iteratec

OWASP

Much More Than Just OWASP Top 10

Sven Strittmatter

iteratec

Sven Strittmatter

Lead Security Expert at iteratec
Chapter Stuttgart Lead at OWASP

- 🤓 Computer nerd since 8.
- 🤑 Computer stuff for money since 20+ years.
- 😭 Got hacked in one of my first jobs.
- 🧐 Since preaching security w/o being asked.
- 😉 Now I’m a security consultant.

My Company

iteratec

iteratec GmbH

- No, we're not the company which makes sound cards 😩
  - That's Terratec 😉
- We do individual software development sinc 25+ years.
  - Java, JavaScript, TypeScript, Go, Python etc.
  - Hire us when failure is not an option!
- Since 10+ years we do security.
  - Because that's part of it!
  - Consulting, Training, Pentesting.
- 500+ Emplyees, 7 Offices.
- TISAX & ISO27k certified.
- It really is my company 😀
  - 49 % is owned by iteratec nurdemteam eG.
  - Remaining 51 % coming soon.
- We use a lot of OWASP stuff 😬
  - BTW: My boss urged me to become OWASP member some years ago 😂

iteratec

No AI Showing Up 😬

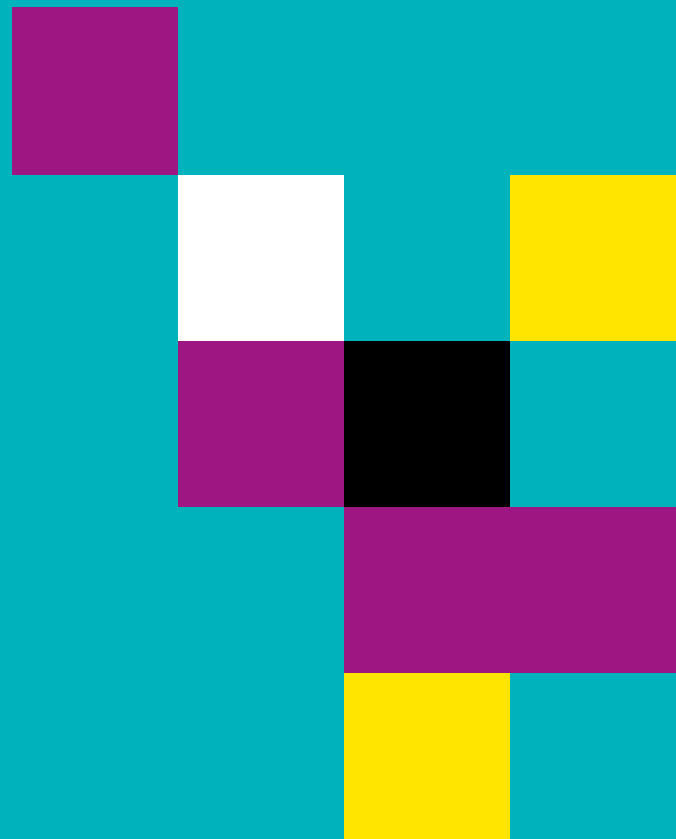
I don’t bother you w/ AI generated images,

but with smileys and GIFs 😂

iteratec

What Is OWASP?

Obviously more than the Top 10 😂



What Is OWASP?

Our Mission

The ***O**pen ~~Web~~**W**orldwide **A**pplication **S**ecurity **P**roject*
is a nonprofit foundation that works
to improve the security of software.

