LB1: OWASP Top Ten Project (Gruppenarbeit)

Rahmenbedingungen

Das Open Web Applicaiton 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 aner-kannten 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- A06:2021 – Vulnerable and Outdated Components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

1. Die 2-Gruppen wurden bereits von der Lehrperson erstellt mit Hilfe von Zufallszahlen.
2. Analysieren Sie die ausgewählten Themen mit Hilfe der OWASP-Seite https://owasp.org/Top10/ (und allfälligen weiterführenden Quellen / Internetrecherche)
3. Erklären Sie in eigenen Worten, was sich hinter der Abkürzung CWE versteckt und wie CWE mit den OWASP Top 10 zusammenhängen.
4. Beschreiben Sie den Unterschied der OWASP Top 10 Risk und OWASP Proactive Controls (https://owasp.org/www-project-proactive-controls/)
5. 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 3 und 4

- Theoretische Hintergründe
- Schwachstelle mit Codebeispiel
- Massnahme mit Codebeispiel
- Resultate, Erkenntnisse
- Hinweise auf weitere Unterlagen, Übungen, Tutorien (inkl. **verwendeter Quellen**)

Zeitrahmen

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.

Termine, Abgabe und Bewertung

Die konkreten Termine und Abgabemodalitäten werden durch die Lehrperson für jede Moduldurchführung individuell festgelegt und entsprechend kommuniziert.

Es gilt für die Bewertung folgendes 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 3 (Beschreibung von CWE)		
Auftrag 4 (OWASP Risk vs Proactive Controls)		
Beschreibung der theoretischen Hintergründe		
Beschreibung des Demo-Codes (der Demo Applikation bzw. des Demo Setup)		
Massnahmen zur Verbesserung		
Erkenntnisse, Empfehlungen		
Quellen		
Allgemeiner Eindruck		**Beurteilung**