Projektarbeit (Gruppenarbeit)

OWASP Top Ten Project

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 potentielle 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:

The OWASP Top 10 Web Application Security Risks for 2017 are:

- A1: Injection
- A2: Broken Authentication and Session Management
- A3: Sensitive Data Exposure
- A4: XML External Entity (XXE)
- A5: Broken Acess Control
- A6: Security Misconfiguration
- A7: Cross-Site Scripting (XSS)
- A8: Insecure Deserialization
- A9: Using Components with Know Vulnerabilities (verletzlich, anfällig)
- A10: Insufficient Logging & Monitoring

Auftrag:

a) Erstellen sie eine Tabelle worin die Veränderungen der Top 10 Risiken von 2013 zu 2017 aufzeigt und beschreiben sie die Veränderungen in kurzen Sätzen.

b) Wählen Sie innerhalb Ihres Teams eines von diesen *Security Risks* aus, das Sie bearbeiten werden.

- Beschreibung der Bedrohung und mögliche Folgen dieser Bedrohungsart (kurze Präsentation)
- Schwachstelle mit konkretem Codebeispiel vorstellen und erläutern (Problem aufzeigen)
- Massnahme wie die Sicherheitslücke geschlossen werden kann, Methoden und an einem konkreten Codebeispiel
- Abgabe der Präsentation und Code Beispiele auf BSCW

Inhalt der Gruppenarbeit

- Überblick
- Vorstellung der Aufgabenstellung
- Theoretische Hintergründe
- Schwachstelle mit Codebeispiel
- Massnahme mit Codebeispiel
- Resultate, Erkenntnisse
- Hinweise auf weitere Unterlagen, Übungen, Tutorien
- Quellen

Zeitrahmen:

Als Vorbereitung stehen 4 Lektionen während der Schule zur Verfügung.
Die Vorstellung soll max. 7 Minuten dauern jedoch Problemstellung und Lösung anhand von praktischen Beispielen (Demo) aufzeigen.

Resultat:

- Vollständige schriftliche Theorie Teil mit praktischen Code Beispielen.
- Präsentation

Termin:

Abgabe und Präsentation gemäss Angabe LP

Bewertung:

Die Bewertung erfolgt gemäss: Bewertung_Arbeit.pdf

D. A. Waldvogel, 17.08.17