OWASP ESAPI SwingSet

Fabio Cerullo
Ireland Chapter Leader
Global Education Committee
fcerullo@owasp.org
+353 87 7817468

OWASP

26 April 2011

About me

- Information Security Specialist at AIB
- OWASP Global Education Committee
- OWASP Ireland Chapter Leader
- ESAPI SwingSet Project Leader
- AppSec EU Co-Chair

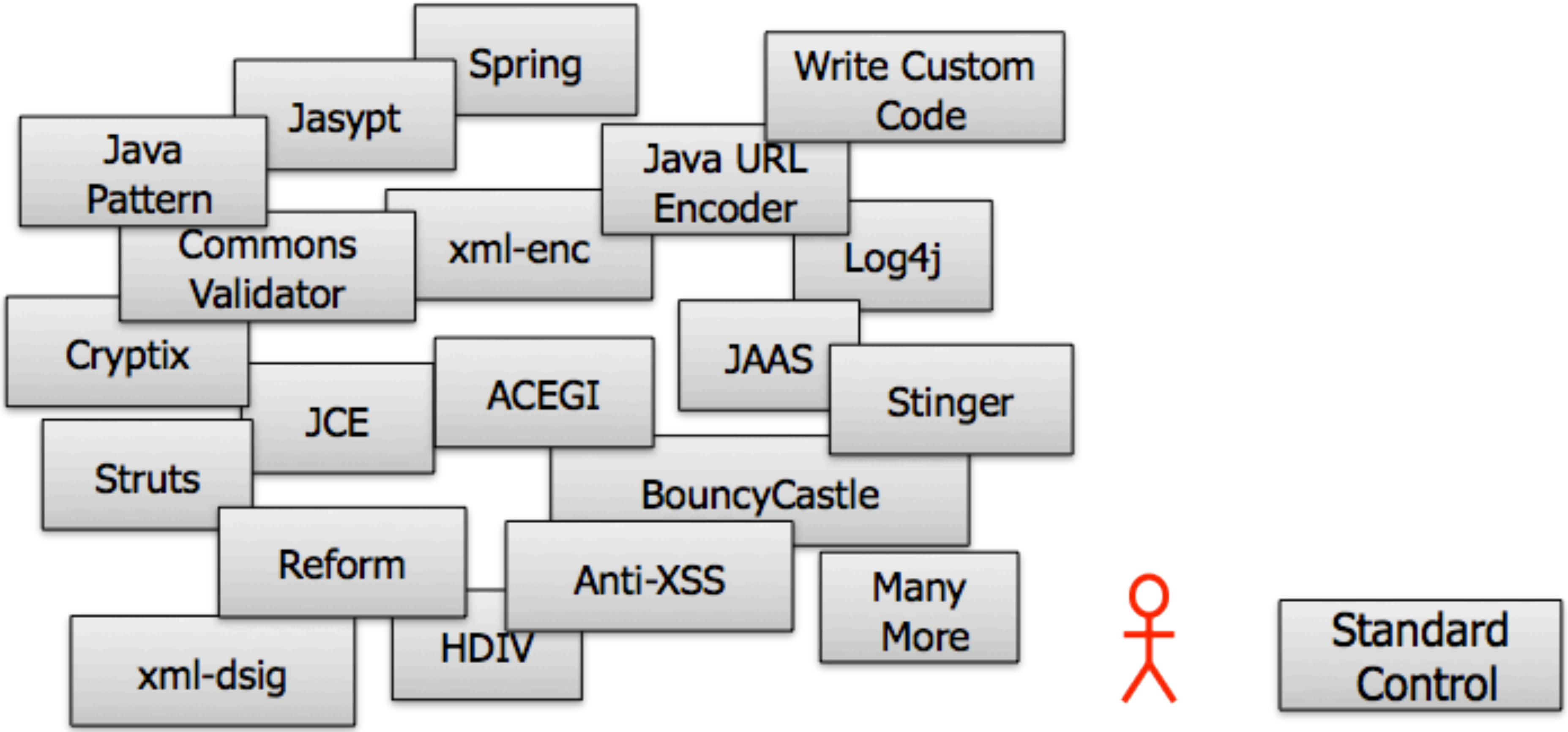
Agenda

- Introduction to OWASP ESAPI
- Security Areas Covered by ESAPI
- Mapping ESAPI > ASVS > Swingset
- SwingSet Demo
- AppSec EU Details
- Q&A

Introduction to ESAPI

- What is the main problem with majority security controls/frameworks?