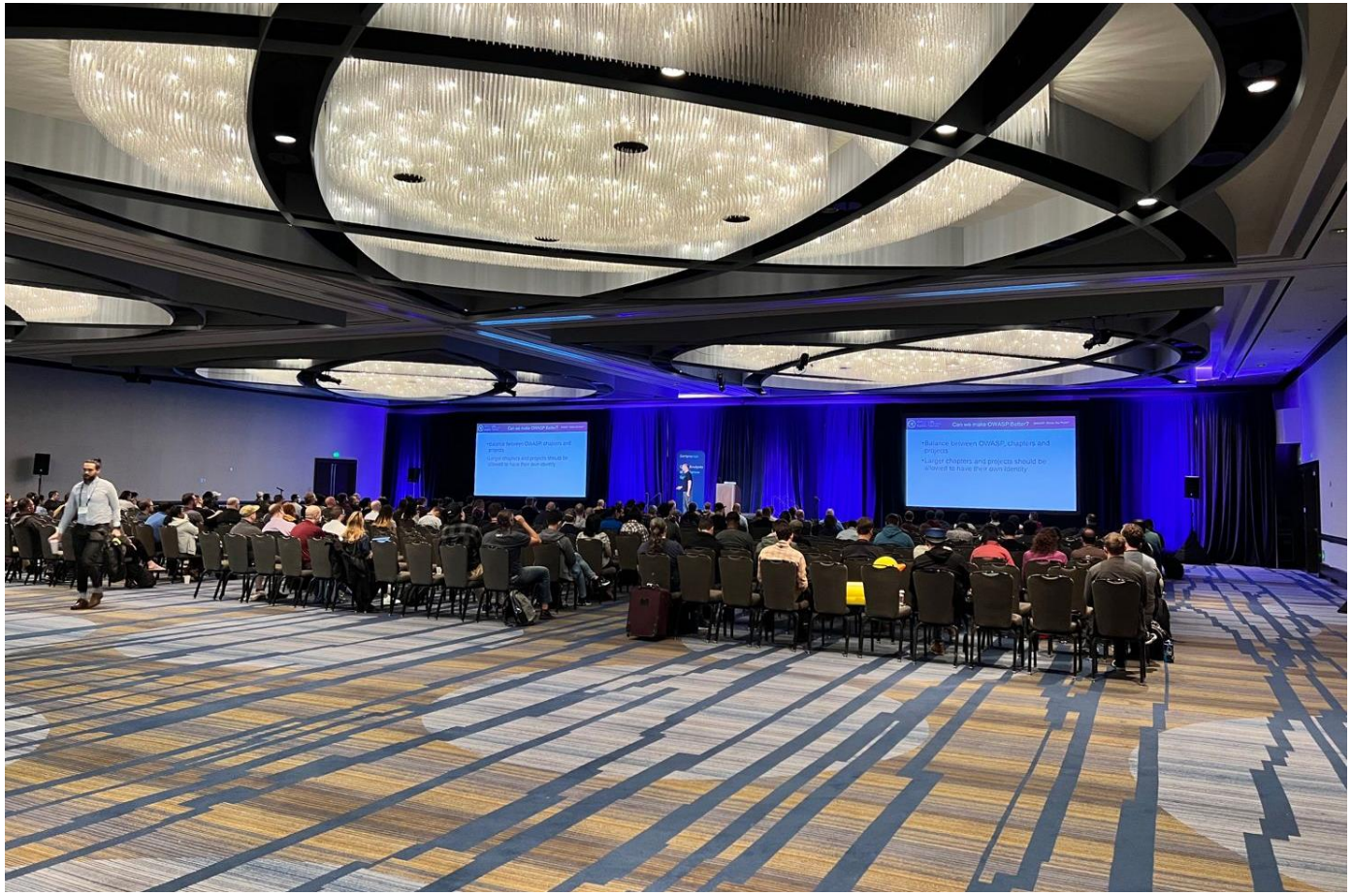
Our offer includes:

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

What Is OWASP?

iteratec

Our Community



- *OWASP* is a worldwide **free** and **open community** focused on improving the security of application software.
- Our goal is to make application security **visible**, so that people and organizations can make **informed decisions** about application security **risks**.

Picture from Global AppSec 2022 by Noah Yisa via LinkedIn.

What Is OWASP?

iteratec

World Wide Organized In Local Chapters

OWASP® Foundation

Members	Groups	Countries
143,110	242	73

- German Chapter:
  - Lead: Tobias Glemser
  - German OWASP Day
  - 2025 maybe Düsseldorf 🤔
- Stuttgart Chapter:
  - Lead: Johannes Merkert & me
  - Stammtisch w/ 🍺 & 🥖
  - Organized via Meetup.
- Lots of other chapters w/ Stammtische/Meetups
  - https://owasp.org/chapters/
- Get in touch
  - Mailing list,
  - Slack, or
  - Just talk to me 🤗

What Is OWASP?

It's All Free

- Everyone is free to participate. 🤗
  - **No membership required**!
- All materials are available under **free** & **open** licenses.
- All *OWASP* events are free to attend for **anyone**.
  - Except conferences, we charge net cost prices. 😀
- No need for any entry qualification.
- All creatures are welcome. 🤗
  - Yes, I know, it's from the CCC. 😬

Picture from:
https://owasp.glueup.com/

What Is OWASP?

iteratec

The *OWASP* Foundation

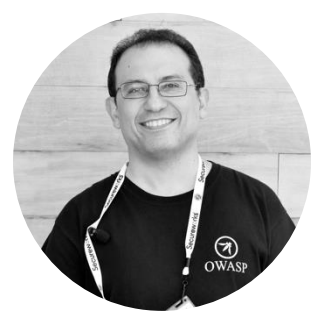
- We are a global **not-for-profit charitable** organization.
- **Vendor-neutral** community.
- **Collective wisdom** of the best minds in application security worldwide.
- Provide **free** tools, guidance, and documentation.
- Relying on **donations**.
  - Corporations can become members, too.
- Board of directors **elected by community**.
- Board meetings **open to the public**.
  - https://owasp.org/www-board/
- Sadly, no women elected to board.

