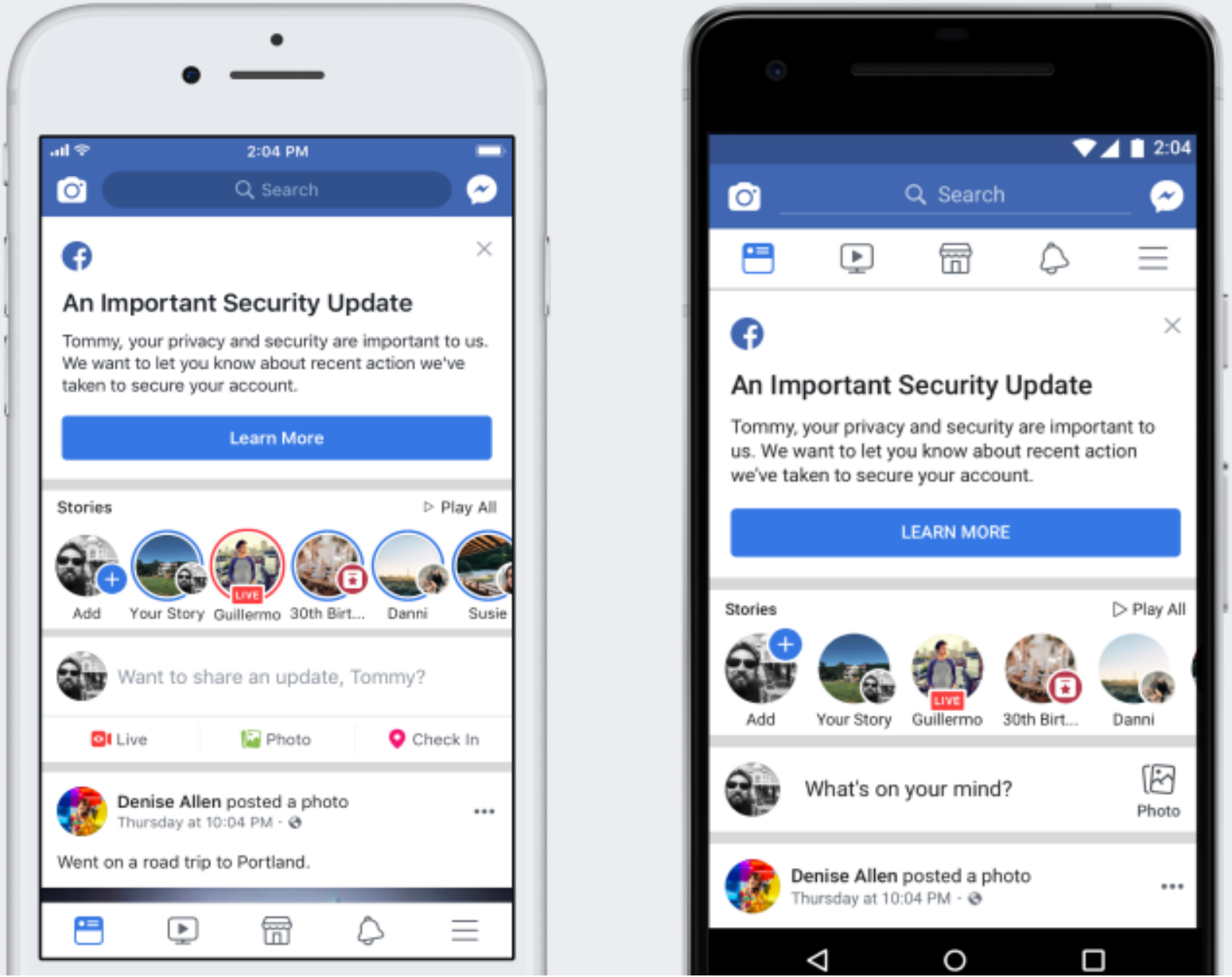
https://about.fb.com/news/2018/09/security-update/