Introduction to ESAPI



Spring

Write Custom Code

Jasypt

Java Pattern

Java URL Encoder

xml-enc

Commons Validator

Log4j

Cryptix

JAAS

ACEGI

Stinger

JCE

Struts

BouncyCastle

Reform

Anti-XSS

Many More

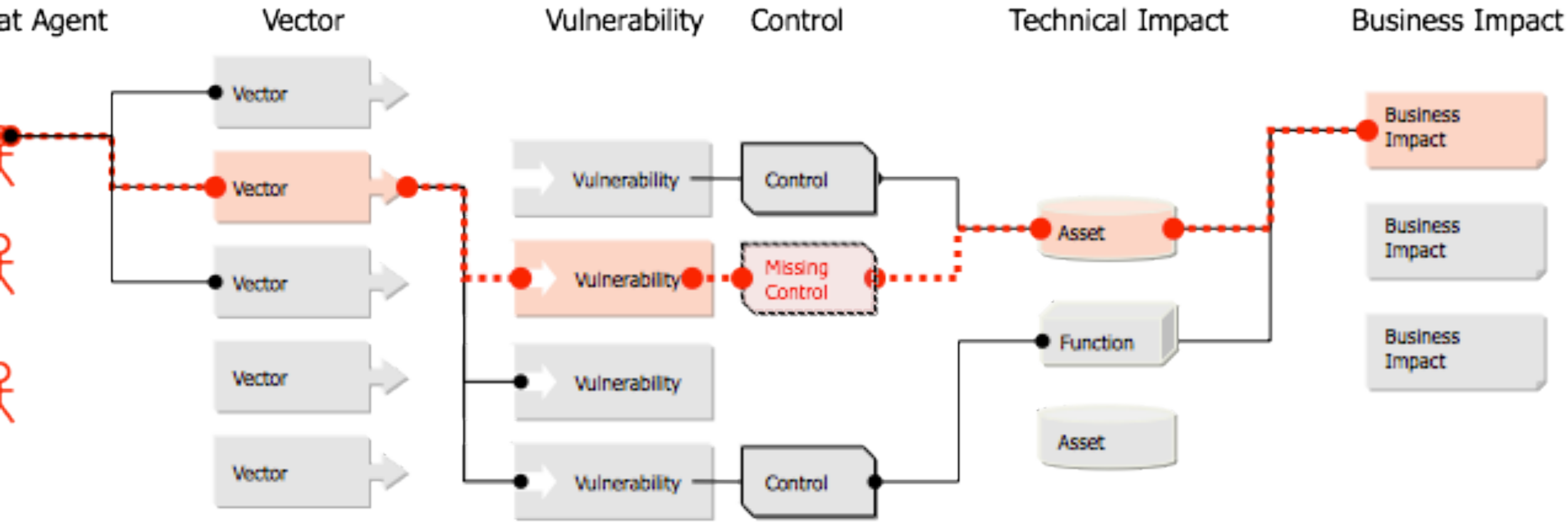
HDIV

xml-dsig

Standard Control

- NOT Intuitive, Integrated nor Dev Friendly.

