OWASP Introduction and Web App Challenge

23-09-2022 - Stefano Maistri - Tony Harris

ROMHACK CAMP

$ whoami

- Stefano Maistri - Cyber Security Engineer
- Senior Software Security Consultant @ IMQ Minded Security
- Ordine degli Ingegneri di Verona #4983

Contacts:

 stefano.maistri@mindedsecurity.com

 https://www.linkedin.com/in/stefano-maistri

Agenda

The Open Web Application Security Project

OWASP Testing Guides

OWASP Guidelines in the SAMM model

OWASP Open Sources Projects

Introduction to Web App Challenge

The Open Web Application Security Project

Open Web Application Security Project® (OWASP)

- Nonprofit foundation since 1-12-2001
- Works to **improve the security** of software
- Community-led **open-source projects**
- Worldwide **local chapters** and members
- Educational and training conferences

OWASP Core Values

Open

- Everything at OWASP is radically **transparent** from our finances to our code

Innovative

- We encourage and **support innovation** and experiments for solutions to software security challenges

Global

- Anyone around the world is **encouraged to participate** in the OWASP community

Integrity

- Our community is respectful, supportive, truthful and **vendor neutral**

The Projects

PROTECT

- security-related design and implementation flaws

DETECT

- security-related design and implementation flaws

LIFE CYCLE

- security-related activities into the Software Development Life Cycle

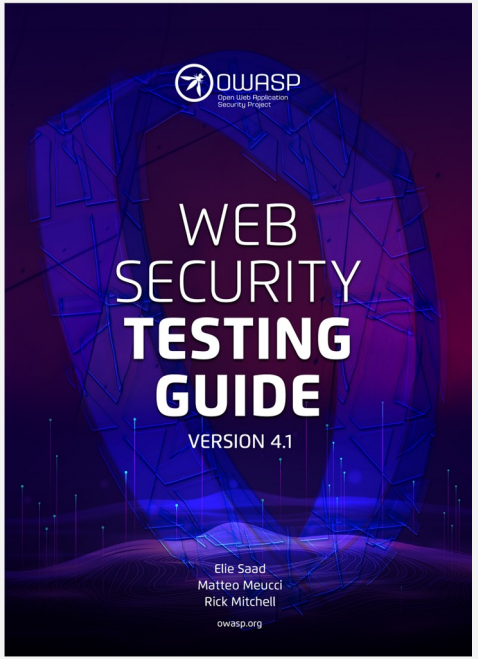
OWASP Testing Guides

Web Security Testing Guide (WSTG)

OWASP Italian Chapter

Premier cybersecurity testing resource for web applications and web services

- Created by the collaborative efforts
- Best practices and methodologies
- Used by penetration testers and organizations all over the world
- Industry standard



Mobile Application Security (MAS)

OWASP Italian Chapter

1. Provides a **security standard** for mobile apps (OWASP MASVS)
    - is the industry standard for mobile app security

1. Comprehensive **testing guide** (OWASP MASTG)
    - comprehensive manual for mobile application security testing

1. **Checklist** bringing everything together
    - used to apply the MASVS controls during security assessments as it conveniently links to the corresponding MASTG test cases

Mobile Application Security (MAS)

MASVS and MASTG are trusted by:

OWASP Code Review Guide

Technical book written for the code review technical teams.

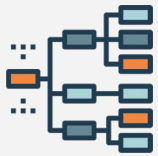
Section one:

- "**why and how** of code reviews"

Section two:

- "types of vulnerabilities and **how to identify** throughout the review"

❏ OWASP Security Knowledge Framework: integrate security by design in SDLC

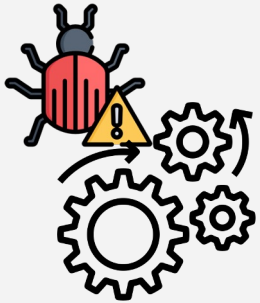


OWASP Guidelines in the SAMM model

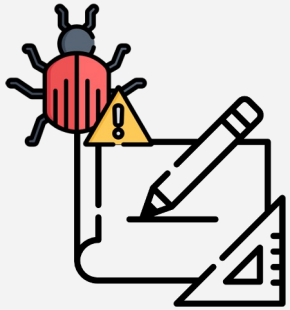
Software Development Life Cycle (SDLC)

"The cost of removing an application security vulnerability during the design phase ranges from 30-60 times less than if removed during production."

