Fachhochschule
Dortmund
University of Applied Sciences and Arts

Informationssicherheit – SoSe 2023
Sichere Software Entwicklung

Prof. Dr. Holger Schmidt
holger.schmidt004[at]fh-dortmund.de

Fachhochschule Dortmund
Fachbereich Informatik
Professur für IT-Sicherheit, Informatik

Themen & Lernziele

Themen

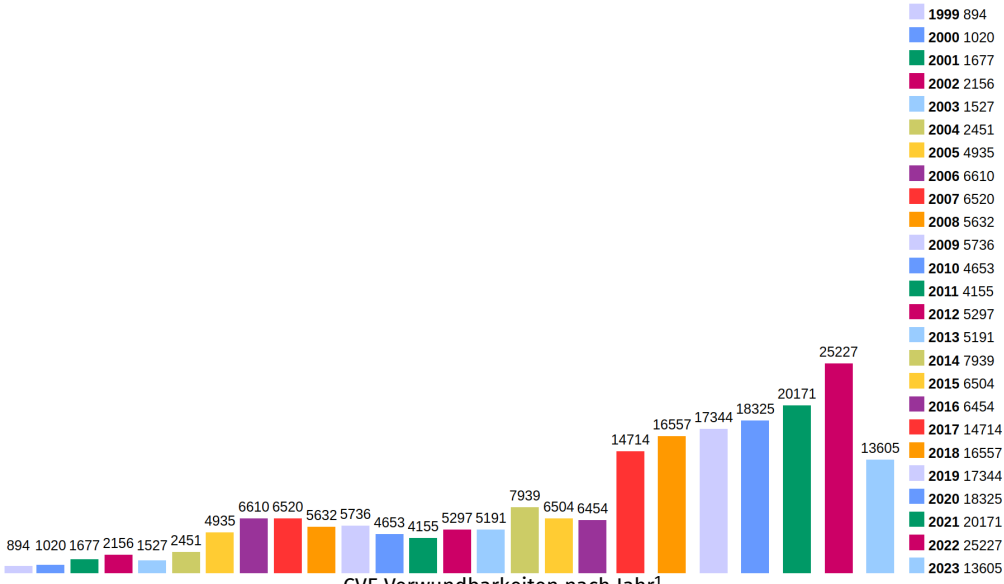
- Standards und Best Practices
- OWASP Top 10
- OWASP Software Assurance Maturity Model (SAMM)
- OWASP Application Security Verification Standard (ASVS)
- OWASP Testing Project

Lernziele

Die Studierenden sind in der Lage,

- die Organisation von OWASP Best Practices als Projekte zu verstehen.
- ausgewählte OWASP Projekte zu beschreiben.

Motivation I



[1] https://www.cvedetails.com/browse-by-date.php, aufgerufen am 28. Juni 2023

Motivation II

Eine Einschätzung von Datadog[2].

- Je mehr Abhängigkeiten, desto höher das Risiko.
- Mit Java, .NET, Node.JS, Python, PHP ist ein erhöhtes Risiko verbunden.
- (Ur)alte Verwundbarkeiten tauchen in neuen Anwendungen auf (z. B. SQL Injection).

Obwohl:

- Nur ein geringer Anteil entdeckter Verwundbarkeiten muss behandelt werden.
- Das Angriffsgeschehen ist weitgehend ungezielt.

[2] https://www.datadoghq.com/state-of-application-security/, aufgerufen am 28. Juni 2023

Übersicht Sicherheitsmaßnahmen

- **Body of Knowledge** Ansätze
- Gesamter **Software Lebenszyklus** adressiert, z. B.
  - Erhebung und Analyse von **Sicherheitsanforderungen**
  - **Auditierung** (z. B. Design Review, Code Review)
  - **Pentesting** mit Software-Werkzeugen
- **Ausbildung**

Standards & Best Practices

- NIST, z. B. Secure Software Development Framework (SSDF) (NIST SP 800-218, 2022)
- ISO, z. B. ISO/IEC 27034-1, 2011 (Application Security)
- Common Criteria aka ISO/IEC 15408:2022
- OWASP (Open Web Application Security Project)[3]
- Computer Emergency Response Team (CERT), z. B. SEI CERT Oracle Coding Standard for Java[4]

