OWASP®

OWASP Phoenix Chapter - July 2024 Meetup

https://www.meetup.com/owasp-phoenix-chapter

https://owasp.org/www-chapter-phoenix

Thank You!

HeatSync Labs

https://www.heatsynclabs.org

- ❖ A hackerspace where you can make things.
- ❖ A grassroots co-op of volunteers— No staff.
- ❖ Open for everyone during public hours and events.

- ✓ Please be courteous of project work.
- ✓ Bathrooms are in back.
- ✓ Snacks and drinks available along East wall. Donation requested (box on fridge).

Agenda

Full Coverage Code Scanning Like a Boss

20 Minutes

Open Discussion / Networking

Time Remainder

Who Am I

Maria Brown

Application Security Engineer

Grumpy Cat BFF

B.S.E. Computer Systems Engineering

ASU Ira A. Fulton Schools of Engineering
Arizona State University

CISSP® Certified Information Systems Security Professional

C|EH Certified Ethical Hacker

Full Coverage Code Scanning Like a Boss

Image Credit:
Carefree Cat Tombili,
https://www.al-monitor.com/originals/2016/10/cat-meme-istanbul-statue-tombili-turkey.html

What is Full Coverage Code Scanning?

- ***Full coverage code scanning*** *is using* ***all types*** *of* ***vulnerability scanners*** *that match the* ***potential types of code vulnerabilities****.*

Vulnerability Scanner Types

01 **SAST** – Static Application Security Testing

02 **DAST** – Dynamic Application Security Testing

03 **IAST** – Interactive Application Security Testing

04 **SCA** – Software Composition Analysis, aka Dependency Scanning

05 **SSL** – Secure Socket Layer Certificate Scanning

06 **IaC** – Infrastructure as Code Scanning

07 **Secret** – Secrets in Code Repositories

08 **Container** – Container Image Scanning, aka Docker

SAST - Static Application Security Testing

✓ Scanning source code without executing code.

Purpose

- Find **common code vulnerabilities** like buffer overflow and SQL injection.

Scan Target

- **Source code files** (i.e., .py for Python, .cpp for C++, etc.

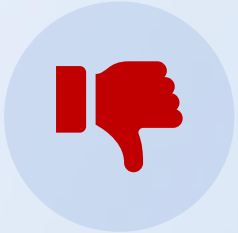
Key Details

- Scanner must **match the programming language**.

SAST Pro’s and Con’s

Pro’s

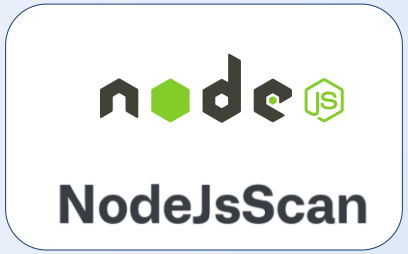
- Checks the code as you work on your build.
- Wide variety of community scanners.



Con’s

- False positives and negatives. Time wasted.
- Need a scanners to match all languages in project

SAST Community Tools



DAST - Dynamic Application Security Testing

✓ Simulating automated attacks on an application, mimicking a malicious attacker.

Purpose

- Find **common code vulnerabilities** like cross-site scripting (XSS) and SQL injections.

Scan Target

- Running application, usually **web app, web service,** or **mobile app.**

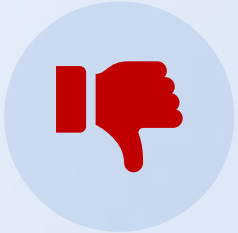
Key Details

- Primarily for web and mobile applications.

DAST Pro’s and Con’s

Pro’s

- Finds both compile-time and runtime vulnerabilities.
- Imitates malicious users.
- Can detect server config and authentication issues.
- Language independent.



Con’s

- False positives and negatives. Time wasted.
- Needs a running application.
- Can run slow. Use DAST only on test systems.

DAST Community Tools

IAST - Interactive Application Security Testing

✓ Testing interacts with a running application and observes it from the inside in real time.

Purpose

- Find **common code vulnerabilities** like buffer overflow and SQL injection.

Scan Target

- **Running application** instrumented using agent installed in web application server or mobile application code.

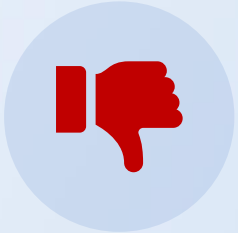
Key Details

- Only for web applications, web services, or mobile apps.
- Must match supported technologies.