Introduction to ESAPI



RISK is a path from Threat Agent to Business Impact

Introduction to ESAPI

Every vulnerability originates from:

Missing Control

- Lack of Input Validation
- Failure to perform Access Control

Broken Control

- Improper Session Handling
- Fail Open

ESAPI could help you here

Ignored Control

- Failure to implement Encryption
- Forgot to use Output Encoding

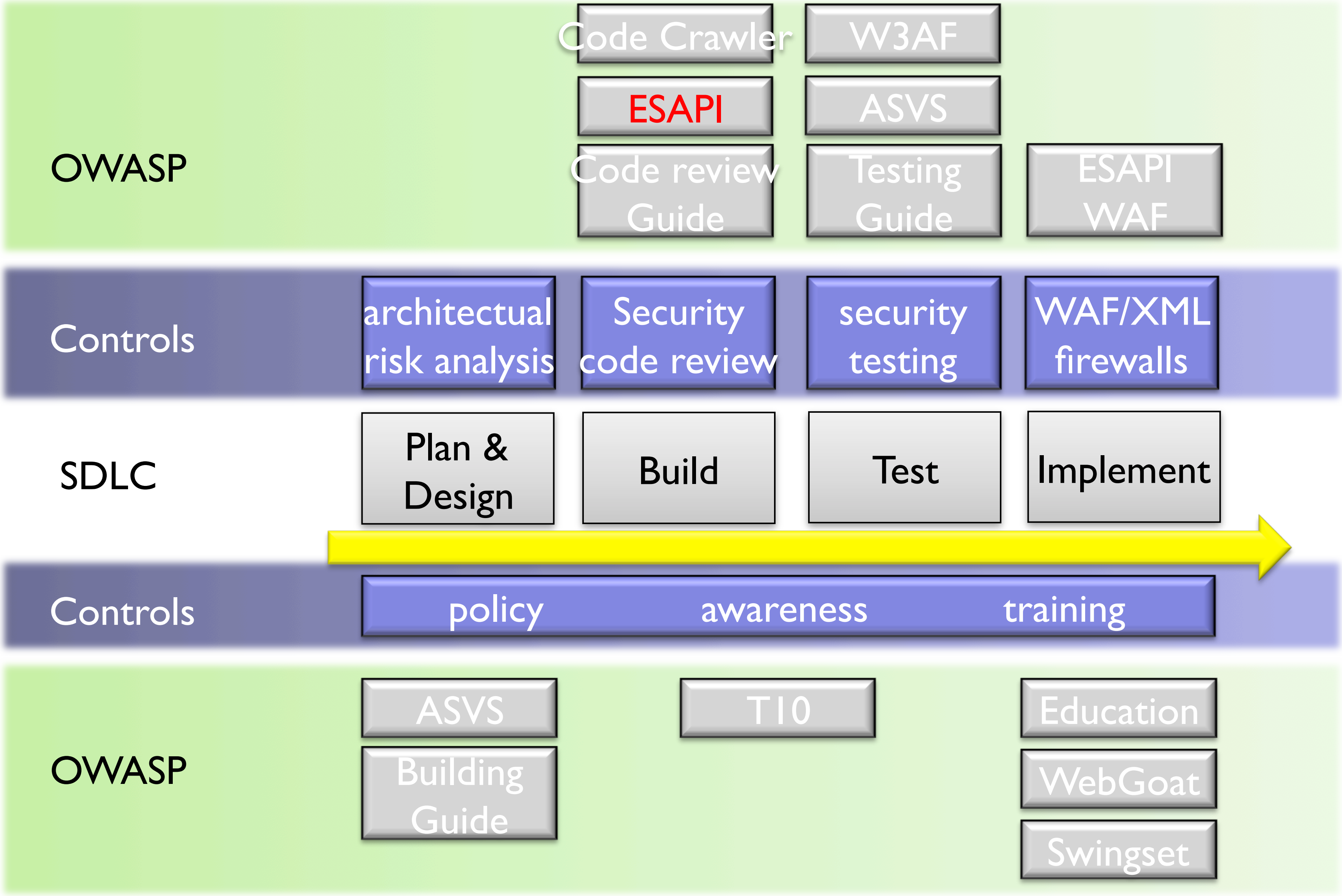
Introduction to ESAPI

- OWASP ESAPI (Enterprise Security API) aims to provide developers with all the security controls they need:
  - Standarized
  - Centralized
  - Organized
  - Integrated
  - High Quality
  - Intuitive
  - Tested

What is ESAPI?

