OWASP
-
so much more than just OWASP Top 10

OWASP Foundation

OWASP

SECURE THE WEB

whoami

Tobias Glemser
CEO of secuvera GmbH (~50 employees)
BSI-certified Pentester
OWASP German Chapter Lead

MISSION

The Open Worldwide 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

The OWASP Community

- OWASP is a worldwide **free** and **open community** focused on improving the security of application software.

- Our mission is to make application security **visible** so that people and organisations can make **informed decisions** about application security **risks**.

Session at Global AppSec Amsterdam

Its all for free

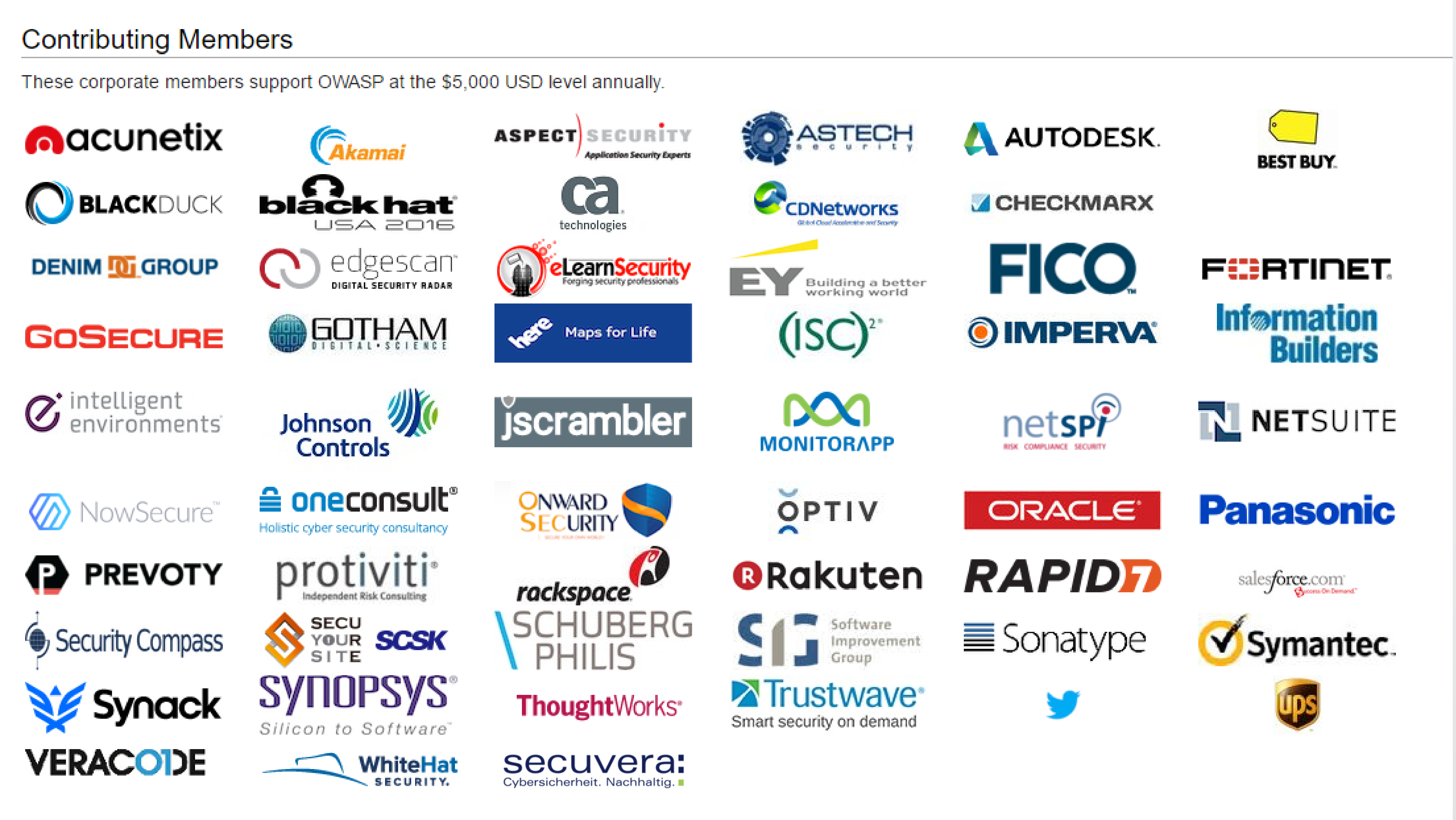
- Everyone is **free** to participate in OWASP and **all** of our materials are available under a **free** and **open** software license.

