OWASP 2024
APPSEC DAYS
SINGAPORE

OCT 1-2 2024
OCT 1 TRAINING
OCT 2 CONFERENCE

Leveraging OWASP Projects and Tools in Your AppSec Program

John DiLeo

About Me

- Past lives
  - Simulation developer and system analyst
  - University lecturer - Math, Comp Sci, IT, *et al.*
  - J2EE developer and architect
- Full-time in AppSec since 2014
- Moved from US to New Zealand late 2017

About My Day Job

Gallagher Security – Application Security Lead

- Oversee Cybersecurity Services Team
- Manage Threat Modelling Program
- AppSec Maturity Uplift
- Feature Security Reviews
- In-House AppSec Training

GALLAGHER™

About My *Other* ‘Job’

Chapter Leader, OWASP New Zealand

- Hamilton Meetup
- Regional Training Days

Chair, OWASP New Zealand Day Conferences, 2019-2024

Chair, OWASP Global AppSec-Auckland, 1-5 Sept 2025

OWASP SAMM Project – Core Team

Launched SAMMwise and State of AppSec Survey Projects

What You Can Expect to Hear

- My thoughts about Software Assurance
- Some information about the OWASP Software Assurance Maturity Model (SAMM)
- The names of *dozens* of OWASP Projects
- A few thoughts on leveraging OWASP Projects

What You Shouldn’t Expect to Hear

- An in-depth treatment of SAMM
- Information about *every* OWASP project
  - There are 225 “active” OWASP projects*
  - I’ll mention only 30 or so by name
  - I’ll provide *brief overviews* of fewer than 20

* 15 Flagship, 8 Production, 34 Lab, 126 Incubator, and 42 “need website update” (new or dormant)
[As listed on *owasp.org*, 5 September 2024]

Reasons to Love OWASP Projects

- Developed and maintained by passionate volunteers…who happen to be experts
- Supportive community of users and contributors
  - OWASP Slack (https://owasp.org/slack/invite)
  - Project channels (e.g., #project-samm)
  - Topical channels (e.g., #threat-modeling)
- Open-source – Public repos on GitHub
- Project deliverables are FREE
  (as in ‘freedom’ *and* as in ‘free beer’)

Software Assurance

> “Level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle and that the software functions in the intended manner.”
>
> *- [US] National Information Assurance (IA) Glossary, April 2010*

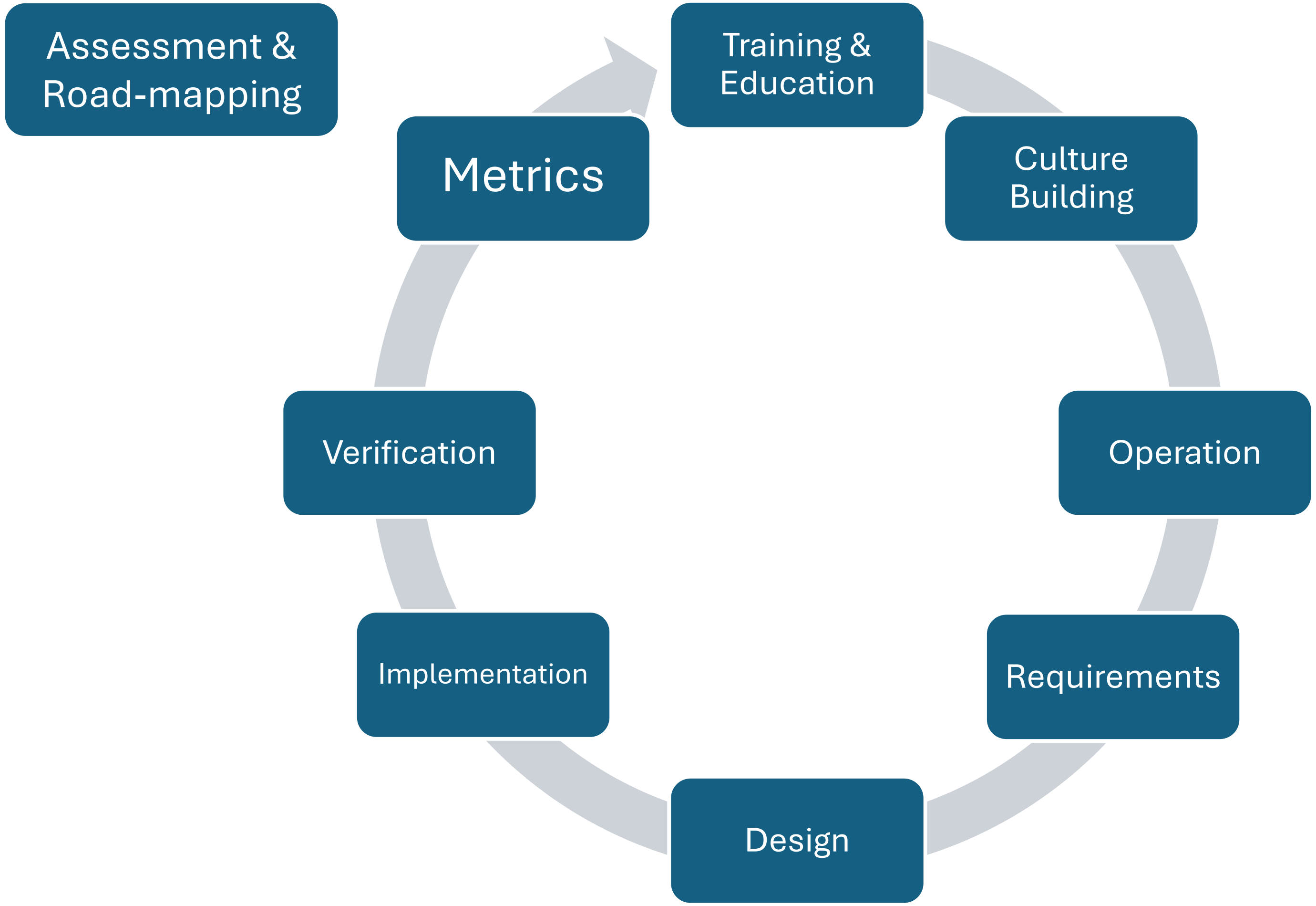
And, by that you mean…?

- Attain and maintain high **stakeholder confidence** in successful delivery of the features you **intended** to deliver
- Prevent, detect, and remove **vulnerabilities**
- Improve **reliability** and **resilience** of the production system

SO MUCH MORE than code reviews or 11th-hour penetration tests

AppSec Program Elements

Ref: OWASP Integration Standards Project



Assessment and Road-Mapping

- **Software Assurance Maturity Model (SAMM)**

Software Assurance Maturity Model (SAMM)

Flagship Project

What is SAMM?

