OWASP Ruhrpott Chapter Meeting

Relaunch

What Is OWASP?

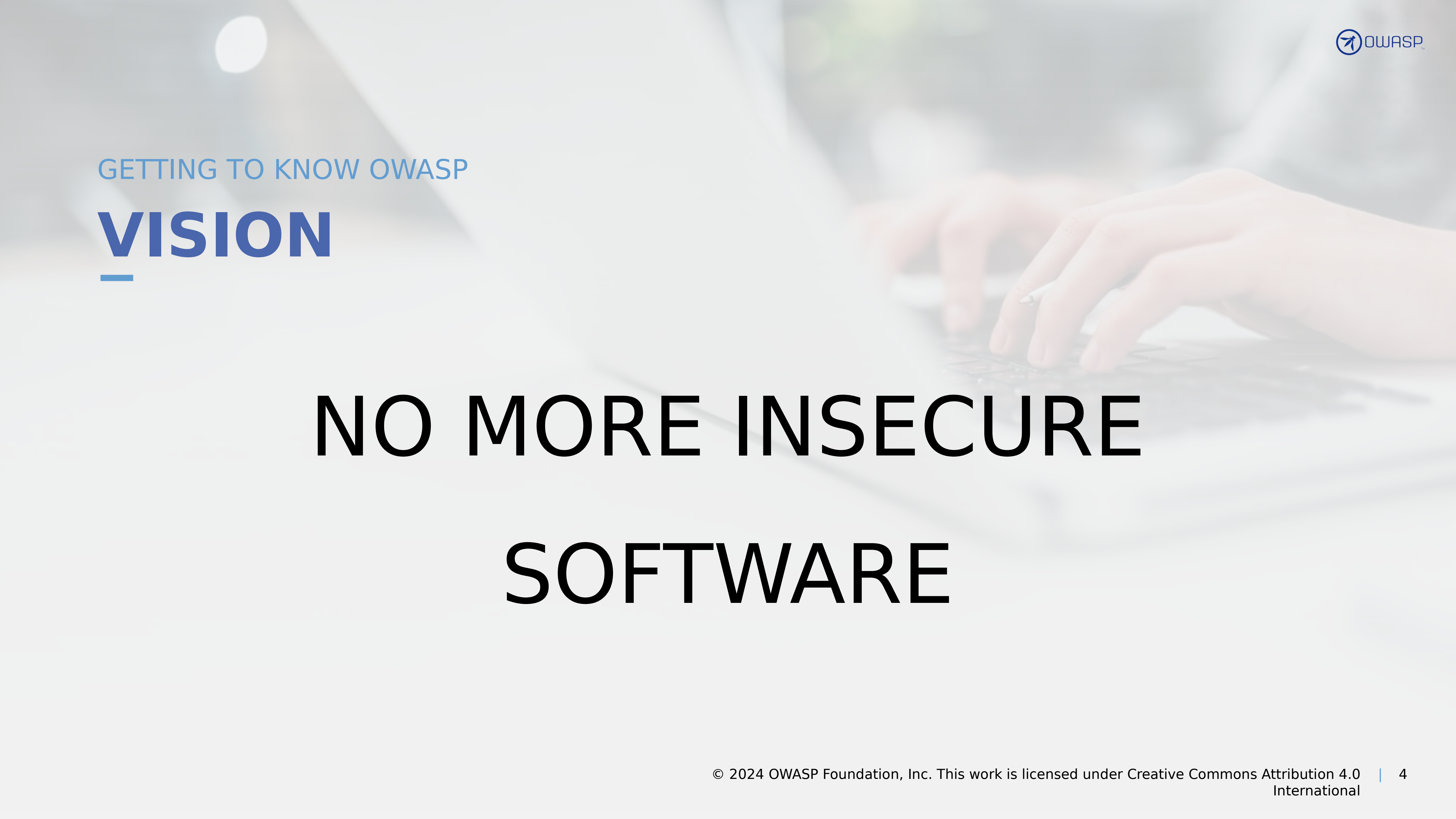
- The ***O****pen* ~~*Web*~~***W****orldwide* ***A****pplication* ***S****ecurity* ***P****roject*
  is a nonprofit foundation that works
  to improve the security of software.