- All OWASP events *(except conferences)* are free to attend by both members and non-members of OWASP - and can be attended by anyone who is interested in Application Security and Cyber Security in general.

Member Lounge at OWASP Conference

The OWASP Foundation

- We are a **Global not-for-profit charitable** organisation
- Vendor-Neutral Community
- **Collective Wisdom** of the **Best Minds in Application Security Worldwide**
- Provide **free** tools, guidance, documentation
- Meetings are **free to attend** *(free drinks & food included)*
- Meetings are usually **2-hour seminars**
  (usually 2 main talks, with optional lightning talks)



Contributing Members

These corporate members support OWASP at the $5,000 USD level annually.

Diamond members

apiiro

CEQUENCE™ SECURITY

Platinum members

Adobe

ATLASSIAN

BIONIC

Bloomberg®

BLACK BELT SECURITY

COALFIRE®

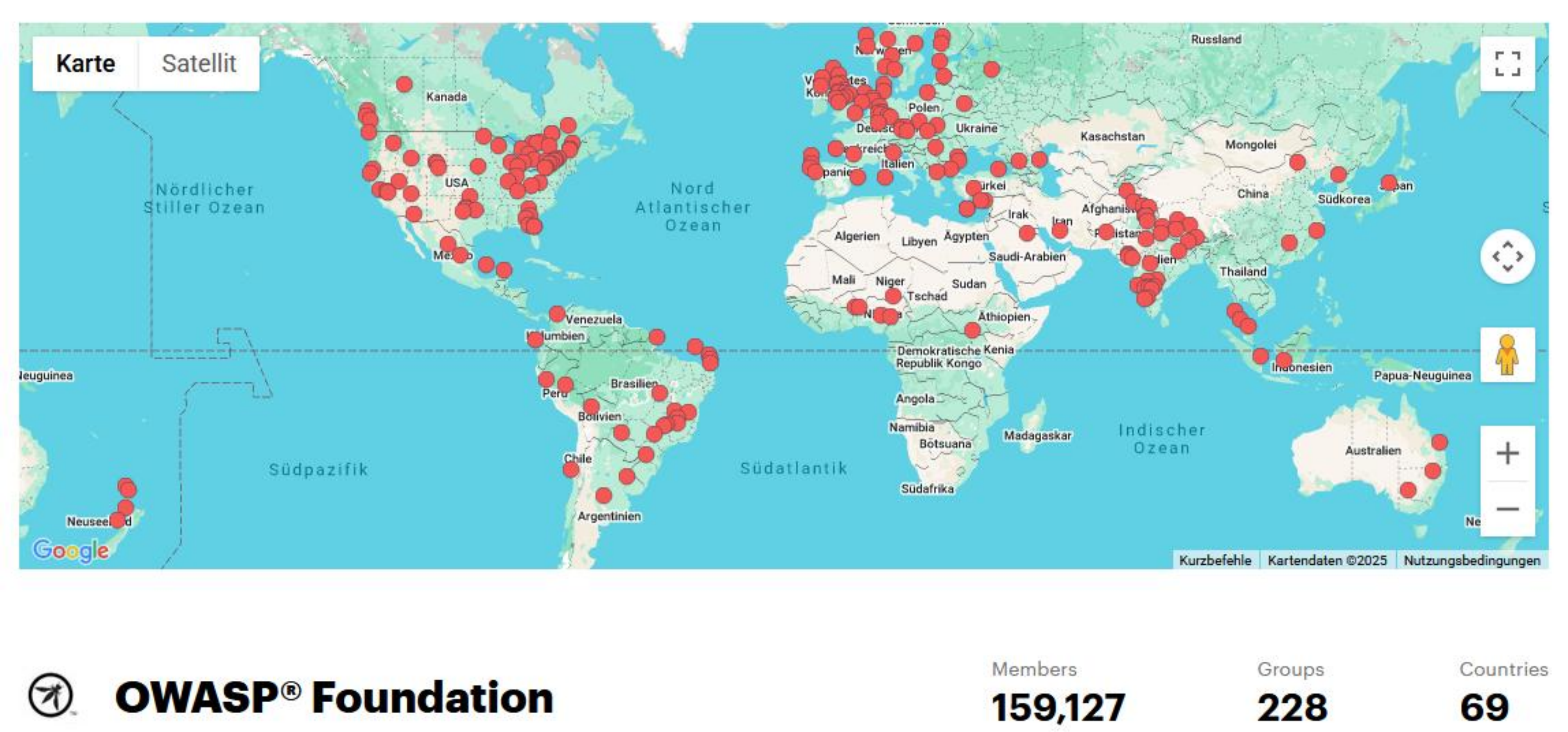
Contrast SECURITY

Fortify

Qualys®

salesforce

World Wide



OWASP® Foundation

Members
159,127

Groups
228

Countries
69

OWASP German Chapter

www.owasp.de

OWASP German Chapter

- City Chapter Meetings
- Regional Chapter Meetings
- German OWASP Day
- German volunteers in famours projects like
  - OWASP Top 10
  - OWASP Juice Shop
  - OWASP CycloneDX
  - OWASP Mobile Application Security (MAS) with MASVS and MASTG
  - OWASP DepencyTrack
  - OWASP CRS (OK, Switzerland ☺)