- NIST, IBM, and Gartner Group



BUG: Implementation issue



FLAW: Design issue

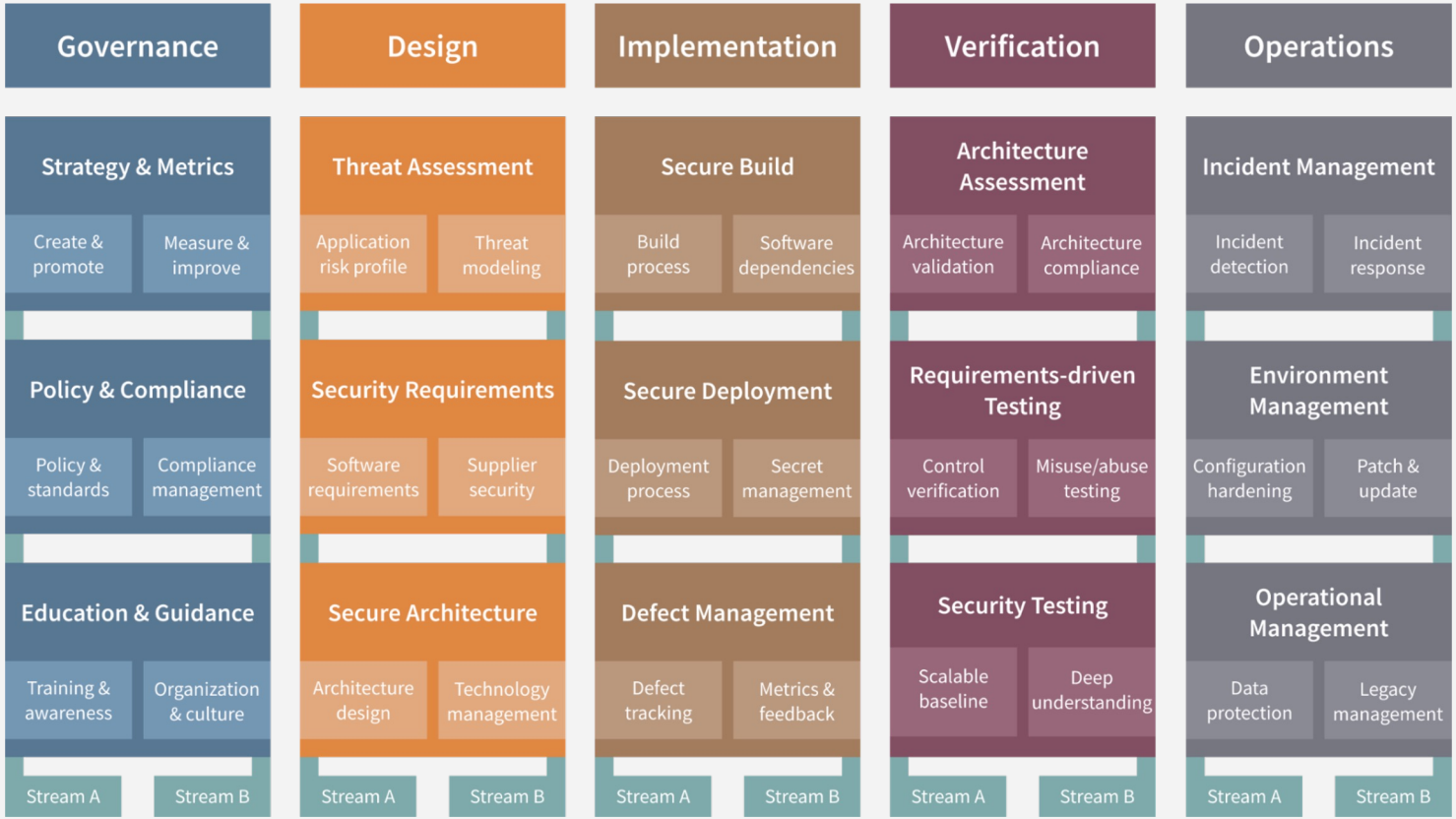
The Software Assurance Maturity Model (SAMM)