Offers include:

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

OWASP Ruhrpott - The Past

- 2015 - 2020 (50 meetings, 1 conference)
- Different locations
- Practical Trainings
- Talks
- Get Together & Discussions



GETTING TO KNOW OWASP

VISION

NO MORE INSECURE SOFTWARE

GETTING TO KNOW OWASP

MISSION

To be the global open community that powers secure software through education, tools, and collaboration.

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

to enable developers to write better software and security professionals to make the world’s software more secure.

GETTING TO KNOW OWASP

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 organizations can make informed decisions about application security risks.

GETTING TO KNOW OWASP

IT’S ALL FOR FREE

Everyone is free to participate in OWASP, and all of our materials are available for free and with an open software license.

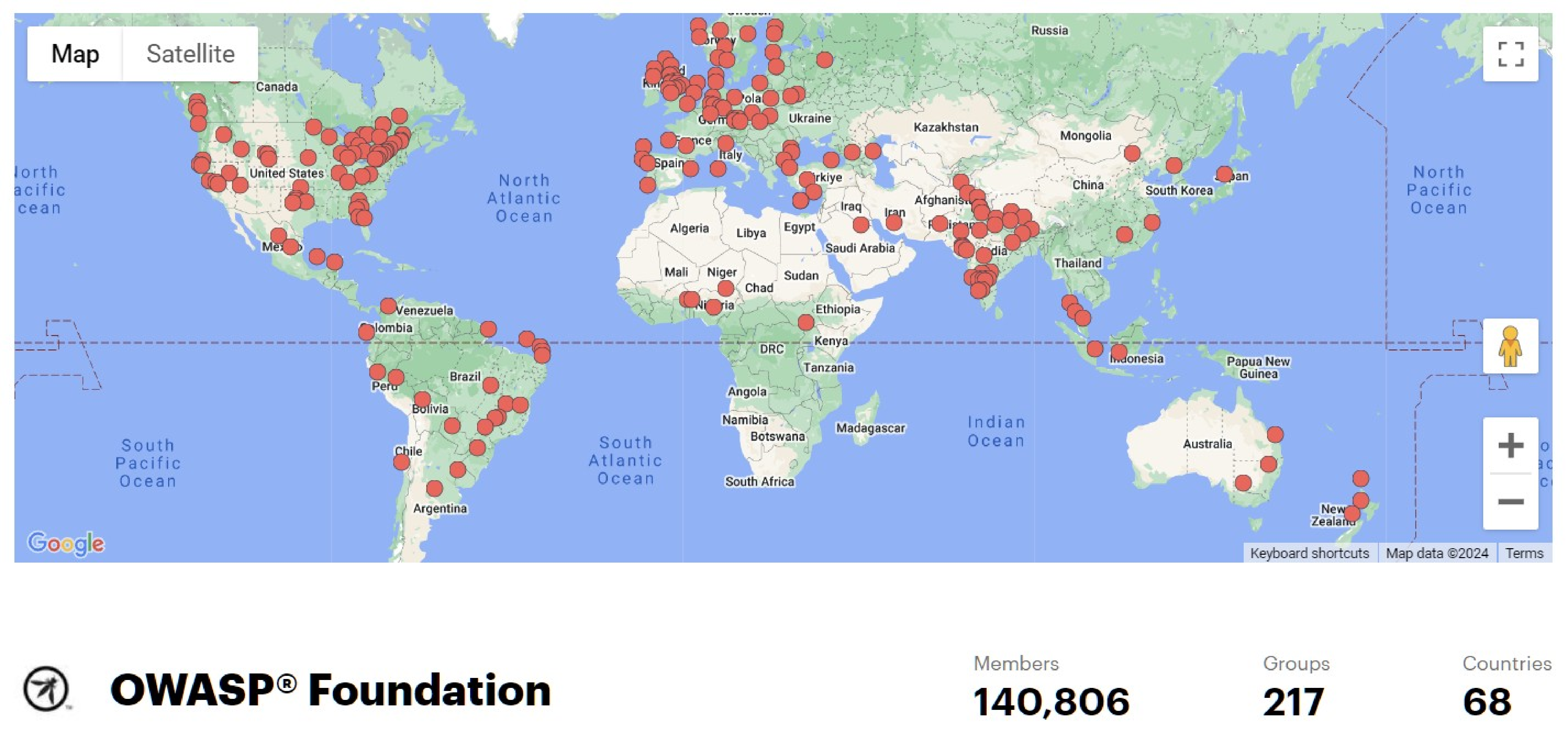
Most OWASP events are free for both members and non-members and can be attended by anyone interested in Application Security and Cyber Security in general.