Current Board 2025:

Ricardo Griffith

Steve Springett

Harold Blankenship



Sam Stepanyan

Contributing Members

iteratec

These Corpotate Members Support *OWASP* at $5.000 Level Annualy (Silver)

Contributing Members

iteratec

Diamond Members

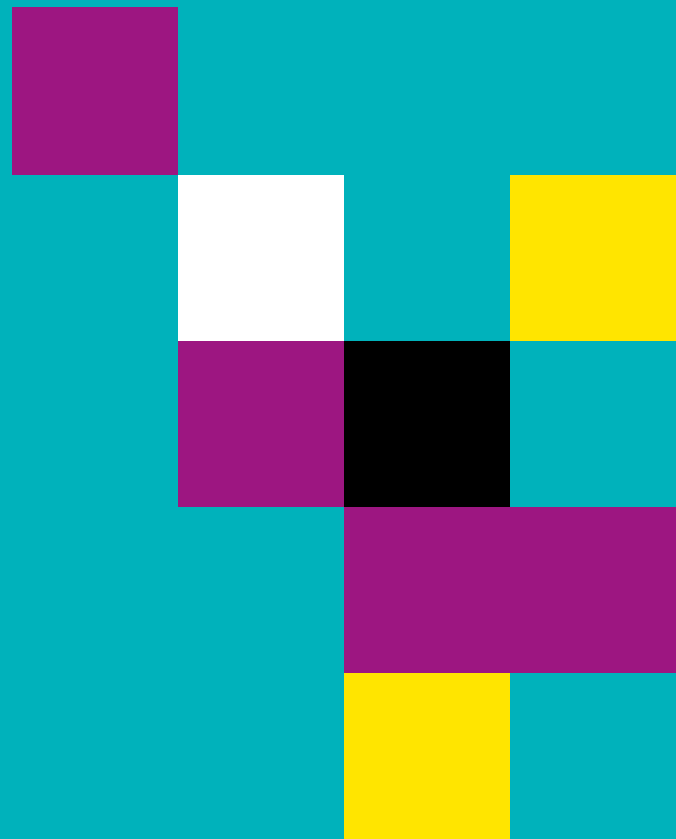
Platinum Members

Become a member and support OWASP: https://owasp.org/supporters/

iteratec

OWASP Projects

There is way more than OWASP Top 10



OWASP Projects

iteratec

You got that wrong

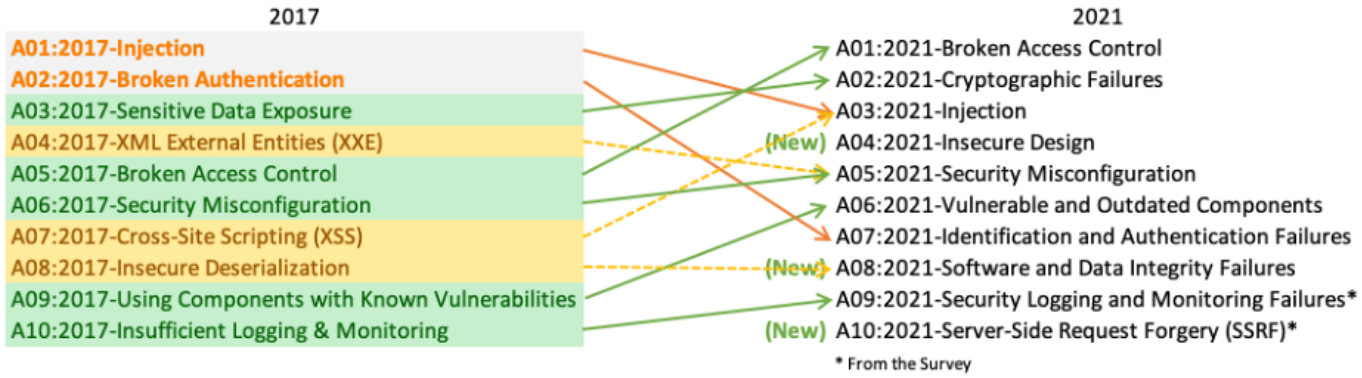
- “We use *OWASP*, we’re secure!”
- “We do *OWASP* penetration testing!”
- “We cover all risks of *OWASP Top 10*, we’re secure!”
- A requirement for a real invitation to tender:
  “You must be *OWASP Top 10* certifierd.” 😂
- Pro-Tipp: If someone wants to sell you an *OWASP* certificate,
  then go ahead and find someone who knows!

BTW:
10 years ago “cyber” was an indicator for people who have no clue. 😳

OWASP Projects

iteratec

Top 10 Web Application Security Risks aka. OWASP Top 10



Use it for

- security awareness,
- security training,
- and push left security.

Don't use it for anything else!

- Pentesting → OWASP Web Security Testing Guide
- Compliance → OWASP ASVS, OWASP SAMM, OWASP DSOMM

