How to be Agile in Security Testing Projects

Security Project Management
whoami # Simone Onofri

- **Security Business Consultant** at Hewlett Packard Enterprise
- **Director** at DSDM Consortium

- Volunteer: **OWASP** (Author TG v4), CoderDojo…
- **Certs:** PRINCE2®, Agile Project Management®, ITIL, Certified ScrumMaster®, ISO 27001…

*Disclaimer:* The opinions expressed in this presentation and on the following slides are solely those of the presenter. Any reference to events or persons is purely coincidental.
About us here

You «offer» Penetration Testing Services

(Provider/Supplier)
About us here

You «receive» Penetration Testing services?
About us here

Something else?
Agenda

• What is Agile in Security Project Management
• The process and how to be Agile
• Embed Security in Agile Software Development Lifecycle
• Q&A
AGILE SECURITY PROJECT MANAGEMENT
What is Agile

“Agile” is an *umbrella* term for several iterative and incremental methodologies. Is a *mindset* and a *style of working* where *requirements and solutions evolve* through *collaboration*. Agile promotes *adaptive planning*, *evolutionary development* and *delivery*, a *timeboxed, iterative* approach and encourages rapid and flexible *response to change*. 
Quote from Sun Tzu

“Order and disorder depends on organization”
What is Project Management

The planning (adaptively), delegating (at the lower level as possible), monitoring-control (without micro-manage) of all aspects of the project, and the motivation of those involved, to achieve the project objectives within the expected performance targets (e.g. time, cost, quality, scope, benefits and risks), delivering proper business product (what?)

(Inspired from PRINCE2® definition)
Question time

• **Question:** which is the typical business product of a Web Application Penetration Test?

• **Scenario:** Security Assessment is the process of determining how effectively an “entity” (e.g. Web Application) meets specific security objectives.

• **Hint:** what the final customer will have at the end of the activities?

*(Security Assessment definition inspired by NIST SP800-115)*
Which is the typical business product of a Web Application Penetration Test?

«Document the Test Results
To conclude the testing process, it is important to produce a formal record of what testing actions were taken, by whom, when they were performed, and details of the test findings. It is wise to agree on an acceptable format for the report which is useful to all concerned parties, which may include developers, project management, business owners, IT department, audit, and compliance.»

OWASP Testing Guide v4 - Introduction
Why Agile in Security Testing?

Environmental factors:
• Nowadays Software Development is already Agile.
• Work is often on a fixed deadline, fixed budget and we still need to deliver results without compromising quality.

Specific Testing factors:
• Security Testing is Agile «by definition».
• We cannot have info «by design» of testing project (e.g. Black-Box).
• Often we will explore from the first technical stage (OTG-INFO-001/010).
How be Agile in Security Testing

• **Transparency** and **communication** between customer and supplier

• Use **Agile techniques** to solve common issues.
  – **Planning Poker** for collaborative planning
  – **Timeboxing** for managing time
  – **MoSCoW** for managing priorities

• Integrate Security in Agile Development
AN AGILE SECURITY TESTING PROJECT
Apply a PM structure to Security being Agile

- **Feasibility**
  - RFP / Tender
  - High-level requirements to estimate (e.g. number of applications and size).
  - Getting business cases.
  - Define output.

- **Foundation**
  - Proposal accepted
  - Planning and technical requirements definition
  - Sign the necessary documentation (e.g. NDA/Authorization*Jail free).

- **Evolutionary**
  - Technical Requirements verification
  - Technical activity
  - Writing Reports...
  - Presents results.

- **Post-Project**
  - Depth analysis
  - Retesting activity
  - ....
Top tips - Feasibility

• In the feasibility phase the issue is to known the Business Case of the Customer: **Why needs a PT?**
  Often there are:
  – Compliance: e.g. laws and regulamentations (e.g. ISO 27001, Bank laws, PCI-DSS).
  – Risk Management to protect the enterprise (e.g. known vulnerabilities first to the attackers can exploit them).

• Define what is the business product (the report), and the structure, of the final output of the project.
Top tips - Reporting

• Is often suggested that the report will have different levels for different audience.
  – Executive Summary
  – Methodology and Tools
  – Technical Summary
  – Technical Details (exploits, TOP 10 mapping, CVSS v2…)

• Specific needs? Be Agile!
Question time

- **Scenario**: You are asked to test a Web Application, using OWASP Testing Guide. The application should be 20-40 dynamic pages with 2 different profiles.
- **Questions**: who have to do the estimate? Other requirements to ask?
Top tips – Estimates!

