PROBLEM:

Test an application that can only be accessed via a Client Certificate (that we have) but that is not accepted by IE or Firefox

SOLUTION:

PROBLEM:

Test an application that can only be accessed via a Client Certificate (that we have) but that is not accepted by IE or Firefox

SOLUTION:

Create a module that used OpenSsl.exe to create a connection with the server (using the certificate) and allow the easy browsing and testing of the target application (i.e. using OpenSsl as a WebProxy)

PROBLEM:

PROBLEM:

CAT.NET: Mass scan large number of assemblies, and analyse its result.

PROBLEM:

CAT.NET: Mass scan large number of assemblies, and analyse its result.

SOLUTION:

PROBLEM:

CAT.NET: Mass scan large number of assemblies, and analyse its result.

SOLUTION:

Created API that wraps and exposes CAT.NET process into easy to consume methods; convert CAT.NET findings into O2 findings, analyse results in the multiple O2 Findings viewers

PROBLEM:

PROBLEM:

Access Java Class Metadata from O2 scripts

PROBLEM:

Access Java Class Metadata from O2 scripts

SOLUTION:

PROBLEM:

Access Java Class Metadata from O2 scripts

SOLUTION:

Used Jython to parse the Java class files, which were exported as XML files and reimported into O2 as strongly typed objects

PROBLEM:

PROBLEM:

Consume and analyse an XML File

PROBLEM:

Consume and analyse an XML File

SOLUTION:

PROBLEM:

Consume and analyse an XML File

SOLUTION:

This is a very common action in O2, which exposes the following workflow in a couple lines of code:

- Load XML file query easily search and view data
- Create XSD from XML file
- Create CSharp file from XSD
- Create an Assembly from the CSharp file
- Load the original XML as a strongly typed object
- Write analysis on top of the “Xml Managed Class”

PROBLEM:

PROBLEM:

Consume and Analyse a non-xml file format or protocol (typical usage of Parser/Token technology (like ANTLR))

PROBLEM:

Consume and Analyse a non-xml file format or protocol (typical usage of Parser/Token technology (like ANTLR))

SOLUTION:

PROBLEM:

Consume and Analyse a non-xml file format or protocol (typical usage of Parser/Token technology (like ANTLR))

SOLUTION:

Used C# Irony Parser library to create an environment were one (via O2 scripting environment) can write and consume the Parser in real time (PoC was in consuming CMD.EXE ***dir*** command)

PROBLEM:

PROBLEM:

Write scripts that consume O2 APIs from other languages (i.e. not in C#) and Operating Systems (i.e. not Windows)

PROBLEM:

Write scripts that consume O2 APIs from other languages (i.e. not in C#) and Operating Systems (i.e. not Windows)

SOLUTION:

PROBLEM:

Write scripts that consume O2 APIs from other languages (i.e. not in C#) and Operating Systems (i.e. not Windows)

SOLUTION:

O2 APIs can be accessed from:

- Python: Using IronPython
- Ruby: Using IronRuby
- Any .NET Language :)
- ***Java: Using IKVM***

Most of O2 compiles in MONO and some GUIs and APIs have been successfully executed in MacOSx

PROBLEM:

PROBLEM:

Monitor TCP traffic without installing WireShark, LibPack

PROBLEM:

Monitor TCP traffic without installing WireShark, LibPack

SOLUTION:

PROBLEM:

Monitor TCP traffic without installing WireShark, LibPack

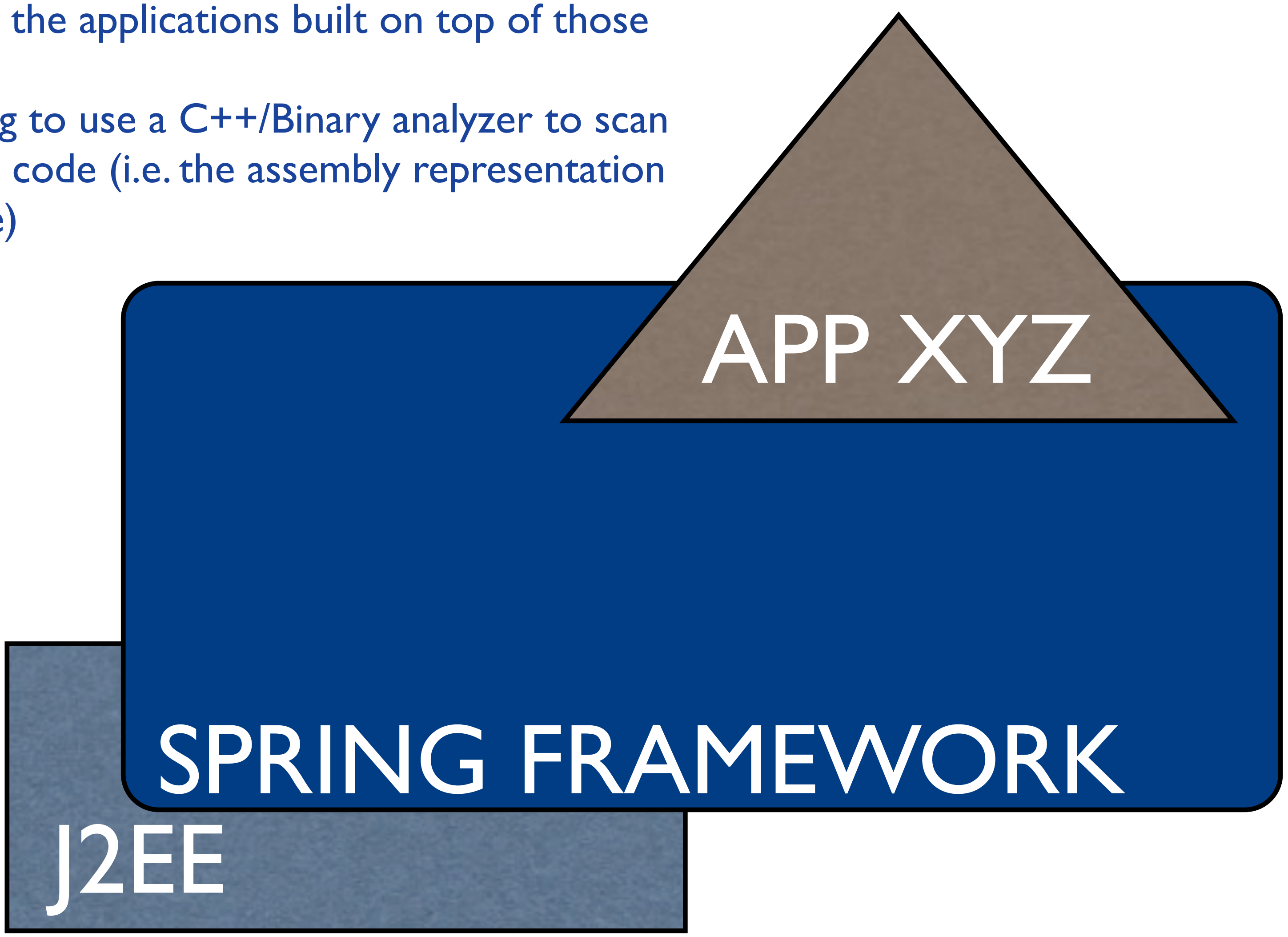
SOLUTION:

O2 :)

THE CHALLENGE

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 were the current level of support is:
  - **1996-2000:** MainFrames, Web Servers, Java, ASP Classic
  - **2000-2004:** C/C++, .NET Framework, J2EE, PHP

‘Out of the box‘ capabilities is here

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

O2 is here

  - **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 :)

We need to be here ASAP

TO SCALE WE NEED TARGETED SOLUTIONS

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 has 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 ....

