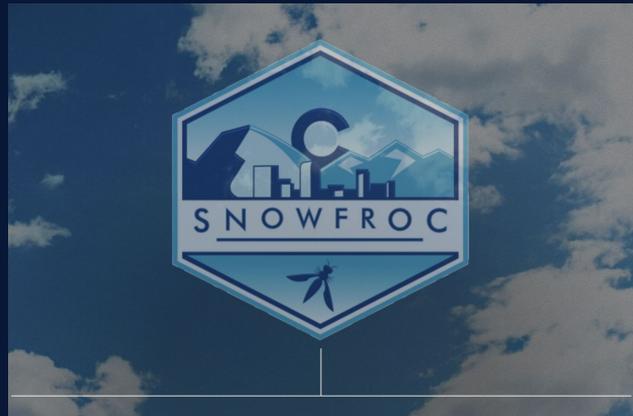




# App Security Does Not Need To Be Fun: Ignoring OWASP To Have A Terrible Time



# Hi, I'm Dwayne



**Dwayne McDaniel**

- I live in Chicago
- I've been a Developer Advocate since 2016
- On Twitter @mcdwayne
- Happy to chat about anything, hit me up
- Besides tech, I love improv, karaoke and going to rock and roll shows!



# About GitGuardian



**GitGuardian is the code security platform for the DevOps generation.**

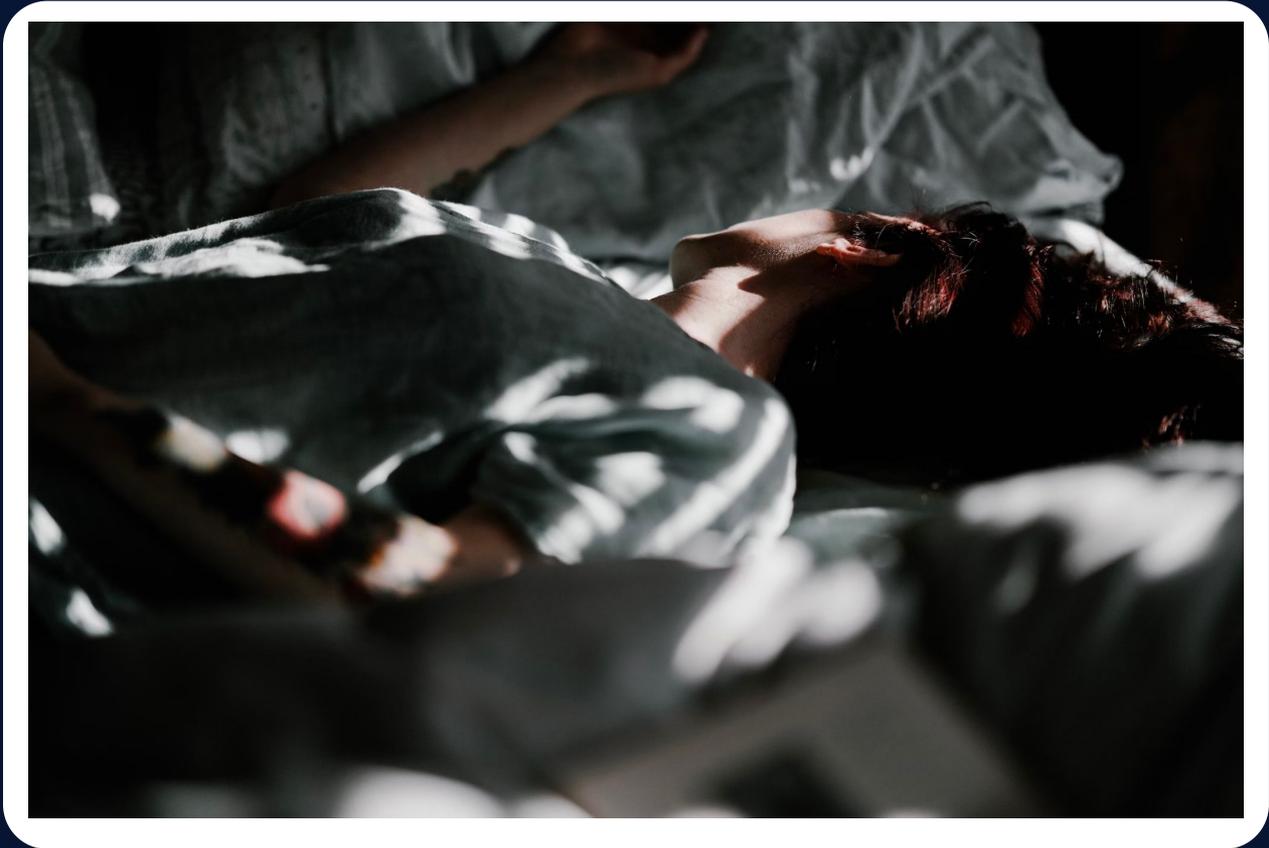
---

**With automated secrets detection and remediation, our platform enables Dev, Sec, and Ops to advance together towards the Secure Software Development Lifecycle.**