We are volunteers

45,000+ OWASP volunteers worldwide

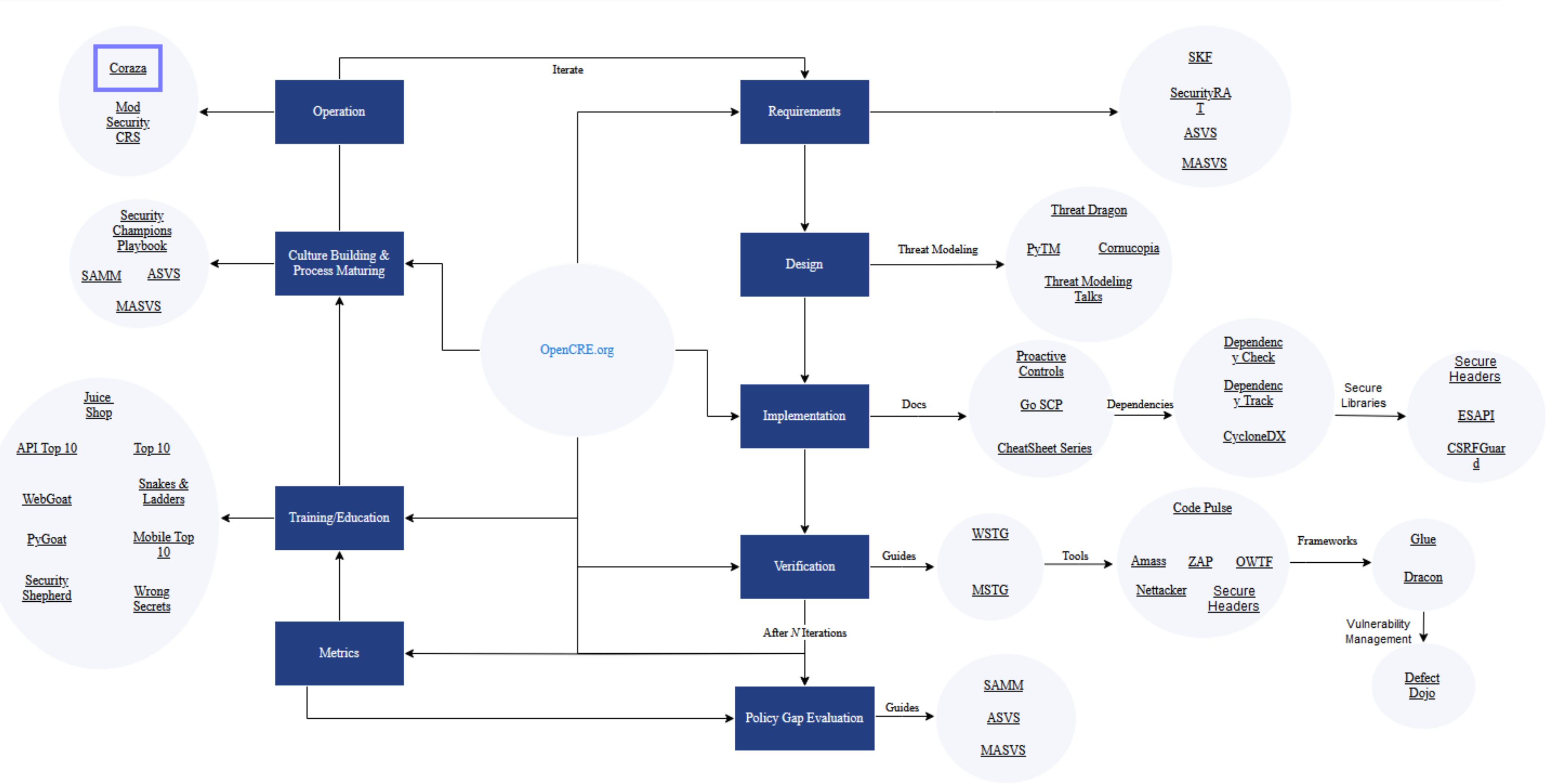
OWASP Projects

(Some. Really.)

OWASP Projects