[3] https://www.owasp.org/, aufgerufen am 28. Juni 2023

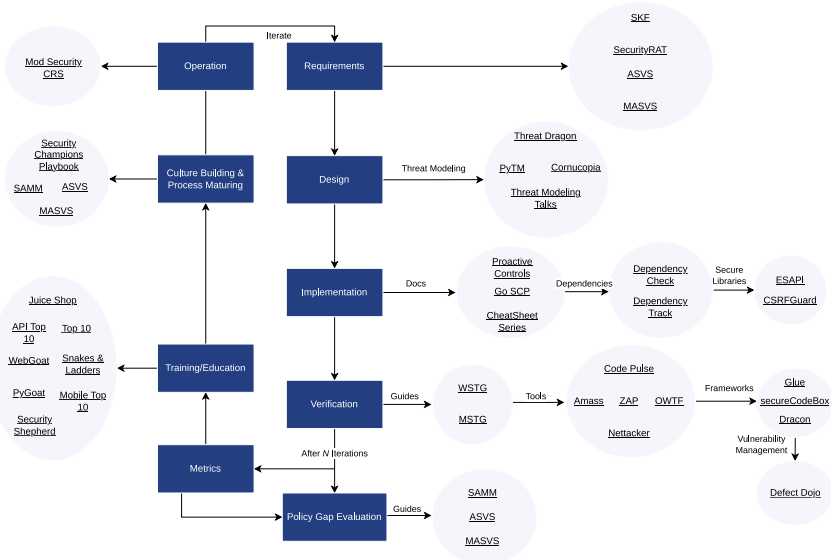
[4] https://wiki.sei.cmu.edu/confluence/display/java/SEI+CERT+Oracle+Coding+Standard+for+Java, aufgerufen am 28. Juni 2023

OWASP Projekte

Open Web Application Security Project (OWASP)

- https://www.owasp.org/, aufgerufen am 28. Juni 2023
- Stifung, frei, offen, nicht Profit-getrieben, **Entwickler-orientiert**
- Best Practices organisiert in **Projekten**
  - Reifegrade: **Flagship**, Production, Lab und Incubator
  - Standardisierte Organisation
  - Untereinander verknüpft
- Bücher, Tools, Cheatsheets, etc.

OWASP Projekte Übersicht



Application Security Wayfinder[5]

[5] https://owasp.org/projects/, aufgerufen am 28. Juni 2023

OWASP Top 10 I

- **Risikokategorien** basierend auf CWE
- Auswahl basierend auf **Umfrage** adressiert an Entwickler und Spezialisten für IT-Sicherheit von Anwendungen, **CVSS Werte** (insb. Exploit und Impact)
- Datensatz umfasst mehr als 500 000 betrachtete Anwendungen
- Nutzung für OWASP Software Assurance Maturity Model (SAMM) und OWASP Application Security Verification Standard (ASVS)

OWASP Top 10 II

A01 Broken Access Control

A02 Cryptographic Failures

A03 Injection

A04 Insecure Design

A05 Security Misconfiguration

OWASP Top 10 III

A06 Vulnerable and Outdated Components

A07 Identification and Authentication Failures

A08 Software and Data Integrity Failures

A09 Security Logging and Monitoring Failures

A10 Server Side Request Forgery (SSRF)

OWASP Software Assurance Maturity Model (SAMM) Project I

- https://owaspsamm.org/, aufgerufen am 28. Juni 2023
- Einrichtung oder Verbesserung eines **Modells für IT-Sicherheit von Anwendungen**
- Benchmarking
- **Ist- und Soll-Analysen**
- Drei Reifegrade: **Maturity Level (MR) 1-3**

OWASP Software Assurance Maturity Model (SAMM) Project II

Fachhochschule Dortmund
University of Applied Sciences and Arts

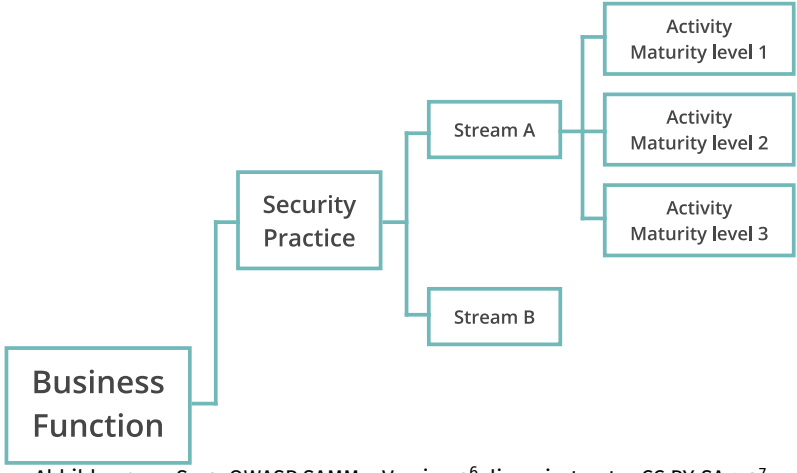


Abbildung aus S. 13, OWASP SAMM – Version 2[6], lizensiert unter CC BY-SA 4.0[7]