An open framework that provides an **effective** and **measurable** way for all types of organizations to **analyze** and **improve** their software security posture.

https://owaspsamm.org

Measurable
Defined maturity levels across business practices

Actionable
Clear pathways for improving maturity levels

Versatile
Technology, process, and organization agnostic

SAMM Model Structure

- Five Business Functions
- 15 Practice Areas
- 2 Activity Streams per Practice Area
- 3 Activities in each Stream – 90 Activities total

Governance	Design	Implementation	Verification	Operations
Strategy & Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
Policy & Compliance	Security Requirements	Secure Deployment	Requirements-driven Testing	Environment Management
Education & Guidance	Secure Architecture	Defect Management	Security Testing	Operational Management

Training and Education

Awareness:

- AppSec Awareness Campaigns
- **OWASP Top 10**

Board Game:

- Snakes & Ladders

Broadcasts:

- DevSlop Show
- Podcast Series

Training Platforms/Applications:

- Cyber Scavenger Hunt
- TimeGap Theory

Intentionally Vulnerable WebApps:

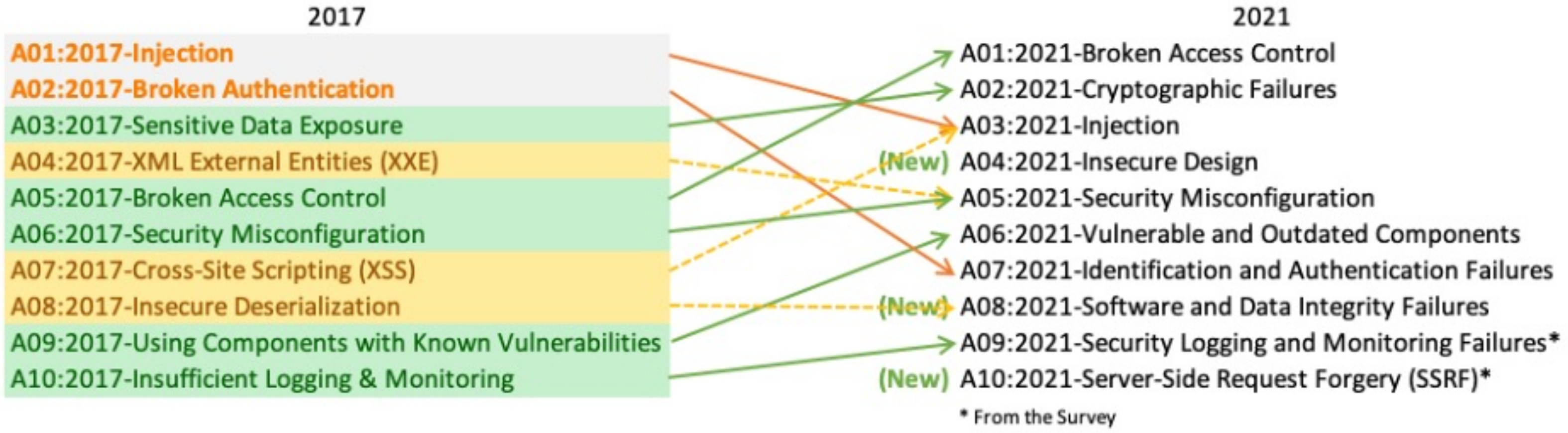
- **Juice Shop**
- Security Shepherd
- WebGoat / PyGoat
- WrongSecrets

OWASP Top 10

Flagship Project

OWASP TOP 10

- Standard awareness document for developers and web application security
- Represents broad consensus about the most critical security risks to web apps
  - Current version: 2021
  - Next version: 2025



2017

A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

2021

A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

OWASP Top 10

Flagship Project

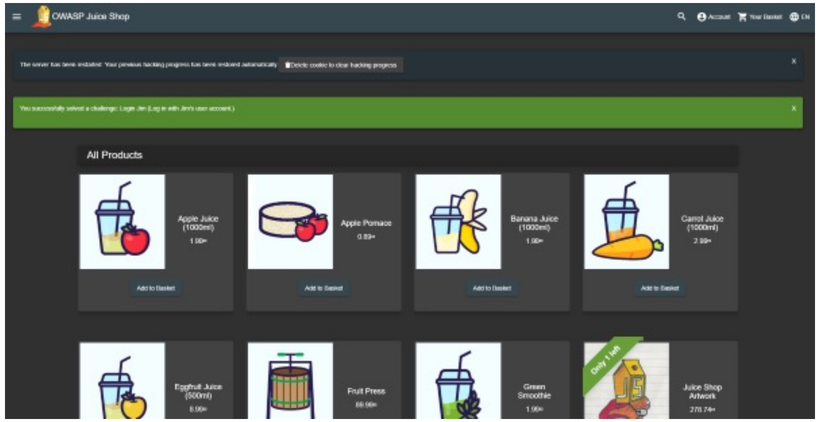
OWASP Projects in the Top Ten “family” include:

- **Lab:** Machine Learning, Mobile, CI/CD, LLM, Low-Code/No-Code, Privacy
- **Incubator:** AI, Cloud-Native AppSec, Data Security, Desktop App Security, DevSecOps, Docker, Kubernetes, Operational Technology (OT), Serverless, Thick Client, Client-Side Security, Drone Security, Maritime, Insider Threats

Juice Shop

Flagship Project

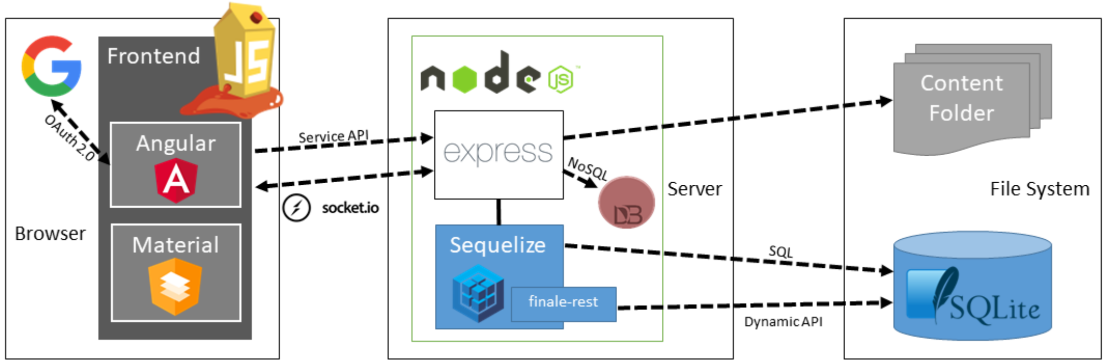
- World’s most modern and sophisticated insecure web application!
- Exhibits vulnerabilities from the entire OWASP Top Ten, and lots more
- Useful for:
  - Security training
  - Awareness demos
  - Capture the Flag events (CTFs)
  - Target app for security tools



The server has been restarted: Your previous hacking progress has been restored automatically. Delete cookie to clear hacking progress

You successfully solved a challenge: Login Jim (Log in with Jim's user account.)