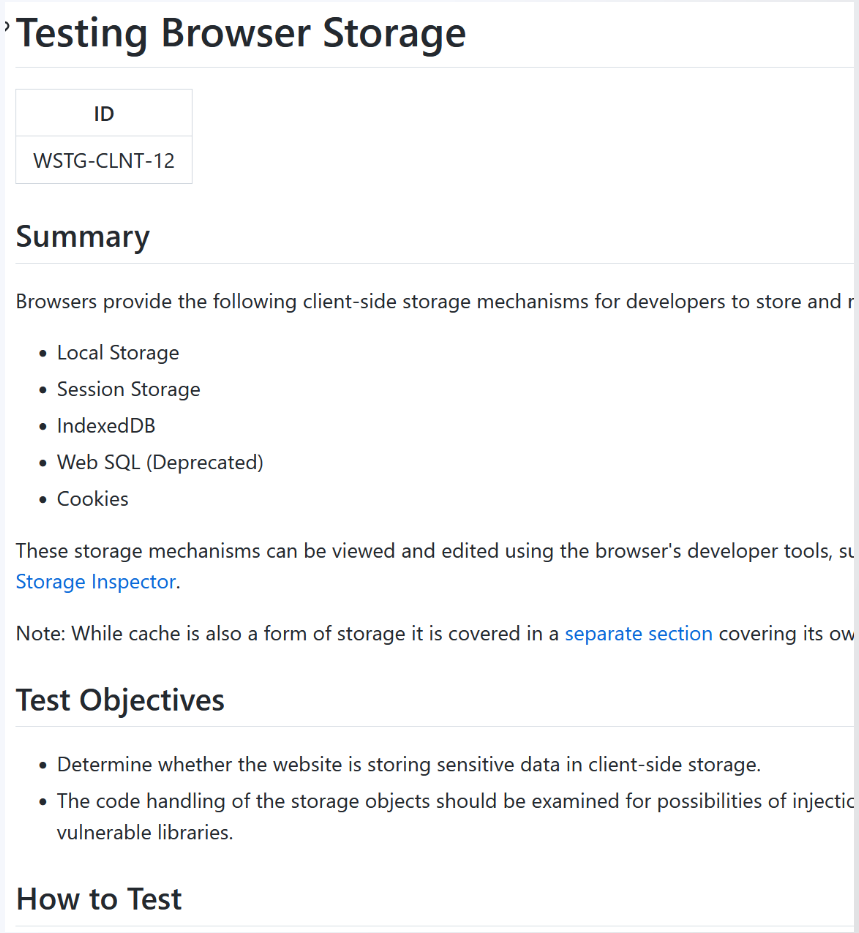
- 377 Projects
- 15 “Flagship” Projects
- Type of projects
  - Tools
  - Documentation
  - Code