- An opinionated list of most comon failures seen in (web) apps
  - Most of them you can also find in IoT, desktop apps, etc.
  - **Largely applicable to non-web apps**.
- Data from static code analysis of 12 manufacturers/service providers.
- The ranking is done by open survey of "experts".
- **There is no science behind it!**
- https://owasp.org/www-project-top-ten/

iteratec

Some More Projects

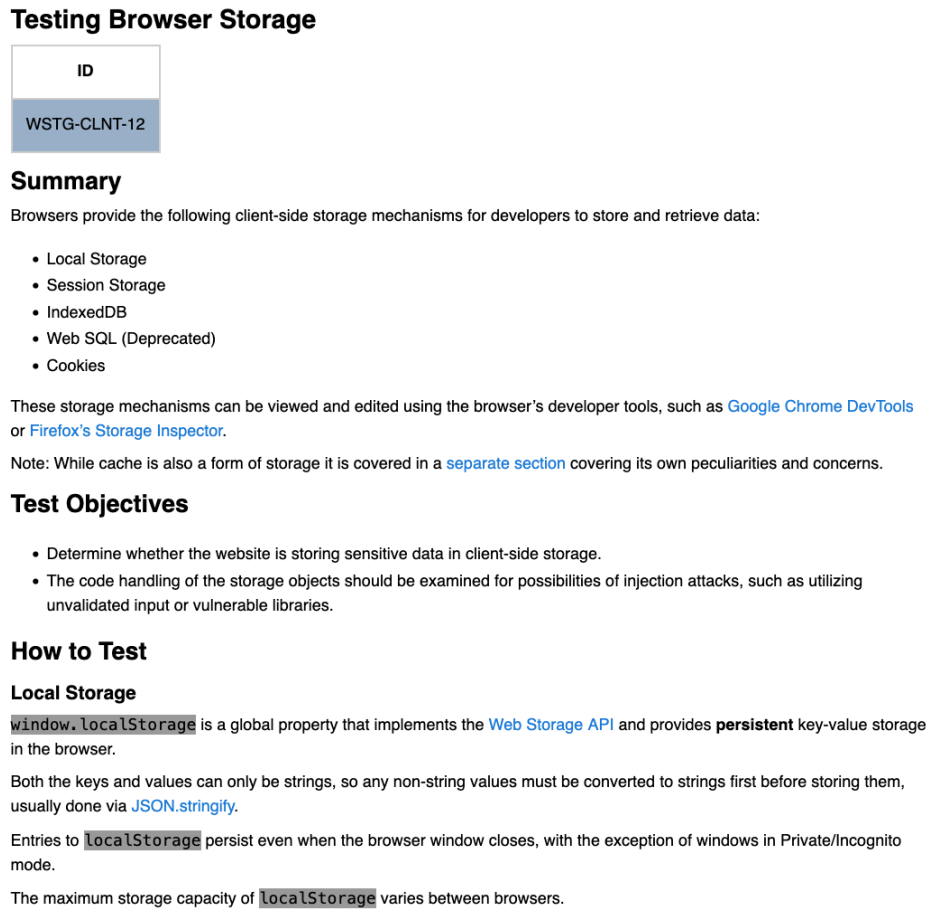
Just a Short, Opinionated Excerpt

OWASP Projects

iteratec

OWASP Web Security Testing Guide (WSTG)

- Comprehensive guide to testing the security of web applications and web services.
- Learn to hack yourself.
- Use as test plan for penetration tests.
- I’m not an OFFSEC guy. 😬
- https://owasp.org/www-project-web-security-testing-guide/



Testing Browser Storage

ID
WSTG-CLNT-12

Summary

Browsers provide the following client-side storage mechanisms for developers to store and retrieve data:

- Local Storage
- Session Storage
- IndexedDB
- Web SQL (Deprecated)
- Cookies

These storage mechanisms can be viewed and edited using the browser’s developer tools, such as Google Chrome DevTools or Firefox’s Storage Inspector.

Note: While cache is also a form of storage it is covered in a separate section covering its own peculiarities and concerns.

Test Objectives

- Determine whether the website is storing sensitive data in client-side storage.
- The code handling of the storage objects should be examined for possibilities of injection attacks, such as utilizing unvalidated input or vulnerable libraries.

How to Test

Local Storage

`window.localStorage` is a global property that implements the Web Storage API and provides **persistent** key-value storage in the browser.

Both the keys and values can only be strings, so any non-string values must be converted to strings first before storing them, usually done via JSON.stringify.

Entries to `localStorage` persist even when the browser window closes, with the exception of windows in Private/Incognito mode.

The maximum storage capacity of `localStorage` varies between browsers.

OWASP Projects

iteratec

OWASP Application Security Verification Standard (ASVS)

- Framework of security requirements.
- Focus on security controls required when designing.
- Comprehensive list of security requirements
  - divided by protection level and
  - grouped by topics (e.g. authentication, session management, input validation etc.).
- Also useful for
  - governance or
  - checklist.
- https://owasp.org/www-project-application-security-verification-standard/

V5.1 Input Validation

Properly implemented input validation controls, using positive allow lists and strong data typing, can eliminate more than 90% of all injection attacks. Length and range checks can reduce this further. Building in secure input validation is required during application architecture, design sprints, coding, and unit and integration testing. Although many of these items cannot be found in penetration tests, the results of not implementing them are usually found in V5.3 - Output encoding and Injection Prevention Requirements. Developers and secure code reviewers are recommended to treat this section as if L1 is required for all items to prevent injections.