OWASP ZAP

EINE METHODE UM WEB SECURITY ZU ERMÖGLICHEN

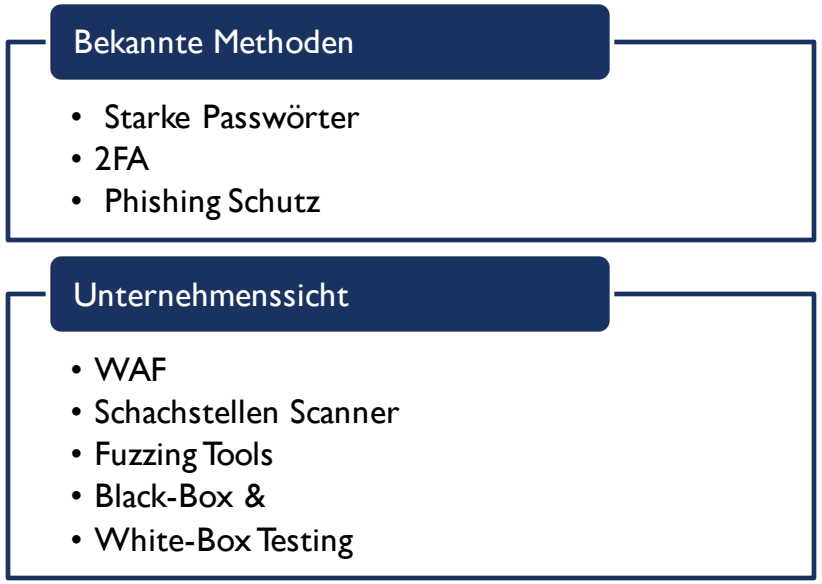
WAS IST WEB SECURITY?

- Schützen von Web Apps vor Bedrohungen im Internet

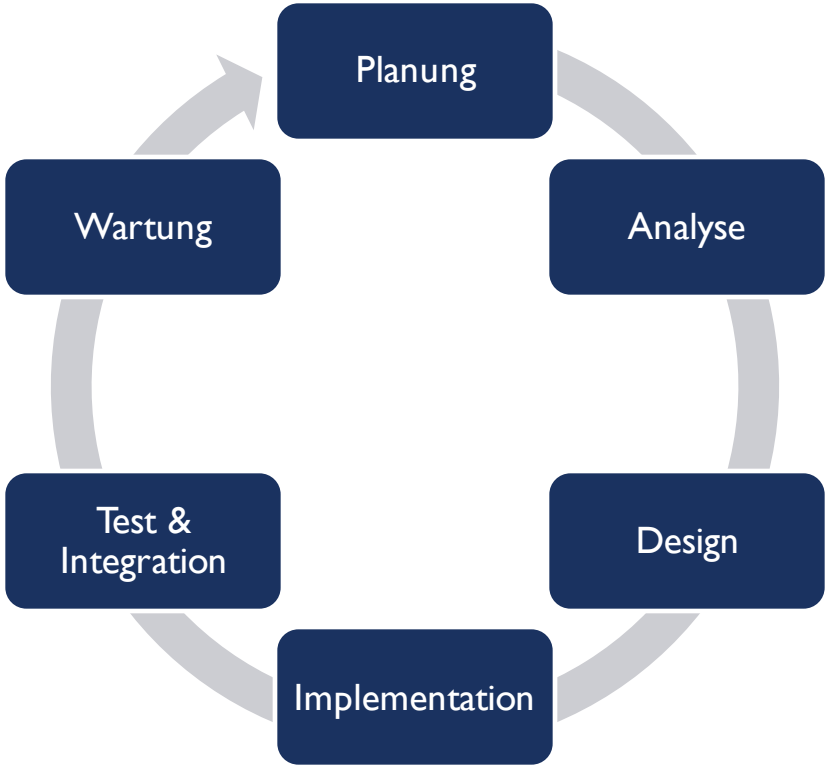
  Zum Beispiel:

WAS IST WEB SECURITY?