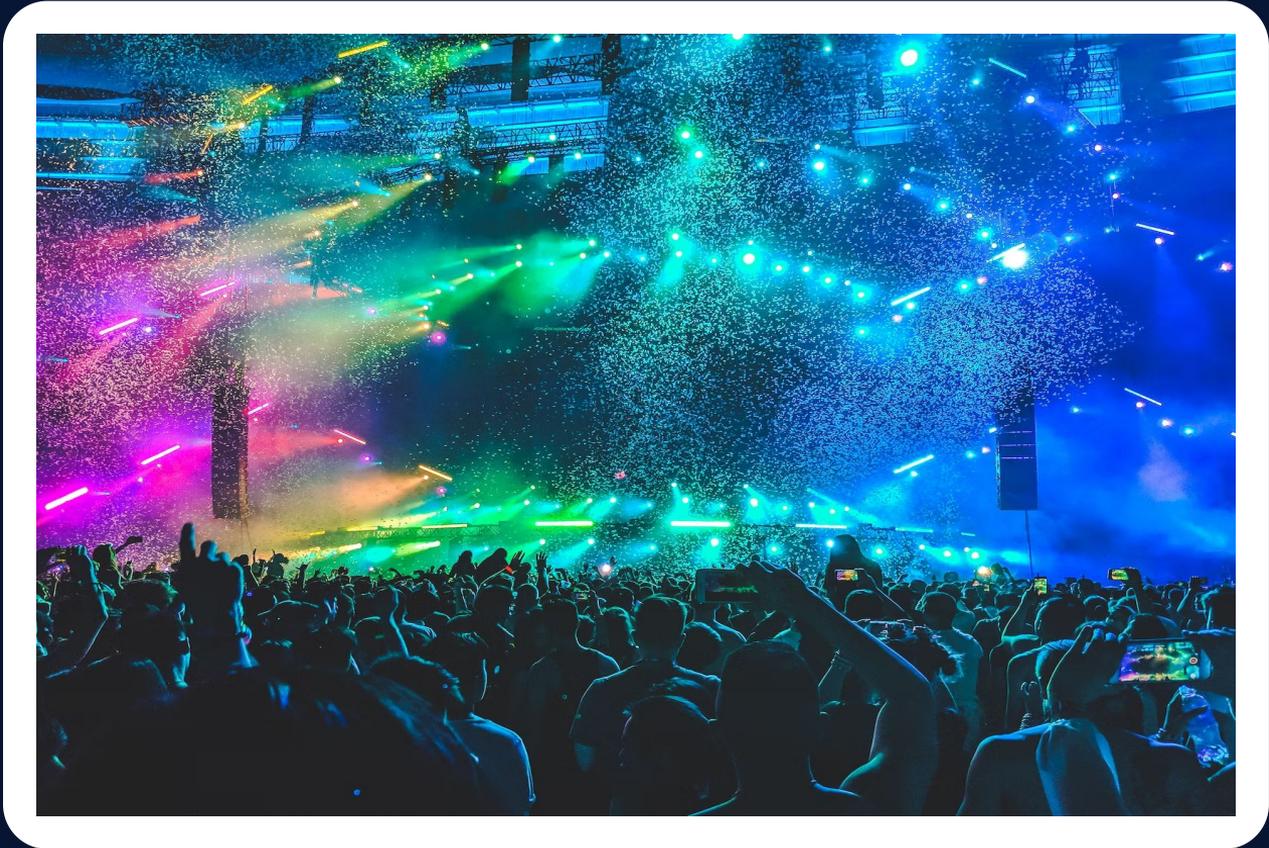


# What Does Good Security Look Like?











# All Technology Has Human Costs

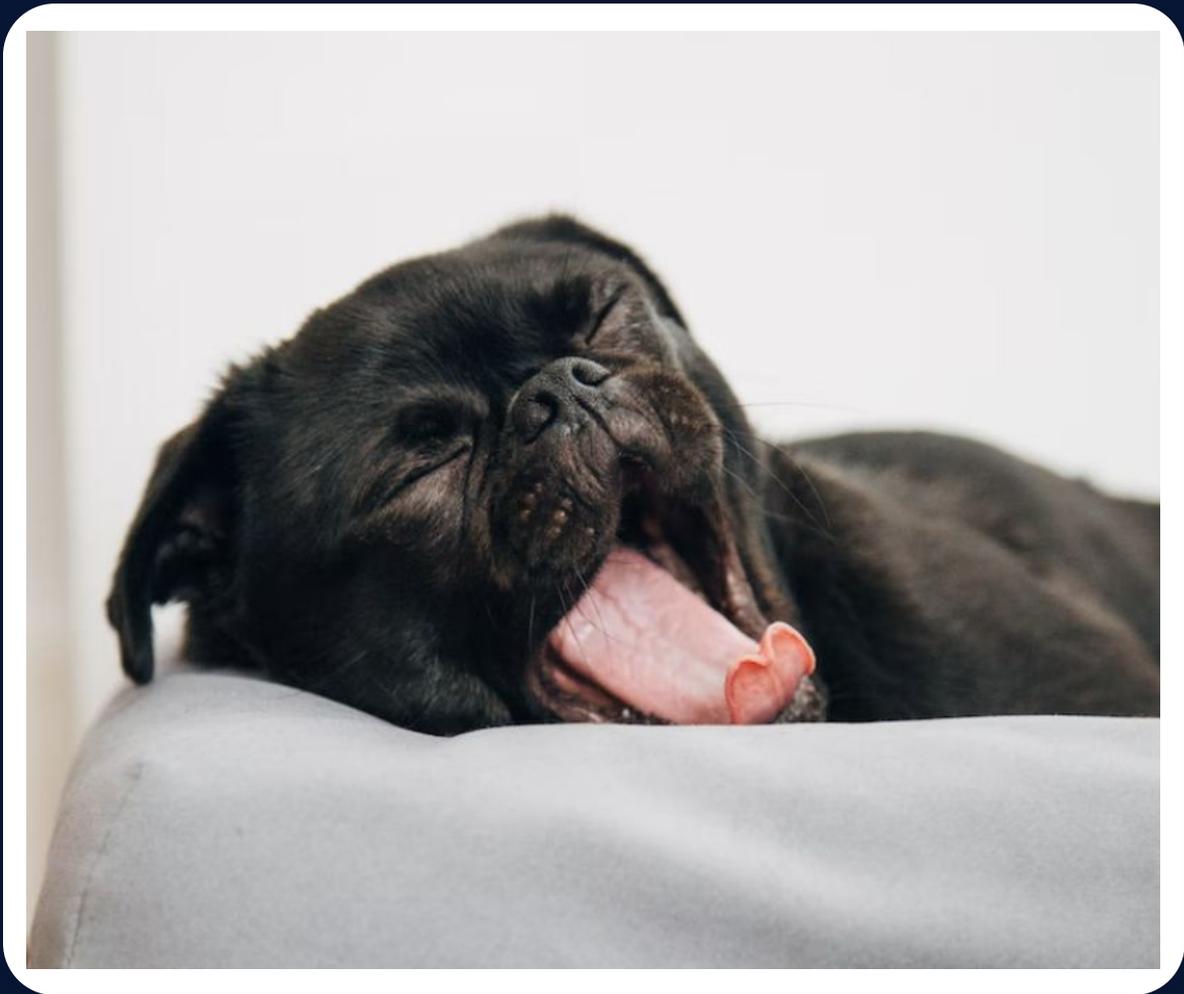


# What Does Bad Security Look Like?





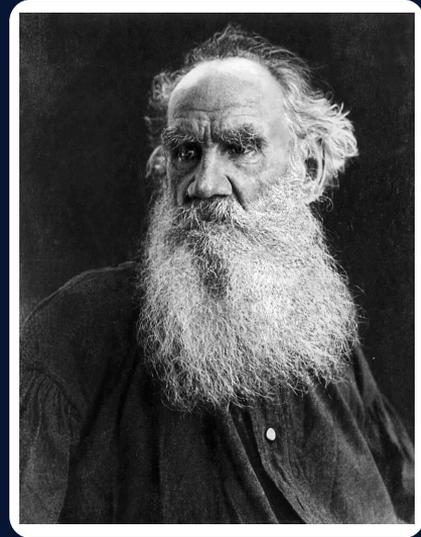




@mcdwayne

“All happy families are alike; each unhappy family is unhappy in its own way.”

— Leo Tolstoy , Anna Karenina



# A Few Unhappy Families Companies

## Apache

### Log4Shell CVE-2021-44228

- Reported: 24 November 2021 - Had existed since 2013
- Log4J allowed requests to arbitrary LDAP and JNDI servers, which in turn could execute any code, including opening interactive shells.
- Impacted over 44 % of corporate networks worldwide.
- Top Companies With Products Affected Include:
  - Adobe, Cisco, AWS, Broadcom, IBM, Okta, VMware



# A Few Unhappy Families Companies

## Uber

- Reported: 15 Sept, 2022
- Teenager from the Lapsus\$ hacking group phished login info from a super admin
- Immediately discovered access credentials hardcoded in PowerShell scripts that allowed pwnage
- Reported first in the New York Times



# A Few Unhappy Families Companies

## CircleCI

- Reported: 4 January, 2023
- An unauthorized third party leveraged malware deployed to a CircleCI engineer's laptop in order to steal a valid, 2FA-backed SSO session.
- Attackers ultimately gained access to many customers' GitHub OAuth credentials and platform security tokens.
- Caused a system wide token rotation, disrupting thousands of customers. Investigation ongoing.



# Security Teams Are Outnumbered



*In the best organizations developers outnumber security team members 100:1*

- Alex Rice, HackerOne  
#Security@2022



@mcdwayne

**Shift Left!**

**"Put Everyone On The Security Team"**



# *But Devs Already Have A Lot To Worry About:*

- *Delivery deadlines*
- *Billable hours*
- *Number of tickets closed*
- *Bugs*
- *DevOps*
- *Fighting Kubernetes*

*Only so much time*



# *Business Priority View of Security*

**Security Incident**



**Focus On New Feature  
Delivery Times**

**Focus On Security**



**Delivery Slows Down**







**Now, here, you see, it takes all  
the running you can do, to keep  
in the same place.  
If you want to get somewhere  
else, you must run at least twice  
as fast as that!**

**— The Red Queen,  
Through the Looking-Glass,  
and What Alice Found There**



**I Wish Some Benevolent  
Group Of Security Experts Could  
Help Me With This Stuff**



# Open Web Application Security Project





- Browse All Projects...
- OWASP Top Ten
- Dependency Track
- Juice Shop
- Mobile Application Security
- ModSecurity Core Rule Set
- Software Assurance Maturity Model (SAMM)
- Security Knowledge Framework
- Web Security Testing Guide
- Zed Attack Proxy
- Start a New Project...
- Google Summer of Code 2021

## Who is the OWASP® Foundation?

The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

- Tools and Resources
- Community and Networking
- Education & Training

For nearly two decades corporations, foundations, developers, and volunteers have supported the OWASP Foundation and its work. [Donate](#), [Join](#), or become a [Corporate Member](#) today.