• **Ask for a lot of information as possible:** technology used,
• **Who?** Technical guys/girls!!!
• **Active/Idle time?** People are active often about 80%
• **Report warning** the writing of the report can take about half the time of technical activities
• **Remote/on-site** Travel time?
• **Specific timeframe?** As a risk reduction and possibility to run automatic tools H24.
• **Project Management Time/Meetings/Writing?**
Agile is your friend

«We have a BrightRay™ Portal with 2 custom portlets and one for payment of membership via SecurePaymentGateway™ portlet»

The Team Lead said to testers. Think about the estimate and pick a card from your deck, wait to show to not influence others.
Planning Poker – first hand

Tester #1

Tester #2

Tester #3

Tester #4
Agile is your friend

Team Lead sees that one tester is not aligned to the others, he/she can has important info to share with others, Tester #3 «I tested BrightRay™ few weeks ago and already automated the procedure for IG (portlet ids enumeration) and have a set of evil portlets for exploitation and post-exploitation» Tester #1 said «this is a good news. From my side I lost a lot of time with SPM portlet because of sophisticated defenses in place."
Planning Poker – second hand

Tester #1: 8
Tester #2: 13
Tester #3: 5
Tester #4: 5
Foundations – Top tips

• Prepare a **document** with **Scope, Rules of Engagements, Limitations, Communication Management Strategy** *(remember Transparency)*.

• **Prioritize activities in particular if we are timeboxed** *(we have an pre-defined and fixed amount of time e.g. to get a fixed price)*, in order to get suitable and useful results. Better a workshop with Supplier/Customer.
Project Variables

Waterfall approach

- Functionalties
- Cost
- Time
- Quality

- Fixed

Agile approach

- Functionalties
- Cost
- Time
- Quality

- Can vary
What to prioritize?

- We have:
  - Vulnerabilities
  - Functionalities / Components
  - Specific «Evil» Use Cases
- And Combine in a Matrix
  - Y axis – Functionalities
  - X axis - OWASP TOP 10
- Think also about:
  - When and how to go deep?
  - When to do manual and automatic activity?
  - False Positive Management

  *Take care of vulnerabilities who have a wide application impact.*
# How to prioritize MoSCoW

<table>
<thead>
<tr>
<th>Level</th>
<th>Importance</th>
<th>Effect if not met</th>
<th>Effort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Must</td>
<td>Vital</td>
<td>Project will fail.</td>
<td>60%</td>
</tr>
<tr>
<td>Should</td>
<td>Important</td>
<td>Not will not fail, but challenged</td>
<td>20%</td>
</tr>
<tr>
<td>Could</td>
<td>Desirable</td>
<td>Contingency</td>
<td>20%</td>
</tr>
<tr>
<td>Won’t</td>
<td>Out of scope</td>
<td>May be a next PT</td>
<td>--</td>
</tr>
</tbody>
</table>
# Wasp in MoSCoW

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Functionality</td>
<td>Must</td>
<td>Must (auto)</td>
<td>Must (AutoScan™), Should (man)</td>
<td>Must (man)</td>
<td>Must (AutoScan™)</td>
</tr>
<tr>
<td>Registration</td>
<td>Must (AutoScan™), Could (man)</td>
<td>Could</td>
<td>Must (AutoScan™), Should (man)</td>
<td>Could</td>
<td>Must (AutoScan™)</td>
</tr>
<tr>
<td>Authentication</td>
<td>Must (AutoScan™), Should (man)</td>
<td>Control itself</td>
<td>Must (AutoScan™), Should (man)</td>
<td>Could</td>
<td>Must (AutoScan™)</td>
</tr>
<tr>
<td>Private Content portlet</td>
<td>Must (AutoScan™), Should (man)</td>
<td>Must (man)</td>
<td>Must</td>
<td>Must (man)</td>
<td>Must (AutoScan™)</td>
</tr>
</tbody>
</table>

**Priorities**

**Exploitation:** No

**False Positive Management:** High (Must), Medium (Should)
Timeboxing – top tips

- **Kick-off**: define objective
- **Investigation**: do initial test and find quick-wins
- **Refinement**: the big testing work
- **Consolidation**: stop starting, start finishing
- **Close-out**: met with customer about the job done
AN AGILE SSDLC
Embedding Security in Agile SSDLC

In some cases, the customer has already an Agile process for SDLC. How Agile can be secure?

- **Security Testing is still needed** for final testing at least (even if my team is competent, it is goofy to ask for a Technical Advisor)
- Implement a **Definition of Done / Acceptance Criteria** for Security
- Implement **Evil User Stories**
- **Pair Programming** with Developers and Security Experts

Image from Wikipedia, Lisamarie Babik
Be Agile, and Lean... how to manage the Vulnerabilities

All todos are blocked (red is present on the Kanban). Now is the time to ask to the Penetration Tester team to Retest.
THANK YOU

Simone Onofri
simone@onofri.org
https://onofri.org/

Trust the QR Code…
(linkedin, will publish slides)