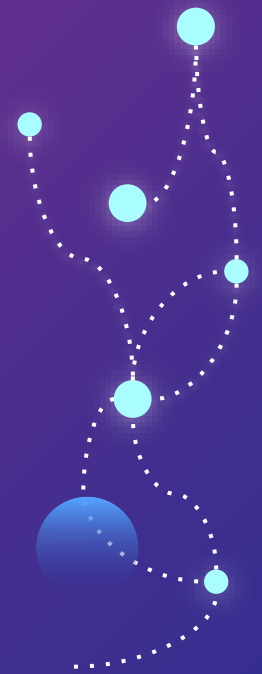
OWASP 101

Application Security & Top 10s

Presented by Taher Amine ELHOUARI
Cyber Security Leader and OWASP Member
https://linkedin.com/in/MrTaherAmine

TABLE OF CONTENTS



01

WHAT IS AppSec?

Presented by **Taher Amine ELHOUARI**
https://linkedin.com/in/MrTaherAmine

Application Security:

AppSec aims to protect software application code and data against cyber threats. It encompasses security measures at the application level that aim to prevent data or code within the app from being stolen or hijacked.

It includes security considerations that happen during application development and design, as well as systems and approaches to protect apps after they get deployed. The final goal of AppSec is to improve security practices and find, fix, and preferably prevent security issues within applications.

Presented by Taher Amine ELHOUARI
https://linkedin.com/in/MrTaherAmine

02

WHAT IS OWASP?

OWASP:

- Stands for: **O**pen **W**orldwide **A**pplication **S**ecurity **P**roject
- Founded in 9 September 2001 – 22 Years of Success
- They produce free: Articles, Methodologies, Documentation, Tools, and Technologies
- The OWASP Foundation Board renamed it from Web to Worldwide in February 2023

Presented by **Taher Amine ELHOUARI**
https://linkedin.com/in/MrTaherAmine

03

OWASP MOST VALUABLE PROJECTS

Presented by **Taher Amine ELHOUARI**
https://linkedin.com/in/MrTaherAmine

OWASP MVPs:

OWASP TOP TEN

The "Top Ten", first published in 2003, is regularly updated. It aims to raise awareness about application security by identifying the most critical risks facing organizations. Three types: TOP 10 WEB, TOP 10 API, TOP 10 MOBILE.

OWASP SAMM

OWASP Software Assurance Maturity Model: project's mission is to provide an effective and measurable way for all types of organizations to analyze and improve their software security posture.

Presented by **Taher Amine ELHOUARI**
https://linkedin.com/in/MrTaherAmine

OWASP MVPs:

OWASP Dev Guide

The Development Guide provides practical guidance and includes J2EE, ASP.NET, and PHP code samples. The Dev Guide covers an extensive array of application-level security issues.

OWASP Testing Guide

It includes a "best practice" penetration testing framework that users can implement in their own organizations and a "low level" penetration testing guide that describes techniques for testing most common web application and web service security issues.

OWASP Code Review Guide

Technical book written for those responsible for code reviews (management, developers, security professionals).

Presented by **Taher Amine ELHOUARI**
https://linkedin.com/in/MrTaherAmine

OWASP MVPs:

OWASP ASVS

OWASP Application Security Verification Standard: This Project provides a basis for testing web apps technical security controls and also provides developers with a list of requirements for secure dev.

OWASP IR Project

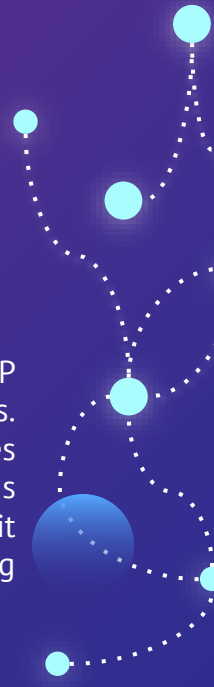
OWASP Incident Response Project provide users with a current set of tools and best practices for dealing with a hacked web application.

OWASP ZAP

The Zed Attack Proxy Project: is a Penetration Testing tool for finding vulnerabilities in web applications. It is designed to be used by people with wide range of security experience.

OWASP WEBGOAT

Insecure web application created by OWASP as a guide for secure programming practices. Once downloaded, the application comes with a tutorial and a set of different lessons that instruct students how to exploit vulnerabilities with the intention of teaching them how to write code securely.



Presented by **Taher Amine ELHOUARI**
https://linkedin.com/in/MrTaherAmine

OWASP MVPs:

AppSec Pipeline

The Application Security (AppSec) Rugged DevOps Pipeline Project is a place to find information needed to increase the speed and automation of an application security program. AppSec Pipelines take the principles of DevOps and Lean and applies that to an application security program.