OWASP Projects



OWASP Web Security Testing Guide (WSTG)

- Test yourself (?)
- Use as testing plan in a pentest



Testing Browser Storage

ID
WSTG-CLNT-12

Summary

Browsers provide the following client-side storage mechanisms for developers to store and r

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

These storage mechanisms can be viewed and edited using the browser's developer tools, su Storage Inspector.

Note: While cache is also a form of storage it is covered in a separate section covering its ow

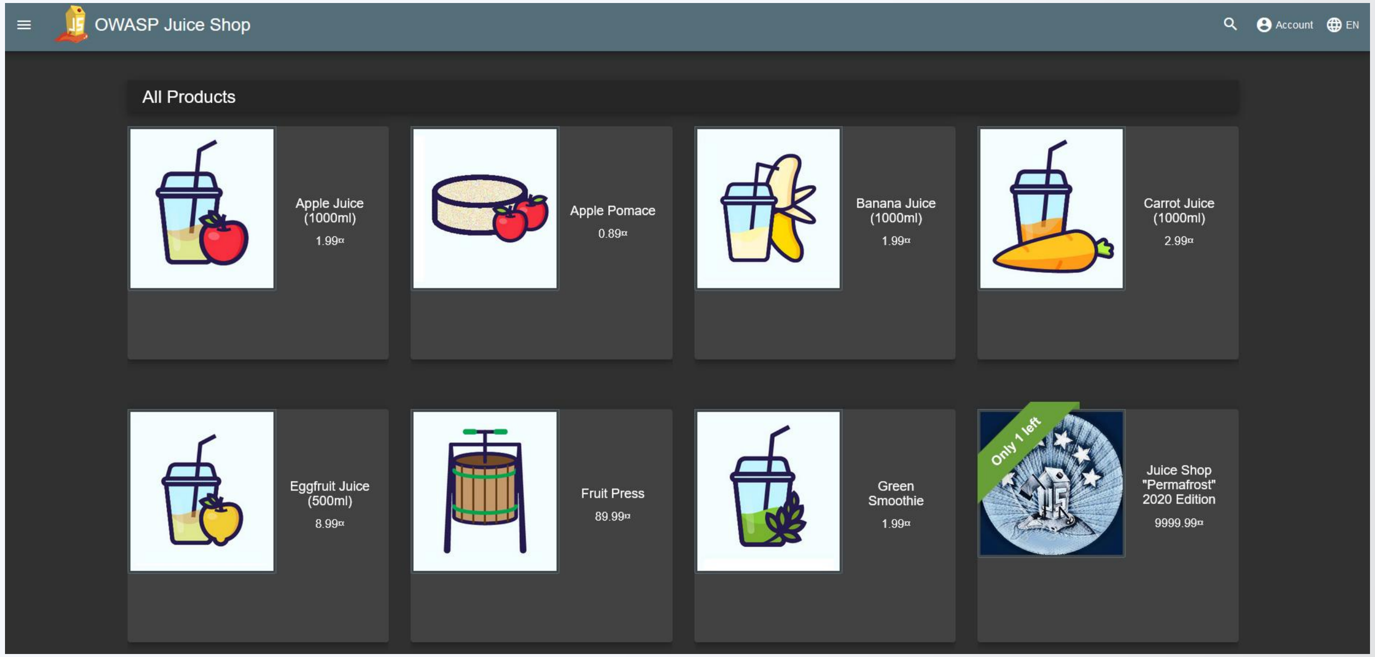
Test Objectives

- 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 injectic vulnerable libraries.