## Project Spotlight: OWASP Top 10

OWASP Top 10  
The Ten Most Critical Web Application Security Risks

We are back again with yet another OWASP Spotlight series and this time we have a project which needs no introduction and I got the chance to interact with Andrew...



## OWASP 2022 Global AppSec APAC Virtual Event



Registration Open!

[Join us](#) virtually August 29 - September 1, for



# OWASP Mission

No more insecure software.



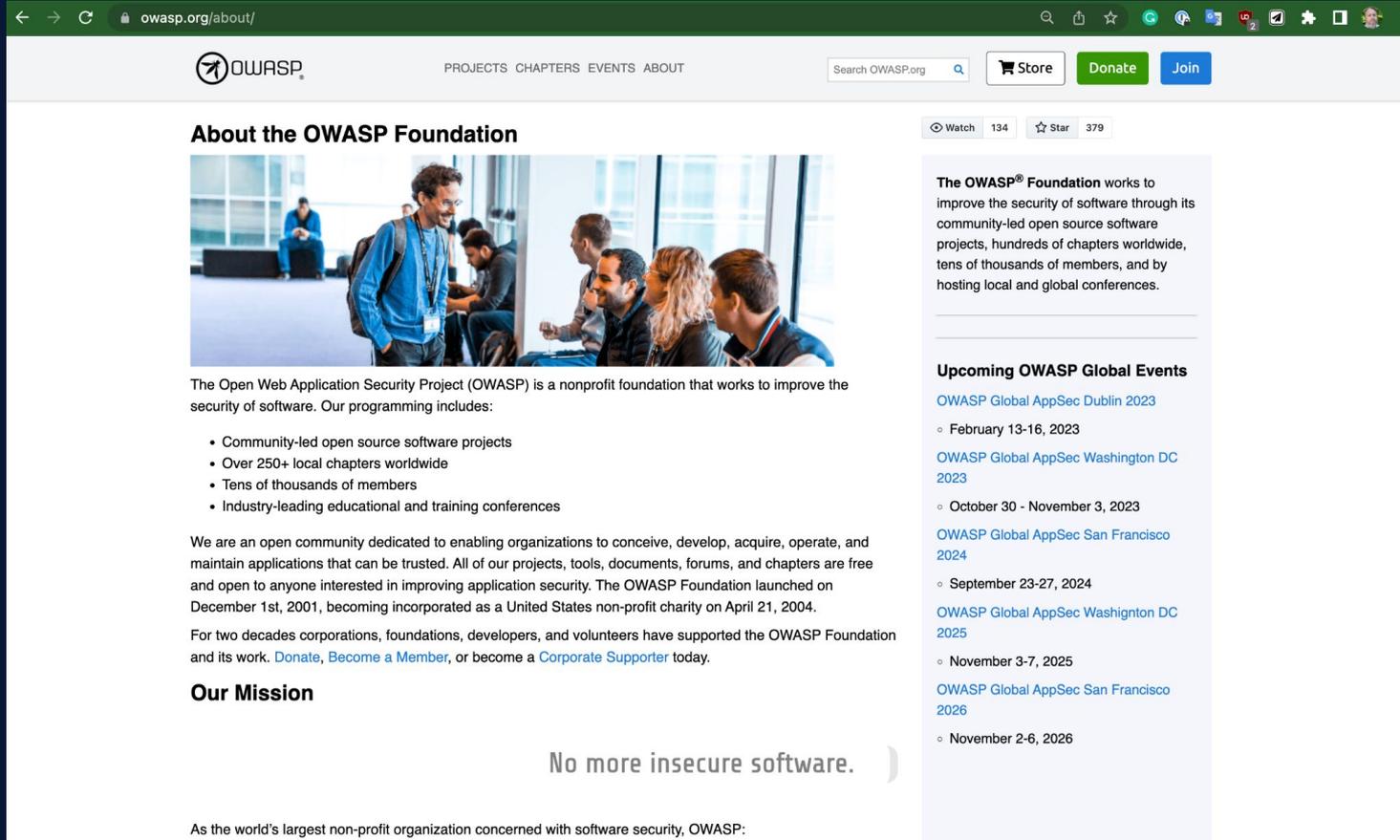
# OWASP Mission

As the world's largest non-profit organization concerned with software security, OWASP:

- Supports the building of impactful **projects**;
- Develops & nurtures **communities** through **events** and chapter meetings worldwide; and
- Provides educational **publications** & **resources** in order to enable developers to write better software, and security professionals to make the world's software more secure.



# OK, But how do I navigate this site?



The screenshot shows the OWASP.org website with a navigation bar at the top containing the OWASP logo, menu items (PROJECTS, CHAPTERS, EVENTS, ABOUT), a search bar, and buttons for Store, Donate, and Join. The main content area features a section titled "About the OWASP Foundation" with a photo of people in a meeting. Below the photo is a paragraph describing OWASP as a nonprofit foundation. A bulleted list follows, detailing community-led projects, chapters, members, and conferences. Further down, a paragraph explains the organization's mission to enable secure software development. A "Our Mission" section is also visible. On the right side, there are social media interaction buttons (Watch, Star) and a list of "Upcoming OWASP Global Events" with dates from 2023 to 2026. At the bottom, a large text block reads "No more insecure software." followed by a closing parenthesis. The footer contains the text "As the world's largest non-profit organization concerned with software security, OWASP:".

owasp.org/about/

OWASP

PROJECTS CHAPTERS EVENTS ABOUT

Search OWASP.org

Store Donate Join

## About the OWASP Foundation



The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. Our programming includes:

- Community-led open source software projects
- Over 250+ local chapters worldwide
- Tens of thousands of members
- Industry-leading educational and training conferences

We are an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. All of our projects, tools, documents, forums, and chapters are free and open to anyone interested in improving application security. The OWASP Foundation launched on December 1st, 2001, becoming incorporated as a United States non-profit charity on April 21, 2004.

For two decades corporations, foundations, developers, and volunteers have supported the OWASP Foundation and its work. [Donate](#), [Become a Member](#), or become a [Corporate Supporter](#) today.

### Our Mission

No more insecure software. )

As the world's largest non-profit organization concerned with software security, OWASP:

Watch 134 Star 379

#### Upcoming OWASP Global Events

- [OWASP Global AppSec Dublin 2023](#)
  - February 13-16, 2023
- [OWASP Global AppSec Washington DC 2023](#)
  - October 30 - November 3, 2023
- [OWASP Global AppSec San Francisco 2024](#)
  - September 23-27, 2024
- [OWASP Global AppSec Washington DC 2025](#)
  - November 3-7, 2025
- [OWASP Global AppSec San Francisco 2026](#)
  - November 2-6, 2026



# OWASP Overview

- **Projects**
- **Communities**
- **Events**
- **Education and Training**
- **Publications and Resources**



OWASP<sup>®</sup>



# OWASP Projects

Watch 16 Star 54

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.