OWASP Juice Shop
Account
Your Basket
EN
All Products
Apple Juice (1000ml) 1.99¤
Apple Pomace 0.89¤
Banana Juice (1000ml) 1.99¤
Carrot Juice (1000ml) 2.99¤
Add to Basket
Eggfruit Juice (500ml) 8.99¤
Fruit Press 89.99¤
Green Smoothie 1.99¤
Only 1 left
Juice Shop Artwork 278.74¤

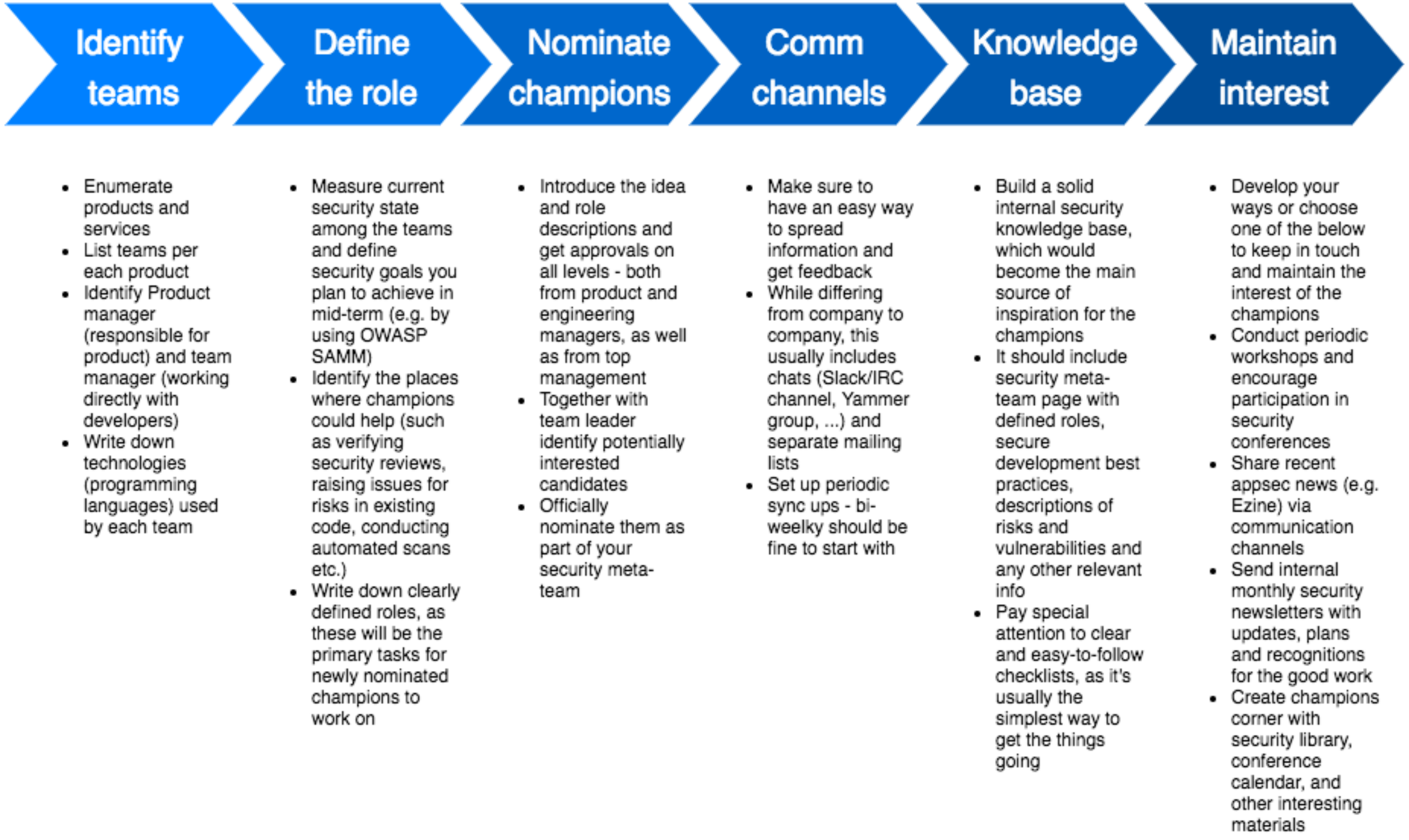


Culture Building

- Security Champions Guide (formerly Playbook)
- Security Culture

Security Champions Guide

Incubator Project



Identify teams

- Enumerate products and services
- List teams per each product
- Identify Product manager (responsible for product) and team manager (working directly with developers)
- Write down technologies (programming languages) used by each team

Define the role

- Measure current security state among the teams and define security goals you plan to achieve in mid-term (e.g. by using OWASP SAMM)
- Identify the places where champions could help (such as verifying security reviews, raising issues for risks in existing code, conducting automated scans etc.)
- Write down clearly defined roles, as these will be the primary tasks for newly nominated champions to work on

Nominate champions

- Introduce the idea and role descriptions and get approvals on all levels - both from product and engineering managers, as well as from top management
- Together with team leader identify potentially interested candidates
- Officially nominate them as part of your security meta-team

Comm channels

- Make sure to have an easy way to spread information and get feedback
- While differing from company to company, this usually includes chats (Slack/IRC channel, Yammer group, ...) and separate mailing lists
- Set up periodic sync ups - bi-weekly should be fine to start with

Knowledge base

- Build a solid internal security knowledge base, which would become the main source of inspiration for the champions
- It should include security meta-team page with defined roles, secure development best practices, descriptions of risks and vulnerabilities and any other relevant info
- Pay special attention to clear and easy-to-follow checklists, as it's usually the simplest way to get the things going