GETTING TO KNOW OWASP

OUR HISTORY

Founded in September 2001, OWASP changed the application security world for the better, with the release of the OWASP Developer Guide and many other free resources.

- OWASP Top 10 First Released January 2003
- OWASP Foundation, Inc incorporated April 2004
- First conference: Global AppSec NY 2005
- First EU conference: Global AppSec EU 2006



OWASP® Foundation

Members	Groups	Countries
140,806	217	68

GETTING TO KNOW OWASP

OWASP BY THE NUMBERS

01

8118+ MEMBERS

Members sustain OWASP

02

226 PROJECTS

We are famous for our projects!

03

1150+ Leaders

Become a leader today!

04

20+ Regional AppSec Days

Medium Sized Regional Events near you!

05

272 CHAPTERS

There’s a chapter near you… or please create one!

06

3 GLOBAL APPSECs

Global AppSec’s are a great place to network and learn

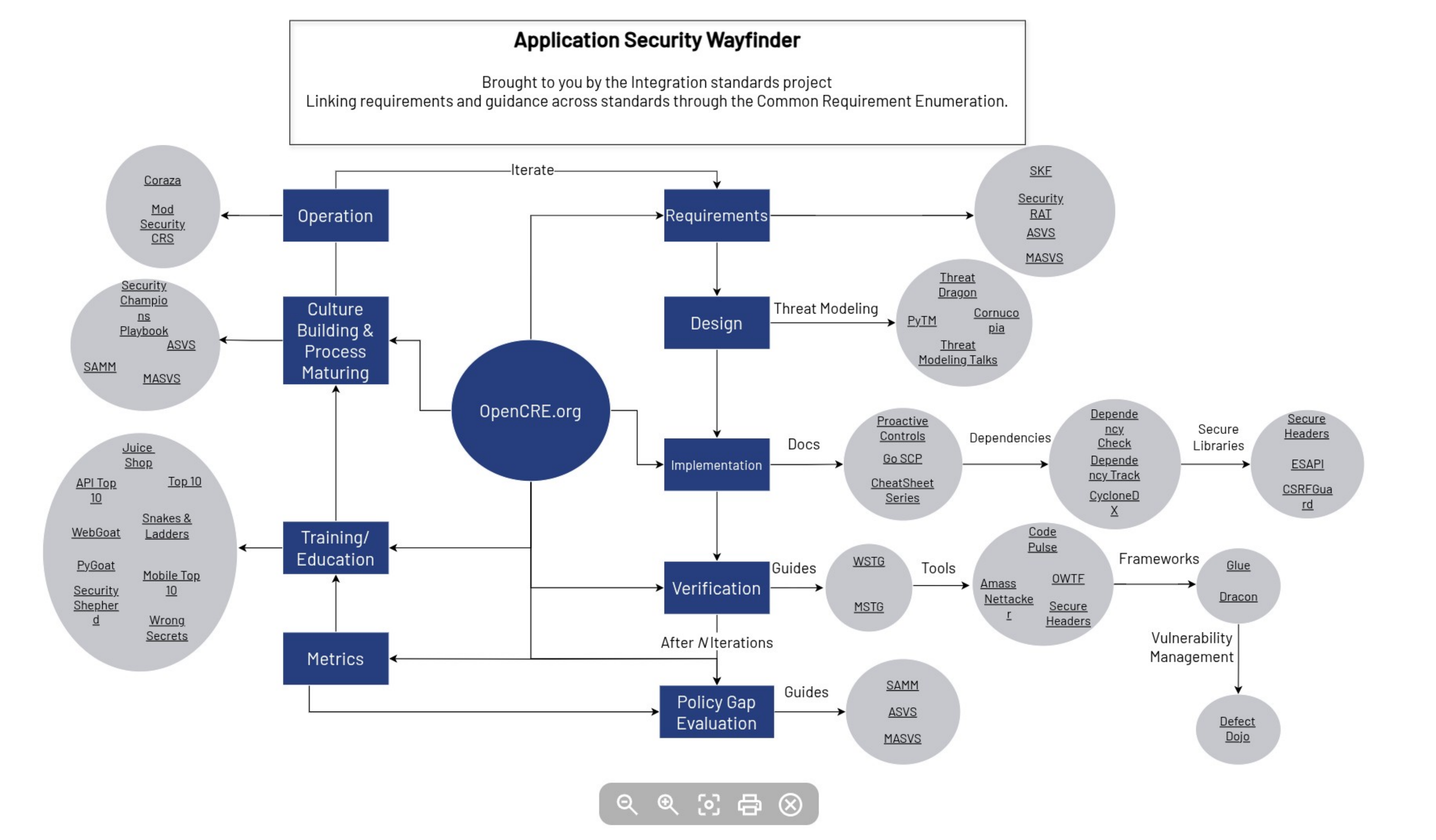
We are all volunteers!

