LU04a - OWASP

Quellen

- Wikipedia: OWASP
- OWASP-International
- OWAPS-TopTen
  - OWASP-TopTen 2017

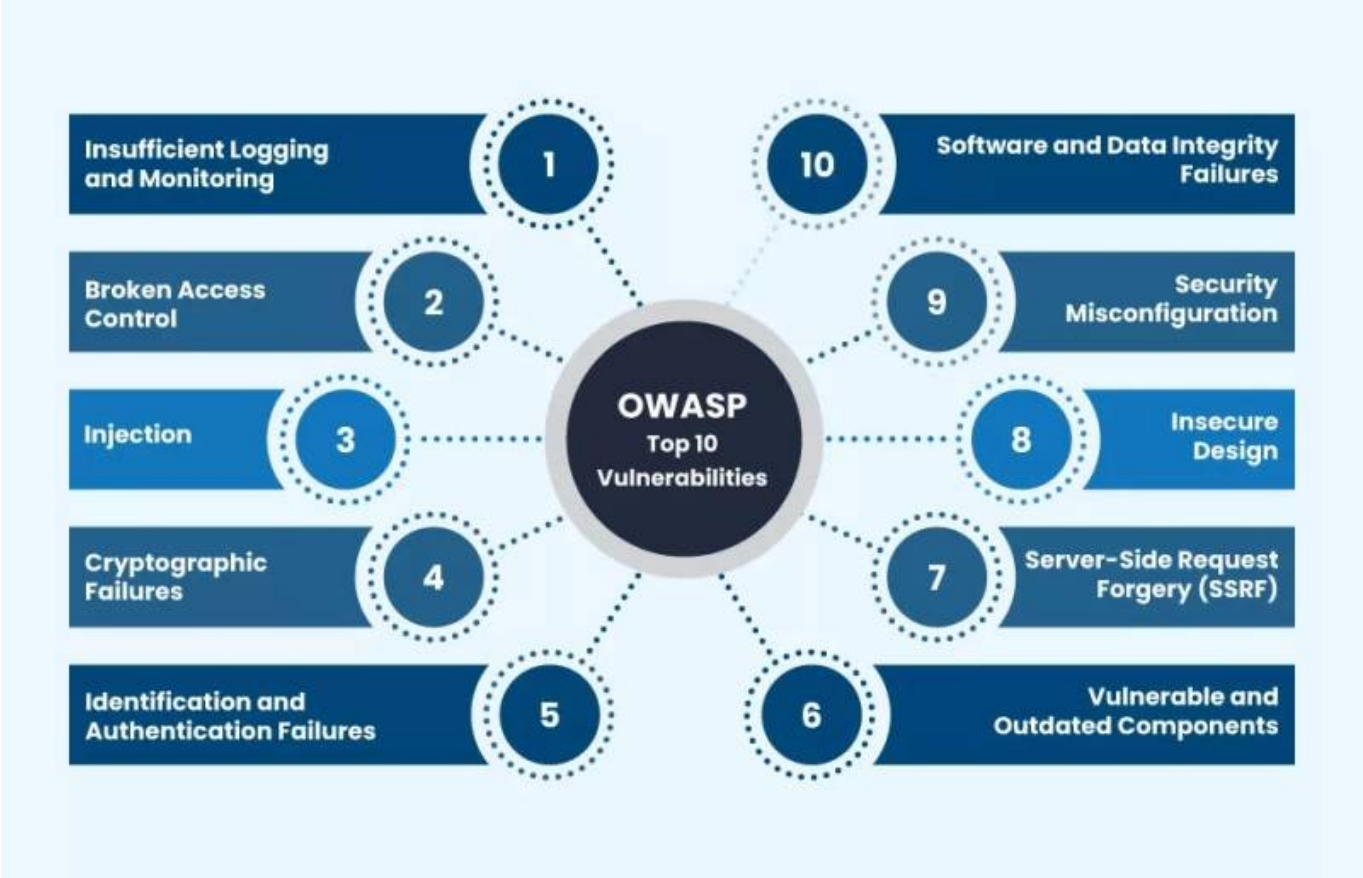
Lernziele

1. Das Akronym OWASP erklären können.
2. Erklären können was OWASP ist und die Zielsetzung beschreiben können.
3. Vorteile von OWASP aufzählen können.
4. Das Konzept des Risikorating erklären können.