---

**Project Classification**

- Flagship Project
- Builder
- Breaker
- Defender
- Tool

**Online Demo OWASP-SKF**

[OWASP-SKF Online Demo](#)  
username: admin  
password: test-skf

**Github Repository**

[OWASP-SKF repo](#)

**Changelog**

[Latest Changelog OWASP-SKF](#)

**Leaders**

[Glenn ten Cate](#)  
[Riccardo ten Cate](#)

**Getting involved**

- Open Source repos
- Built by volunteers and experts
- New weekly submissions from the community
- 250 total projects in any state
  - 157 in "usable" state



# OWASP Projects Categories

- **Flagship Projects**
- **Production Projects (new)**
- **Lab Projects**
- **Incubator Projects**



# OWASP Flagship Projects

## 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 Application Security
- OWASP ModSecurity Core Rule Set
- OWASP OWTF
- OWASP SAMP
- OWASP Security Knowledge Framework
- OWASP Security Shepherd
- OWASP Top Ten
- OWASP Web Security Testing Guide
- OWASP ZAP

18 Current Flagship Projects:

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



# OWASP Lab Projects

## 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 Top 10
- OWASP Mutillidae II
- OWASP Podcast
- OWASP Proactive Controls
- OWASP pytm
- OWASP SamuraiWTF
- OWASP Secure Coding Dojo
- OWASP Secure Headers Project
- OWASP secureCodeBox
- OWASP SecureTea Project
- OWASP Security Pins

34 Lab Projects:

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



# OWASP Incubator Projects

## 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
- ASVS-Graph
- OWASP Automotive EMB 60
- OWASP AWSScanner
- 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

105 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.



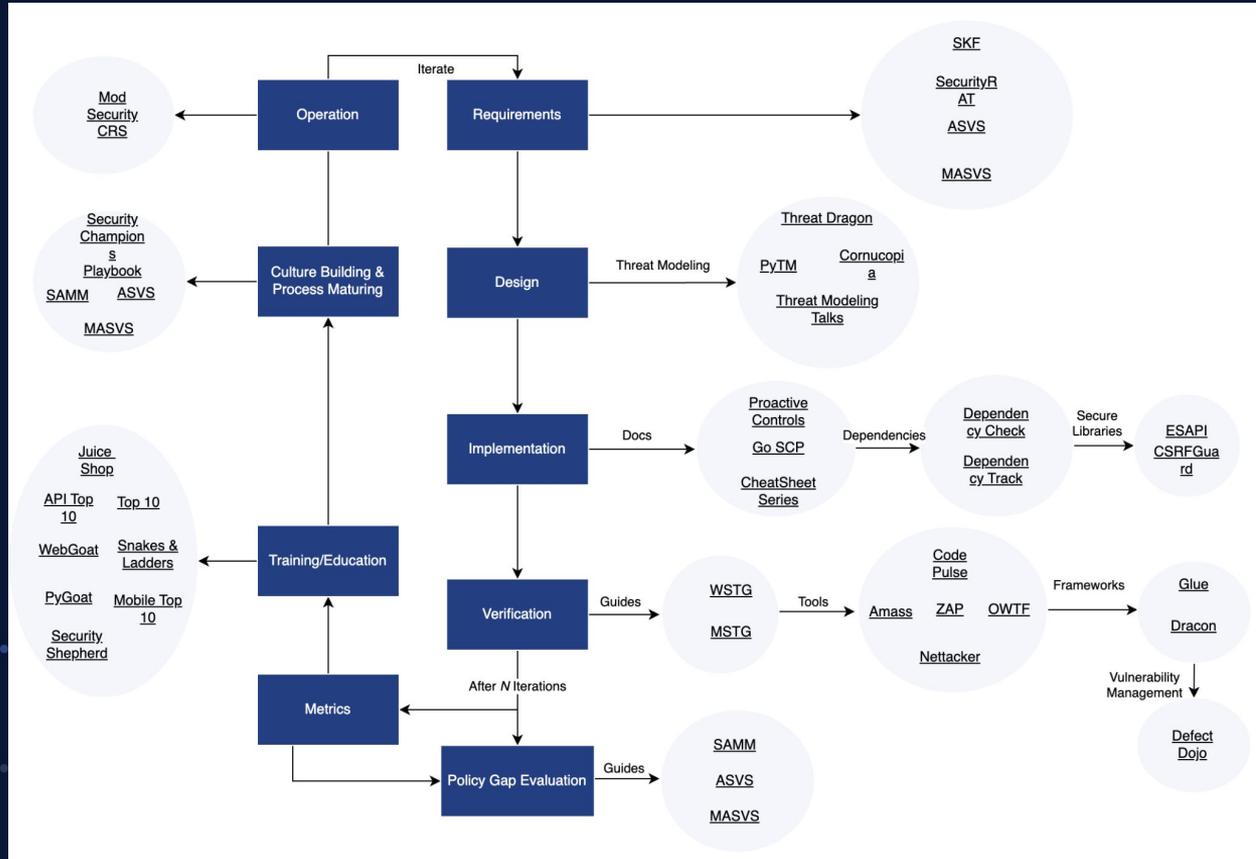
# OWASP Projects Types

- **Tool Projects - 75**
- **Documentation Projects - 80**
- **Code Projects - 34**
- **Other - 3**



# OWASP Projects

Organized around CRE, Common Requirement Enumeration



# OWASP CRE

Links together standards (NIST, CWE) in a coherent way

Helps clarify what each OWASP project is specifically addressing

<https://www.opencre.org>  
allows you to just search the high level topic

The screenshot shows the OWASP CRE website interface. At the top, the URL is [opencre.org](https://opencre.org). The main heading is "Common Requirement Enumeration<sup>Beta</sup>" with the tagline "Your gateway to security topics". Below this is a search bar with a "Search" button and a "Topic text" dropdown menu.

The main content area is titled "OPEN CRE" and contains the following text:

CRE is an interactive content linking platform for uniting security standards and guidelines. It offers easy and robust access to relevant information when designing, developing, testing and procuring secure software.

**WHY?**  
Independent software security professionals got together to find a solution for the complexity and fragmentation in today's landscape of security standards and guidelines. These people are Spyros Gasteratos, Elie Saad, Rob van der Veer and friends, in close collaboration with the SKF, OpenSSF and Owasp Top 10 project.

**HOW?**  
The CRE links each section of a standard to a shared topic (a Common Requirement), causing that section to also link with all other resources that link to the same topic. This 1) enables users to find all combined information from relevant sources, 2) it facilitates a shared and better understanding of cyber security, and 3) it allows standard maintainers to maintain their own content while always redirecting to the relevant security information.

**Example:** the search results for "secret storage" show related documents and CREs.

The search results for "secret storage" are displayed in two columns:

- Results matching : secret storage**
- Related CRE's**
  - 223-780 - Secret storage
  - CRE: Secret storage - is linked to:
    - Cheat\_sheets - Secrets Management Cheat Sheet
    - OWASP WrongSecrets
  - CRE: Secret storage - is related to:
    - 170-772 - Cryptography
  - CRE: Cryptography - is linked to:
    - NIST 800-53 v5 - SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
    - NIST 800-53 v5 - SC-13 Cryptographic Protection
    - NIST 800-53 v5 - SC-17 Public Key Infrastructure Certificates
  - CRE: Cryptography - is the same as:
    - Cloud Controls Matrix - AIS-01 Applications and interfaces (API) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g. OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.
    - Cloud Controls Matrix - AAC-03 An inventory of the organization's external legal, statutory,
- Related Documents**



# Community



# OWASP Community

Chapters all over the world.

Organized via MeetUp in most areas

Many online events

OWASP® Foundation  
70 countries • 231 groups • 111,099 members

Upcoming events Groups Near Me

Map Satellite

Members **111,099** Groups **231** Countries **70**

Upcoming events

In person events  Online events

**OWASP CHAPTER SPRINGS** TUE, OCT 18 - 5:30 PM CDT  
**Scammers and Scams - Part of Our Modern Lives**  
OWASP Bonita Springs Chapter • Bonita Springs, FL  
4 attendees

TUE, OCT 18 - 7:30 PM CDT  
**Monthly Presentation Featuring Cybera**  
OWASP Edmonton Chapter • Edmonton, AB  
2 attendees

WED, OCT 19 - 6:00 PM CDT



 Featured event

THU, MAR 2, 2023, 8:00 AM MST

## Denver OWASP SNOWFROC Conference

 Cable Center - University of Denver campus



SnowFROC 23 is on Thursday March 2nd - all day long. While billed as, "Denver's premier application security conference", SnowFROC's presentations and workshops focus on many facets of cybersecurity and over the years, SnowFROC...