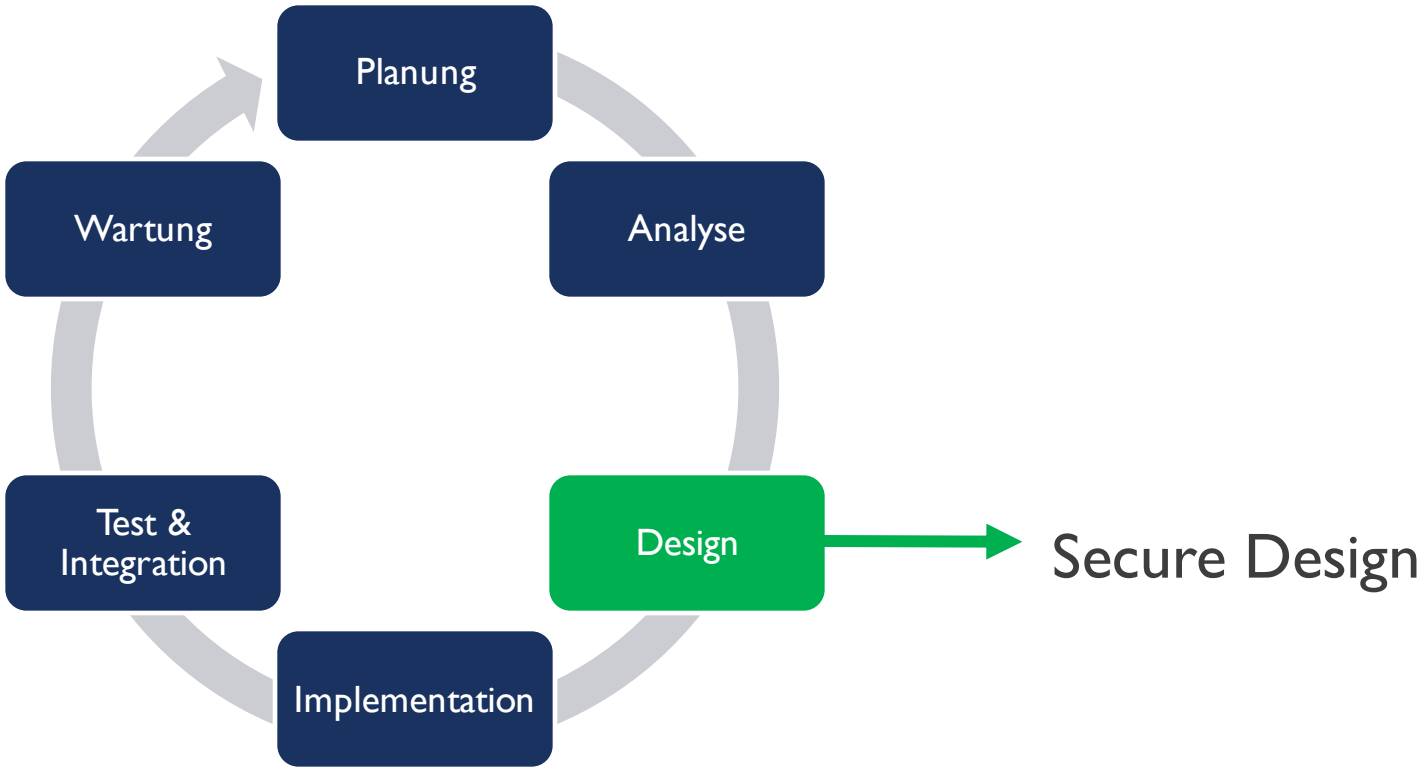
- Werkzeuge um Web Security zu ermöglichen