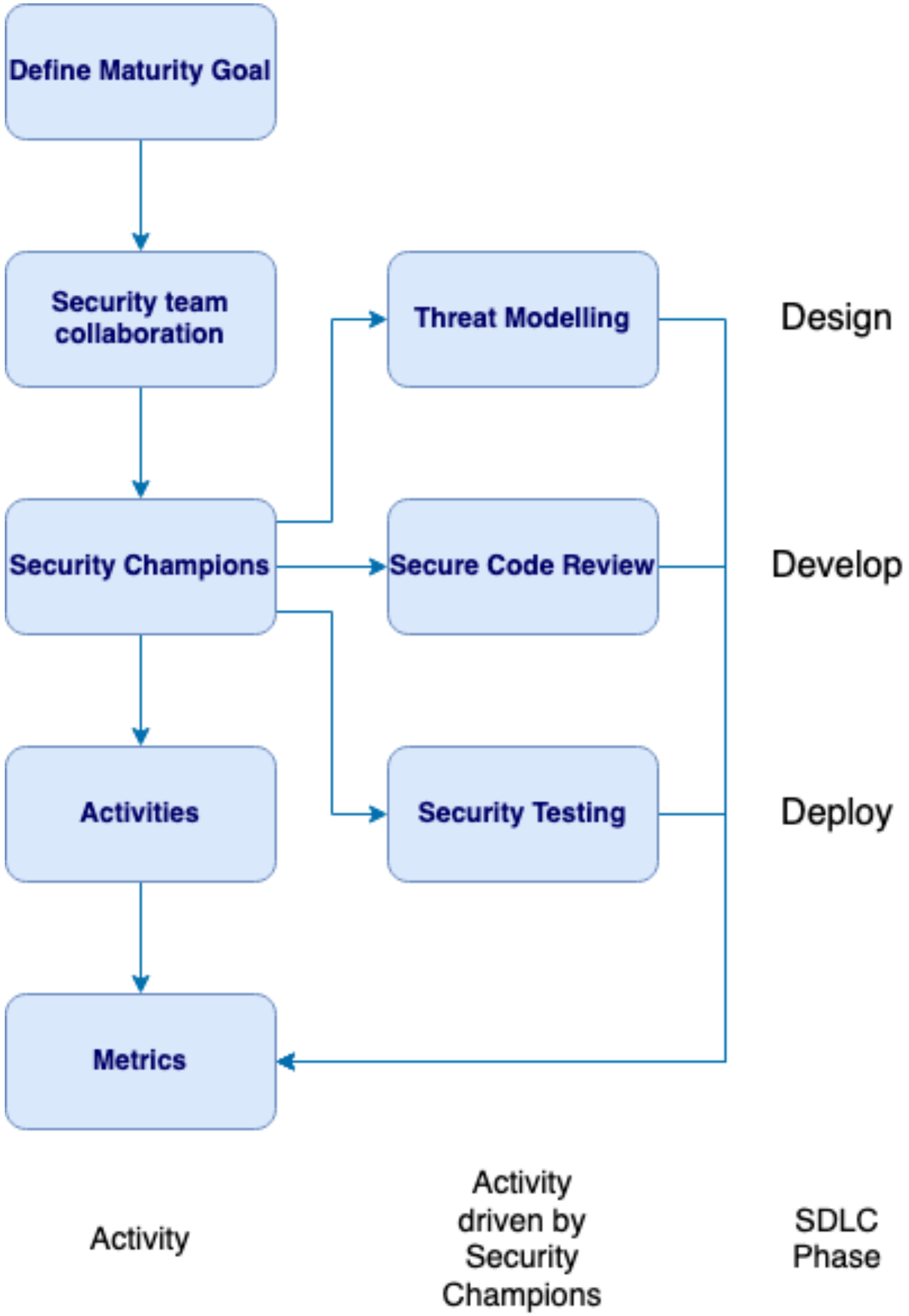
Maintain interest

- Develop your ways or choose one of the below to keep in touch and maintain the interest of the champions
- Conduct periodic workshops and encourage participation in security conferences
- Share recent appsec news (e.g. Ezine) via communication channels
- Send internal monthly security newsletters with updates, plans and recognitions for the good work
- Create champions corner with security library, conference calendar, and other interesting materials

(Legacy Artifact)

Security Culture

Incubator Project



Operation

- **Core Rule Set (CRS)**
- **Coraza Web Application Firewall (WAF)**

Core Rule Set (CRS)

Production Project

- Set of generic attack detection rules for use with ModSecurity or compatible web application firewalls
- Sims to protect web applications from a wide range of attacks, including the OWASP Top Ten, with a minimum of false alerts.
- Provides protection against many common attack categories

OWASP CRS

THE 1ST LINE OF DEFENSE

Coraza Web Application Firewall (WAF)

Flagship Project

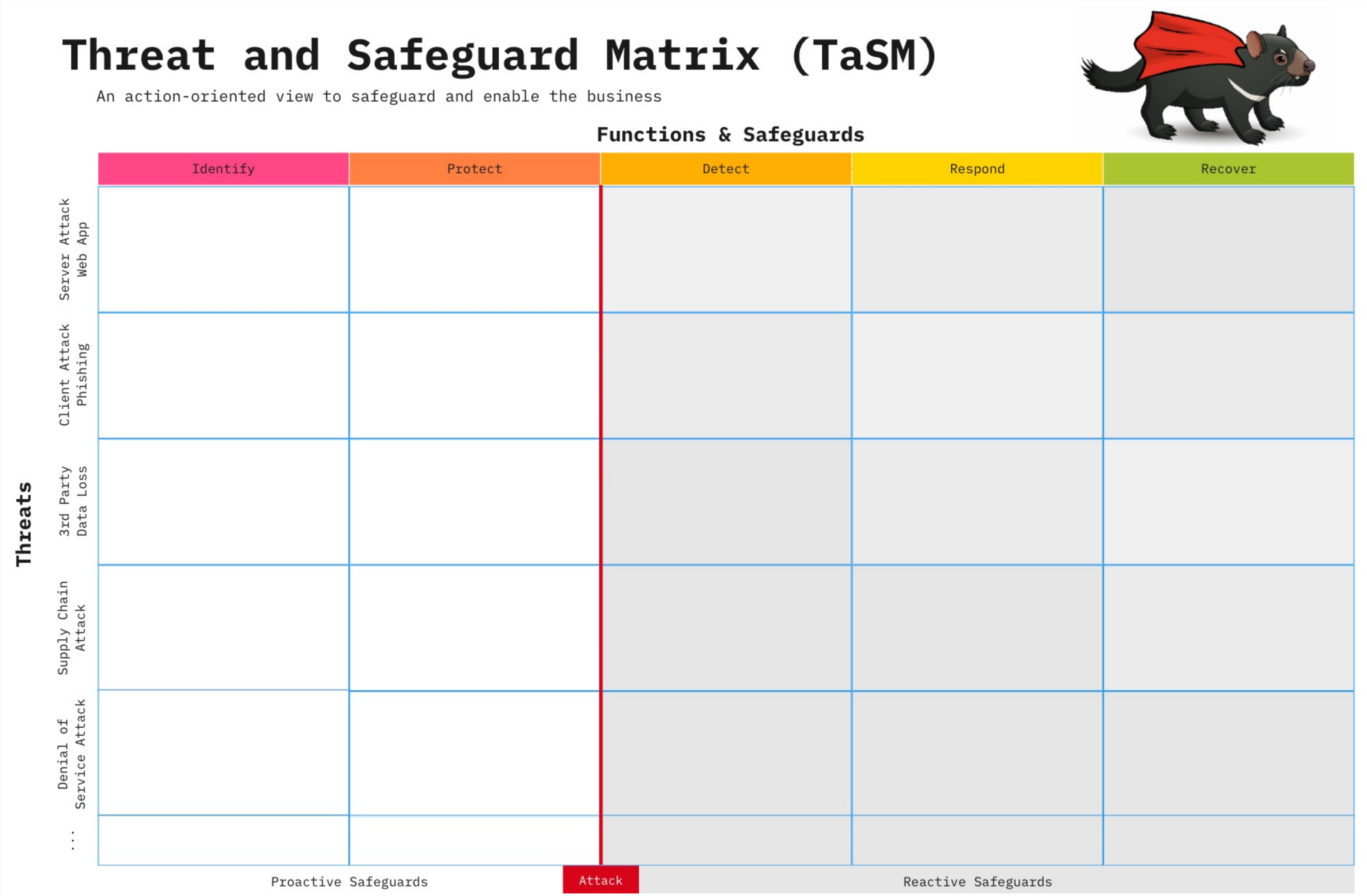
- golang enterprise-grade Web Application Firewall framework
    - Supports Modsecurity’s seclang language
    - 100% compatible with OWASP CRS
- Enrich your web application’s security with powerful rules that comprehensively enforce good cybersecurity behavior.

Requirements

- Application Security Verification Standard (ASVS)
- **Threat and Safeguard Matrix (TaSM)**
- Mobile Application Security – Verification Standard (MASVS)
- **SecurityRAT**

Threat and Safeguard Matrix (TaSM)

Incubator Project



Threat and Safeguard Matrix (TaSM)

An action-oriented view to safeguard and enable the business

Functions & Safeguards

Threats	Identify	Protect	Detect	Respond	Recover
Server Attack Web App					
Client Attack Phishing					
3rd Party Data Loss					
Supply Chain Attack					
Denial of Service Attack					
...					

Proactive Safeguards | Attack | Reactive Safeguards

SecurityRAT

Incubator Project

Security Requirement Automation Tool (SecurityRAT) focuses on automating the generation and management of security requirements

1. You specify the type of software artifact.
2. SecurityRAT tells you which requirements you should fulfill.
3. You decide how to handle those desired requirements.
4. You persist the artifact state in an issue tracker and create tickets for the requirements where an explicit action is necessary.
5. You document relevant changes in requirement compliance whenever appropriate.

