OWASP.

PROJECTS CHAPTERS EVENTS ABOUT

Search OWASP.org 🔍

🛒 Store   Donate   Join

Projects

👁 Watch 124   ⭐ Star 327

Projects for Good

We are a community of developers, technologists and evangelists improving the security of software. The OWASP Foundation gives aspiring open source projects a platform to improve the security of software with:

- Visibility: Our website gets more than six million visitors a year
- Credibility: OWASP is well known in the AppSec community
- Resources: Funding and Project Summits are available for qualifying Programs
- Community: Our Conferences and Local Chapters connect Projects with users

OWASP Projects are a collection of related tasks that have a defined roadmap and team members. Our projects are open source and are built by our community of volunteers - people just like you! OWASP project leaders are responsible for defining the vision, roadmap, and tasks for the project. The project leader also promotes the project and builds the team. OWASP currently has over 100 active projects, and new project applications are submitted every week.

> Code, software, reference material, documentation, and community all working to secure the world's software.

Projects gives members an opportunity to freely test theories and ideas with the professional advice and support of the OWASP community. Every project minimally has their own webpage, mailing list, and Slack Channel. Most projects maintain their content in our GitHub organization.

Who Should Start an OWASP Project?

- Application Developers
- Software Architects
- Information Security Authors
- Those who would like the support of a world wide professional community to develop or test an idea.

OWASP Projects, the SDLC, and the Security Wayfinder

Thanks to the OWASP Integration Standards Project for mapping OWASP projects in a diagram of the Software Development LifeCycle. This resource should help you determine which projects fit into your SDLC.
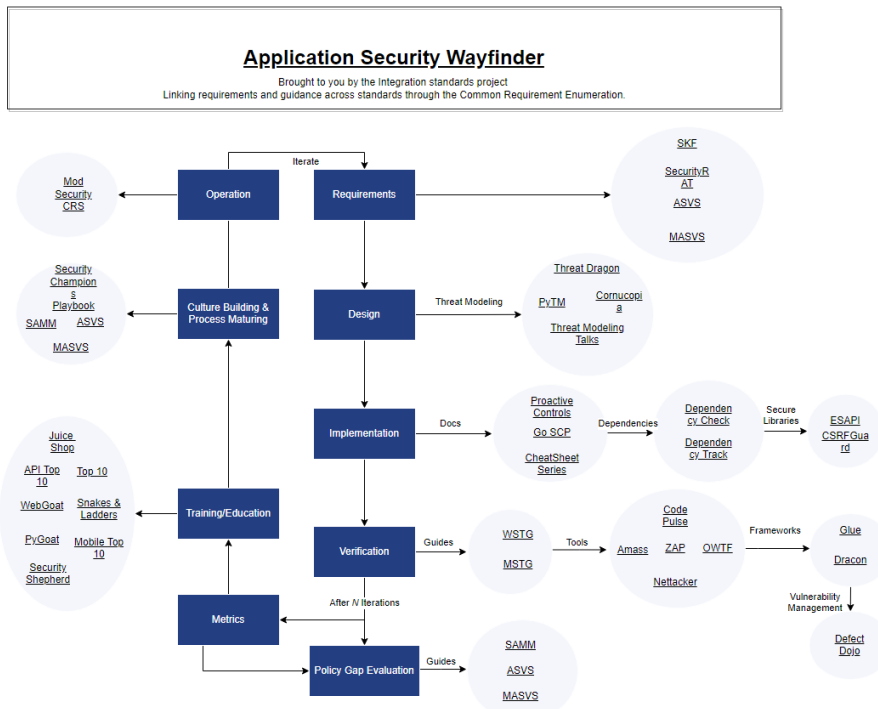

The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

Important Links

Project Handbook
Start a New Project
Project Graduation Application
OWASP Github
All Project Leaders
Project Status
Project Committee
Google Summer of Code 2021

Upcoming OWASP Global Events

OWASP 2022 Global AppSec AsiaPac Virtual Event
- August 29 - September 1, 2022 Singapore Time (SGT)