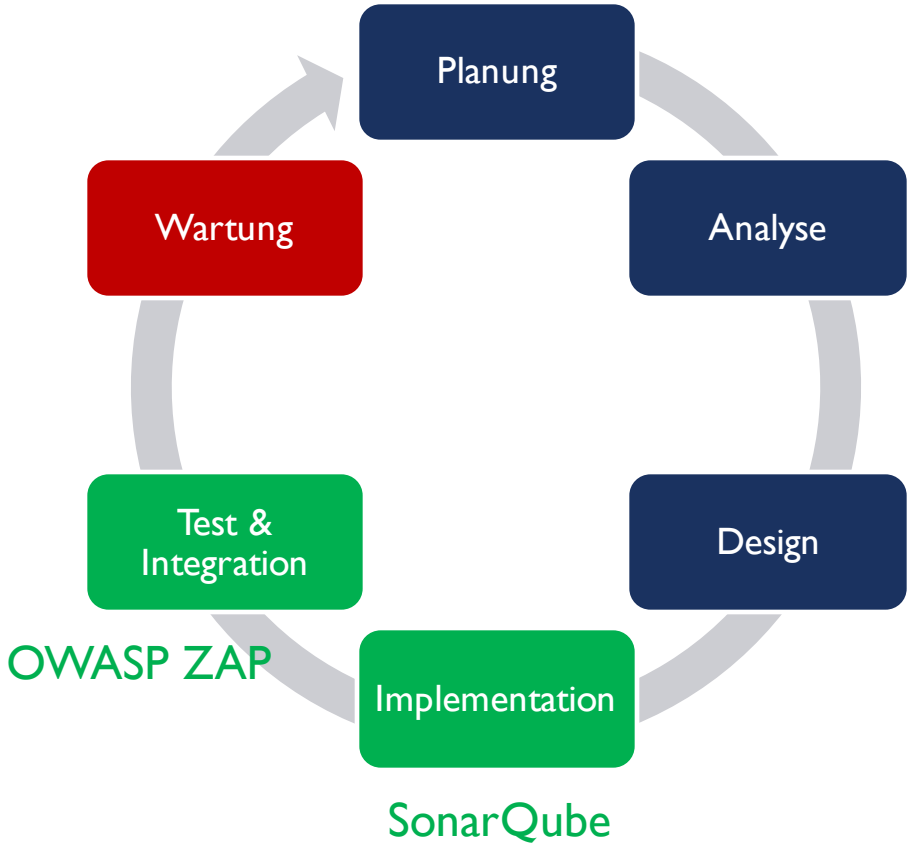
WAS IST WEB SECURITY?



WAS IST WEB SECURITY?



WAS IST WEB SECURITY?



- Shift-Left Ansatz
- Dynamische Code Analyse
  Bsp.: SonarQube
- Statische Pentest-Tools
  Bsp.: OWASP ZAP

OWASP
OPEN WEB APPLICATION SECURITY PROJECT

- Community
- Ziel: Sichere Software ermöglichen
- Open-Source Projekte
  Alle Inhalte sind unter der Creative Commons Lizenz

PROJEKTE

- OWASP Amass
- OWASP Application Security Verification Standard
- OWASP Cheat Sheet Series
- OWASP CSRFGuard
- OWASP CycloneDX
- OWASP Defectdojo
- OWASP Dependency-Check
- OWASP Dependency-Track
- OWASP Juice Shop
- OWASP Mobile Application Security
- OWASP ModSecurity Core Rule Set
- OWASP OWTF
- OWASP SAMM
- OWASP Security Knowledge Framework
- OWASP Security Shepherd
- OWASP Top Ten
- OWASP Web Security Testing Guide
- OWASP ZAP