Demo instance (usually) at https://securityrat.org

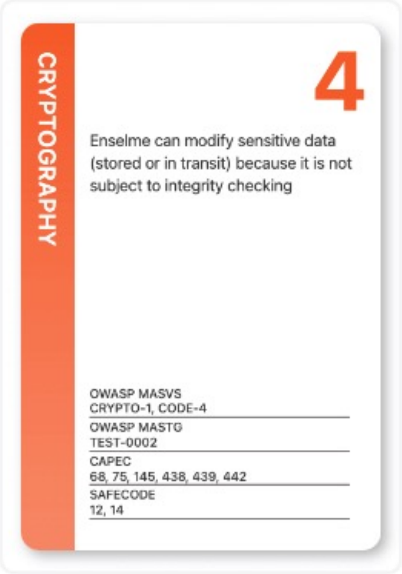
Design

- Cheat Sheet Series
- **Cornucopia**
- Ontology Driven Threat Modeling Framework (OdTM)
- **PyTM**
- **Threat Dragon**
- Threat Modeling Playbook (OTMP)

Cornucopia – Website App Edition

Lab Project

- Card game to support secure coding design, similar to *Elevation of Privilege (EoP)*
- Based on Secure Code Practices (SCP) – Quick Reference Guide
- Six suits:
  - Data validation and encoding
  - Authentication
  - Session management
  - Authorization
  - Cryptography
  - Cornucopia
- Download card images and print locally
- Play online at: https://copi.securedelivery.io/



CRYPTOGRAPHY

4

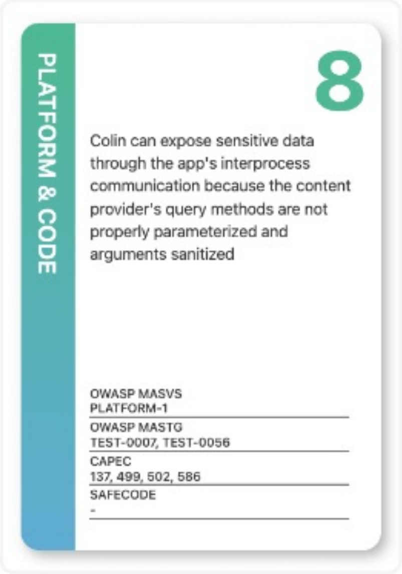
Enselme can modify sensitive data (stored or in transit) because it is not subject to integrity checking

OWASP MASVS
CRYPTO-1, CODE-4

OWASP MASTG
TEST-0002

CAPEC
68, 75, 145, 438, 439, 442

SAFECODE
12, 14



PLATFORM & CODE

8

Colin can expose sensitive data through the app's interprocess communication because the content provider's query methods are not properly parameterized and arguments sanitized

OWASP MASVS
PLATFORM-1

OWASP MASTG
TEST-0007, TEST-0056

CAPEC
137, 499, 502, 586

SAFECODE
-

PyTM

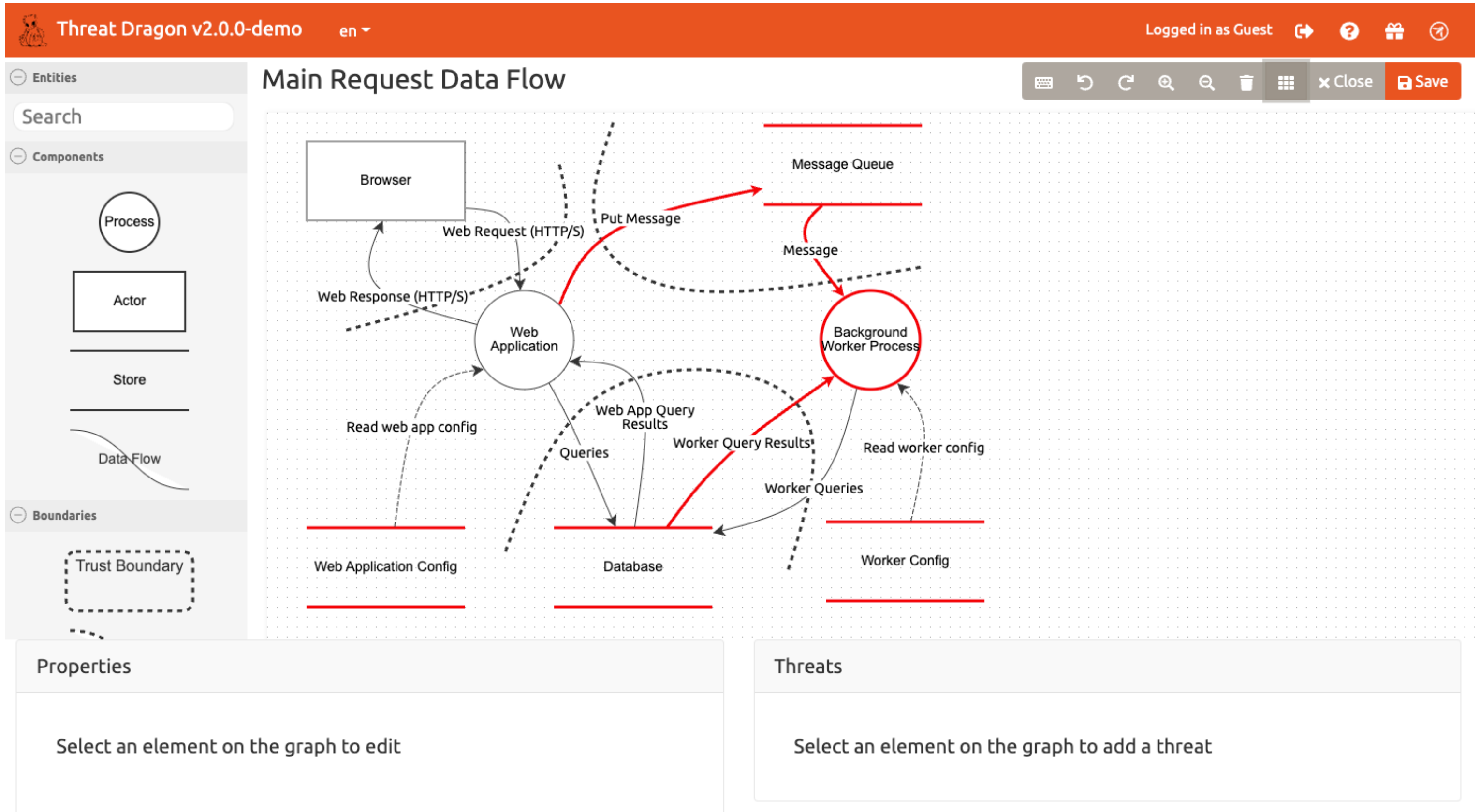
Lab Project

- A ‘Pythonic’ framework for threat modeling
- Define your system *in Python*, using the elements and properties described in the pytm framework
- Can generate Data Flow Diagram (DFD) or Sequence Diagram views of system and threats

Threat Dragon

Lab Project

- Open-source threat model diagram creation tool
- Runs as desktop app or web app



Main Request Data Flow

Properties

Select an element on the graph to edit

Threats

Select an element on the graph to add a threat

Implementation

Documentation:

- **Proactive Controls**
- Go Secure Code Practices (SCP) Guide
- Cheat Sheet Series

Software Composition Analysis (SCA):

- Dependency-Check
- **Dependency-Track**

Libraries:

- Enhanced Security API (ESAPI)
- CSRFGuard

Proactive Controls for Developers

Lab Project

Describes the most important control and control categories that **every architect and developer** should absolutely, 100% include in every project