IAST Pro’s and Con’s

Pro’s

- Highly accurate.
- Includes vulnerable library scan (SCA).
- Results in central portal.

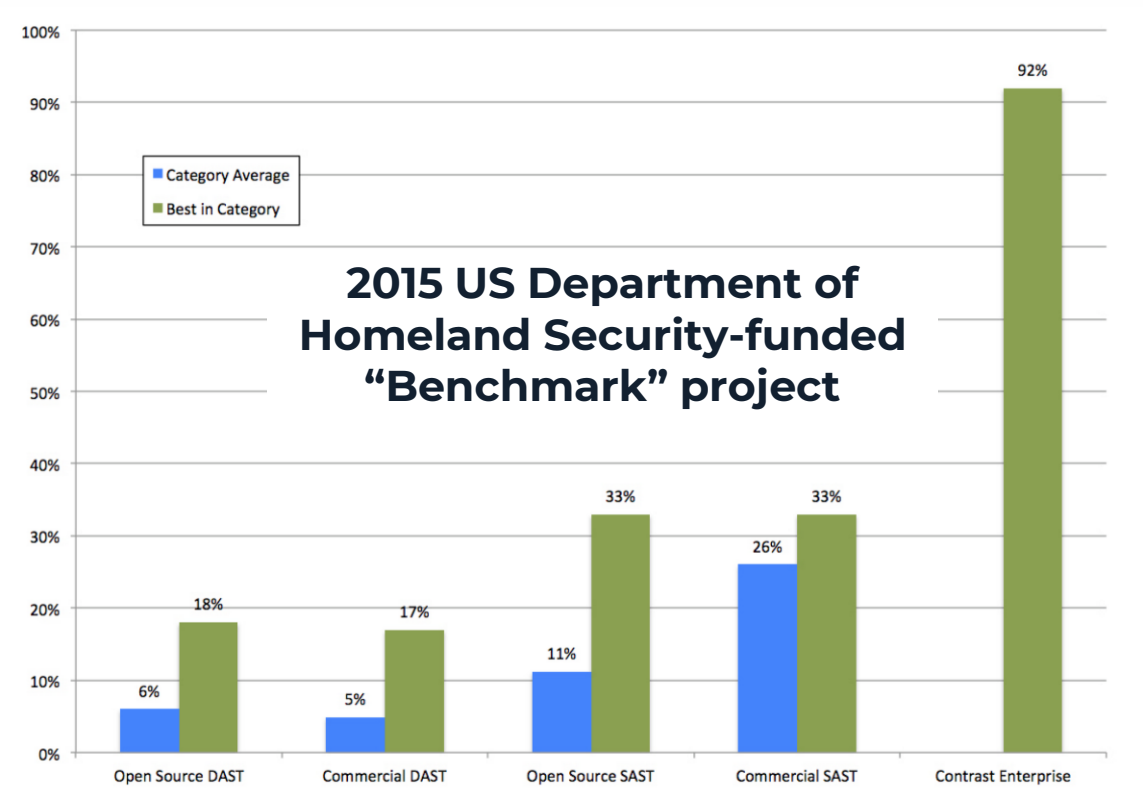


Con’s

- Requires agent installation and version updates.
- Needs running application.
- Needs connectivity to central portal.

IAST Community Tools

SAST vs DAST vs IAST Accuracy



- Using OWASP Benchmark Project designed to evaluate the accuracy, coverage, and speed of automated software vulnerability detection tools.
- Accuracy scores for products across all 11 Benchmark Project vulnerability categories.

https://www.contrastsecurity.com/security-influencers/cyber-security-benchmark-highlights-legacy-product-failures

SCA – Software Composition Analysis aka Vulnerable Dependencies or 3rd Party Libraries

✓ Scans 3rd party & open-source components for vulnerabilities

Purpose

- Find **vulnerabilities in 3rd party open source libraries and dependencies**.

Scan Target

- **Package manager files** associated with library package manager used.

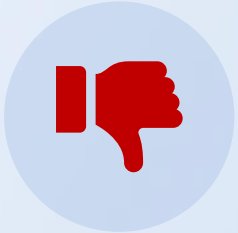
Key Details

- Critical to match tool to package manager used, not just programming language.
- Dependencies have dependencies.