OWASP
OPEN WEB APPLICATION SECURITY PROJECT

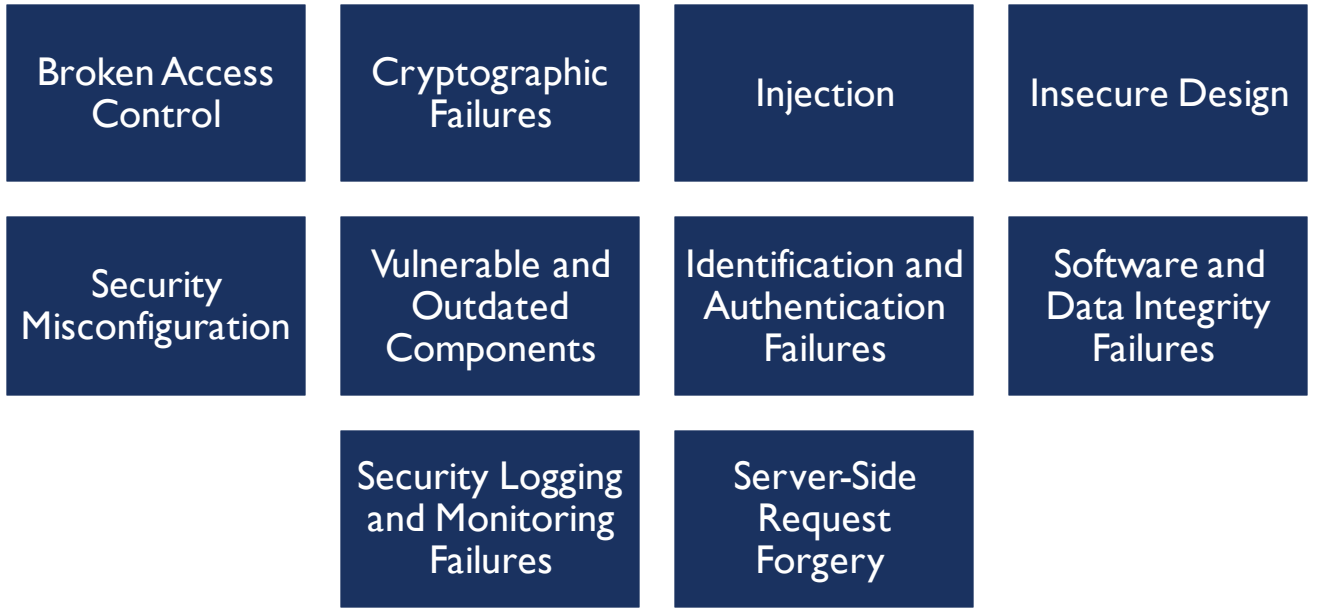
- Community
- Ziel: Sichere Software ermöglichen
- Open-Source Projekte
  Alle Inhalte sind unter der Creative Commons Lizenz

PROJEKTE

- OWASP Amass
- OWASP Application Security Verification Standard
- OWASP Cheat Sheet Series
- OWASP CSRFGuard
- OWASP CycloneDX
- OWASP Defectdojo
- OWASP Dependency-Check
- OWASP Dependency-Track
- OWASP Juice Shop
- OWASP Mobile Application Security
- OWASP ModSecurity Core Rule Set
- OWASP OWTF
- OWASP SAMM
- OWASP Security Knowledge Framework
- OWASP Security Shepherd
- OWASP Top Ten
- OWASP Web Security Testing Guide
- OWASP ZAP