80,000+ participants and volunteers worldwide

OWASP Projects

There is way more than OWASP Top 10

Application Security Wayfinder



Application Security Wayfinder

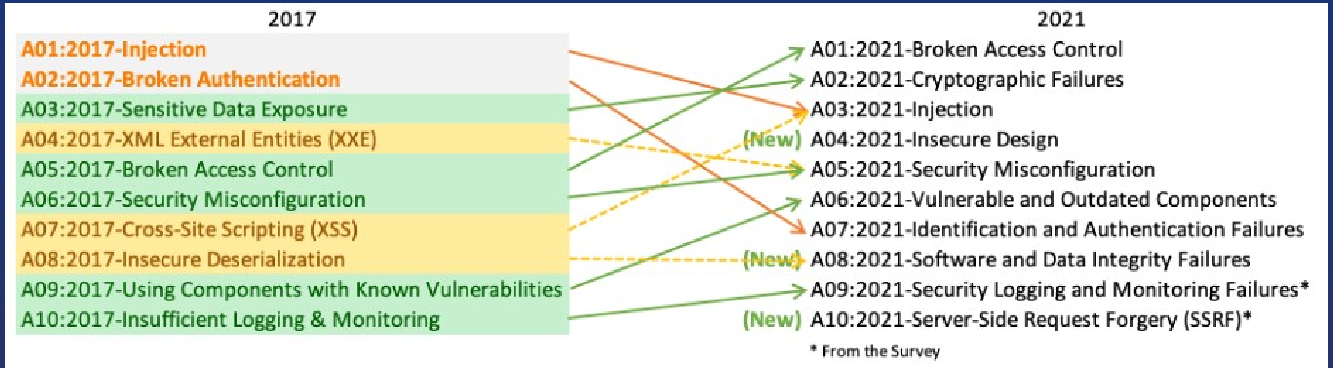
Brought to you by the Integration standards project
Linking requirements and guidance across standards through the Common Requirement Enumeration.