OWASP End of Summer Training
- September 13 - 14, 2022 (BST)

OWASP September Webinar
- September 22-23, 2022 Eastern Daylight Time (EDT)

OWASP October Webinar
- October 11-12, 2022 Australian Western Standard Time (AWST)

OWASP 2022 Global AppSec San Francisco
- November 14-18, 2022 Pacific Standard Time (PST)

Happy Holidays Training
- December 12-13, 2022 Eastern Standard Time (EST)

OWASP Global AppSec Dublin 2023
- February 13-16, 2023
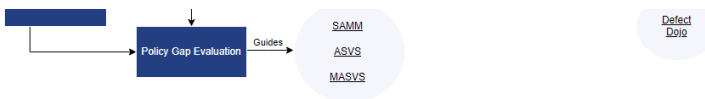
OWASP Project Inventory (261)

All OWASP tools, document, and code library projects are organized into the following categories:

Flagship Projects: The OWASP Flagship designation is given to projects that have demonstrated strategic value to OWASP and application security as a whole.

Lab Projects: OWASP Labs projects represent projects that have produced an OWASP reviewed deliverable of value.

Incubator Projects: OWASP Incubator projects represent the experimental playground where projects are still being fleshed out, ideas are still being proven, and development is still underway.

List of Projects by Level or Type

Flagship Projects

- OWASP Amass
- OWASP Application Security Verification Standard
- OWASP Cheat Sheet Series
- OWASP CSRFGuard
- OWASP CycloneDX
- OWASP Defectdojo
- OWASP Dependency-Check
- OWASP Dependency-Track
- OWASP Juice Shop
- OWASP Mobile Security Testing Guide
- OWASP ModSecurity Core Rule Set
- OWASP OWTF
- OWASP SAMM
- OWASP Security Knowledge Framework
- OWASP Security Shepherd
- OWASP Top Ten
- OWASP Web Security Testing Guide
- OWASP ZAP

Lab Projects

- OWASP AntiSamy
- OWASP API Security Project
- OWASP Attack Surface Detector
- OWASP Automated Threats to Web Applications
- OWASP Benchmark
- OWASP Code Pulse
- OWASP Code Review Guide
- OWASP Coraza Web Application Firewall
- OWASP Cornucopia
- OWASP Devsecops Maturity Model
- OWASP Enterprise Security API (ESAPI)
- OWASP Find Security Bugs
- OWASP Integration Standards
- OWASP Internet of Things
- OWASP Java HTML Sanitizer
- OWASP mobile security
- OWASP Mobile Top 10
- OWASP Mutillidae II
- OWASP Podcast
- OWASP Proactive Controls
- OWASP pytm
- OWASP SamuraiWTF
- OWASP Secure Coding Dojo
- OWASP secureCodeBox
- OWASP SecureTea Project
- OWASP Security Pins
- OWASP Snakes And Ladders
- OWASP Software Component Verification Standard
- OWASP Threat Dragon
- OWASP Top 10 Privacy Risks
- OWASP TorBot
- OWASP Vulnerable Web Applications Directory
- OWASP WebGoat
- OWASP WrongSecrets

Incubator Projects

- OWASP .Net
- OWASP aegis4j
- OWASP Android Security Inspector Toolkit
- OWASP APICheck
- OWASP Application Gateway
- OWASP Application Security Awareness Campaigns
- OWASP Appsec Pipeline
- OWASP AppSensor