[6] https://drive.google.com/file/d/1cI3Qzfrly_X89z7StLWI5p_Jfqso-OZv/view?usp=sharing, aufgerufen am 28. Juni 2023

[7] https://creativecommons.org/licenses/by-sa/4.0/

OWASP SAMM Overview

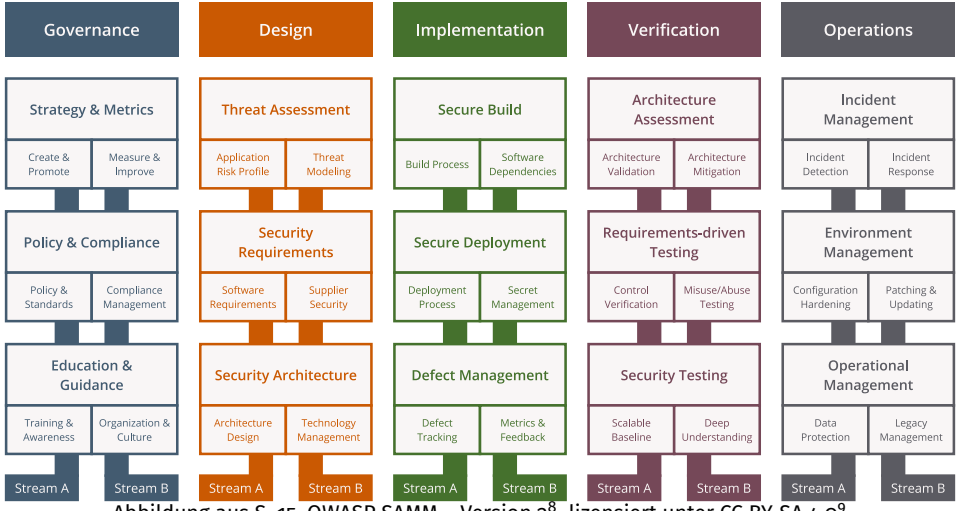


Abbildung aus S. 15, OWASP SAMM – Version 2[8], lizensiert unter CC BY-SA 4.0[9]

[8] https://drive.google.com/file/d/1cI3Qzfrly_X89z7StLWI5p_Jfqso-OZv/view?usp=sharing, aufgerufen am 28. Juni 2023

[9] https://creativecommons.org/licenses/by-sa/4.0/

OWASP SAMM Verification Overview

Fachhochschule Dortmund
University of Applied Sciences and Arts

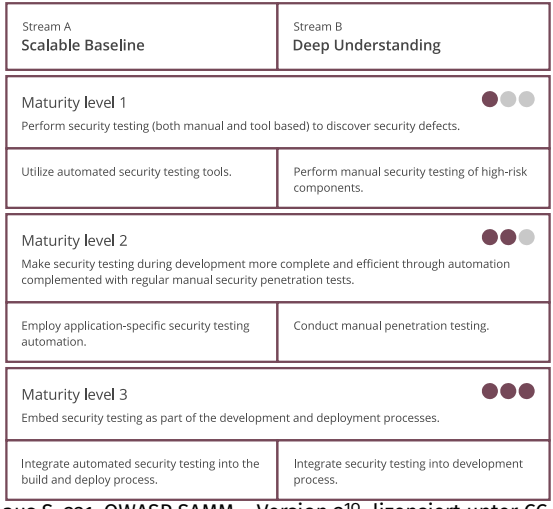


Abbildung aus S. 231, OWASP SAMM – Version 2[10], lizensiert unter CC BY-SA 4.0[11]

[10] https://drive.google.com/file/d/1cI3Qzfrly_X89z7StLWI5p_Jfqso-OZv/view?usp=sharing, aufgerufen am 28. Juni 2023

[11] https://creativecommons.org/licenses/by-sa/4.0/

OWASP Application Security Verification Standard (ASVS) Project I

- https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project, aufgerufen am 28. Juni 2023
- Anleitung, **Audit**, Metrik, Vertragsbasis
- **Anwendungskontext**: Finanzwesen, Gesundheitswesen, etc.
- **Anpassbarkeit**: Level 1-3 (gem. Anwendungsfall)
- **Umfang**: Architektur/Entwurf, **Authentisierung**, Sessions, Zugriffskontrolle, Ein-/Ausgabe, Fehlerbehandlung, Schutz persistierter Daten, Kommunikation, Konfiguration, Business Logik, Dateien, Web Dienste, Konfiguration, etc.