OWASP in a nutshell

OWASP steht für **Open Worldwide Application Security Project** und ist eine internationale, gemeinnützige (Non-Profit) Organisation, die sich der Verbesserung der Sicherheit von Software verschrieben hat. Das Ziel: Entwickler, Unternehmen und Sicherheitsverantwortliche mit frei zugänglichen Informationen, Tools und Best Practices zu unterstützen – ganz ohne kommerzielle Interessen. OWASP ist besonders in der Webentwicklung bekannt, da es praktische Hilfen zur Identifikation und Absicherung von Sicherheitslücken bietet.

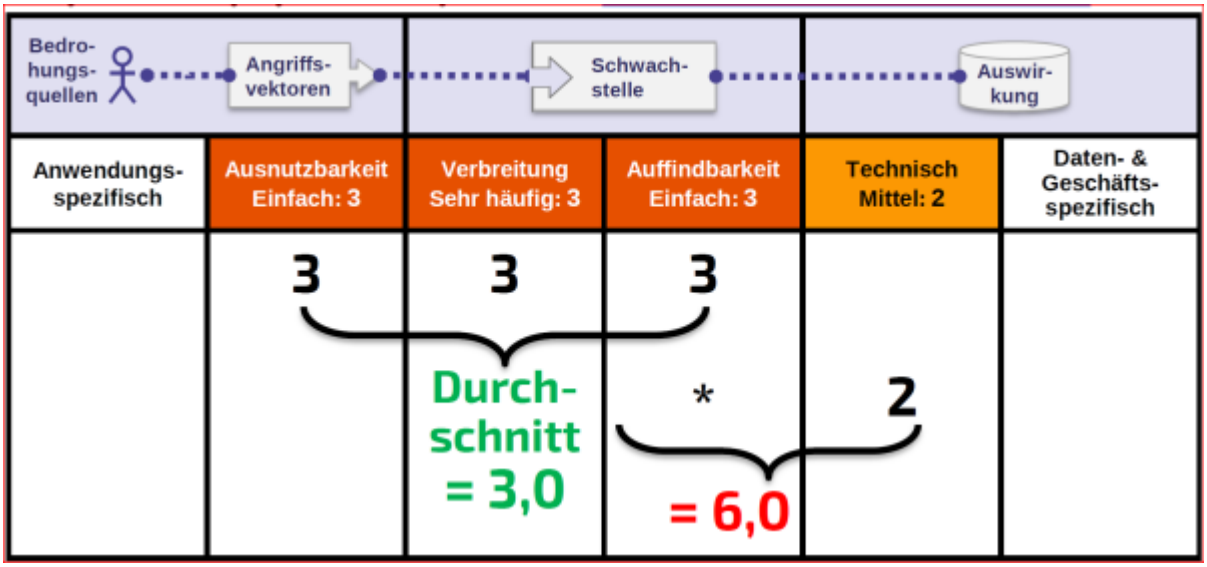
Das bekannteste Projekt ist die **OWASP Top 10**: eine regelmäßig aktualisierte Liste der zehn kritischsten Sicherheitsrisiken bei Webanwendungen, darunter Klassiker wie **Injection (z. B. SQL-Injection)**, **Broken Authentication**, **Security Misconfiguration** oder **Insecure Design**. Diese Liste dient als Referenz für Entwickler und Entscheidungsträger, um Schwachstellen frühzeitig zu erkennen und zu vermeiden.



Neben der Top 10 stellt OWASP viele weitere Projekte und Werkzeuge bereit, z. B. **ZAP (Zed Attack Proxy)** zur automatisierten Sicherheitsüberprüfung oder das **Cheat Sheet Series**, eine Sammlung kompakter Empfehlungen zu sicheren Entwicklungspraktiken.