- 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
Open Web Application Security Project

OWASP PRO Active CONTROLS

FOR DEVELOPERS

2018 v 3.0

10 Critical Security Areas That Software Developers Must Be Aware Of

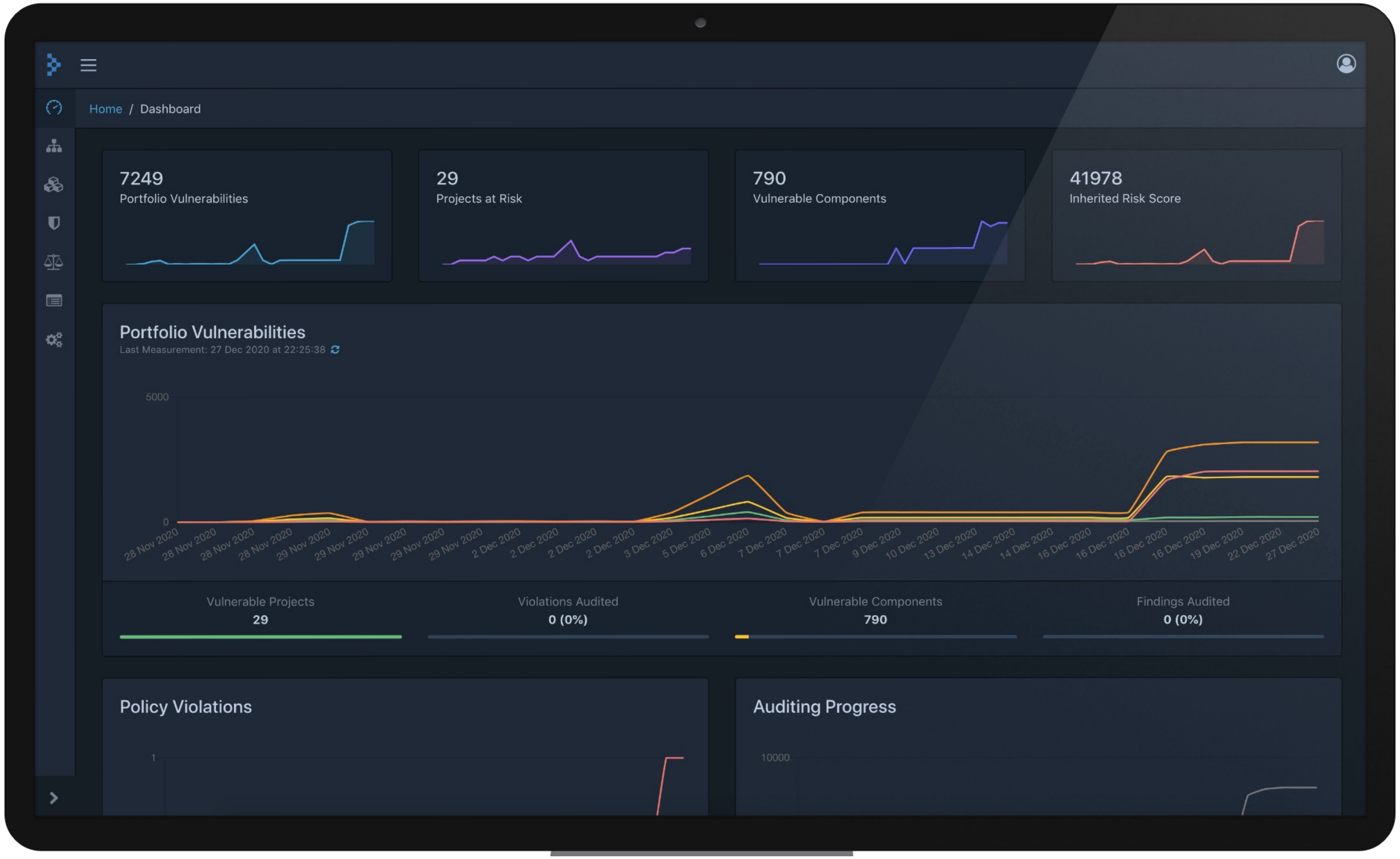
PROJECT LEADERS

KATY ANTON
JIM MANICO
JIM BIRD

Dependency-Track

Flagship Project

- Intelligent Supply Chain Component Analysis platform
- Leverages capabilities of Software Bill of Materials (SBOM)



Home / Dashboard

7249 Portfolio Vulnerabilities

29 Projects at Risk

790 Vulnerable Components

41978 Inherited Risk Score

Portfolio Vulnerabilities

Last Measurement: 27 Dec 2020 at 22:25:38

Vulnerable Projects 29

Violations Audited 0 (0%)

Vulnerable Components 790

Findings Audited 0 (0%)

Policy Violations

Auditing Progress

Verification

Documentation:

- **Application Security Verification Standard (ASVS)**
- Mobile Application Security Verification Standard (MASVS)
- Web Security Testing Guide
- Mobile Security Testing Guide

Tools:

- Attack Surface Detector
- **Amass**
- **Code Pulse**
- Offensive Web Testing Framework (OWTF)
- Nettacker
- **DefectDojo**

Frameworks:

- Glue
- Dracon

Application Security Verification Standard (ASVS)

Flagship Project

The OWASP **Application Security Verification Standard (ASVS)** Project provides a basis for testing web application technical security controls and provides developers with a list of requirements for secure development.