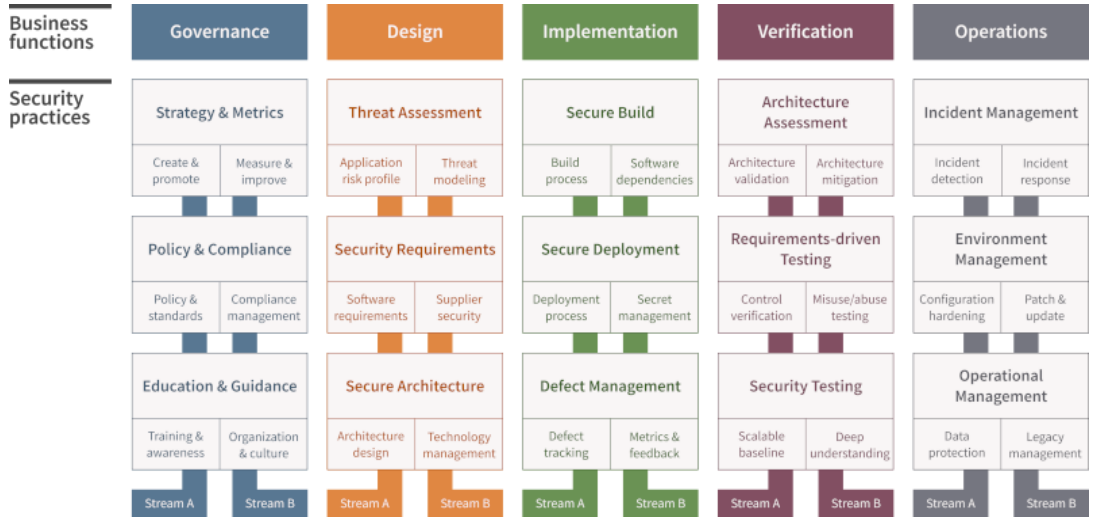
#	Description	L1	L2	L3	CWE
5.1.1	Verify that the application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, or environment variables).	✓	✓	✓	235
5.1.2	Verify that frameworks protect against mass parameter assignment attacks, or that the application has countermeasures to protect against unsafe parameter assignment, such as marking fields private or similar. (C5)	✓	✓	✓	915
5.1.3	Verify that all input (HTML form fields, REST requests, URL parameters, HTTP headers, cookies, batch files, RSS feeds, etc) is validated using positive validation (allow lists). (C5)	✓	✓	✓	20
5.1.4	Verify that structured data is strongly typed and validated against a defined schema including allowed characters, length and pattern (e.g. credit card numbers, e-mail addresses, telephone numbers, or validating that two related fields are reasonable, such as checking that suburb and zip/postcode match). (C5)	✓	✓	✓	20
5.1.5	Verify that URL redirects and forwards only allow destinations which appear on an allow list, or show a warning when redirecting to potentially untrusted content.	✓	✓	✓	601

OWASP Projects

iteratec

OWASP Software Assurance Maturity Model (SAMM)

- Effective and measurable way for you to analyse and improve your secure development lifecycle.
- Very mature.
- Push security left.
- But…
  - may need organization change
  - and nothing you can do in a few weeks.
- https://owasp.org/www-project-samm/

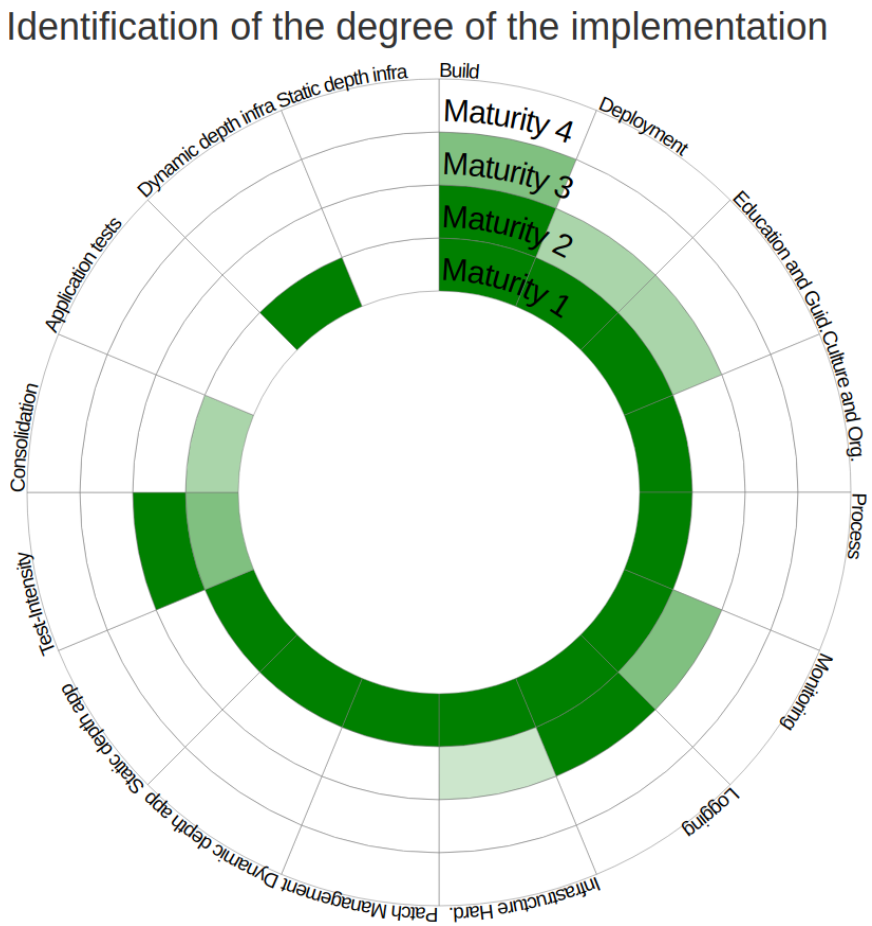


OWASP Projects

iteratec

OWASP DevSecOps Maturity Model (DSOMM)