OWASP Top 10

- An opinionated list of most common 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”.
- https://owasp.org/www-project-top-ten/

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

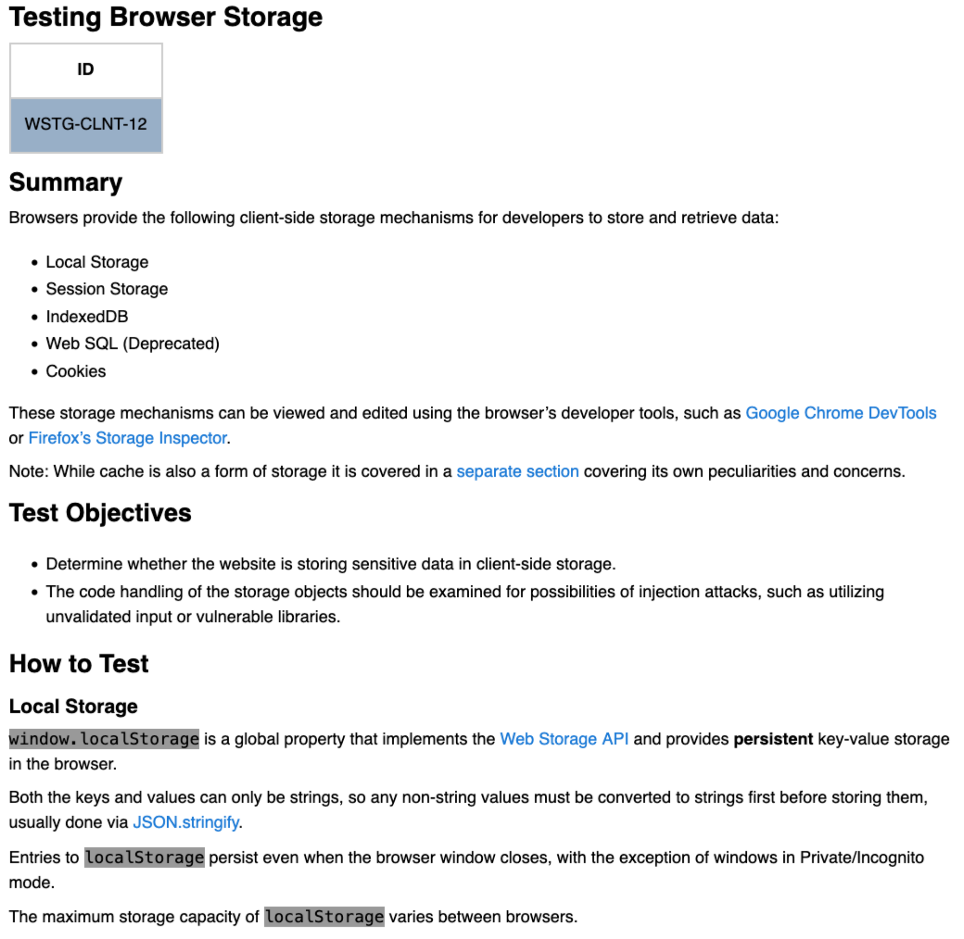


2017	2021
A01:2017-Injection	A01:2021-Broken Access Control
A02:2017-Broken Authentication	A02:2021-Cryptographic Failures
A03:2017-Sensitive Data Exposure	A03:2021-Injection
A04:2017-XML External Entities (XXE)	(New) A04:2021-Insecure Design
A05:2017-Broken Access Control	A05:2021-Security Misconfiguration
A06:2017-Security Misconfiguration	A06:2021-Vulnerable and Outdated Components
A07:2017-Cross-Site Scripting (XSS)	A07:2021-Identification and Authentication Failures
A08:2017-Insecure Deserialization	(New) A08:2021-Software and Data Integrity Failures
A09:2017-Using Components with Known Vulnerabilities	A09:2021-Security Logging and Monitoring Failures*
A10:2017-Insufficient Logging & Monitoring	(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

OWASP Web Security Testing Guide (WSTG)

- Comprehensive guide to testing the security of web applications and web services.
- 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.