OWASP Application Security Verification Standard (ASVS) Project II

Fachhochschule Dortmund
University of Applied Sciences and Arts

#	Description	L1	L2	L3	CWE	NIST §
2.1.1	Verify that user set passwords are at least 12 characters in length (after multiple spaces are combined). (C6)	✓	✓	✓	521	5.1.1.2
2.1.2	Verify that passwords of at least 64 characters are permitted, and that passwords of more than 128 characters are denied. (C6)	✓	✓	✓	521	5.1.1.2
2.1.3	Verify that password truncation is not performed. However, consecutive multiple spaces may be replaced by a single space. (C6)	✓	✓	✓	521	5.1.1.2
2.1.4	Verify that any printable Unicode character, including language neutral characters such as spaces and Emojis are permitted in passwords.	✓	✓	✓	521	5.1.1.2
2.1.5	Verify users can change their password.	✓	✓	✓	620	5.1.1.2
2.1.6	Verify that password change functionality requires the user's current and new password.	✓	✓	✓	620	5.1.1.2

Abbildung aus S. 23, OWASP Application Security Verification Standard 4.0.3[12], lizensiert unter CC BY 3.0[13]

[12] https://github.com/OWASP/ASVS/raw/v4.0.3/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-en.pdf, aufgerufen am 28. Juni 2023

[13] https://creativecommons.org/licenses/by-sa/3.0/

OWASP Testing Project I

- https://www.owasp.org/index.php/OWASP_Testing_Project, aufgerufen am 28. Juni 2023
- Anleitung, **Testfälle**, Tools
- Umfang wie ASVS, z. B. „Testing for weak cryptography“

OWASP Testing Project II

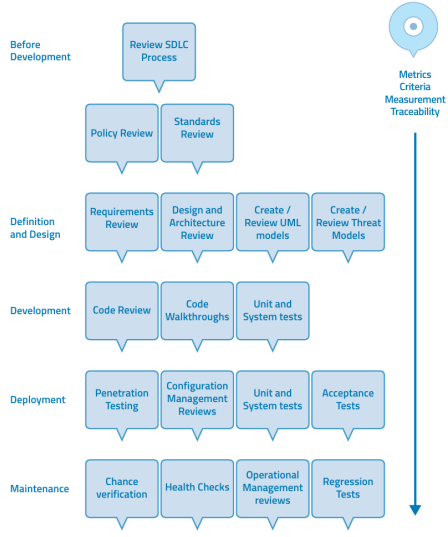


Abbildung aus S. 40, OWASP Testing Guide 4.2[14], lizensiert unter CC BY-SA 4.0[15]

[14] https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf, aufgerufen am 28. Juni 2023
[15] https://creativecommons.org/licenses/by-sa/4.0/

Zusammenfassung

Zusammenfassung

- Organisation von OWASP Best Practices als Projekte gelernt
- OWASP Top 10, SAMM, ASVS, Testing Projekt dargestellt

Weiterführende Literatur

Weiterführende Literatur

- OWASP Projekte
  - Juice Shop (https://owasp.org/www-project-juice-shop/, aufgerufen am 28. Juni 2023)
  - Cheat Sheets (https://cheatsheetseries.owasp.org/, aufgerufen am 28. Juni 2023)
  - Dependency-track (https://dependencytrack.org/, aufgerufen am 28. Juni 2023)
- *Application Security Program Handbook: A Guide for Software Engineers and Team Leaders* von Fisher (2022)

Literatur

- Fisher, D. (2022). *Application Security Program Handbook: A Guide for Software Engineers and Team Leaders*. Manning Publications. (Siehe S. 26).
- ISO/IEC 27034-1. (2011). ISO/IEC 27034-1: Information technology – Security techniques – Application Security. (Siehe S. 8).
- NIST SP 800-218. (2022). NIST Special Publication 800-218. Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf (siehe S. 8).