56 attendees

[Attend](#)



# OWASP Community

OWASP Meetup at the GitGuardian Office October 2022



# Events



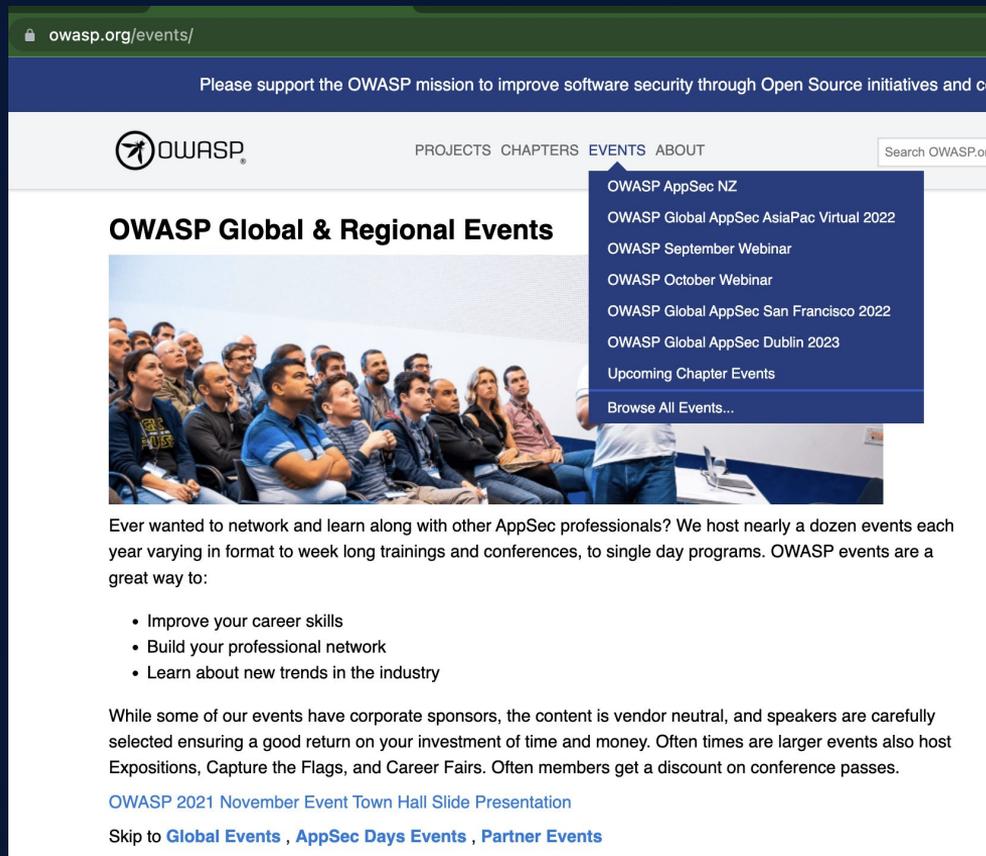
# OWASP Events

Multiple events per year

- Global Events

- AppSec Days

- Partner Events



The screenshot shows the OWASP Events page. At the top, there is a navigation bar with the OWASP logo and links for PROJECTS, CHAPTERS, EVENTS, and ABOUT. A search bar is also present. Below the navigation, the main heading is "OWASP Global & Regional Events". A large image shows a group of people sitting in an audience, listening to a presentation. To the right of the image, a dropdown menu is open, listing several events: OWASP AppSec NZ, OWASP Global AppSec AsiaPac Virtual 2022, OWASP September Webinar, OWASP October Webinar, OWASP Global AppSec San Francisco 2022, OWASP Global AppSec Dublin 2023, Upcoming Chapter Events, and Browse All Events... Below the image, there is a paragraph of text and a bulleted list of benefits. At the bottom, there is a link to a slide presentation and a skip-to section link.

owasp.org/events/

Please support the OWASP mission to improve software security through Open Source initiatives and c

OWASP

PROJECTS CHAPTERS EVENTS ABOUT

Search OWASP.or

## OWASP Global & Regional Events



- OWASP AppSec NZ
- OWASP Global AppSec AsiaPac Virtual 2022
- OWASP September Webinar
- OWASP October Webinar
- OWASP Global AppSec San Francisco 2022
- OWASP Global AppSec Dublin 2023
- Upcoming Chapter Events
- Browse All Events...

Ever wanted to network and learn along with other AppSec professionals? We host nearly a dozen events each year varying in format to week long trainings and conferences, to single day programs. OWASP events are a great way to:

- Improve your career skills
- Build your professional network
- Learn about new trends in the industry

While some of our events have corporate sponsors, the content is vendor neutral, and speakers are carefully selected ensuring a good return on your investment of time and money. Often times are larger events also host Expositions, Capture the Flags, and Career Fairs. Often members get a discount on conference passes.

[OWASP 2021 November Event Town Hall Slide Presentation](#)

Skip to [Global Events](#) , [AppSec Days Events](#) , [Partner Events](#)



# OWASP Events



OWASP 2023  
GLOBAL  
AppSec | DUBLIN  
IRELAND  
FEB 13-16

TRAINING

FEB 13 - 14

CONFERENCE

FEB 15 - 16



# Education and Training



# OWASP Education And Training

## 10 Best Owasp Courses, Training, Classes & Tutorials Online

Course Name	Enrolled Students (Count)	Reviews (count)
1. <a href="#">Web Application Security for Absolute Beginners (no coding!)</a> <b>Our Best Pick</b>	7525+	2453+
2. <a href="#">Complete guide to OWASP top 10 (2020)</a>	635+	278+
3. <a href="#">Certified Secure Coder- PHP (CSC- PHP)</a>	1356+	128+
4. <a href="#">Complete Ethical Hacking &amp; Penetration Testing for Web Apps</a>	4763+	96+
5. <a href="#">OWASP: Threats Fundamentals</a>	210+	79+
6. <a href="#">OWASP Proactive Controls</a>	116+	43+
7. <a href="#">PenTesting with OWASP ZAP: Mastery course</a>	498+	41+
8. <a href="#">OWASP: Avoiding Hacker Tricks</a>	70+	21+
9. <a href="#">OWASP: Forgery and Phishing</a>	50+	19+
10. <a href="#">OWASP Mobile Security Testing Top 10 Vulnerabilities</a>	56+	8+



# OWASP Education And Training



SecureFlag

Real-world | Secure Coding Training

<https://secureflag.owasp.org/>



# OWASP Education And Training

secureflag.owasp.org/user/index.html#/exercises/paths

SecureFlag

Assigned Activities 1 Running Labs ▶ 🔔 d

## Learning Paths

Technology  Level  Status

 Not Completed

### OWASP Top 10:2021 in Java

Number of Activities: **30**

Level    Beginner

[Browse Learning Path](#)

 Not Completed

### Cryptography in Java

Number of Activities: **10**

Level    Intermediate

[Browse Learning Path](#)

 Not Completed

### PCI-DSS in Java

Number of Activities: **18**

Level    Intermediate

[Browse Learning Path](#)

 Not Completed

### Intermediate Secure Coding in Java

Number of Activities: **18**

Level    Intermediate

[Browse Learning Path](#)

 Not Completed

### Secure Authentication in Java

Number of Activities: **12**

Level    Intermediate

[Browse Learning Path](#)

 Not Completed

### OWASP API Security Top 10:2019 in Java

Number of Activities: **24**

Level    Intermediate

[Browse Learning Path](#)

powered by  SecureFlag Learning Path

Dashboard  
Labs  
Learning Paths  
Tournaments  
Achievements  
Team  
Settings  
Help  
Log Out



# Publications and Resources



# OWASP Publications and Resources

OWASP AppSec Asia Pacific 2012 Training

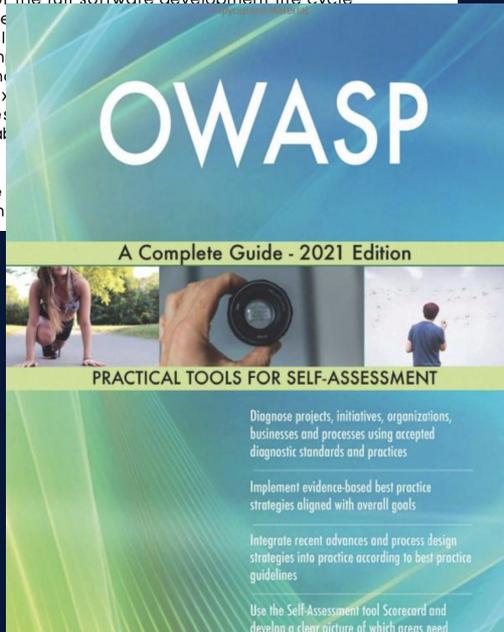
## Building Secure Web Applications

Web application security breaches on websites of major corporations and government entities have received significant media attention due to large number of users affected and the leaking of sensitive personal information.