OWASP Threat Dragon

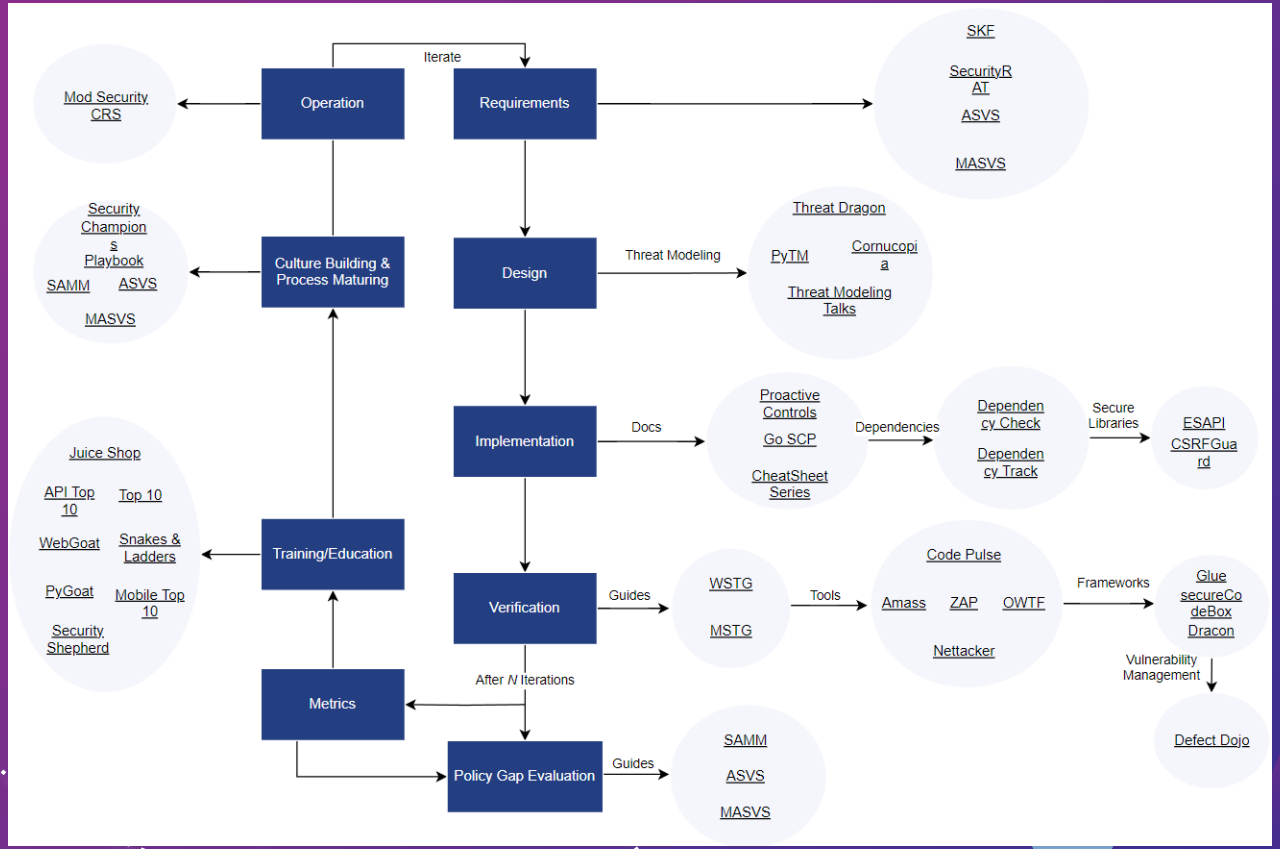
Modeling tool used to create threat model diagrams as part of a secure development lifecycle. It follows the values and principles of the threat modeling manifesto. It can be used to record possible threats and decide on their mitigations, as well as giving a visual indication of the threat model components and threat surfaces.

OTHER PROJECTS..

Simply we can not include every single OWASP Project, since they have a dozen more of different tools and frameworks that cover different AppSec purposes and fields....

Presented by **Taher Amine ELHOUARI**
https://linkedin.com/in/MrTaherAmine

MORE OWASP PROJECTS:



Presented by Taher Amine ELHOUARI
https://linkedin.com/in/MrTaherAmine

04

OWASP Web App Security Top 10

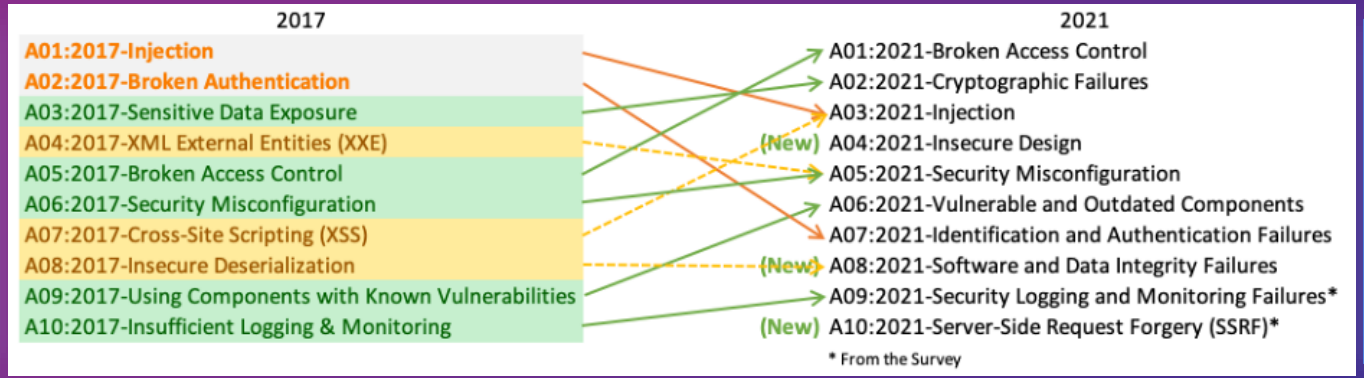
Presented by **Taher Amine ELHOUARI**
https://linkedin.com/in/MrTaherAmine

OWASP Web Application Security TOP 10:

- The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.
- Globally recognized by developers as the first step towards more secure coding.
- Installment of the Top 10 is more data-driven than ever but not blindly data-driven.

Presented by Taher Amine ELHOUARI
https://linkedin.com/in/MrTaherAmine

OWASP Web App Security TOP 10



Presented by Taher Amine ELHOUARI
https://linkedin.com/in/MrTaherAmine

05

OWASP Mobile Security Top 10

Presented by **Taher Amine ELHOUARI**
https://linkedin.com/in/MrTaherAmine

OWASP Mobile Security TOP 10:

- ‘Top 10 Mobile Controls’ is a work made through a collaboration between OWASP and ENISA. Globally recognized by developers as the first step towards more mobile secure coding.
- The new Mobile Top 10 list for 2023 is being worked upon.

Presented by Taher Amine ELHOUARI
https://linkedin.com/in/MrTaherAmine

OWASP Mobile Security Top 10

Comparison Between 2016-2023		
OWASP-2016	**OWASP-2023-Initial Release**	**Comparison Between 2016-2023**
M1: Improper Platform Usage	M1: Improper Credential Usage	**New**
M2: Insecure Data Storage	M2: Inadequate Supply Chain Security	**New**
M3: Insecure Communication	M3: Insecure Authentication / Authorization	**Merged M4&M6 to M3**
M4: Insecure Authentication	M4: Insufficient Input/Output Validation	**New**
M5: Insufficient Cryptography	M5: Insecure Communication	**Moved from M3 to M5**
M6: Insecure Authorization	M6: Inadequate Privacy Controls	**New**
M7: Client Code Quality	M7: Insufficient Binary Protections	**Merged M8&M9 to M7**
M8: Code Tampering	M8: Security Misconfiguration	**Rewording [M10]**
M9: Reverse Engineering	M9: Insecure Data Storage	**Moved from M2 to M9**
M10: Extraneous Functionality	M10: Insufficient Cryptography	**Moved from M5 to M10**

Presented by Taher Amine ELHOUARI
https://linkedin.com/in/MrTaherAmine

06

OWASP API Security Top 10

Presented by **Taher Amine ELHOUARI**
https://linkedin.com/in/MrTaherAmine

OWASP API Security Top 10:

- API Security focuses on strategies and solutions to understand and mitigate the unique vulnerabilities and security risks of Application Programming Interfaces (APIs).

Presented by **Taher Amine ELHOUARI**
https://linkedin.com/in/MrTaherAmine

OWASP API Security Top 10

2019	#	2023
API1:2019 - Broken Object Level Authorization	1	API1:2023 - Broken Object Level Authorization
API2:2019 - Broken User Authentication	2	API2:2023 - Broken Authentication
API3:2019 - Excessive Data Exposure	3	API3:2023 - Broken Object Property Level Authorization
API4:2019 - Lack of Resources & Rate Limiting	4	API4:2023 - Unrestricted Resource Consumption
API5:2019 - Broken Function Level Authorization	5	API5:2023 - Broken Function Level Authorization
API6:2019 - Mass Assignment	6	API6:2023 - Unrestricted Access to Sensitive Business Flows
API7:2019 - Security Misconfiguration	7	API7:2023 - Server Side Request Forgery
API8:2019 - Injection	8	API8:2023 - Security Misconfiguration
API9:2019 - Improper Assets Management	9	API9:2023 - Improper Inventory Management
API10:2019 - Insufficient Logging & Monitoring	10	API10:2023 - Unsafe Consumption of APIs

Presented by Taher Amine ELHOUARI
https://linkedin.com/in/MrTaherAmine

THANKS!

DO YOU HAVE ANY QUESTIONS?

Taher.AmineElhouari@OWASP.org

https://linkedin.com/in/MrTaherAmine