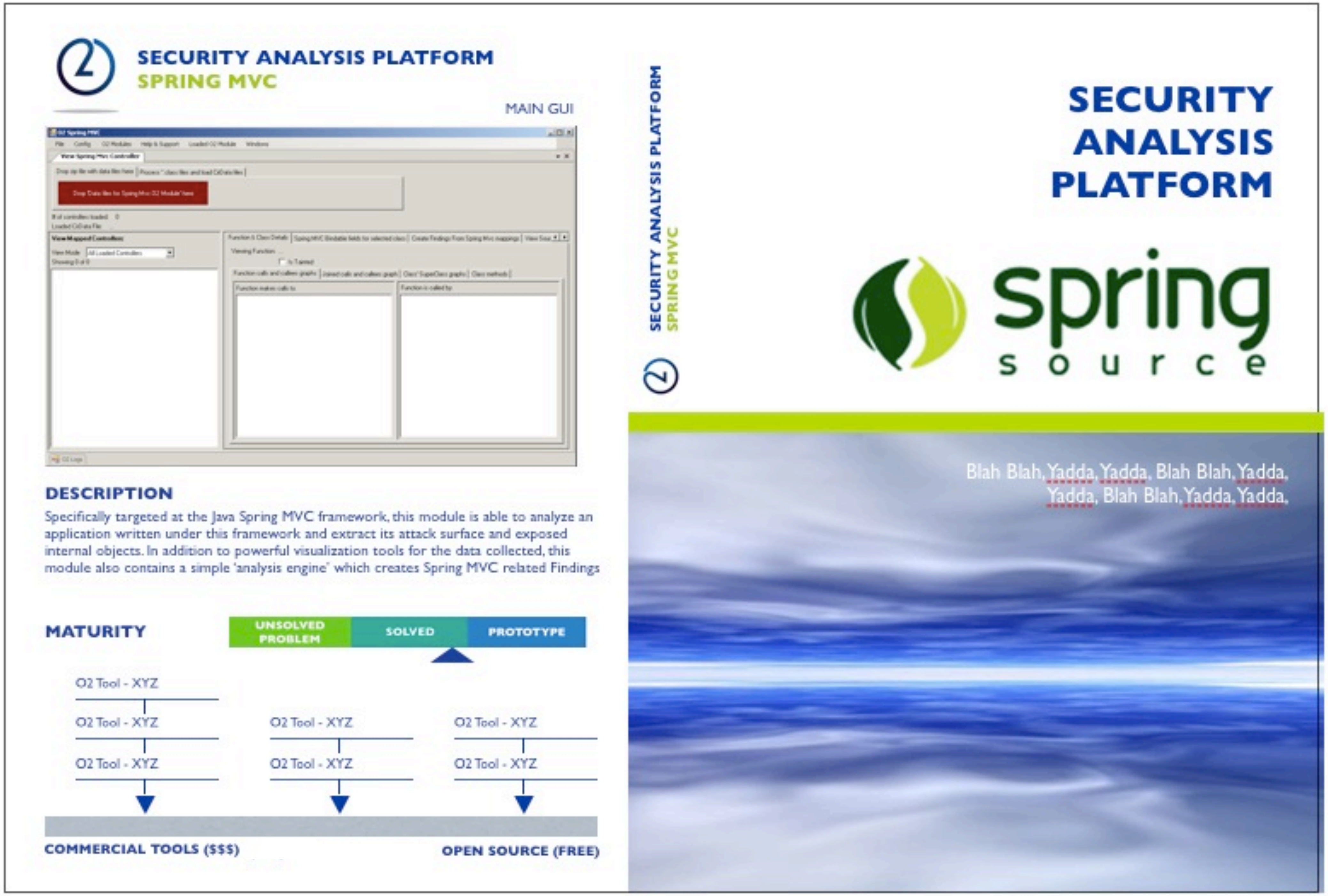
WE CREATE TARGETED SOLUTIONS & PRODUCT

(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



SECURITY ANALYSIS PLATFORM
SPRING MVC

MAIN GUI

O2 Spring MVC
File
Config
O2 Modules
Help & Support
Loaded O2 Module
Windows
View Spring Mvc Controller
Drop zip file with data files here
Process *.class files and load CirData files
Drop 'Data files for Spring Mvc O2 Module' here
# of controllers loaded 0
Loaded CirData File
View Mapped Controllers
View Mode
All Loaded Controllers
Showing 0 of 0
Function & Class Details
Spring MVC Bindable fields for selected class
Create Findings From Spring Mvc mappings
Viewing Function
Is Tainted
Function calls and callees graphs
Joined calls and callees graph
Class' SuperClass graphs
Class methods
Function makes calls to
Function is called by
O2 Logs

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

SECURITY ANALYSIS PLATFORM

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.