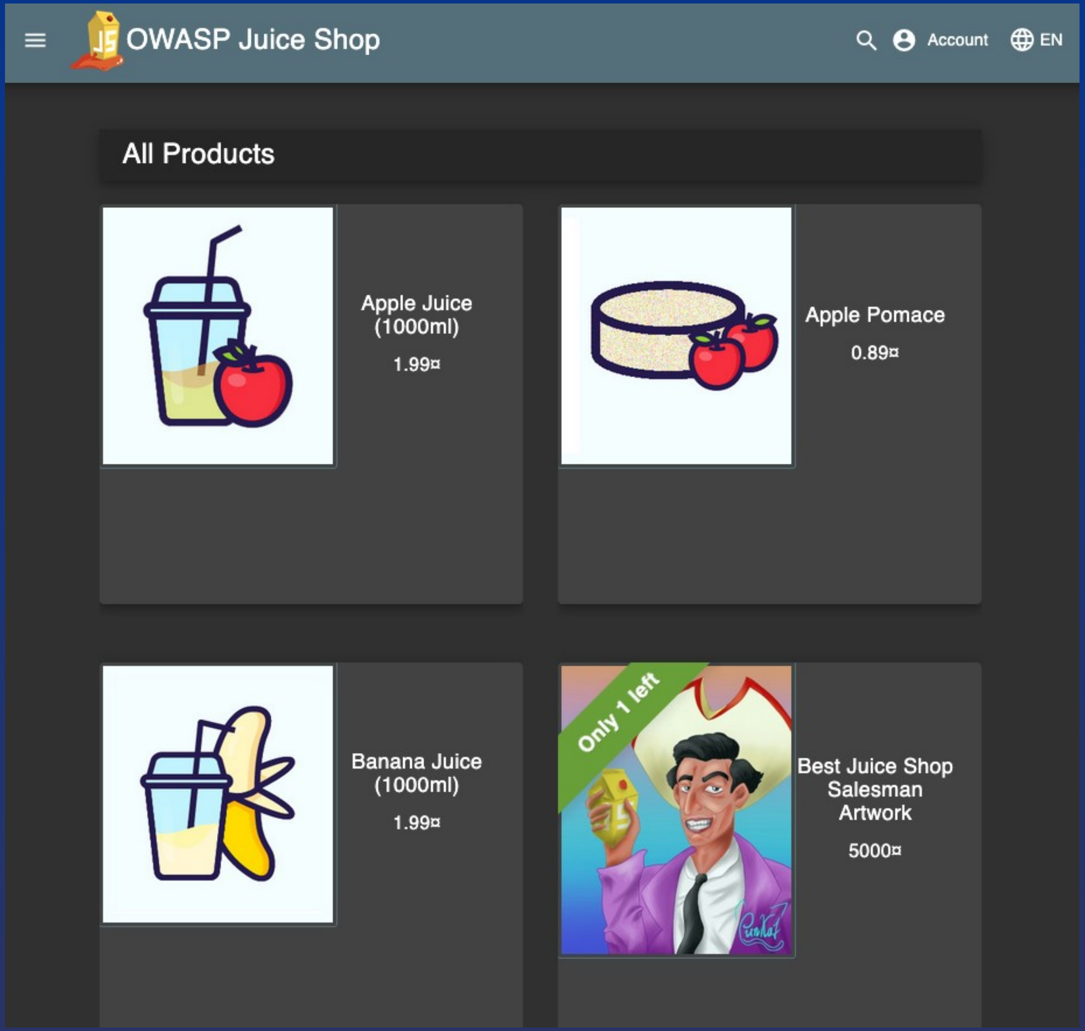
The maximum storage capacity of `localStorage` varies between browsers.

OWASP Cheat Sheet Series

- No time to read the OWASP Developer Guide
  or role out OWASP SAMM? 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 Juice Shop

- Insecure web shop.
- Learn to hack & understand attack vectors.
- You can use it for CTFs.
- https://owasp.org/www-project-juice-shop/



OWASP Ruhrpott - The Future

OWASP Ruhrpott - The Future

- Different locations (2 month?)
- Practical Trainings
- Talks from Different Industries
- Get Together & Discussions

- **Meetup**: https://www.meetup.com/owasp-ruhrpott-chapter
- **Chapter**: https://owasp.org/www-chapter-ruhrpott/