OWASP Italian Chapter

- **Maturity model** for software assurance
- Provides an effective and **measurable** way to analyze and improve their software security posture
- Supports the complete **software lifecycle**
- Technology and process **agnostic**
- Evolutive and **risk-driven** in nature.

Trusted by: 

OWASP SAMM

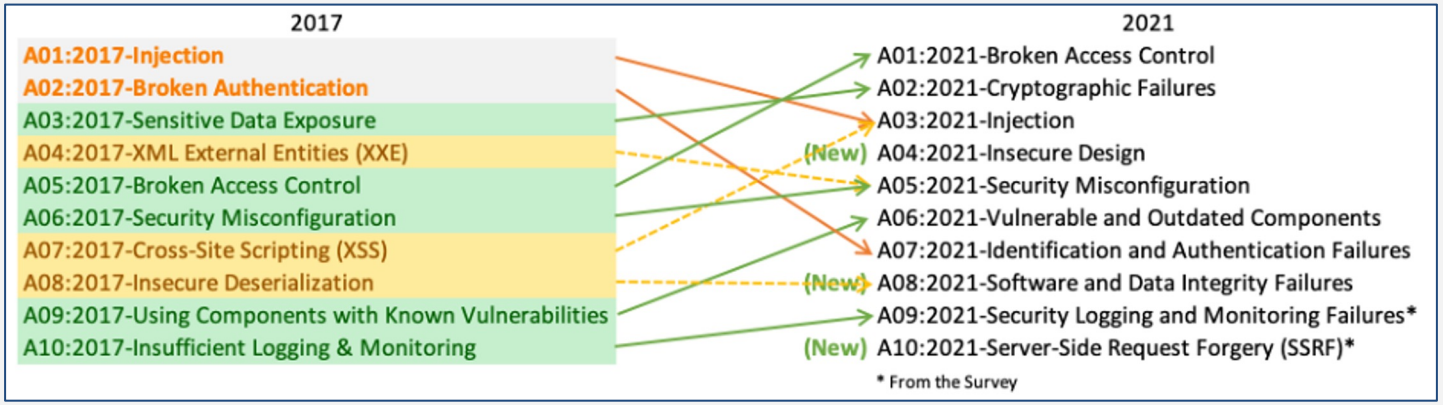

Governance
Design
Implementation
Verification
Operations
Strategy & Metrics
Create & promote
Measure & improve
Policy & Compliance
Policy & standards
Compliance management
Education & Guidance
Training & awareness
Organization & culture
Stream A
Stream B
Threat Assessment
Application risk profile
Threat modeling
Security Requirements
Software requirements
Supplier security
Secure Architecture
Architecture design
Technology management
Stream A
Stream B
Secure Build
Build process
Software dependencies
Secure Deployment
Deployment process
Secret management
Defect Management
Defect tracking
Metrics & feedback
Stream A
Stream B
Architecture Assessment
Architecture validation
Architecture compliance
Requirements-driven Testing
Control verification
Misuse/abuse testing
Security Testing
Scalable baseline
Deep understanding
Stream A
Stream B
Incident Management
Incident detection
Incident response
Environment Management
Configuration hardening
Patch & update
Operational Management
Data protection
Legacy management
Stream A
Stream B