SECURITY ANALYSIS PLATFORM
Microsoft Office SharePoint Server

Microsoft Office SharePoint Server 2007

SECURITY ANALYSIS PLATFORM

Security Analysis Platform specifically customized for Microsoft's Office Sharepoint Server (MOSS)

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: "*... 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...*"

SECURITY ANALYSIS PLATFORM

ShareWorks

ShareWorkz

SECURITY ANALYSIS PLATFORM

ShareWorkz Unified User Interface
ShareWorkz Template Libraries
ShareWorkz Core Components
BizTalk Server
Office System
Sharepoint Portal Server
MS CRM
Windows Sharepoint S
Microsoft SQL Server
Microsoft Windows Server
Extranet Complex Multi-party Collaboration
Extranet Information
Intranet Information
ShareWorkz CORE
Extranet Project
Intranet Project
Intranet Process
Extranet Process
Intranet Community
Extranet Community
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*")

Where to go next?

O2
Commercial Services

Not an OWASP initiative

Just to be very clear:

- The services and commercial services described in this presentation are NOT provided by the OWASP foundation, they are NOT an OWASP driven activity and OWASP has no responsibility on the allocation of these funds
- The financial entity behind these services is an UK Limited company owned by O2 Platform's main developer (Dinis Cruz)

Funding model for: O2 Software Development

Three core revenue sources:

1) Subscriptions
2) O2 pledges
3) Training

Funding is to pay for O2 Development costs, NOT to provide commercial consulting services

Commercial consulting services to be provided by 'O2 Certified VARs'

Funds independent from OWASP

O2
Subscriptions

Subscription model

- In order to fully support to the companies that commit to using O2 and use it on commercial engagements, the following subscription-based services are now available:

- **Bronze : 1,000 USD per Quarter**

  * Certified Monthly Build (with customization(16h) of modules included)
  * Monthy Documentation (with customization of modules included)
  * 1x shared amazon EC Image (containing latest version of O2 and demo files)
  * 4h of Personalized Training (remote)
  * Private discusion forum (with 48h max response time)
  * Officially recognized as 'O2 Platform BRONZE Service Provider'

- **Silver: 5,000 USD per Quarter**

  * Certified Monthly Build (with customization(32h) of modules included)
  * Monthy Documentation (with customization of modules included)
  * 3x shared amazon EC Images + 1x dedicated amazon EC Image (containing latest or the customized version of O2)
  * 8h of Personalized Training (remote)
  * Private discusion forum (with 32h max response time)
  * Officially recognized as 'O2 Platform SILVER Service Provider'

- **Gold: 15,000 USD per Quarter**

  * Certified Monthly Build (with customization (48h) modules included and GUI Branding)
  * Monthy Documentation (with customization of modules included and GUI Branding)
  * 5x dedicated amazon EC Image (containing latest or the customized version of O2)
  * 2 days of personalized training (either remote or locally (if logistically possible))
  * Private discusion forum (with 24h max response time)
  * Officially recognized as 'O2 Platform GOLD Service Provider'

Subscription model

	Bronze	Silver	Gold
Custom version of O2	YES	YES	YES
Certified Monthly Build:	with **16h** of module's customisation	with **32h** of module's customisation	with **48h** of module's customisation and GUI Branding
Monthly Documentation:	customised to used modules	customised to used modules	customised to used modules and GUI Branding
EC Images:	1x shared	3x shared, 1x dedicated	5x dedicated
Private discussion forum:	48h response time SLA	32h response time SLA	24h response time SLA
Personalised Training:	4h (remote)	8h (remote)	2 days (either remote or onsite)
Officially recognised as:	O2 Platform BRONZE Service Provider'	O2 Platform SILVER Service Provider'	O2 Platform GOLD Service Provider'
COST (per Quarter)	**1,000 USD**	**5,000 USD**	**15,000 USD**