- Use as a metric
- Use as guidance
- Use during procurement

Current Version is 4.0.3; 5.0 underway

OWASP

Application Security Verification Standard 4.0.3

Final

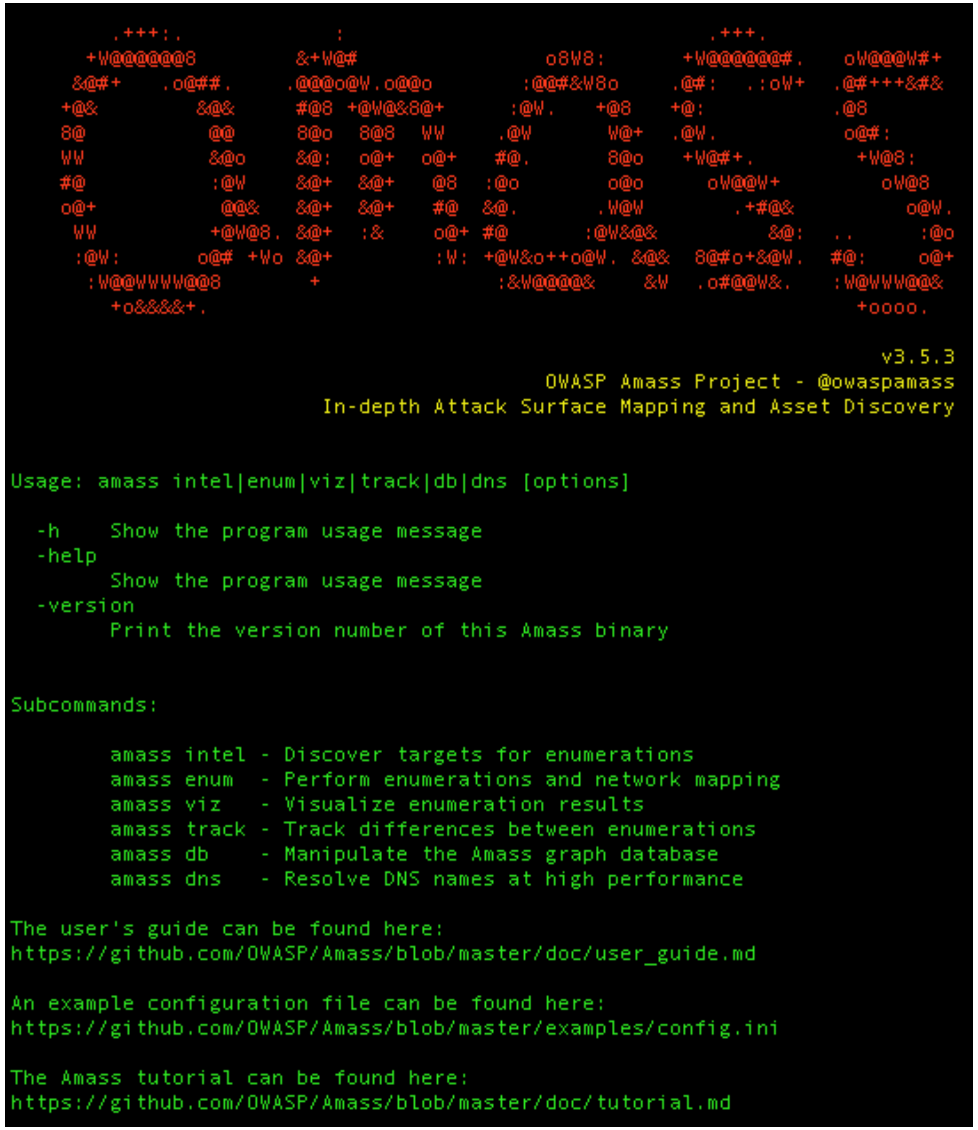
October 2021

Amass

Flagship Project

Our Goal - In-depth DNS Enumeration, Attack Surface Mapping and External Asset Discovery!

- Mapping of network attack surfaces
- External asset discovery
- Open-source information gathering and active reconnaissance techniques

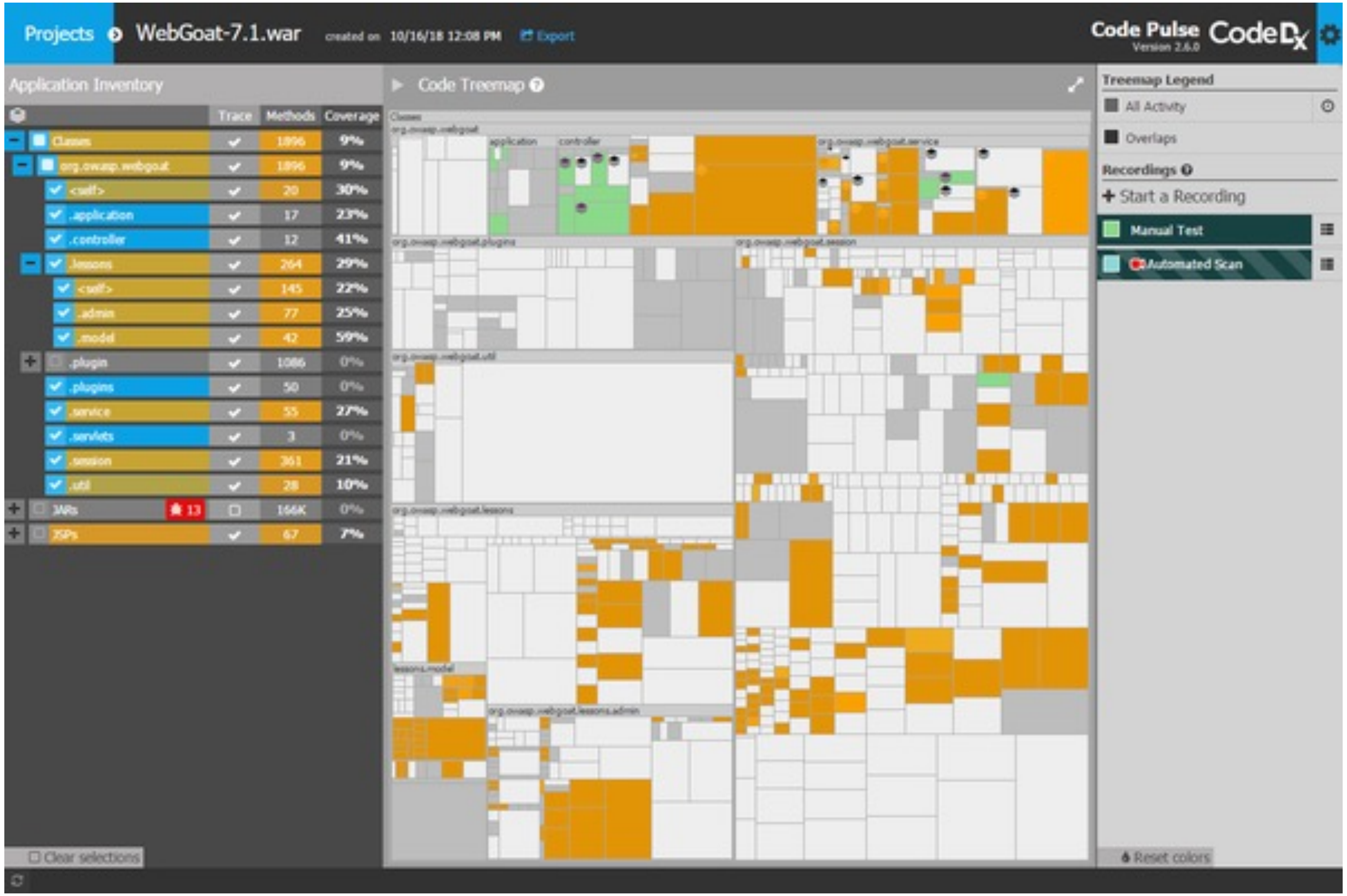


```
        .+++:.            :                             .+++.
      +W@@@@@@8        &+W@#               o8W8:      +W@@@@@@#.   oW@@@W#+
     &@#+   .o@##.    .@@@o@W.o@@o       :@@#&W8o    .@#:  .:oW+  .@#+++&#&
    +@&        &@&     #@8 +@W@&8@+     :@W.   +@8   +@:          .@8
    8@          @@     8@o  8@8  WW    .@W      W@+  .@W.          o@#:
    WW          &@o    &@:  o@+  o@+   #@.      8@o   +W@#+.        +W@8:
    #@          :@W    &@+  &@+   @8  :@o       o@o     oW@@W+        oW@8
    o@+          @@&   &@+  &@+   #@  &@.      .W@W       .+#@&         o@W.
     WW         +@W@8. &@+  :&    o@+ #@      :@W&@&         &@:  ..     :@o
     :@W:      o@# +Wo &@+        :W: +@W&o++o@W. &@&  8@#o+&@W.  #@:    o@+
      :W@@WWWW@@8       +              :&W@@@@&    &W  .o#@@W&.   :W@WWW@@&
        +o&&&&+.                                                    +oooo.

                                                                      v3.5.3
                                           OWASP Amass Project - @owaspamass
                         In-depth Attack Surface Mapping and Asset Discovery


Usage: amass intel|enum|viz|track|db|dns [options]

  -h    Show the program usage message
  -help
        Show the program usage message
  -version
        Print the version number of this Amass binary


Subcommands:

        amass intel - Discover targets for enumerations
        amass enum  - Perform enumerations and network mapping
        amass viz   - Visualize enumeration results
        amass track - Track differences between enumerations
        amass db    - Manipulate the Amass graph database
        amass dns   - Resolve DNS names at high performance

The user's guide can be found here:
https://github.com/OWASP/Amass/blob/master/doc/user_guide.md

An example configuration file can be found here:
https://github.com/OWASP/Amass/blob/master/examples/config.ini

The Amass tutorial can be found here:
https://github.com/OWASP/Amass/blob/master/doc/tutorial.md
```