How to Test

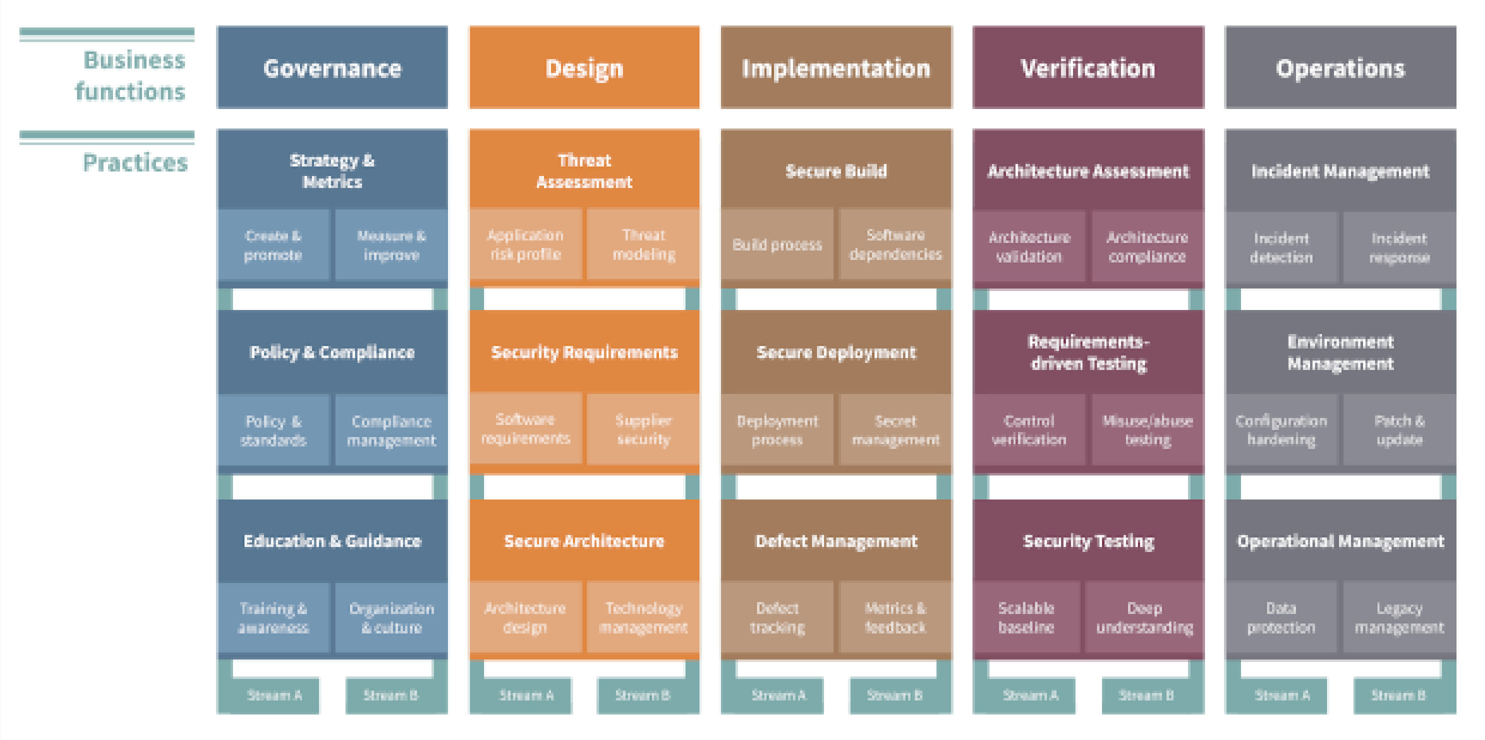
OWASP Juice Shop

- Educate yourself
- Flagship Project
- Björn!
- node.js, Angular, Express, NoSQL, Websockets,…



