OWASP Developer Guide

Presentation to Bristol (UK) Chapter

Who am I?

- C/C++ developer for 25 years
- Security engineer for 11 years

Active in OWASP :

- Leader + contributor to OWASP Threat Dragon project
- Co-leader + contributor for OWASP Developer Guide project
- Co-Leader of Bristol (UK) OWASP Chapter

I am a developer, and I need help!

Have you ever said to yourself:

"*I am a developer and I need a reference source to navigate the numerous projects and describes the security activities I really should be doing*"

Quiz

How many official OWASP projects are there?

Quiz

How many official OWASP projects are there?

There are (at least) 322

Quiz

How many official OWASP projects are there?

There are (at least) 322

Bonus question

Name the OWASP projects categories

Quiz

How many official OWASP projects are there?

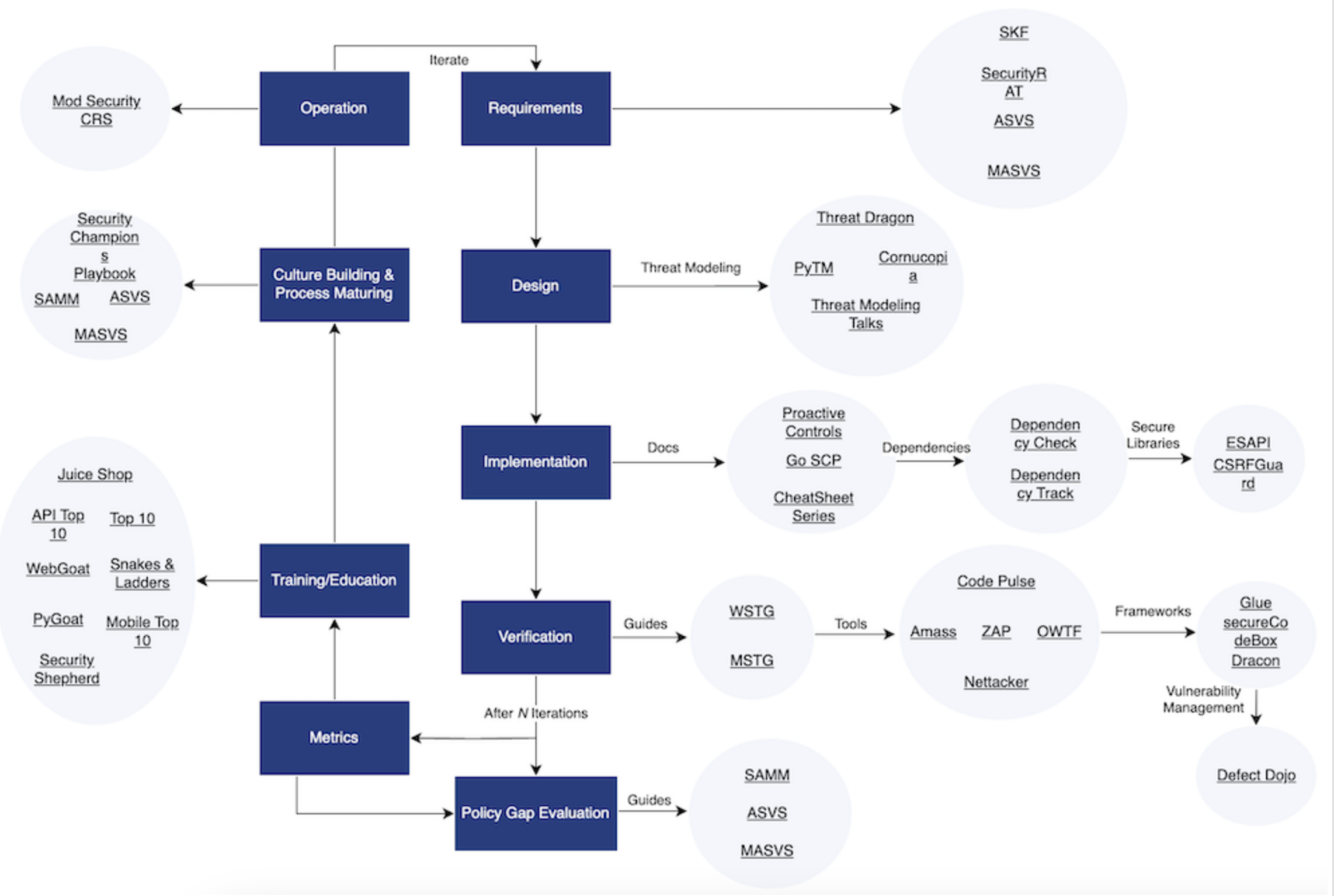
There are (at least) 322

Bonus question

Name the OWASP projects categories

1. Flagship : 15 projects
2. Production : 6 projects
3. Laboratory : 36 projects
4. Incubator : at least 265 and counting

The OWASP Project Wayfinder



What is in the Developer Guide?

What it does do :

- Enough theory to get you started, but no more
- Brief introduction to each project in the Wayfinder
  - What it does, why it is useful
  - Where to get it, how to run it

What is in the Developer Guide?

What it does ***not*** do :

- No topic in detail, lists further reading for that
- No project in detail, refer to the documentation for that

Requirements

Software security requirements are important to get right

- Overview of requirements
- Descriptions of tools, notably
  - ASVS
  - MAS
  - SKF

Design

Software design and architecture requires wide ranging skills and tools

OWASP tools for threat modeling:

- PyTM
- Threat Dragon
- Cornucopia

Implementation

Many tools and guides

- Dependencies
  - For example CycloneDX
- Libraries
  - For example Secure Headers
- Documentation
  - For example Cheat sheet series
  - Top 10 Proactive Controls

Verification

Wide range of tools and documentation

- Guides, such as WSTG
- Tools such as ZAP and Amass
- Frameworks such as Dracon
- Vulnerability Management using DefectDojo

Metrics

Nothing on metrics

- Some introduction, that is all
- No projects or tools :/
- Obviously a gap :)

Training and Education

OWASP provides a wide range of tools

- Secure Coding Dojo
- SKF
- Juice Shop
- Web Goat
- PyGoat
- Security Shepherd
- Samuari WTF
- OWASP Top 10
- Mobile Top 10
- API Top 10
- Wrong Secrets
- Snakes & Ladders

Culture Building and Process Maturing

A good culture is beneficial in many ways and processes need constant refinement

- Security Champions
- SAMM
- ASVS
- MAS

Operations

- A very wide subject
- OWASP restricts itself to WAFs
  - Coraza
  - ModSecurity
  - Core Rule Set for ModSecurity

Gap Analysis

OK, maybe not everyone's favourite, but there is:

- Bug Logging Tool
- Guides:
  - ASVS
  - MAS
  - SAMM

Contribute

- >115 pages done
- ~25 projects still to do:
  - What is it?
  - Why is it useful?
  - Where to get it
  - How to run it

Time for a demo ?

OWASP

TM