O2 Subscribers - Silver

Service Provider, US Based

Service Provider, EU Based

BlackBox Tool

O2 Pledges

Development Pledges

10 ‘Funding Packages’ with specific delivery targets:

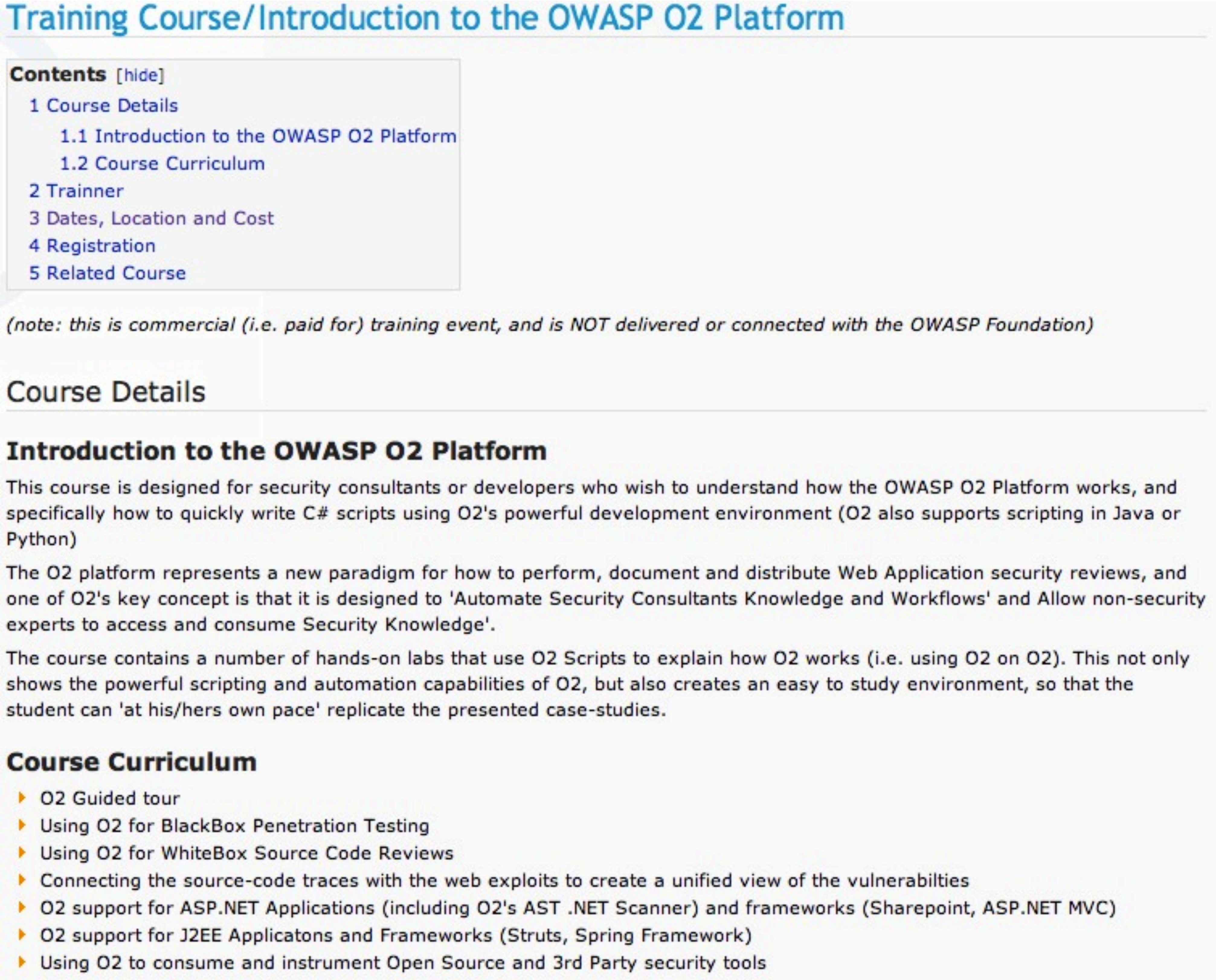
pledgie Helping you help others

using http://pledgie.com/

- O2 specific:
  - #1 OWASP O2 Platform v2.0
  - #2 Support FOSS projects used by O2
- by language:
  - #3 Java Static Analysis Engine (TDB)
- by industry
  - #4 BlackBox Rule Pack
  - #5 WhiteBox Rule Pack
  - #6 WAF/IDS Rule Pack
- by framework
  - #7 Struts Rule Pack
  - #8 Spring MVC Rule Pack
  - #9 SharePoint Rule Pack
  - #10 ASP.NET MCV Rule Pack