This training will show how to develop secure Web applications and covers security aspects of the full software development life cycle

(SDLC). Participants will learn to review common risks, including technical and business implementation, white-box While most code examples content is equally applicable database engines.

Participants are welcome for review during the train



## Books

Many free resources online

There is a good deal of crossover with Projects



**OK, OWASP Does A Lot**

**How can I use this?**



# OWASP Getting Started

1. Top 10s
2. Cheat Sheet Series
3. Goats
4. ZAP



# Top 10s



# The OWASP 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.



# OWASP Top 10 Vulnerabilities

## 2021

**A01:2021**-Broken Access Control

**A02:2021**-Cryptographic Failures

**A03:2021**-Injection

**A04:2021**-Insecure Design

**A05:2021**-Security Misconfiguration

**A06:2021**-Vulnerable and Outdated Components

**A07:2021**-Identification and Authentication Failures

**A08:2021**-Software and Data Integrity Failures

**A09:2021**-Security Logging and Monitoring Failures\*

**A10:2021**-Server-Side Request Forgery\*

\*From The Survey



# OWASP Top 10 Vulnerabilities

## A02:2021 – Cryptographic Failures



### Table of contents

Factors

Overview

Description

How to Prevent

Example Attack Scenarios

References

List of Mapped CWEs

### Factors

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Avg Weighted Exploit	Avg Weighted Impact	Max Coverage	Avg Coverage
29	46.44%	4.49%	7.29	6.81	79.33%	34.85%



### How to Prevent

Do the following, at a minimum, and consult the references:

- Classify data processed, stored, or transmitted by an application. Identify which data is sensitive according to privacy laws, regulatory requirements, or business needs.



# OWASP Top 10s

1. [Mobile Security](#)
2. [API Security](#)
3. [CI/CD Security](#)
4. [Kubernetes](#)
5. [Low-Code/No-Code](#)
6. [Privacy Risks](#)
7. [Cloud-Native Application Security](#)
8. [Data Security](#)
9. [Desktop App](#)
10. [Docker](#)
11. [Serverless](#)
12. [Thick Client](#)
13. [Client-Side Security Risks](#)



# Cheat Sheet Series



# OWASP Cheat Sheet Series

<https://cheatsheetseries.owasp.org/>



# OWASP Cheat Sheet Series

## Kubernetes Security Cheat Sheet

### Kubernetes

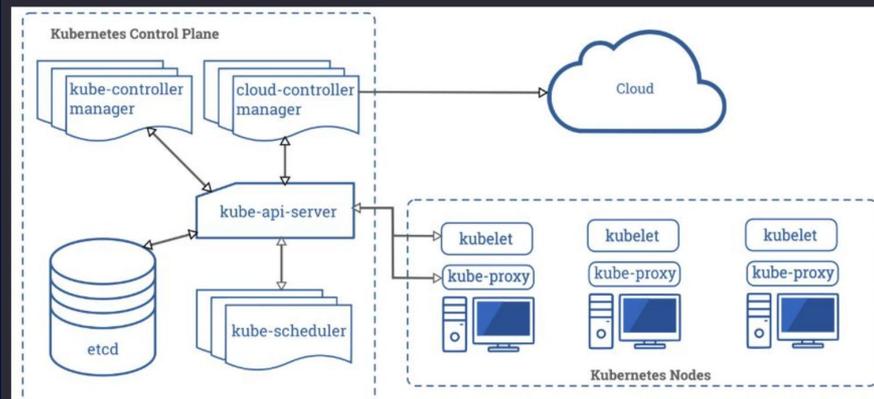
Kubernetes is an open source container orchestration engine for automating deployment, scaling, and management of containerized applications. The open source project is hosted by the Cloud Native Computing Foundation (CNCF).

When you deploy Kubernetes, you get a cluster. A Kubernetes cluster consists of a set of worker machines, called nodes that run containerized applications. The control plane manages the worker nodes and the Pods in the cluster.

### Control Plane Components

The control plane's components make global decisions about the cluster, as well as detecting and responding to cluster events. It consists of components such as kube-apiserver, etcd, kube-scheduler, kube-controller-manager and cloud-controller-manager

Component	Description
kube-apiserver	kube-apiserver exposes the Kubernetes API. The API server is the front end for the Kubernetes control plane.
etcd	etcd is a consistent and highly-available key-value store used as Kubernetes' backing store for all cluster data.
kube-scheduler	kube-scheduler watches for newly created Pods with no assigned node, and selects a node for them to run on.
kube-controller-manager	kube-controller-manager runs controller processes. Logically, each controller is a separate process, but to reduce complexity, they are all compiled into a single binary and run in a single process.



This cheatsheet provides a starting point for securing Kubernetes cluster. It is divided into the following categories:

- Securing Kubernetes hosts
- Securing Kubernetes components
- Kubernetes Security Best Practices: Build Phase
- Kubernetes Security Best Practices: Deploy Phase
- Kubernetes Security Best Practices: Runtime Phase



# Goats

‘Greatest Of All Time???’



# OWASP Goats

Goats are deliberately insecure applications for testing and training purposes

## Lab Projects

- WebGoat
- Node.js Goat
- WrongSecrets

## Incubator Projects or Proposed

- Pygoat
- AndroGoat
- ChainGoat
- Laravel Goat
- Webgoat PHP
- SupplyChainGoat



# OWASP Goats



## OWASP Juice Shop

owasp flagship project release v14.3.0 Follow 4.8k Follow r/owasp\_juiceshop 239

CI/CD Pipeline passing test coverage 89% maintainability A technical debt 2% tests passed

