Hacker greifen an! – Referat zu Web-Bedrohungen

Öffentliche Web-Applikationen sind täglich zahlreichen Hacker-Angriffen ausgesetzt. Es existieren zahlreiche Bedrohungsszenarien und Gegenmassnahmen gegen diese. Web-Entwickler müssen diese Bedrohungen kennen und Gegenmassnahmen vorsehen können.

Aufgabe

Sie recherchieren selbständig **eines** der folgenden Themen zu Web-Bedrohungen. Sie erarbeiten eine **Präsentation** und ein **Handout/Merkblatt** zu einer spezifischen Bedrohung im Web-Umfeld. Das Thema wird ausgelost:

- SQL-Injection
- Cross Site Scripting (XSS)
- Session Hijacking
- Directory Traversal Attack
- Cross Site Request Forgery (CSRF)
- Brute Force Attacks

Die Präsentation soll eine Einführung zum Thema und eine praktische Vorführung (Live-Demo) umfassen. Das Handout fasst die Bedrohung und mögliche Schutzmassnahmen zusammen.

Präsentation

- Umfang: 10-15 Minuten Vortrag zum Thema, 5 Min Live-Demo (Total 15-20min)
- Vortrag: Beschreibung der Problematik / der Bedrohung, mögliche Schutzmassnahmen
- Live-Demo: Zeigt den Angriff «in Aktion» sowie die funktionierende Schutzmassnahme dazu

Handout/Merkblatt

Das Handout ist ein 2-3-seitiges PDF mit folgenden Themen:

- Beschreibung der Bedrohung, wenn notwendig mit Grafik
- Beschreibung der möglichen Schutzmassnahmen, wenn notwendig mit Grafik
- Beispiel sowohl des Angriffs wie auch der Schutzmassnahme (als Programmcode und/oder mit Screenshots illustriert)

Bewertung

Dieses Referat zählt **mit 20% zur Gesamtmodulnote.**

Präsentation und Demo (8 Pt.)

- Das Bedrohungsszenario wurde technisch korrekt erläutert (1)
- Mind. 1 mögliche Schutzmassnahme wurde technisch korrekt erläutert (1)
- Klare Sprache, verständliche Ausdrucksweise, Nervosität im Griff (1)
- Sinnvoller Einsatz von Hilfsmitteln / Medien (1)
- Demo: Der Kandidat kann die Anwendung der Bedrohung demonstrieren (1)
- Demo: Der Kandidat kann die Schutzmassnahme demonstrieren (1)
- Demo: Die Demo ist gut vorbereitet und kann flüssig durchgeführt werden (1)
- Die vorgegebene Zeit wurde eingehalten (1)

Handout (8Pt.)

- Das Handout hält den vorgegebenen Rahmen ein (Anz. Seiten, Themen) (1)
- Das Handout ist sauber, fehlerfrei und übersichtlich gestaltet (1)
- Das Handout erklärt das Bedrohungsszenario korrekt (1)
- Das Handout erklärt die mögliche(n) Schutzmassnahme(n) korrekt (1)
- Das Handout zeigt ein Code-Beispiel und / oder Screenshot des Angriffsszenarios (2)
- Das Handout zeigt ein Code-Beispiel für die Schutzmassnahme (2)