O2 Training

O2 Training Course - Introduction to O2



Training Course/Introduction to the OWASP O2 Platform

Contents [hide]

(note: this is commercial (i.e. paid for) training event, and is NOT delivered or connected with the OWASP Foundation)

Course Details

Introduction to the OWASP O2 Platform

This course is designed for security consultants or developers who wish to understand how the OWASP O2 Platform works, and specifically how to quickly write C# scripts using O2's powerful development environment (O2 also supports scripting in Java or Python)

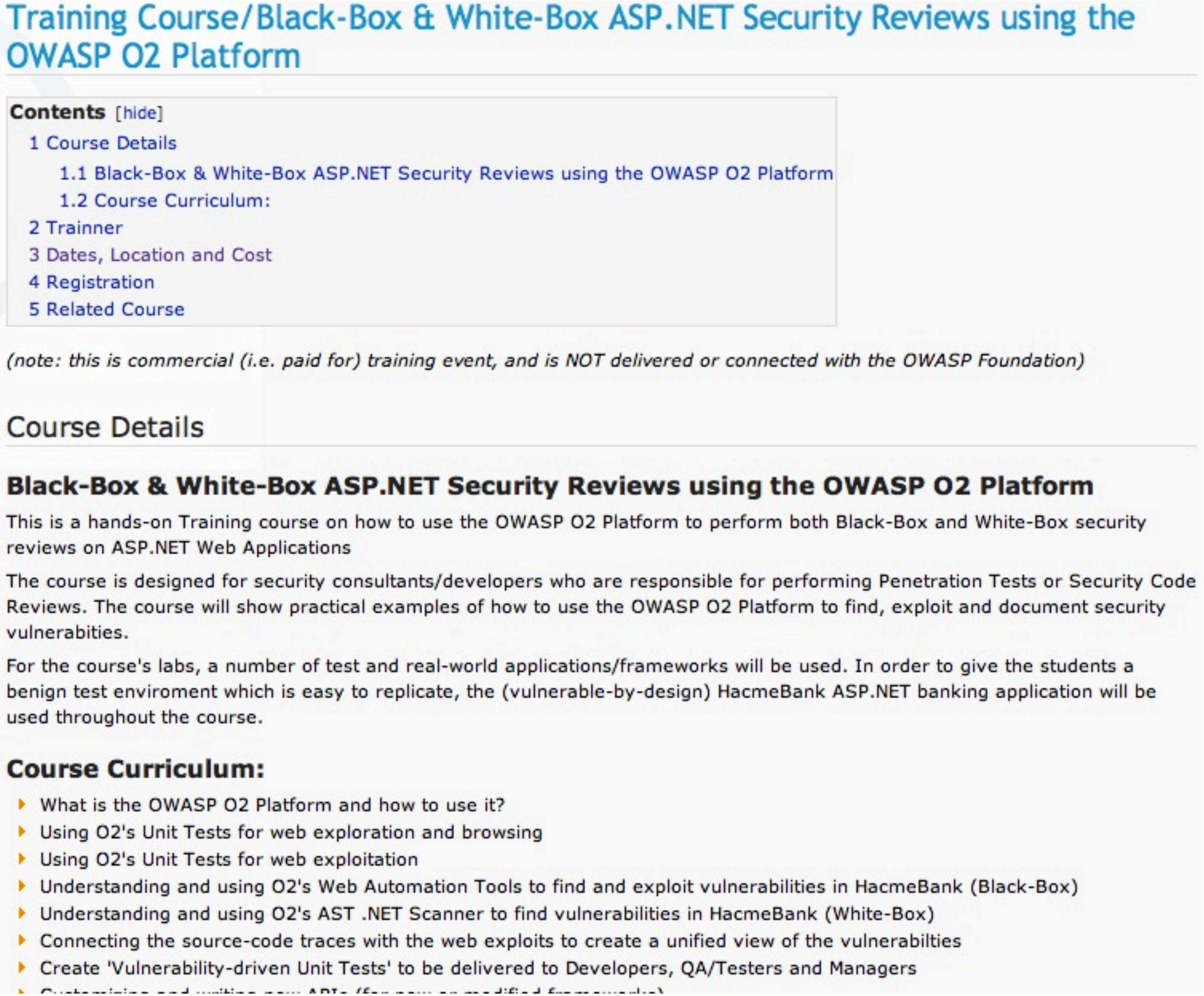
The O2 platform represents a new paradigm for how to perform, document and distribute Web Application security reviews, and one of O2's key concept is that it is designed to 'Automate Security Consultants Knowledge and Workflows' and Allow non-security experts to access and consume Security Knowledge'.