SCA Scanning Pro’s and Con’s

Pro’s

- Catches key vulnerabilities in library dependencies.



Con’s

- Sometimes vulnerability is not reachable.
- Tools need connectivity to vulnerability databases.

SCA High Profile Impact Events

Sept 2017 – 147 Million People

- Hackers exploit an **unpatched version of Apache Struts software** running on a server in their DMZ, facing the internet.
- Security patch had been available since March 7, 2017.

Nov 2021

- Discovered “10 out of 10” critical vulnerability in Apache log4j library since 2013.
- In 2021, estimated that over 38,000 unique applications across 4,000 organizations were running vulnerable Log4j libraries.

SCA Scanning Community Tools

SSL – Secure Socket Layer Certificate Scanner

- ✓ Scans SSL certificates and TLS (transport layer security) for validity, credibility, and configuration

Purpose

- Find **SSL and TLS configuration issues** and vulnerabilities.

Scan Target

- Public **web address.**

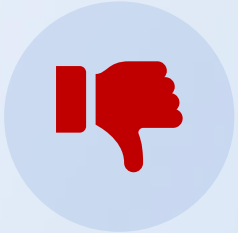
Key Details

- Web address must be **accessible** to scanner.

SSL Scanning Pro's and Con's

Pro's

- Catches vulnerabilities like POODLE, Heartbleed, and more.
- Easy as entering accessible web address into website.



Con's

- Not always clear how website uses findings.
- Some sites publish findings on website, need to "opt out" of sharing.
- Scanning production sites can impact performance.

SSL Scanning Sites

IaC – Infrastructure as Code Scanning

✓ Analyzing the scripts that automatically provision and configure infrastructure.

Purpose

- Find **vulnerabilities and misconfigurations** in code that provisions cloud environments and services.

Scan Target

- **IaC code files** (i.e., .tf for Terraform, .cft for CloudFormation, etc.)

Key Details

- Scanner must **scan the IaC platform**.

IaC Scanning Pro's and Con's

Pro's

- Catch vulnerabilities and misconfigurations early, before instantiating insecure cloud environments and services.

Con's

- Developer misconception that all security concerns are addressed with scanning.

IaC Scanning Community Tools

Secret Scanning

✓ Scanning code repositories and other data sources for sensitive information.

Purpose

- Locate **secret** and **sensitive data** such as passwords, access keys, etc. in before committing files.

Scan Target

- Source **code repository files.**

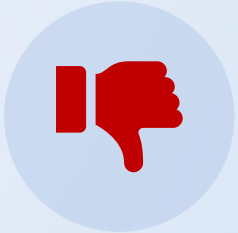
Key Details

- Scanning should be done prior to commiting files and block commits if secrets found.

Secret Scanning Pro’s and Con’s

Pro’s

- Prevent secrets from being committed to source code history.



Con’s

- Potential for false positives and negatives.

AppSec & Supply Chain Security | February 23, 2023

Secrets Exposed: Why modern development, open source repos spill secrets en masse

The Circle CI breach and other recent hacks expose why the secrets problem is so prolific. Here's what you need to know about the state of secrets security.

4. Secrets can disappear in as little as 20 seconds

The same features that make platforms like GitHub so powerful for accessing, analyzing and sharing code also make them easy for both good actors and bad to spot security and privacy lapses. By one estimate, the median time to discovery for a key leaked to GitHub is 20 seconds, with detection times ranging from half a second to over four minutes. In other words: By the time most development teams realize they have accidentally exposed secrets, those secrets have almost certainly been detected by a malicious actor.

By the time most development teams realize they have accidentally exposed secrets, those secrets have almost certainly been detected by a malicious actor.

https://www.reversinglabs.com/blog/secrets-exposed-modern-development-open-source-repositories-expose-secrets-en-masse

Secret Scanning Community Tools

Yelp
detect-secrets

Container – Image Security Scanning

- ✓ Scans application container layers for vulnerabilities.

Purpose

- Find **common code vulnerabilities,outdated code, secrets, misconfigurations, and malware** in container layers.