- Maturity model for DevSecOps.
- Very useful to see where you are.
- More lightweight than *OWASP SAMM*.
- Push security left.
- Can be done in a team.
- Mappings to
  - *OWASP SAMM*
  - ISO27001
- https://owasp.org/www-project-devsecops-maturity-model/



OWASP Projects

iteratec

OWASP Developer Guide

- Introduction to security concepts.
- Cross-reference to tools & documents from *OWASP*.
- Must read for everyone doing IT.
- Successor of the archived *OWASP Secure Coding Practices-Quick Reference Guide*.
- I wish I had known about this ten years ago. 😂
- https://owasp.org/www-project-developer-guide/

OWASP Projects

iteratec

OWASP Cheat Sheet Series

- No time to read the *OWASP Developer Guide* or role out *OWASP SAMM*?
- Your bossy boss demands for features?
- Just want to implement a secure…
  - … file upload
  - … password forgotten
  - … xyz
- Just look for the right cheat sheet and follow it. 👍
- https://owasp.org/www-project-cheat-sheets/

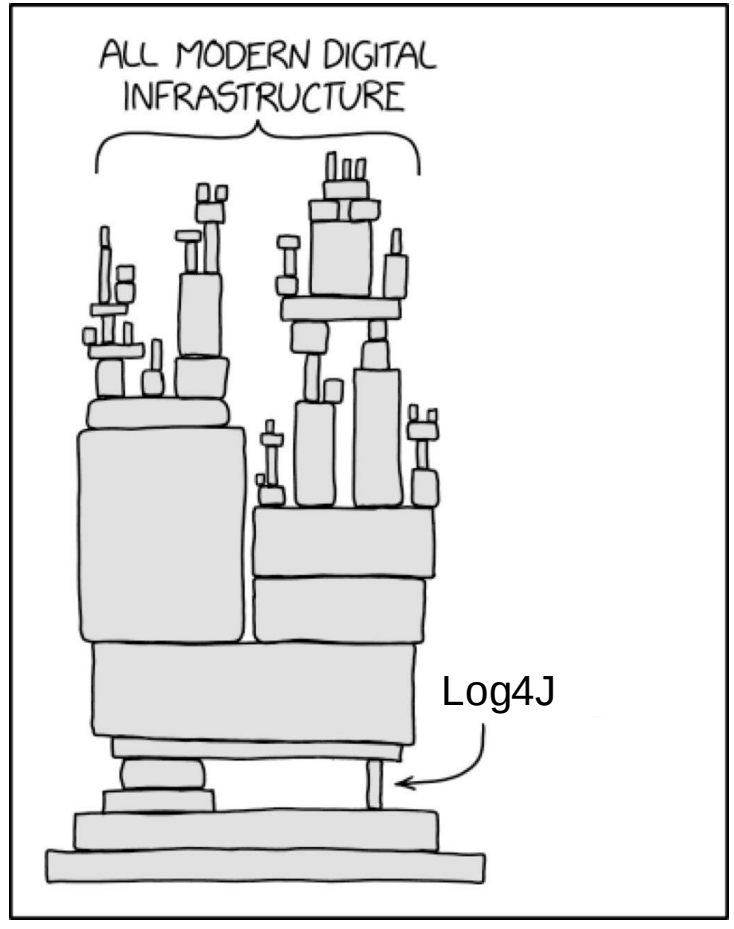
OWASP Projects

iteratec

OWASP CycloneDX (ECMA-424)

- Software bill of materials (SBOM) standard.
- Why you need SBOMs?
  - You don’t want to syft through all your software, when next Log4J come around (right before x-mas).
  - You may have a chance to check what quadrillion dependencies the JS hackers added last week 😂
- https://owasp.org/www-project-cyclonedx/

BTW: If you use free software in your company and you don’t pay for that, then you should read this Wikipedia article about *gratis versus libre* and tell your boss: https://en.wikipedia.org/wiki/Gratis_versus_libre



OWASP Projects

iteratec

OWASP Dependency-Check

- Software Composition Analysis (SCA) tool.
- Checks project dependencies for known vulns.
- Easy to use & some integrations:
  CLI, Ant (yes, still exists), Maven, Gradle, Jenkins, Circle CI, SonarQube, …
- Works for Java/JavaScript (done that) and others.
  - C/C++ → you're screwed 😂
- Output quite difficult to understand.
  - Personal advise: Just simply update everything regularly (at least weekly, use Renovate or such). 😉
- https://owasp.org/www-project-dependency-check/