The course contains a number of hands-on labs that use O2 Scripts to explain how O2 works (i.e. using O2 on O2). This not only shows the powerful scripting and automation capabilities of O2, but also creates an easy to study environment, so that the student can 'at his/hers own pace' replicate the presented case-studies.

Course Curriculum

- O2 Guided tour
- Using O2 for BlackBox Penetration Testing
- Using O2 for WhiteBox Source Code Reviews
- Connecting the source-code traces with the web exploits to create a unified view of the vulnerabilties
- O2 support for ASP.NET Applications (including O2's AST .NET Scanner) and frameworks (Sharepoint, ASP.NET MVC)
- O2 support for J2EE Applicatons and Frameworks (Struts, Spring Framework)
- Using O2 to consume and instrument Open Source and 3rd Party security tools

O2 Training Course



Training Course/Black-Box & White-Box ASP.NET Security Reviews using the OWASP O2 Platform

Contents [hide]

(note: this is commercial (i.e. paid for) training event, and is NOT delivered or connected with the OWASP Foundation)

Course Details

Black-Box & White-Box ASP.NET Security Reviews using the OWASP O2 Platform

This is a hands-on Training course on how to use the OWASP O2 Platform to perform both Black-Box and White-Box security reviews on ASP.NET Web Applications

The course is designed for security consultants/developers who are responsible for performing Penetration Tests or Security Code Reviews. The course will show practical examples of how to use the OWASP O2 Platform to find, exploit and document security vulnerabities.

For the course's labs, a number of test and real-world applications/frameworks will be used. In order to give the students a benign test enviroment which is easy to replicate, the (vulnerable-by-design) HacmeBank ASP.NET banking application will be used throughout the course.

Course Curriculum:

- What is the OWASP O2 Platform and how to use it?
- Using O2's Unit Tests for web exploration and browsing
- Using O2's Unit Tests for web exploitation
- Understanding and using O2's Web Automation Tools to find and exploit vulnerabilities in HacmeBank (Black-Box)
- Understanding and using O2's AST .NET Scanner to find vulnerabilities in HacmeBank (White-Box)
- Connecting the source-code traces with the web exploits to create a unified view of the vulnerabilties
- Create 'Vulnerability-driven Unit Tests' to be delivered to Developers, QA/Testers and Managers
- Customizing and writing new APIs (for new or modified frameworks)

Where Next?

Try O2 and Join the community

Try O2 and Join the community

- Go to http://o2platform.com to download O2 and read the documentation

Try O2 and Join the community

- Go to http://o2platform.com to download O2 and read the documentation
- Join the O2 Mailing list

Try O2 and Join the community

- Go to http://o2platform.com to download O2 and read the documentation
- Join the O2 Mailing list
- Ask questions

Try O2 and Join the community

- Go to http://o2platform.com to download O2 and read the documentation
- Join the O2 Mailing list
- Ask questions
- Use O2 on your engagements and create Unit Tests for your clients

Any Questions