- OWASP Enterprise Security API Toolkits helps software developers guard against security-related design and implementation flaws.
- Collection of classes that encapsulate the key security operations most applications need.
- There are Java EE, .Net, Javascript, Classic ASP ColdFusion/CFML, PHP and Python language versions.
- The ESAPI for JAVA EE version includes a Web Application Firewall (WAF) that can be used to give development teams breathing room while making fixes.
- All language versions of ESAPI Toolkits are licensed under the BSD license.
- You can use or modify ESAPI however you want, even include it in commercial products.

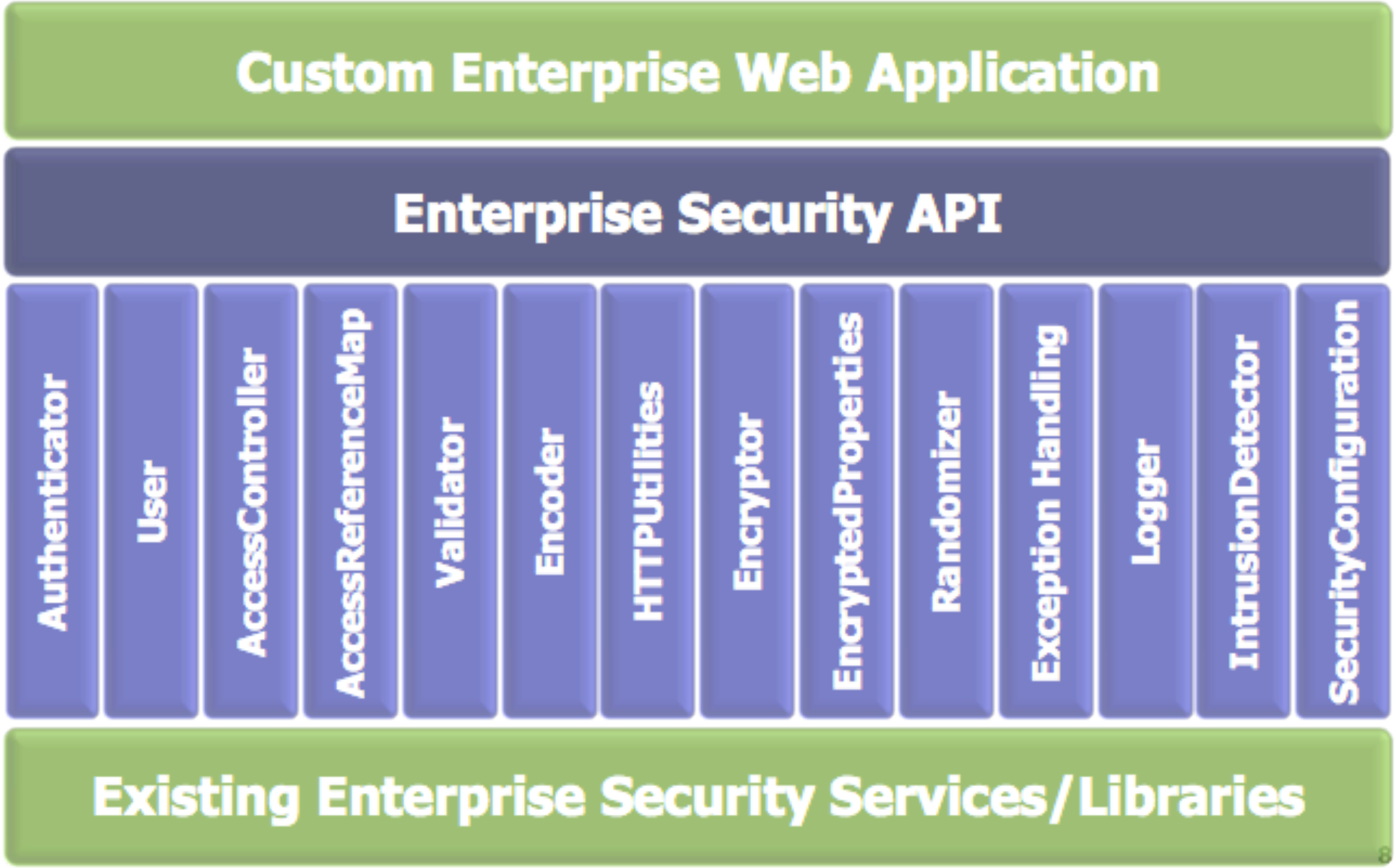
Where does ESAPI fit?