OWASP Projects

iteratec

OWASP Dependency-Track

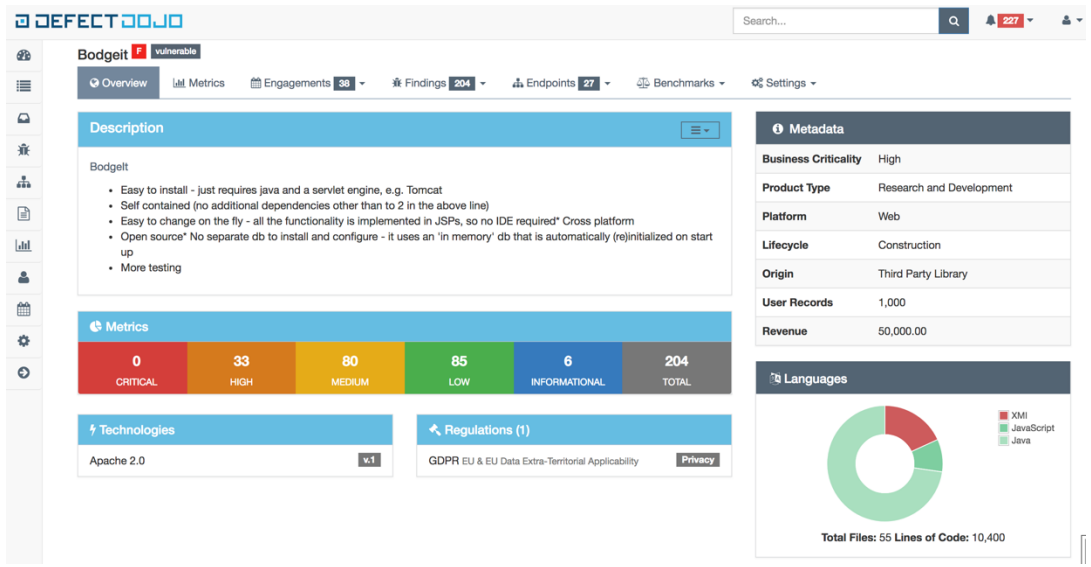
- Consumes SBOMs.
- Nice Web UI for all your dependencies (in your organization).
- Log4J? → click, click, click and you know your usual suspects.
- https://owasp.org/www-project-dependency-track/

OWASP Projects

iteratec

OWASP Defectdojo

- Vuln management tool.
- Use it to track-down the process of fixing vulns.
- You can add vulns
  - manually, e.g. found by penetration test.
  - Automatically, e.g. found by tools like
    - *OWASP Dependency-Track*,
    - *OWASP secureCodeBox*,
    - whatever (has a rich REST API).
- https://owasp.org/www-project-defectdojo/



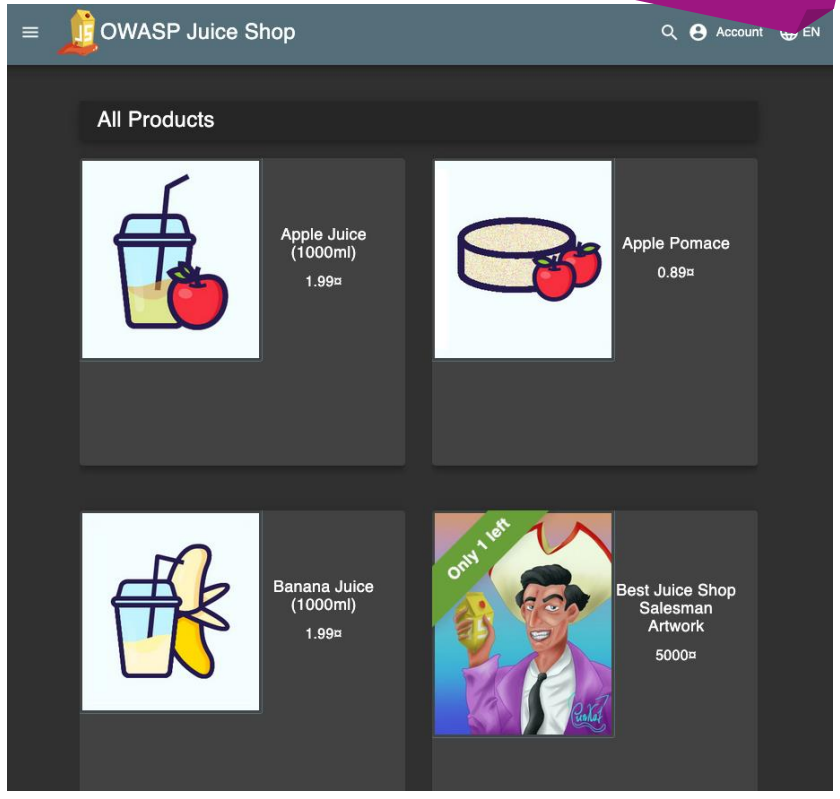
OWASP Projects

iteratec

OWASP Juice Shop

- Insecure web shop.
  - Hence the name “Saftladen”, German slang for “lousy shop”.
- Learn to hack & understand attack vectors.
- IMO one of the **greatest projects** from *OWASP*!
  - Shout out to the maintainers Björn & Jannik 🙌
- We use this for developer trainings combined w/ the *Top 10*.
- You can use it for CTFs.
- We donated MultiJuicer for easier setup of multiple instances.
  - If you can’t afford monetary donations, consider donating software.
  - Even patches/tranlations of documentation are worthy. 🤗
- https://owasp.org/www-project-juice-shop/

