M183 Applikationssicherheit implementieren

Applikationen sicher planen, entwickeln und in Betrieb nehmen.

Inhalt

- Modulidentifikation
- Prüfungen und Noten
- Organisatorisches und Administratives

Modulidentifikation

Handlungsziele und *handlungsnotwendige Kenntnisse* des Modul 183

Handlungsziel 1

Aktuelle Bedrohungen erkennen und erläutern können. **Aktuelle Informationen zum Thema beschaffen** und mögliche Auswirkungen aufzeigen und erklären können.

- Kennt **Informationsquellen** zu aktuellen Bedrohungen.
- Kennt **Sicherheitslücken und mögliche Folgen** von Angriffen.

Handlungsziel 2

Sicherheitslücken und ihre Ursachen in einer Applikation erkennen können. Gegenmassnahmen vorschlagen und implementieren können.

- Kennt mögliche **Ursachen** von Sicherheitslücken in Applikationen.
- Kennt ein Vorgehen zur **Identifikation** von Sicherheitslücken in Applikationen.
- Kennt geeignete **Gegenmassnahmen** zu den verschiedenen Kategorien von Bedrohungen und wie diese implementiert werden.

Handlungsziel 3

Mechanismen für die **Authentifizierung und Autorisierung** umsetzen können.

- Kennt **Authentifizierungsmechanismen** und deren Funktionsweise.
- Kennt **Verschlüsselungsmechanismen** und deren Einbindung in der Applikation.
- Kennt verschiedene Verfahren zur **Zugriffssteuerung**.

Handlungsziel 4

Sicherheitsrelevante Aspekte bei **Entwurf, Implementierung und Inbetriebnahme** berücksichtigen.

- Kennt sicherheitsrelevante Aspekte beim Entwurf von Applikationen.
- Kennt Techniken bei der Realisierung zur **Vermeidung von Sicherheitslücken** (z.B. Input-/Output-Validierung, Defensives Programmieren, Session-Management, Error Handling)

Handlungsziel 5

Informationen für **Auditing und Logging** generieren. Auswertungen und Alarme definieren und implementieren.

- Kennt Sinn, Aufbau und Inhalt eines **Logs**.
- Kennt Sinn, Aufbau und Inhalt eines **Audit-Trails**.
- Kennt mögliche Formen der **Alarmierung** und Regeln für eine Alarmauslösung.

Unterlagen und Arbeitsformen

- Alle Unterlagen sind/werden in elektronischer Form zur Verfügung gestellt
- Praktische Arbeiten (Praxisarbeiten und praktische Prüfung) erfolgen über Git
- Skript: Umfangreich und relevant (!)
- Typischer Lektionsablauf:
  1. Repetition / Besprechung Aufgaben
  2. Input mit neuen Inhalten
  3. Vertiefung und Aufgaben
- Prüfungen...

Schlagworte M183

- Verschlüsselungsverfahren
- Input Validation
- Multifactor Authentication
- Sessions
- Cross-Site-Scripting (XSS)
- Cross-Site-Request-Forgery (CSRF)
- Injections
- URL-Guessing
- Data Access
- Password Hashing, Rainbow Tables, Brute-Force
- Monitoring, Logging
- Intrusion Detection and Prevention
- ...

Anmerkungen

Das Modul 183 enthält (bewusst) viele Inhalte und Konzepte aus anderen Modulen. Als "*Abschlussmodul*" können hier viele Grundlagen aufgezeigt, zusammengefasst und end-to-end umgesetzt werden.

Das Modul 183 lebt von der Aktualität und ihren eigenen Beteiligung. **Bringen Sie sich aktiv ein - fordern und fördern Sie relevante, aktuelle Beiträge!**

Organisatorisches und Administratives

Die praktischen Inhalte dieses Moduls (Ubungen, praktische Prüfung) werden über ein Git-Repository abgewickelt.

1. Erstellen Sie auf *Gitlab* (gitlab.com) ein **privates** Repository
2. Fügen Sie (nur) den Benutzer **GIPE** (peter.gisler@gibz.ch) mit der Rolle **Reporter** zu diesem Repository hinzu
3. Fügen Sie zum soeben erstellten Repository eine Datei **`README.md`** hinzu (Inhalt: mindestens ihr vollständiger Name)
4. Tragen Sie die URL zum Repository im entsprechenden Forum auf Moodle ein