How does ESAPI work?

- Just extract ESAPI distribution package to an appropriate location.
- The ESAPI security control interfaces include an “ESAPI” class that is commonly referred to as a “locator” class.
- The ESAPI locator class is called in order to retrieve instances of individual security controls, which are then called in order to perform security checks.

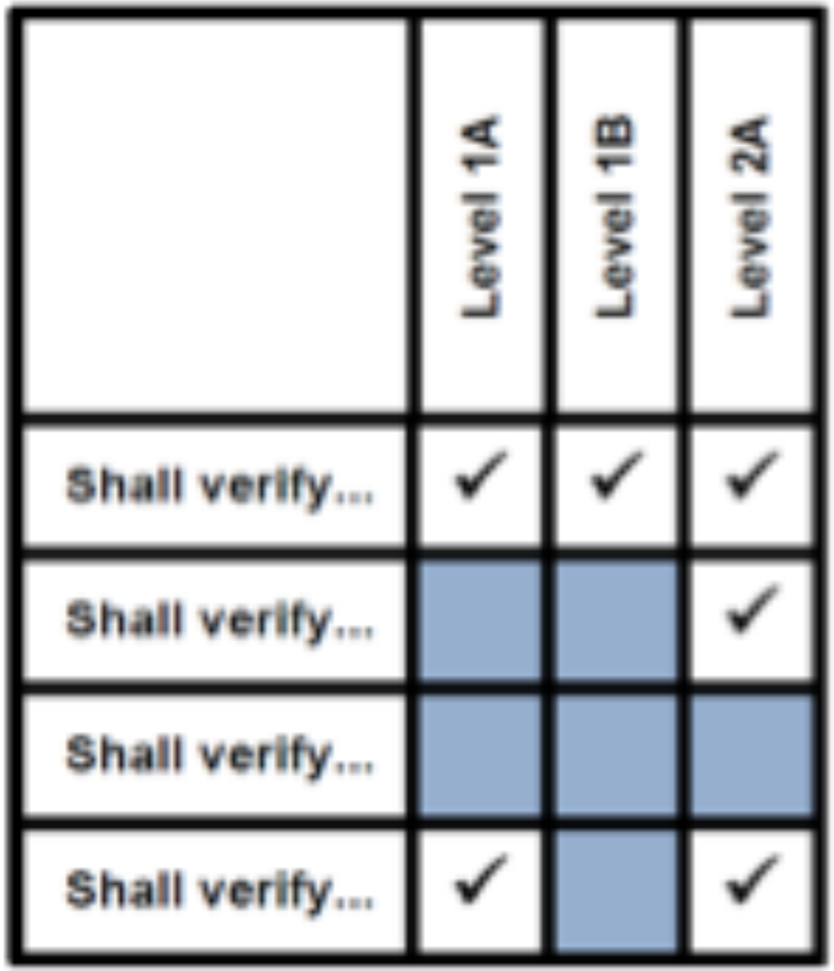
Security Areas Covered by ESAPI



ere are 120+ methods organized in different interfaces

Mapping ESAPI to ASVS

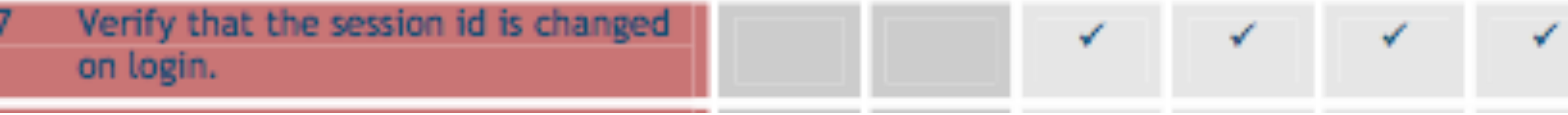
- ASVS can be used to establish a **level of confidence** in the security of Web applications.
  - Authentication
  - Session Management
  - Access Control
  - Input Validation
  - Output Encoding
  - Cryptography
  - Error Handling & Logging
  - Data Protection
  - HTTP S