OWASP SAMM

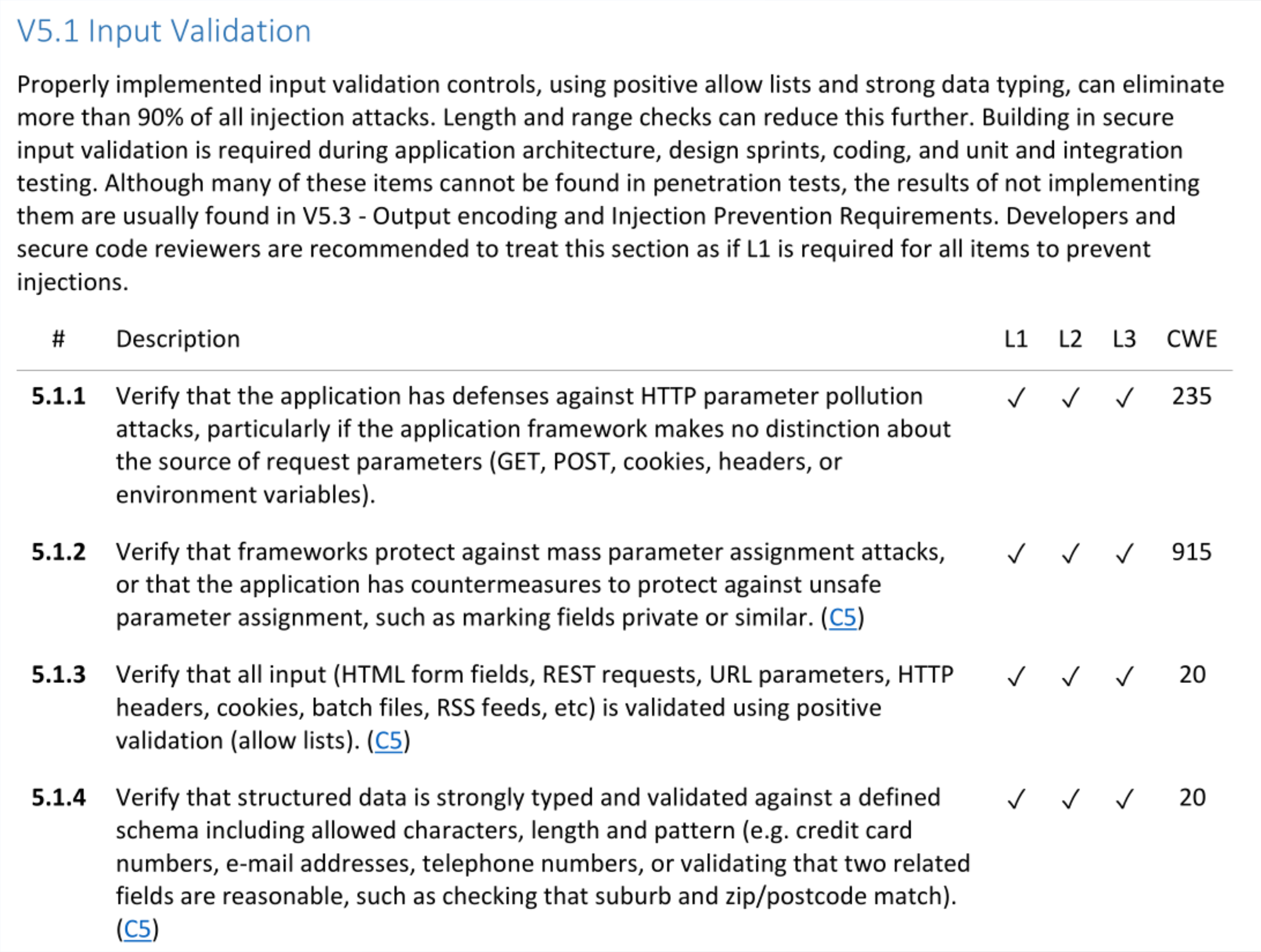
- Push Left
- Secure Development Lifecycle
- Very mature
- Usable ourside web (e. g. IEC 62443-4-1)
- CRA coverage



Business functions	Governance		Design		Implementation		Verification		Operations	
Practices	Strategy & Metrics		Threat Assessment		Secure Build		Architecture Assessment		Incident Management	
	Create & promote	Measure & improve	Application risk profile	Threat modeling	Build process	Software dependencies	Architecture validation	Architecture compliance	Incident detection	Incident response
	Policy & Compliance		Security Requirements		Secure Deployment		Requirements-driven Testing		Environment Management	
	Policy & standards	Compliance management	Software requirements	Supplier security	Deployment process	Secret management	Control verification	Misuse/abuse testing	Configuration hardening	Patch & update
	Education & Guidance		Secure Architecture		Defect Management		Security Testing		Operational Management	
	Training & awareness	Organization & culture	Architecture design	Technology management	Defect tracking	Metrics & feedback	Scalable baseline	Deep understanding	Data protection	Legacy management
	Stream A	Stream B	Stream A	Stream B	Stream A	Stream B	Stream A	Stream B	Stream A	Stream B