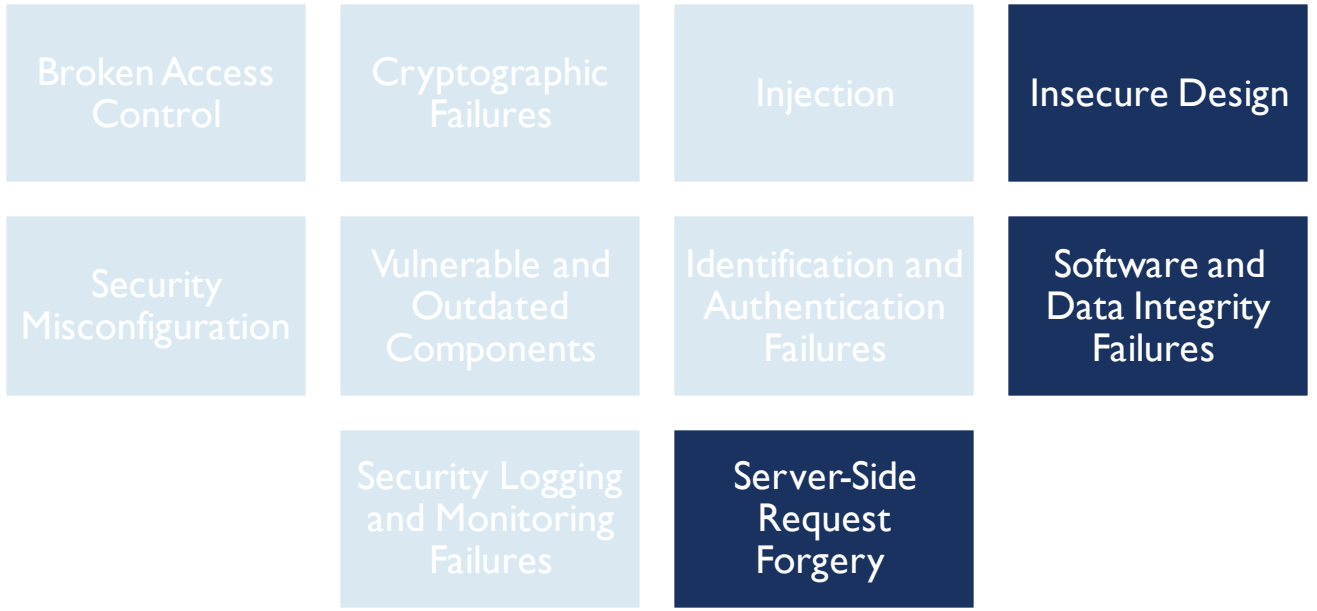
OWASP TOP TEN

- Seit 2003
- Häufigsten krit. Schwachstellen
- Anhand: Statistiken, Umfragen und CWEs
- "Awareness-Dokument"