	Level 1A	Level 1B	Level 2A
Shall verify...	✓	✓	✓
Shall verify...	▨	▨	✓
Shall verify...	▨	▨	▨
Shall verify...	✓	▨	✓

Mapping ESAPI to ASVS - An example -

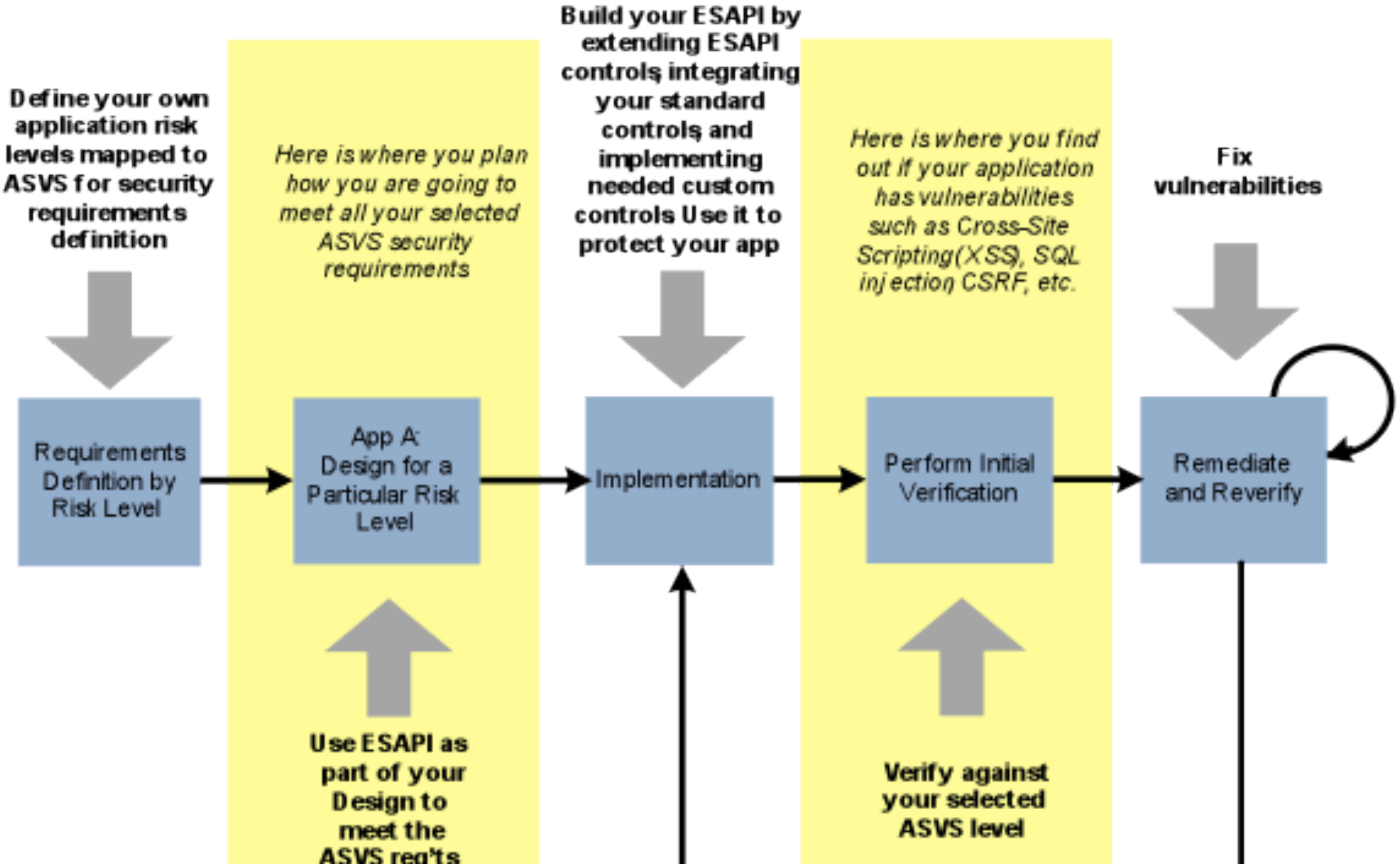
- ASVS Session Management



7	Verify that the session id is changed on login.			✓	✓	✓	✓

- ESAPI Implementation
- ESAPI.httpUtilities().changeSessionIdentifier() changes the session id in the login process
- BTW: prevents session fixation

Mapping ESAPI to ASVS



Define your own application risk levels mapped to ASVS for security requirements definition

Requirements Definition by Risk Level

Here is where you plan how you are going to meet all your selected ASVS security requirements