OWASP Application Security Verification Standard (ASVS)

- Governance
- Checkliste
- Heatmap



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

OWASP ModSecurity Core Rule Set

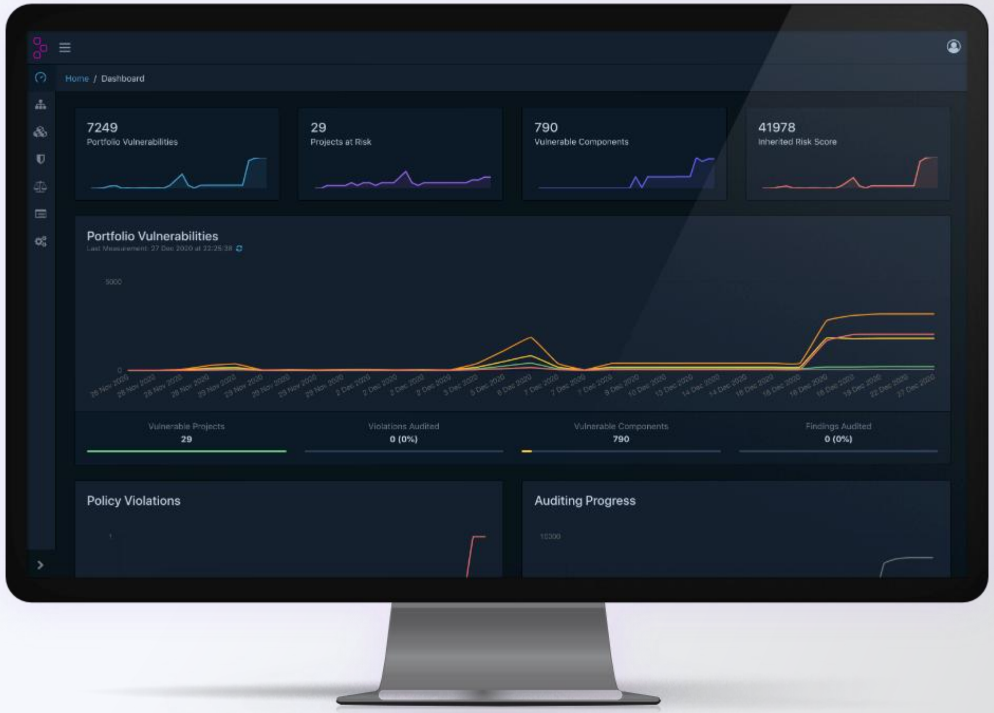
- WAF 😳
- Baseline security
- No false positives

OWASP
ModSecurity
Core Rule Set
THE 1ST LINE OF DEFENSE

DependencyTrack (e.g. SBOM)

Keep track on

- libraries ,
- frameworks,
- applications,
- containers,
- operating systems,
- firmware,
- hardware and
- services



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

OWASP AI Exchange

AI-Security material “storage”

- LLM Top 10,
- Threats,
- AI Security Testing,
- AI Privacy

Flagship project

OWASP
AI EXCHANGE

OWASP Top 10

- What to expect
  - „only“ a Top 10
  - No list of weaknesses → CWE
  - Nothing you can pentest againgst (anymore) There is no Pentest against A4 or A9? → OWASP Testing Guide
  - No standard for compliance → OWASP ASVS
- Usage
  - „The OWASP Top 10 is a standard awareness document for developers and web application security.“
  - First Workshops, even with PO/PMs and Stakeholdern
  - Perfect start for „Push Left“ e.g. by applying OWASP SAMM

Volunteer!

www.owasp.de
tobias.glemser@owasp.org