OWASP fördert auch den Austausch in der Community: In lokalen Chapters, auf Konferenzen und über Online-Plattformen werden Erfahrungen geteilt und Sicherheitswissen verbreitet – für alle offen, die Software ein kleines bisschen weniger angreifbar machen wollen.

Risikoanalyse nach OWASP Risk-Rating-Methode



Die Risikoanalyse der OWASP Top 10 basiert auf der **OWASP Risk-Rating-Methode**. Ziel ist es,

Schwachstellen danach zu bewerten, welches Risiko sie für eine typische Webanwendung darstellen. Dabei werden **Wahrscheinlichkeit** (z. B. Verbreitung, Ausnutzbarkeit, Auffindbarkeit) und **Auswirkungen** (z. B. technische oder geschäftliche Folgen) berücksichtigt.

Die Methode ist **anwendungsspezifisch unabhängig**, also eher allgemein gehalten. Sie beurteilt nicht, wie stark eine konkrete Anwendung gefährdet ist, sondern bewertet Schwachstellen allgemein, um Sicherheitsbewusstsein zu schaffen.

Die Risikobewertung erfolgt auf Basis von vier Faktoren:

1. **Ausnutzbarkeit**
2. **Verbreitung**
3. **Auffindbarkeit**
4. **Technische Auswirkungen**

Jeder dieser Faktoren wird auf einer Skala von 1 (niedrig) bis 3 (hoch) bewertet. Daraus ergibt sich ein Risiko-Wert:

- **Durchschnitt der drei Wahrscheinlichkeits-Faktoren**
- Multipliziert mit dem Wert für die Auswirkungen

Beispiel:

- Ausnutzbarkeit = 3, Verbreitung = 3, Auffindbarkeit = 3 → Durchschnitt = 3
- Technische Auswirkung = 2
- **Risiko = 3 × 2 = 6**

Wichtig: Diese Methode **berücksichtigt keine Bedrohungsquellen oder konkreten Unternehmenskontexte**. Sie dient ausschließlich zur generellen Einstufung von Risiken – nicht zur Anwendung individueller Sicherheitsbewertungen.

OWASP-Risiko-Rating 2017

RISIKO	Bedrohungsquellen	Angriffsvektoren: Ausnutzbarkeit	Schwachstelle: Verbreitung	Schwachstelle: Auffindbarkeit	Auswirkung: Technisch	Auswirkung: Geschäftl.	Wert
A1:2017-Injection	Anwendungs-spezifisch	Einfach: 3	Häufig: 2	Einfach: 3	Schwerwiegend: 3	Daten- & Geschäfts-spezifisch	8,0
A2:2017-Fehler in Authentifizierung		Einfach: 3	Häufig: 2	Durchschnittlich: 2	Schwerwiegend: 3		7,0
A3:2017-Verlust der Vertr. Sens. Daten		Durchschnittlich: 2	Sehr häufig: 3	Durchschnittlich: 2	Schwerwiegend: 3		7,0
A4:2017-XML External Entities (XXE)		Durchschnittlich: 2	Häufig: 2	Einfach: 3	Schwerwiegend: 3		7,0
A5:2017-Fehler in der Zugriffskontrolle		Durchschnittlich: 2	Häufig: 2	Durchschnittlich: 2	Schwerwiegend: 3		6,0
A6:2017-Sicherh.rel. Fehlkonfiguration		Einfach: 3	Sehr häufig: 3	Einfach: 3	Mittel: 2		6,0
A7:2017-Cross-Site Scripting (XSS)		Einfach: 3	Sehr häufig: 3	Einfach: 3	Mittel: 2		6,0
A8:2017-Unsichere Deserialisierung		Schwierig: 1	Häufig: 2	Durchschnittlich: 2	Schwerwiegend: 3		5,0
A9:2017-Komp. mit bek. Schwachstellen		Durchschnittlich: 2	Sehr häufig: 3	Durchschnittlich: 2	Mittel: 2		4,7
A10:2017-Unzureich. Logging&Monitoring		Durchschnittlich: 2	Sehr häufig: 3	Schwierig: 1	Mittel: 2		4,0