- OWASP Application Gateway
- OWASP Application Security Awareness Campaigns
- OWASP Appsec Pipeline
- OWASP AppSensor
- ASVS-Graph
- OWASP Automotive EMB 60
- OWASP AWScanner
- OWASP Barbarus
- OWASP Big Data Security Verification Standard
- OWASP Bug Logging Tool
- OWASP Cloud-Native Application Security Top 10
- OWASP Cloud-Native Security Project
- OWASP Code the Flag
- OWASP Continuous Penetration Testing Framework
- OWASP Core Business Application Security
- OWASP crAPI
- OWASP CSRFProtector Project
- OWASP CWE Toolkit
- OWASP Cyber Controls Matrix (OCCM)
- OWASP Cyber Defense Framework
- OWASP Cyber Defense Matrix
- OWASP Cyber Scavenger Hunt
- OWASP D4N155
- OWASP Damn Vulnerable Web Sockets
- OWASP Data Security Top 10
- OWASP Desktop App Security Top 10
- OWASP AppSec Days Developer Outreach Program
- OWASP DevSecOps Guideline
- OWASP DevSecOps Verification Standard
- OWASP DevSlop
- OWASP Docker Top 10
- OWASP DPD (DDOS Prevention using DPI)
- OWASP Enterprise DevSecOps
- OWASP Forensics Testing Guide
- OWASP G0rKing
- OWASP Go Secure Coding Practices Guide
- OWASP Honeypot
- OWASP How to Get Into AppSec
- OWASP Information Security Metrics Bank
- OWASP IoT Security Verification Standard
- OWASP Kubernetes Security Testing Guide
- OWASP Kubernetes Top Ten
- OWASP Maryam
- OWASP Mobile Audit
- OWASP Nettacker
- OWASP Nightingale
- OWASP Node.js Goat
- OWASP O-Saft
- OWASP Ontology Driven Threat Modeling Framework
- OWASP Open Source Security Application Platform
- OWASP Patton
- OWASP Penetration Testing Kit
- OWASP PenText
- OWASP Port and Service Information
- OWASP PurpleTeam
- OWASP Pygoat
- OWASP Raider
- OWASP Risk Assessment Framework
- OWASP safetypes
- OWASP Scan IT
- OWASP Sectudo
- OWASP Secure Headers Project
- OWASP Secure Logging Benchmark
- OWASP SecureBank
- OWASP SecureFlag Open Platform
- OWASP Security Champions Guidebook
- OWASP Security Culture
- OWASP Security Qualitative Metrics
- OWASP SecurityRAT
- OWASP Serverless Top 10
- OWASP SideKEK
- OWASP Snow
- OWASP Project Spotlight Series
- OWASP Single Sign-On
- OWASP Thick Client Security Testing Guide
- OWASP Thick Client Top 10 Project
- OWASP Threat and Safeguard Matrix (TaSM)
- OWASP Threat Modeling Project
- OWASP Threat Model Cookbook
- OWASP Threat Modeling Playbook (OTMP)
- OWASP TimeGap Theory
- OWASP Top 10 Card Game
- OWASP Top 10 Client-Side Security Risks
- OWASP Top 10 Low-Code/No-Code Security Risks

- OWASP TimeGap Theory
- OWASP Top 10 Card Game
- OWASP Top 10 Client-Side Security Risks
- OWASP Top 10 Low-Code/No-Code Security Risks
- OWASP Vulnerability Management Center
- OWASP Vulnerability Management Guide
- OWASP Vulnerable Container Hub
- OWASP VulnerableApp
- OWASP VulnerableApp-Facade
- OWASP Web Application Firewall Evaluation Criteria Project (WAFEC)
- OWASP Web Mapper
- OWASP Web Testing Environment
- OWASP WinFIM.NET