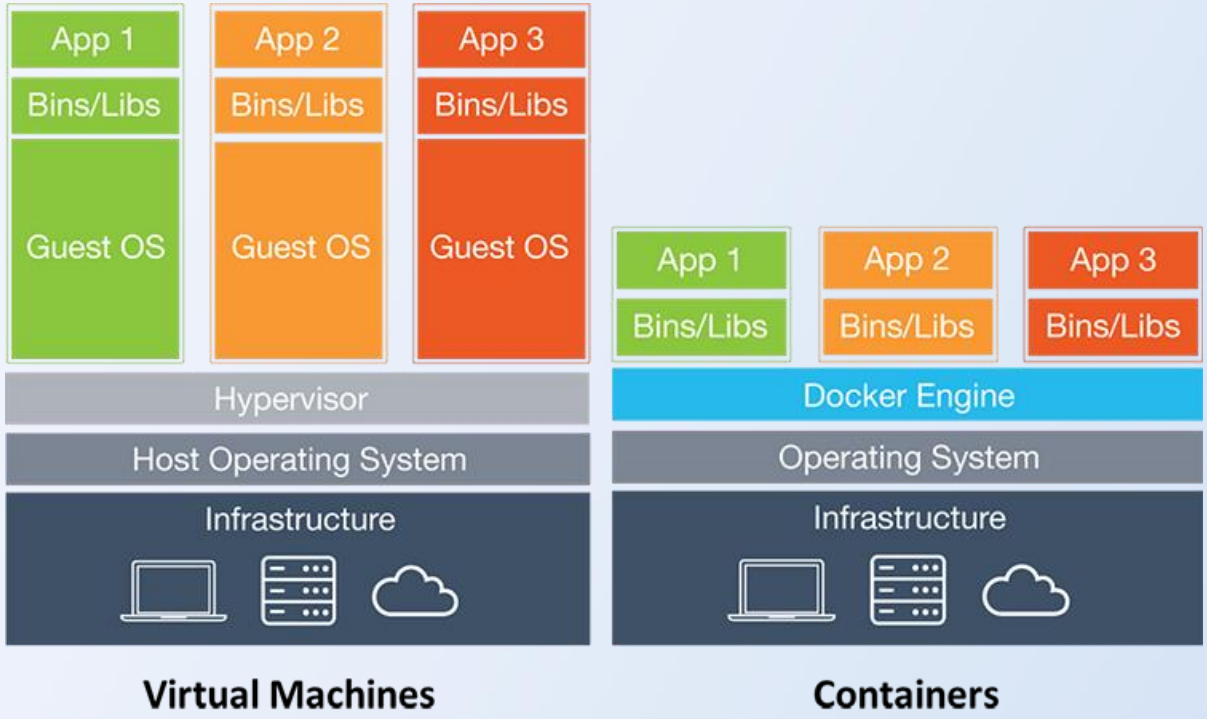
Scan Target

- **Container image** (i.e. docker pull busybox)

Key Details

- Need container runtime to pull image for scanning.

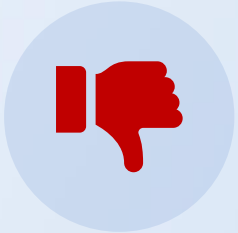
Containers vs. Virtual Machines



Container Scanning Pro's and Con's

Pro's

- Single scanner can catch multiple types of vulnerabilities found in container layers (i.e., code vulnerabilities, outdated code, open-source vulnerabilities, malware, secrets, privilege issues, etc.)



Con's

- Need to retrieve image from repository for scanning (i.e., "pull").

Container Scanning Community Tools

Vulnerability Scanner Types Recap

01 **SAST** – Static Application Security Testing

02 **DAST** – Dynamic Application Security Testing

03 **IAST** – Interactive Application Security Testing

04 **SCA** – Software Composition Analysis, aka Dependency Scanning

05 **SSL** – Secure Socket Layer Certificate Scanning

06 **IaC** – Infrastructure as Code Scanning

07 **Secret** – Secrets in Code Repositories

08 **Container** – Container Image Scanning, aka Docker

Thank You!

Have fun vulnerability scanning LIKE A BOSS!

CREDITS: This presentation template was created by **Slidesgo**, and includes icons by **Flaticon** and infographics & images by **Freepik**

Noun Project Icons Credit

Maria Brown
maria.brown@owasp.org
https://www.linkedin.com/in/mariabrown

Open Discussion and Networking

LinkedIn Profile Sharing with Barcode