openssf best practices gold GitHub ★ 7.3k Contributor Covenant v2.0 adopted

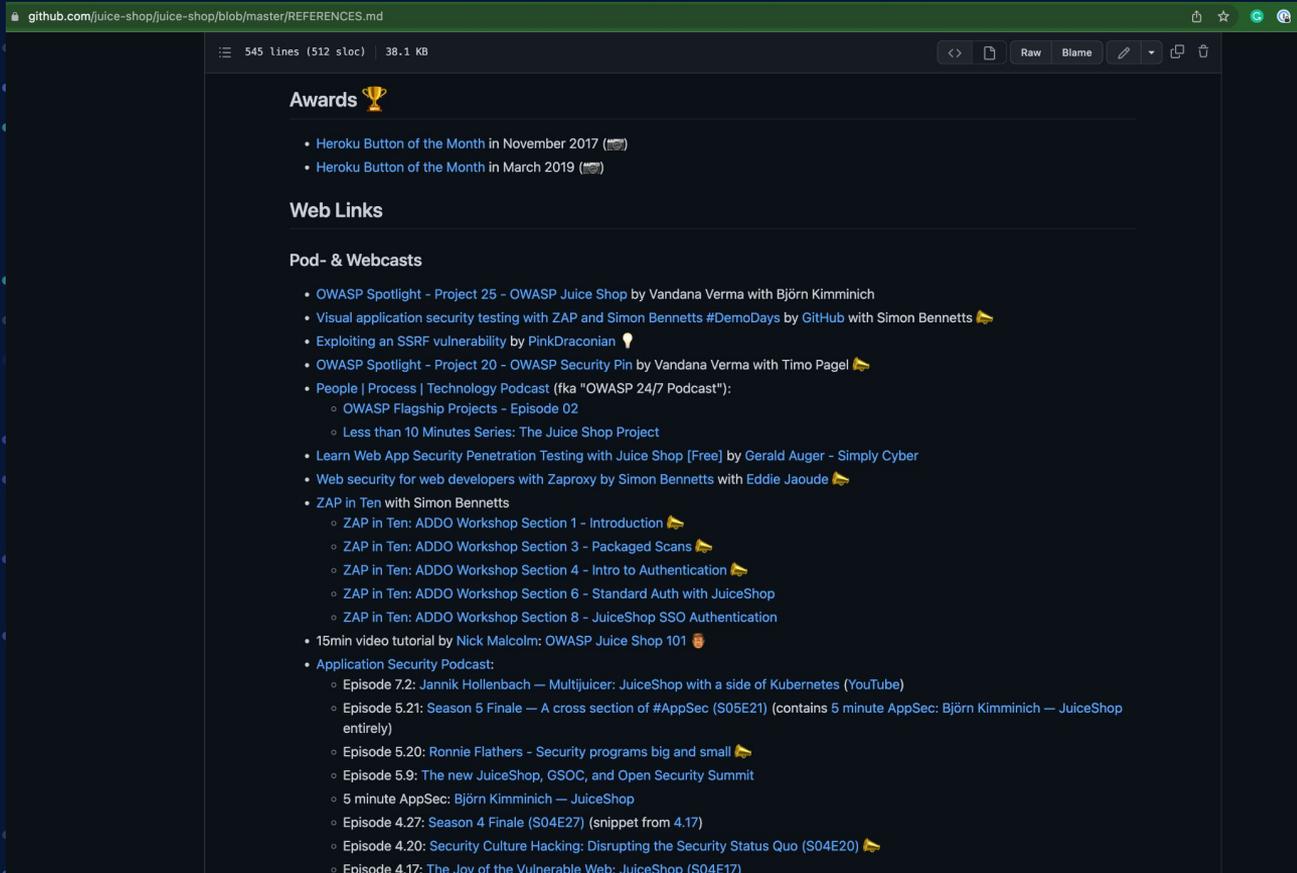
The most trustworthy online shop out there. (@dschadow) — The best juice shop on the whole internet! (@shehackspurple) — Actually the most bug-free vulnerable application in existence! (@vanderaj) — First you 😂😂 then you 🤔 (@kramse) — But this doesn't have anything to do with juice. (@coderPatros' wife)

OWASP Juice Shop is probably the most modern and sophisticated insecure web application! It can be used in security trainings, awareness demos, CTFs and as a guinea pig for security tools! Juice Shop encompasses vulnerabilities from the entire [OWASP Top Ten](#) along with many other security flaws found in real-world applications!



# OWASP Goats

Extremely well  
documented  
and discussed  
in media



github.com/juice-shop/juice-shop/blob/master/REFERENCES.md

545 lines (512 sloc) | 38.1 KB

## Awards 🏆

- Heroku Button of the Month in November 2017 📧
- Heroku Button of the Month in March 2019 📧

## Web Links

### Pod- & Webcasts

- OWASP Spotlight - Project 25 - OWASP Juice Shop by Vandana Verma with Björn Kimminich
- Visual application security testing with ZAP and Simon Bennetts #DemoDays by GitHub with Simon Bennetts 🗑
- Exploiting an SSRF vulnerability by PinkDraconian 🔒
- OWASP Spotlight - Project 20 - OWASP Security Pin by Vandana Verma with Timo Pagel 🗑
- People | Process | Technology Podcast (fka "OWASP 24/7 Podcast"):
  - OWASP Flagship Projects - Episode 02
    - Less than 10 Minutes Series: The Juice Shop Project
- Learn Web App Security Penetration Testing with Juice Shop [Free] by Gerald Auger - Simply Cyber
- Web security for web developers with Zaproxy by Simon Bennetts with Eddie Jaoudé 🗑
- ZAP in Ten with Simon Bennetts
  - ZAP in Ten: ADDO Workshop Section 1 - Introduction 🗑
  - ZAP in Ten: ADDO Workshop Section 3 - Packaged Scans 🗑
  - ZAP in Ten: ADDO Workshop Section 4 - Intro to Authentication 🗑
  - ZAP in Ten: ADDO Workshop Section 6 - Standard Auth with JuiceShop
  - ZAP in Ten: ADDO Workshop Section 8 - JuiceShop SSO Authentication
- 15min video tutorial by Nick Malcolm: OWASP Juice Shop 101 📺
- Application Security Podcast:
  - Episode 7.2: Jannik Hollenbach — Multijuicer: JuiceShop with a side of Kubernetes (YouTube)
  - Episode 5.21: Season 5 Finale — A cross section of #AppSec (S05E21) (contains 5 minute AppSec: Björn Kimminich — JuiceShop entirely)
  - Episode 5.20: Ronnie Flathers - Security programs big and small 🗑
  - Episode 5.9: The new JuiceShop, GSOC, and Open Security Summit
  - 5 minute AppSec: Björn Kimminich — JuiceShop
  - Episode 4.27: Season 4 Finale (S04E27) (snippet from 4.17)
  - Episode 4.20: Security Culture Hacking: Disrupting the Security Status Quo (S04E20) 🗑
  - Episode 4.17: The Jov of the Vulnerable Web: JuiceShop (S04E17)



# Demo by maintainer on YouTube

## OWASP Juice Shop 14.0.1

Probably the most modern and sophisticated insecure web application



<https://owasp-juice.shop>

Copyright (c) 2014-2022 Björn Kimminich / @bkimminich



[https://www.youtube.com/watch?v=n9DK87g\\_Alo](https://www.youtube.com/watch?v=n9DK87g_Alo)



**ZAP**



# OWASP ZAP

## OWASP® Zed Attack Proxy (ZAP)

The world's most widely used web app scanner. Free and open source. Actively maintained by a dedicated international team of volunteers.

[Quick Start Guide](#)

[Download Now](#)



# OWASP ZAP

The screenshot displays the OWASP ZAP web interface. At the top, the title "Automated Scan" is centered. Below the title, a brief instruction states: "This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically given permission to test." The configuration area includes a text input field for the URL to attack, currently set to "http://localhost:3000/#/". Below this, there are checkboxes for "Use traditional spider" (checked) and "Use ajax spider" (checked) with a dropdown menu set to "Firefox Headless". There are "Attack" and "Stop" buttons. The progress indicator shows "Attack complete - see the Alerts tab for details of any issues found".

The bottom section of the interface shows the "Alerts" tab with a list of 9 alerts. The first alert is selected and expanded, showing details for "Content Security Policy (CSP) Header Not Set".