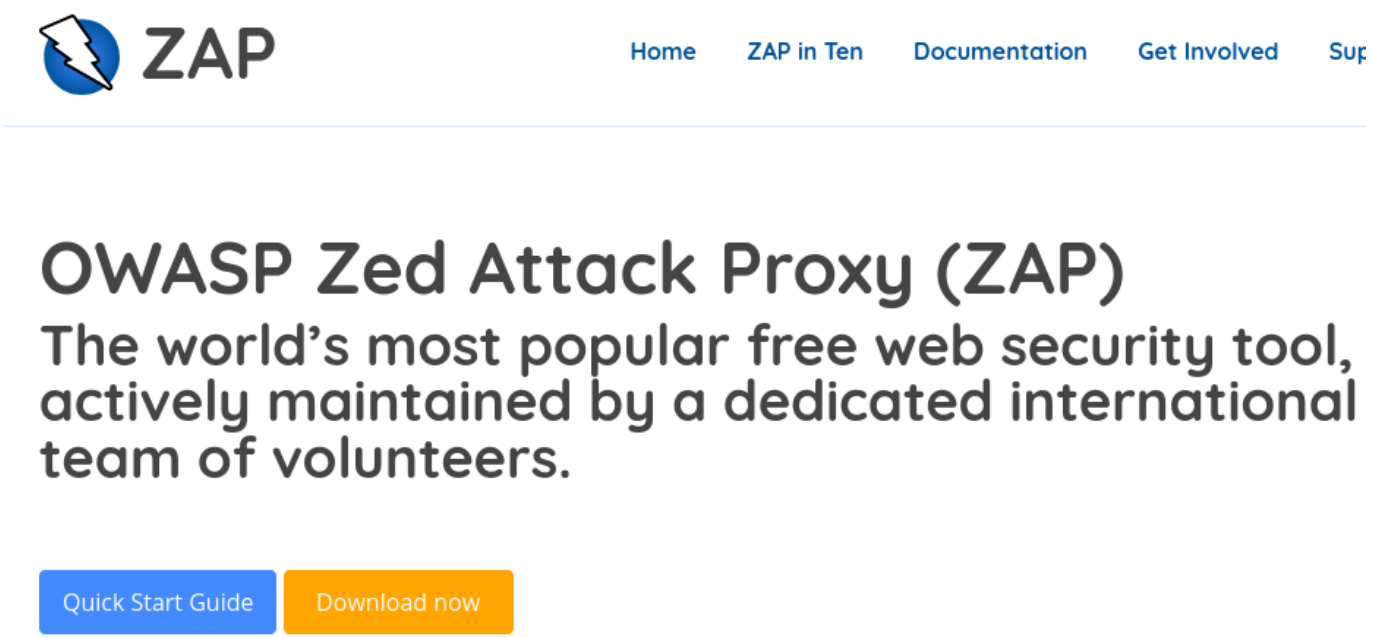
OWASP TOP TEN

- Seit 2003
- Häufigsten krit. Schwachstellen
- Anhand: Statistiken, Umfragen und CWEs
- "Awareness-Dokument"



ZED ATTACK PROXY

- Was ist das?
- Wofür wird es genutzt?
- Wie funktioniert es?



GitHub: https://github.com/zaproxy

ZED ATTACK PROXY

- Was ist das?
- Wofür wird es genutzt?
- Wie funktioniert es?

- Testen von Web Apps auf bekannten Schwachstellen
- Möglichkeit...

  ...White-Box-Tests

  ...Black-Box-Tests

  ...Passive Scans

  ...Automation von Scans

ZED ATTACK PROXY

- Was ist das?
- Wofür wird es genutzt?
- Wie funktioniert es?

1. Erlaubnis die App zu testen

2. Manuelles Testen:
   a) Aktiver Scan
   b) Manual Explore

   Stellt bekannte Angriffs Muster auf Web Apps nach

3. Passiver Scan:
   Proxy im Browser, Analysiert Anfragen und Antworten

4. Markiert jede gefundene Schwachstelle

ZED ATTACK PROXY

- Was ist das?
- Wofür wird es genutzt?
- Wie funktioniert es?

Automation mit ZAP:

- Baseline Scan
- Full Scan
- API Scan

- Fertige GitHub Actions
  -> erstellen Issues
- Docker Images verfügbar
- Framework:
  -> nicht Container-gebunden
  -> Steuerung über eine YAML-Datei

ZED ATTACK PROXY

- Was ist das?
- Wofür wird es genutzt?
- Wie funktioniert es?

WICHTIGER HINWEIS:

Aktiver Scan = echter Angriff

→ nur mit ERLAUBNIS oder bei eigener Anwendung machen

LIVE DEMO DES TOOLS

- Web App mit Schwachstellen
- OWASP ZAP: Scan der App
- Zeigen der Schwachstellen und ihre Auswirkungen

Injection

Identification and Authentication Failures

LIVE – DEMO

ZAP VS. BURP SUITE

ZAP

- Kostenlos
- Open Source
- Automation Framework
- Add-ons notwendig
- Weniger Dokumentation
- Skalierbar, aber nicht so flexibel
- Akkurate Scans, aber Limit im Scope

Vs.

Burp Suite

- Community: kostenlos
  Pro: 499€/Jahr
  Enterprise: ab 8.395€/Jahr
- Automatisiert und semi-Automatisiert
- Viel Testabdeckung
- Mehr Dokumentation
- Large-Scale Testing (evtl. Enterprise)
- Weniger false-positives

DANKE FÜR EURE AUFMERKSAMKEIT