Code Pulse

Lab Project

- Provides insight into the real-time code coverage of black box testing activities
- Cross-platform desktop application
- Agent-based runtime monitoring



WebGoat-7.1.war created on 10/16/18 12:08 PM

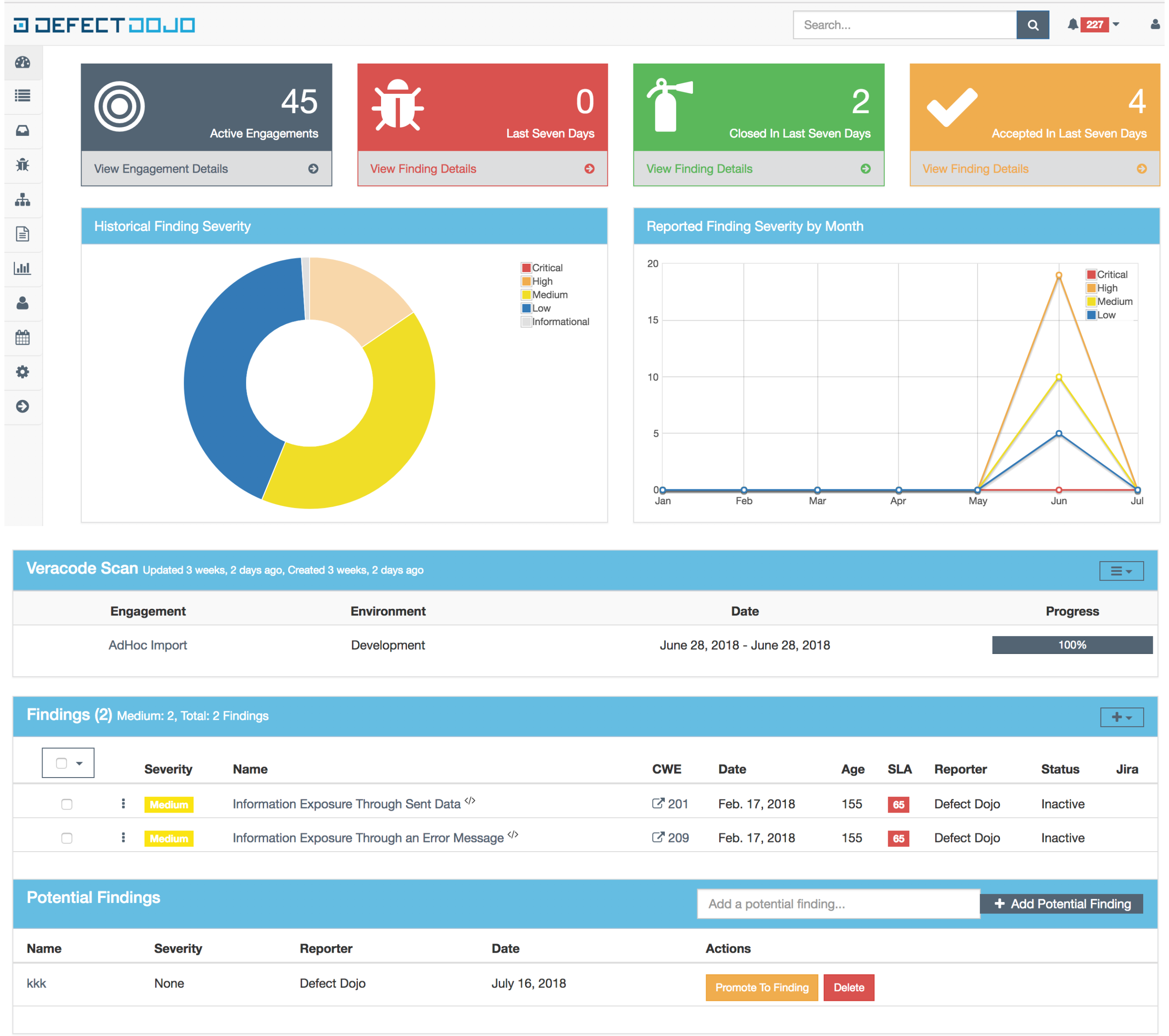
Application Inventory

	Trace	Methods	Coverage
Classes	✓	1896	9%
org.owasp.webgoat	✓	1896	9%
<self>	✓	20	30%
.application	✓	17	23%
.controller	✓	12	41%
.lessons	✓	264	29%
<self>	✓	145	22%
.admin	✓	77	25%
.model	✓	42	59%
.plugin	✓	1086	0%
.plugins	✓	50	0%
.service	✓	55	27%
.servlets	✓	3	0%
.session	✓	361	21%
.util	✓	28	10%
JARs 13	□	166K	0%
JSPs	✓	67	7%

DefectDojo

Flagship Project

- Open-source vulnerability management tool
- Streamlines the testing process
  - Templating
  - Report generation
  - Metrics



Veracode Scan Updated 3 weeks, 2 days ago, Created 3 weeks, 2 days ago

Engagement	Environment	Date	Progress
AdHoc Import	Development	June 28, 2018 - June 28, 2018	100%

Findings (2) Medium: 2, Total: 2 Findings

□		Severity	Name	CWE	Date	Age	SLA	Reporter	Status	Jira
□	⋮	Medium	Information Exposure Through Sent Data	201	Feb. 17, 2018	155	65	Defect Dojo	Inactive	
□	⋮	Medium	Information Exposure Through an Error Message	209	Feb. 17, 2018	155	65	Defect Dojo	Inactive	

Potential Findings

Add a potential finding...

+ Add Potential Finding

Name	Severity	Reporter	Date	Actions
kkk	None	Defect Dojo	July 16, 2018	Promote To Finding Delete

Some Closing Thoughts

- Don’t oversell – “free” tools aren’t *really* free
  - Be honest and realistic about total cost of ownership: instance charges, admin hours, etc.
- Use the right tool for your use case
  - When the OWASP tool isn’t the right one, it can still provide a cost-effective proof-of-concept
- Don’t be too proud to ask for help
  - OWASP community
  - Local AppSec community
  - Internal Security Team (if you have one)
  - External consultants and trainers

Resources

- OWASP Website: https://owasp.org
- OWASP Integration Standards Project: https://owasp.org/www-project-integration-standards/
- OWASP SAMM: https://owaspsamm.org/
- Security Champions Playbook: https://github.com/c0rdis/security-champions-playbook
- Join the OWASP Slack: https://owasp.org/slack/invite

Questions?

Connect / Reach out

- Email:
  - Day job: *john.dileo@gallagher.com*
  - “Other job”: *john.dileo@owasp.org*
- Twitter (rarely): *@gr4ybeard*
- LinkedIn: *john-dileo*
- OWASP Slack *https://owasp.org/slack/invite*

OWASP 2024
APPSEC DAYS
SINGAPORE

THANK YOU!