**Alerts (9)**

- Content Security Policy (CSP) Header Not Set (11)
- Cross-Domain Misconfiguration (48)
- Missing Anti-clickjacking Header
- Session ID in URL Rewrite (4)
- Cross-Domain JavaScript Source File Inclusion (4)
- Private IP Disclosure
- Timestamp Disclosure - Unix (5)
- X-Content-Type-Options Header Missing (4)
- Information Disclosure - Suspicious Comments (3)

**Content Security Policy (CSP) Header Not Set**

URL: http://localhost:3000/  
Risk: Medium  
Confidence: High  
Parameter:  
Attack:  
Evidence:  
CWE ID: 693  
WASC ID: 15  
Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)

Description:  
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page - covered types are

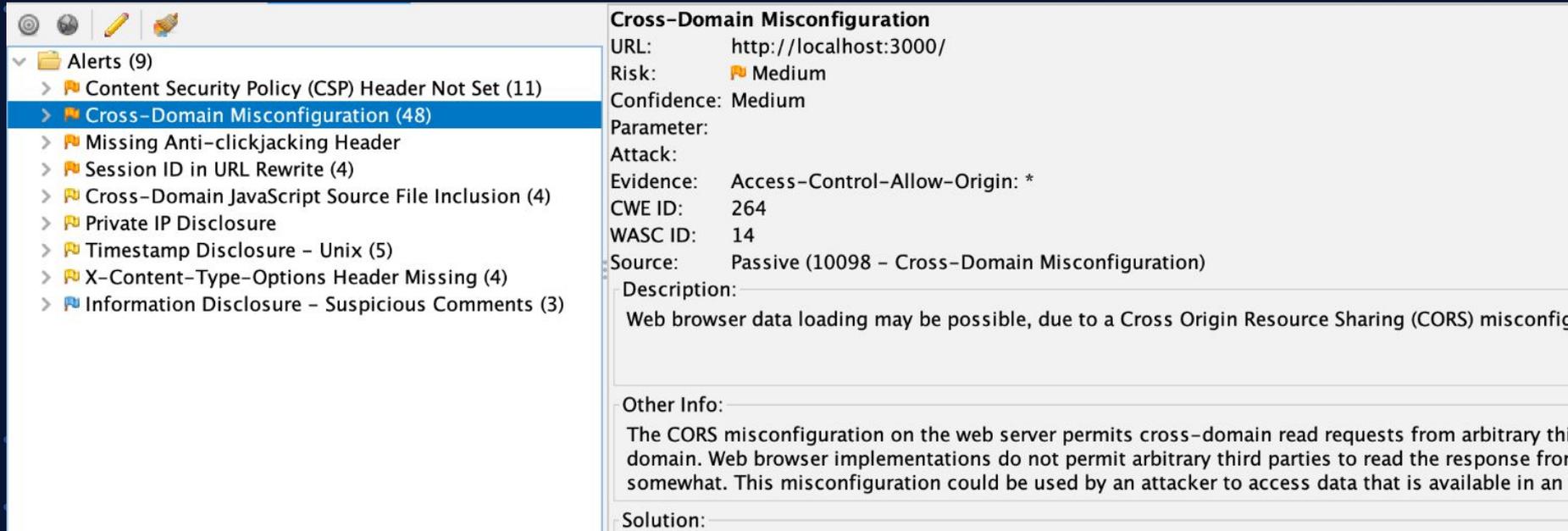
Other Info:

Solution:

Alerts 0 4 4 1 Primary Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0 0 0



# OWASP ZAP



The screenshot displays the OWASP ZAP interface. On the left, a tree view shows a list of alerts under the 'Alerts (9)' folder. The 'Cross-Domain Misconfiguration (48)' alert is selected and highlighted in blue. The right pane shows the details for this alert, including its URL, risk level, confidence, parameter, attack type, evidence, CWE ID, WASC ID, source, description, other info, and solution.

**Alerts (9)**

- > Content Security Policy (CSP) Header Not Set (11)
- > **Cross-Domain Misconfiguration (48)**
- > Missing Anti-clickjacking Header
- > Session ID in URL Rewrite (4)
- > Cross-Domain JavaScript Source File Inclusion (4)
- > Private IP Disclosure
- > Timestamp Disclosure - Unix (5)
- > X-Content-Type-Options Header Missing (4)
- > Information Disclosure - Suspicious Comments (3)

**Cross-Domain Misconfiguration**

URL: http://localhost:3000/  
Risk: Medium  
Confidence: Medium  
Parameter:  
Attack:  
Evidence: Access-Control-Allow-Origin: \*  
CWE ID: 264  
WASC ID: 14  
Source: Passive (10098 - Cross-Domain Misconfiguration)

Description:  
Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration.

Other Info:  
The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third parties. Web browser implementations do not permit arbitrary third parties to read the response from the server, but they do allow them to read the response from the server somewhat. This misconfiguration could be used by an attacker to access data that is available in an application.

Solution:

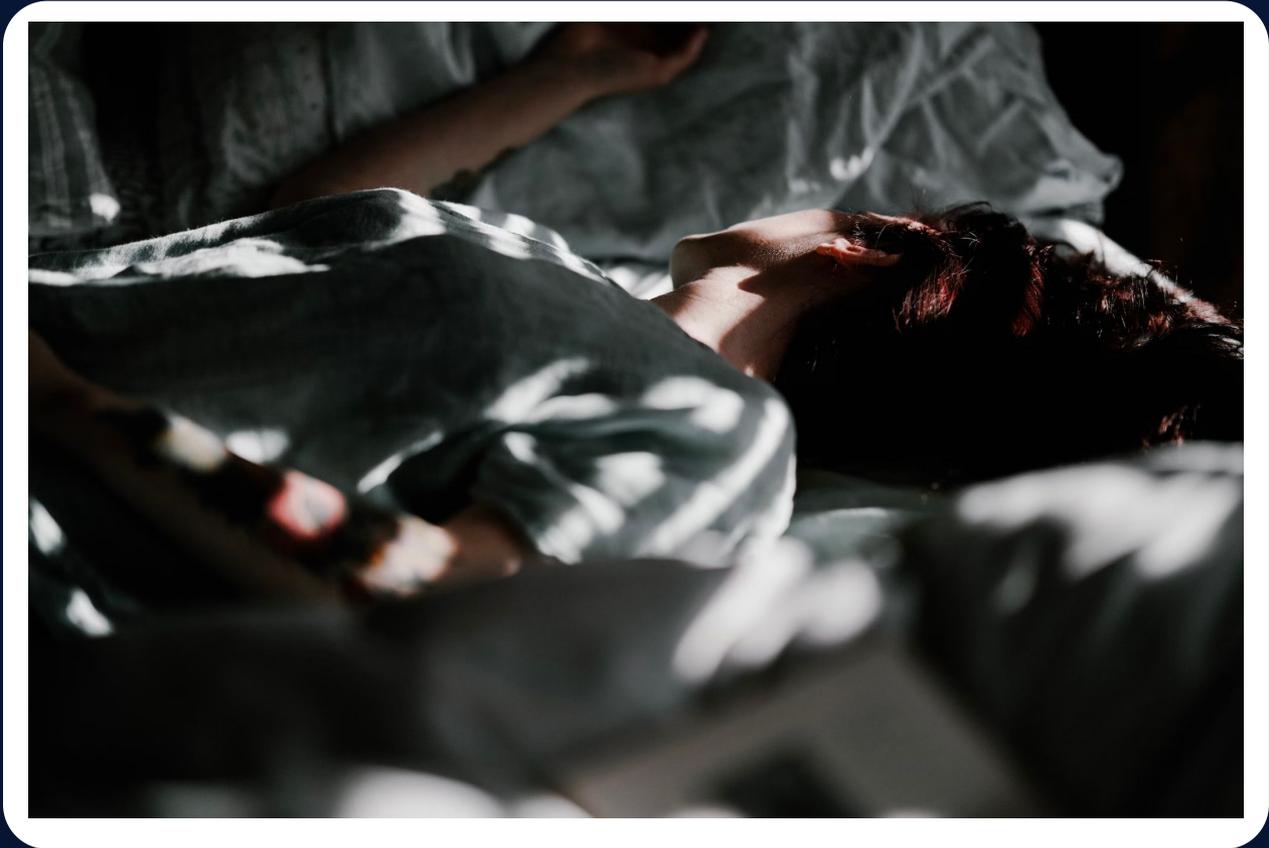


# In Conclusion



IT'S DANGEROUS TO GO  
ALONE! TAKE THIS.





# OWASP Getting Started

1. Top 10
2. Cheat Sheet Series
3. Goats (not the 'greatest of all time')
4. ZAP



# Hi, I'm Dwayne



**Dwayne McDaniel**

- I live in Chicago
- I've been a Developer Advocate since 2016
- On Twitter @mcdwayne
- Happy to chat about anything, hit me up
- Besides tech, I love improv, karaoke and going to rock and roll shows!





# App Security Does Not Need To Be Fun: Ignoring OWASP To Have A Terrible Time