App A: Design for a Particular Risk Level

Use ESAPI as part of your Design to meet the ASVS req'ts

Build your ESAPI by extending ESAPI controls integrating your standard controls and implementing needed custom controls Use it to protect your app

Implementation

Here is where you find out if your application has vulnerabilities such as Cross-Site Scripting (XSS), SQL injection CSRF, etc.

Perform Initial Verification

Verify against your selected ASVS level

Fix vulnerabilities

Remediate and Reverify

Swingset

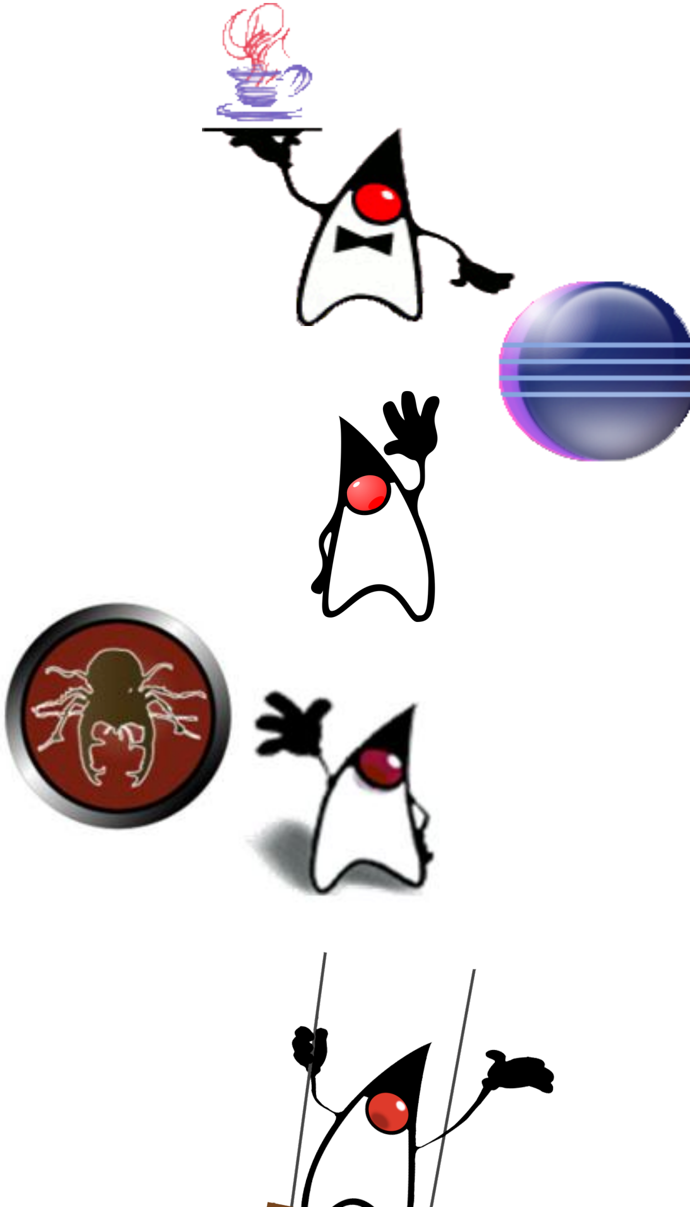
- Originally designed as a Web Application which demonstrates the many uses of ESAPI.
- One issue... lacked interactivity with devs.