Disclaimer:
Jannik is my co-worker 😬



OWASP Projects

iteratec

OWASP secureCodeBox

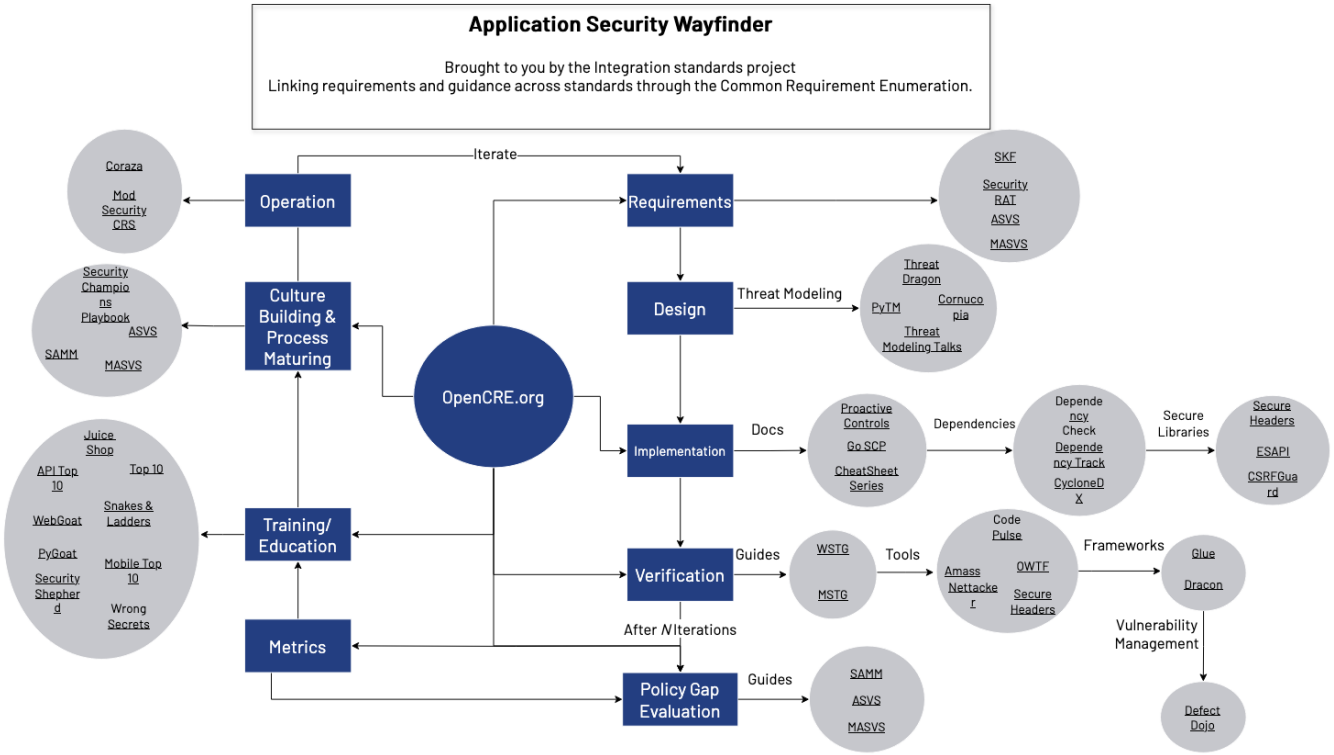
Disclaimer:
I'm one of the maintainer 😬

- Orchestration of security scanners:
  - 20+ integrated by default: https://www.securecodebox.io/docs/scanners
  - Any scanner runnable in a container can be integrated 😀
  - Windows possible, but PITA! We tried it with Pingcastle 😩
- Kubernetes based.
- Only UI is CLI 🤓
- Mainly sponsored by iteratec & some customers.
  - We us it to scan the whole company once day.
- You can try out a simple scan on our new free SaaS: https://scd.iterate.de/
- https://owasp.org/www-project-securecodebox/

OWASP Projects

iteratec

So much more…



- 370 Projects
- Categorized as
  - Flagship Projects
  - Production Projects
  - Lab Projects
  - Incubator Projects
- All **free** and **open source** 🤗
- Read *OWAP Developer Guide* for more comprehensive overview.
- https://owasp.org/projects/

iteratec

Thank You!

Are there any questions?

Download slides here 🤗

iteratec

Sven Strittmatter

Lead Security Expert

sven.strittmatter@iteratec.com

Click an appointment w/ me →

No, its not a phishing website 😇