Projects Needing Website Update

- OWASP Access Log Parser
- OWASP AndroGoat
- OWASP Anti-Ransomware Guide
- OWASP Application Security Curriculum
- OWASP Application Security Hardening
- OWASP Application Security Playbook
- OWASP AppSec Minimum Requirements
- OWASP Auth
- OWASP belva
- OWASP Best Practices In Vulnerability Disclosure And Bug Bounty Programs
- OWASP Blend
- OWASP Blockchain Distributed Infrastructure
- OWASP Broken Web Applications
- OWASP ChainGoat
- OWASP cloud security
- OWASP Cloud Security Mentor
- OWASP Cloud Security Testing Guide
- OWASP Cloud Testing Guide
- OWASP CloudSheep
- OWASP Container Security Verification Standard
- OWASP Ctf
- OWASP Cyber Security Enterprise Operations Architecture
- OWASP Cybersecurity Risk Register
- OWASP Damn Vulnerable Crypto Wallet
- OWASP Damn Vulnerable Thick Client Application
- OWASP deepviolet-tls-ssl-scanner
- OWASP Drill
- OWASP Ende
- OWASP Financial Systems Security
- OWASP Game Security Framework
- OWASP Glue Tool
- OWASP hacking-lab
- OWASP Igoat Tool
- OWASP Incident Response
- OWASP InjectBot
- OWASP internet of things top 10
- OWASP Iot Analytics 4Industry4
- OWASP JavaScript Security
- OWASP Joomscan
- OWASP Jotp
- OWASP Json Sanitizer
- OWASP jvmxray
- OWASP Knowledge Based Authentication Performance Metrics
- OWASP Laravel Goat
- OWASP Learning Gateway
- OWASP little web application firewall
- OWASP Lock It
- OWASP Low Code Security
- OWASP Machine Learning Security Top 10
- OWASP Mimosa
- OWASP Mth3L3M3Nt Framework
- OWASP Nasi Lemak
- OWASP O2 Platform
- OWASP Off The Record 4 Java
- OWASP Online Academy
- OWASP Open AppSec Tooling API
- OWASP Passfault
- OWASP Php
- OWASP Php Security Training
- OWASP Python Honeypot
- OWASP Python Security
- OWASP Pyttacker
- OWASP Qrljacker
- OWASP rat
- OWASP Redteam Toolkit
- OWASP Revelo
- OWASP Reverse Engineering And Code Modification Prevention
- OWASP Seclists

- OWASP Knowledge Based Authentication Performance Metrics
- OWASP Laravel Goat
- OWASP Learning Gateway
- OWASP little web application firewall
- OWASP Lock It
- OWASP Low Code Security
- OWASP Machine Learning Security Top 10
- OWASP Mimosa
- OWASP Mth3L3M3Nt Framework
- OWASP Nasi Lemak
- OWASP O2 Platform
- OWASP Off The Record 4 Java
- OWASP Online Academy
- OWASP Open AppSec Tooling API
- OWASP Passfault
- OWASP Php
- OWASP Php Security Training
- OWASP Python Honeypot
- OWASP Python Security
- OWASP Pyttacker
- OWASP Qrljacker
- OWASP rat
- OWASP Redteam Toolkit
- OWASP Revelo
- OWASP Reverse Engineering And Code Modification Prevention
- OWASP Seclists
- OWASP Secure Coding Practices-Quick Reference Guide
- OWASP Secure Medical Device Deployment Standard
- OWASP Security Busters
- OWASP Security Integration System
- OWASP Security Logging
- OWASP Security Resource Framework
- OWASP SEDATED®
- OWASP Seeker
- OWASP Software Composition Security
- OWASP State of AppSec Survey
- OWASP SupplyChainGoat
- OWASP Threatspec
- OWASP TOCTOURex
- OWASP Top 10 CI/CD Security Risks
- OWASP Top 10 Fuer Entwickler
- OWASP University Challenge
- OWASP Vbscan
- OWASP Vicnum
- OWASP Virtual Patching Best Practices
- OWASP VITCC Open Source Initiative
- OWASP Voice Automated Application Security
- OWASP Vue 3 Password Input
- OWASP Vulnerable Web Application
- OWASP webgoat php
- OWASP Webspa
- OWASP Wpbullet
- OWASP Zsc Tool

 Edit on GitHub

Spotlight: Noname Security

 noname

Noname Security is the only company taking a complete, proactive approach to API Security. Noname works with 20% of the Fortune 500 and covers the entire API security scope across three pillars — Posture Management, Runtime Security, and Secure API SDLC. Noname Security is privately held, remote first with headquarters in Palo Alto, California, and an office in Tel Aviv and Amsterdam.

Corporate Supporters

waratek

Cobalt
Pentest as a Service

Adobe

Invicti

Rezilion

Heyhack

DNST

Bloomberg

SALT

Become a corporate supporter