OWASP Open Sources Projects

OWASP TOP 10

OWASP Italian Chapter

Awareness document for developers and web application security



OWASP TOP10

OWASP Top 10 Proactive Controls

C1: Define Security Requirements

C2: Leverage Security Frameworks and Libraries

C3: Secure Database Access

C4: Encode and Escape Data

C5: Validate All Inputs

C6: Implement Digital Identity

C7: Enforce Access Controls

C8: Protect Data Everywhere

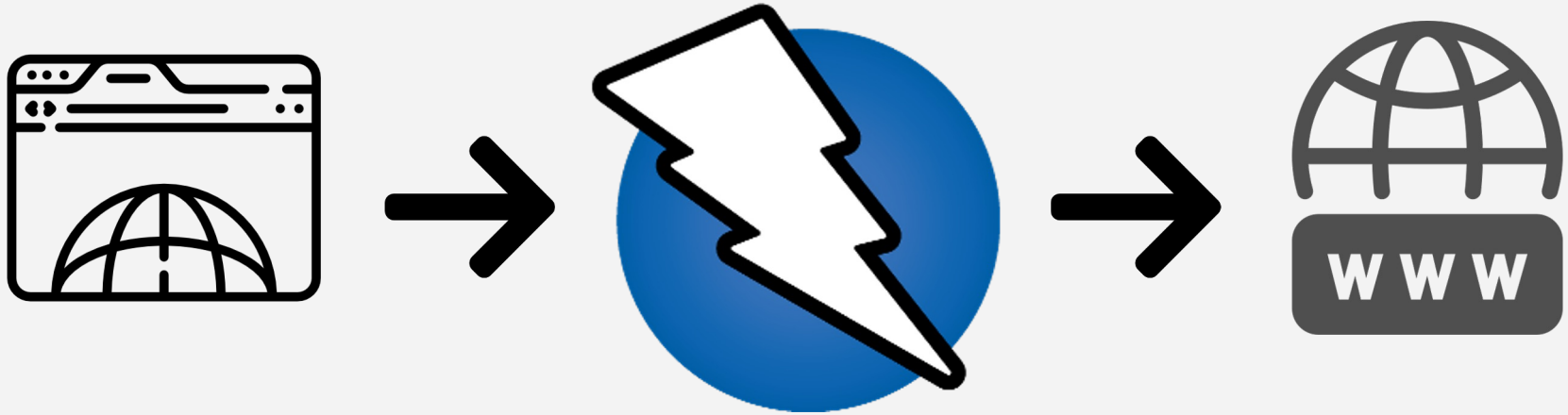
C9: Implement Security Logging and Monitoring

C10: Handle All Errors and Exceptions

OWASP Zed Attack Proxy (ZAP)

OWASP Italian Chapter

- Open Source Penetration Testing Tool
- Man-in-the-middle proxy



Introduction to Web App Challenge

$ whoami

- Tony Harris
- Pentester @ Sky Italia

Contacts:

 @tonyarris

 linkedin.com/in/asjharris

OWASP Juice Shop

OWASP Italian Chapter

- A really vulnerable web app
- Contains 100 challenges covering a wide range of vulnerability categories: Broken Access Control, XSS, XXE etc
- Beginner friendly! tutorials included for some challenges

The Web App Challenge

OWASP Italian Chapter

- The Juice Shop is now open!
- Accessible from the WiFi network RHC22-hackspace
- Register your team and solve some challenges
- The top 5 teams (with the most challenges solved) will win an exclusive OWASP/RomHack Camp ~~Mug~~ Trophy!
- The shop closes on Sunday at 9AM
- Come and see our ZAP lab tomorrow @3pm in Perimetro!

QUESTIONS?

THANKS!

OWASP Italian Chapter

Tony Harris - Stefano Maistri