Swingset Interactive

- Customized version of Swingset
- Aligned with OWASP GEC mission
- Aimed to train developers on ESAPI
  - ➡ Each lab presents a vulnerability
  - ➡ Developer needs to fix it using ESAPI
- Labs organized around ASVS

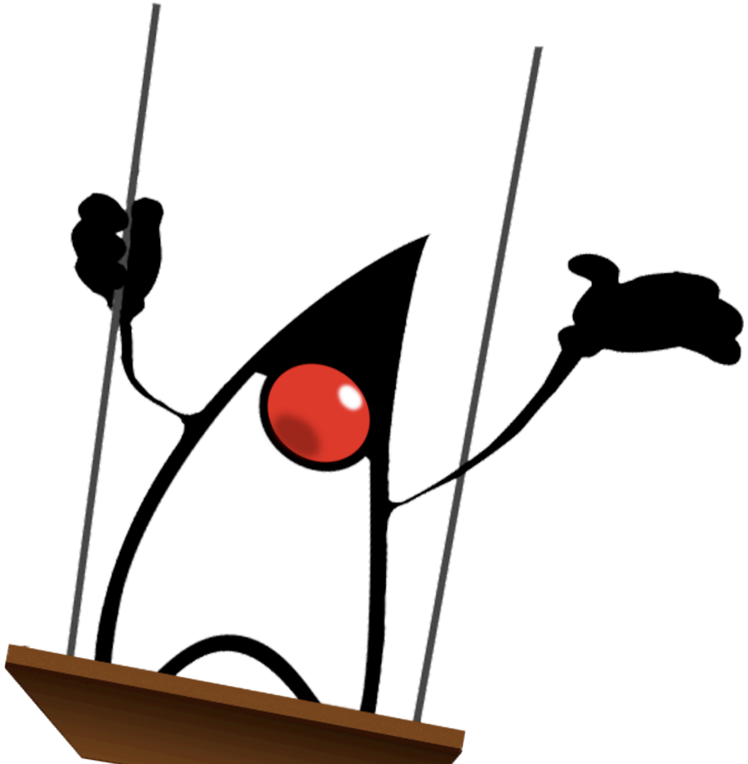
Swingset Interactive

- Installation Requirements:
  - JDK or JRE
  - Eclipse
  - ESAPI for Java
  - Swingset



Swingset Interactive Demo

- Let's go for a swing!



Swingset Interactive Demo

- ESAPI provides a "positive" set of security controls
- ESAPI could be used to improve the security of your applications in alignment with ASVS
- Swingset is a great tool to train developers on how to achieve this.

Swingset Interactive

Future Plans

- Automate installation as much as possible
- Better GUI (side menu/graphics)
- More lessons (eg. beginners/advanced)
- Virtual Lab
- Interested? Drop me an email!

Additional Resources

- ESAPI Swingset Interactive
- https://www.owasp.org/index.php/ESAPI_Swingset
- ESAPI Javadocs
- http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/index.html
- ESAPI book (needs update)
- https://www.owasp.org/images/7/79/ESAPI_Book.pdf

AppSec EU Details

OWASP APPSEC EUROPE 2011
DUBLIN, IRELAND

-Training Days 7th/8th June 2011
-Conference Days 9th/10th June 2011
-Challenges to win a free ticket

Hackademic

SURPRISE!

Raffle this evening among attendees

Q&A

Want to contribute or provide feedback?

FCERULLO@OWASP.ORG

Thank you!