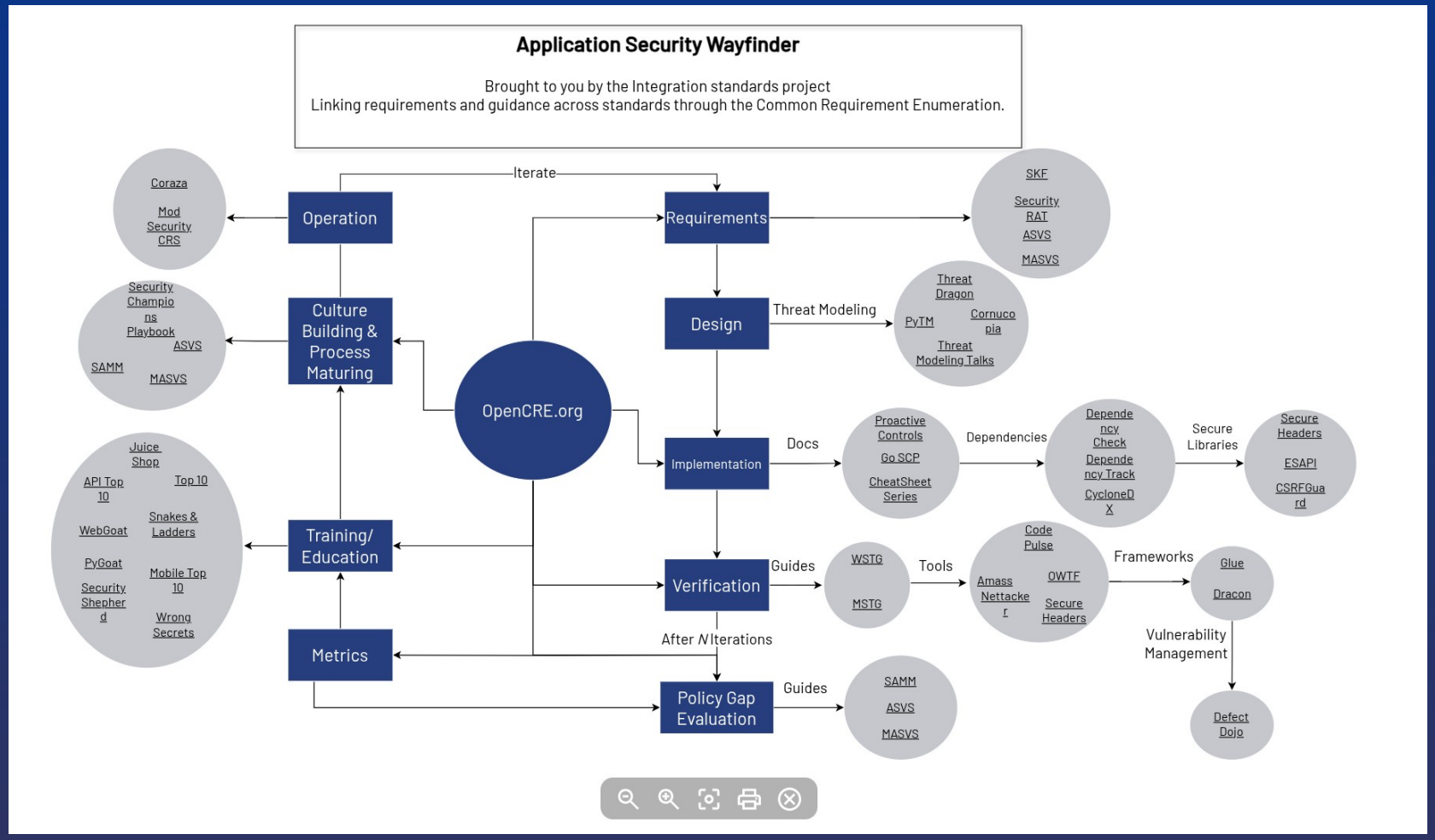
OWASP Ruhrpott Chapter Meeting

Application Security

Today’s Agenda

- Open Discussion about Application Security from different view points
  - How do you develop?
  - How do you ensure application security?
  - How do you verify your approach?
- Preparation for next Chapter Meetings (06.11.25: AI/ML/DL/CV/NLP/RL/LLM, Hands On Workshop?)

Application Security Wayfinder

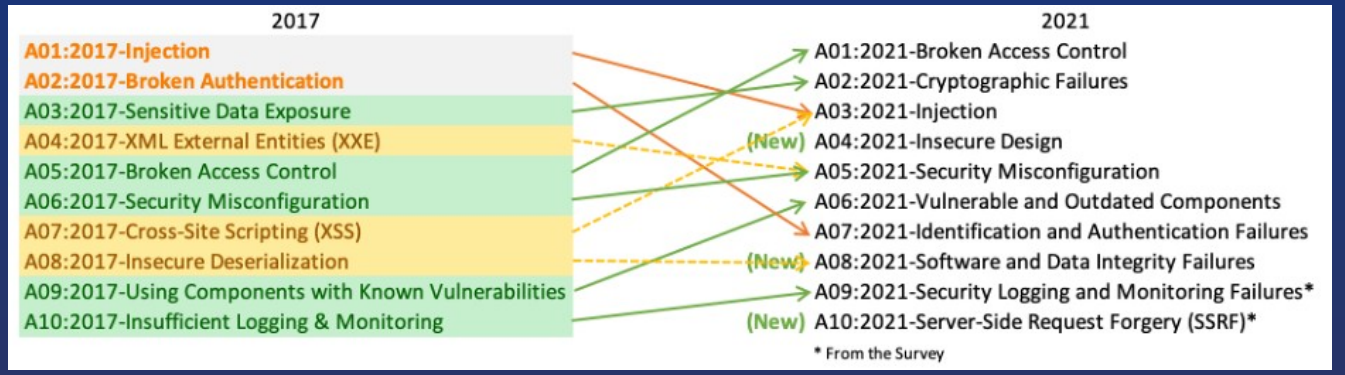


OWASP Top 10

- 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



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 WSTG Categories

- Information Gathering
- Configuration and Deployment Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing
- Testing for Error Handling
- Testing for Weak Cryptography
- Business Logic Testing
- Client-side Testing

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/