

OWASP Top Ten Project (Gruppenarbeit)

Rahmenbedingungen:

Das *Open Web Application Security Project* (OWASP) ist eine weltweite non-Profit Organisation, die sich zum Ziel setzt, Qualität und Sicherheit von Software zu verbessern. Es ist das Ziel, Entwickler, Designer, Softwarearchitekten für potenzielle Schwachstellen zu sensibilisieren und aufzuzeigen, wie sich diese vermeiden lassen. Die folgenden „OWASP Top Ten“ stellen unter Web-Sicherheitsexperten einen anerkannten Konsens dar, was die derzeit kritischen Lücken in Web-Anwendungen betrifft (stand 2021):

- A01:2021 – Broken Access Control
- A02:2021 – Cryptographic Failures
- A03:2021 – Injection
- A04:2021 – Insecure Design
- A05:2021 – Security Misconfiguration
- A06:2021 – Vulnerable and Outdated Components
- A07:2021 – Identification and Authentication Failures
- A08:2021 – Software and Data Integrity Failures
- A09:2021 – Security Logging and Monitoring Failures
- A10:2021 – Server-Side Request Forgery (SSRF)

Auftrag:

- a) Wählen Sie OWASP Top 10 Themen aus (Anzahl Gruppenmitglieder = Anzahl zu wählender Themen), die Sie in diesem Auftrag bearbeiten möchten (jedes Thema muss von der Klasse **mind. einmal ausgearbeitet werden!**)
- b) Analysieren Sie die ausgewählten Themen mit Hilfe der OWASP-Seite <https://owasp.org/Top10/> (und allfälligen weiterführenden Quellen / Internetrecherche)
- c) Erklären Sie in eigenen Worten, was sich hinter der Abkürzung CWE versteckt und wie CWE mit den OWASP Top 10 zusammenhängen.
- d) Beschreiben Sie den Unterschied der OWASP Top 10 Risk und OWASP Proactive Control (<https://owasp.org/www-project-proactive-controls/>)
- e) Die ausgewählten Themen werden wie folgt ausgearbeitet:
 - Beschreibung der theoretischen Hintergründe und der Bedrohung sowie mögliche Folgen
 - Schwachstelle mit konkretem Codebeispiel vorstellen und erläutern
 - Massnahme wie die Sicherheitslücke geschlossen werden kann, an einem konkreten Codebeispiel
 - Abgabe von **Dokumentation und Code Beispiele** via Teams-Aufgabe

Inhalt der Dokumentation

- Überblick
- Erläuterungen zu Aufgabe c) und d)
- Theoretische Hintergründe
- Schwachstelle mit Codebeispiel
- Massnahme mit Codebeispiel

- Resultate, Erkenntnisse
- Hinweise auf weitere Unterlagen, Übungen, Tutorien (inkl. **verwendeter Quellen**)

Zeitraahmen:

Als Vorbereitung stehen 7 Lektionen während der Schule zur Verfügung. Die Vorstellung soll die Problemstellung (Angriffspunkt, Auswirkung, Technologie) und Lösung (Technologie und sinnvolle Gegenmassnahmen) anhand von praktischen Beispielen (Live Demo der Codebeispiele – keine PowerPoint), aufzeigen. Die Live Demo darf pro Thema maximal 7 Min dauern und ist in Standardsprache zu halten.

Resultat:

- Vollständiger schriftlicher Theorie Teil mit praktischen Code Beispielen.
- Live Demo anhand von Beispielen von Sicherheitslücken und geeignete OWASP Gegenmassnahmen.

Termin:

Abgabe Dokumentation und Code: vor dem 03.03.2025 08:00 Uhr

Präsentation Live Demo: 03.03.2025 oder 10.03.2025 (gemäss Einteilung in Excel)

Bewertung:

Die Bewertung erfolgt gemäss dem folgenden Bewertungsraster:

Präsentation	Bemerkungen		Beurteilung
Einführung, Ablauf			
Arbeit wird verständlich vorgestellt			
Sicherheitsprobleme gut erklärt			
interessant und lehrreich			
Regeln der Präsentation eingehalten			
Kompetenz ist erkennbar			
Inhalt der Gruppenarbeit	Beurteilung		
Überblick			
Auftrag c)			
Auftrag d)			
Beschreibung der theoretischen Hintergründe			
Beschreibung des Demo-Codes (der Demo Applikation bzw. des Demo Setup)			
Massnahmen zur Verbesserung			
Erkenntnisse, Empfehlungen			
Quellen			