

## t.SSI - Software-Sicherheit

---

**Kursverantwortung:** Marc Rennhard, rema  
**verantwortliche OE:**  
**ECTS:** 4  
**Schuljahr:** 2012/2013  
**Zuletzt gespeichert:** 22.01.2013 17:27

---

### Fachkompetenz:

-

---

### Methodenkompetenz:

-

---

### Sozialkompetenz:

-

---

### Selbstkompetenz:

-

---

### Lernziel:

Die Studierenden erhalten eine fundierte Einführung in die Software-Sicherheit. Die Schwerpunkte liegen dabei in den Bereichen "Sicherer Softwareentwicklungsprozess", "Testen von Software und Systemen hinsichtlich Sicherheit" und "Sicheres Programmieren am Beispiel Java". Nach erfolgreichem Absolvieren des Moduls können die Studierenden folgendes:

- Sie wissen und verstehen, was man bei der sicheren Softwareentwicklung grundsätzlich beachten muss.
  - Sie können die Prinzipien der sicheren Softwareentwicklung auf einen beliebigen Softwareentwicklungsprozess anwenden, so dass dieser zum sicheren Entwicklungsprozess wird.
  - Sie können Applikation und Systeme durch Verwendung geeigneter Methoden und Tools hinsichtlich Sicherheit testen und gefundene Schwachstellen auch ausnutzen.
  - Sie kennen typische, sicherheitsrelevante Programmierfehler, die oft gemacht werden, und wissen, wie Sie diese in Ihren Programmen verhindern können.
  - Sie können sichere Java Applikationen (mit einem Fokus auf Java EE Webapplikationen) entwickeln und setzen dabei die von Java gebotenen Sicherheitsfeatures und Security Libraries zweckmässig ein.
- 

### Lerninhalt:

Vorlesung:

Sicherer Software-Entwicklungsprozess (10 Lektionen)

- Einführung in die Software-Sicherheit
  - Der Secure Development Lifecycle
  - Security Design Principles / Controls
-

- Security Requirements Engineering und Threat Modeling
- Security Risk Analysis

Security-Testing (6 Lektionen)

- Aufspüren und Ausnutzen von Schwachstellen in Webapplikationen
- Security-Testing Tools: Static Code Analysis und Schwachstellenscanner
- Penetration Testing

Sicheres Programmieren mit einem Fokus auf Java (12 Lektionen)

- Typische Programmierfehler (Buffer-Overflows, Race Conditions...)
- Java Security Libraries (JCA, JCE, JSSE)
- Sichere Programmierung von Webapplikationen in Java (Input Validation, Access Control...)

Praktikum:

Es werden praktische Aufgabenstellungen zu allen wichtigen Hauptthemen der Vorlesung durchgeführt. Die Aufgaben sind ein Mix aus den Bereichen Security-Analysis, Security-Design, Security-Testing und sicherer Implementierung.

**Vorkenntnisse:**

SWE (Software Engineering) und ISI (Internet-Sicherheit) empfohlen

**Durchführung:**

Unterrichtsart	Anzahl Lektionen pro Woche
Vorlesung	14*2
Übung/Praktika	14*2
Blockunterricht	

**Leistungsnachweise:**

Laut Tabelle oder gemäss schriftlicher Festlegung des Dozierenden zu Semesterbeginn!

Bezeichnung	Art	Form	Umfang	Bewertung	Gewichtung
Leistungsnachweise während Unterrichtszeit	Bewertete Praktika	Schriftlich und mündlich	Alle Praktika	Punkte, die zur Punktzahl der Schlussprüfung addiert werden	20%
Semesterendprüfung	Prüfung	Schriftlich	90 Minuten	Note	80%

**Unterrichtssprache:**

Deutsch

**Unterrichtsunterlagen:**

Vorlesungsfolien mit zusätzlichen Kommentaren

**Ergänzende Literatur:**

-

**Bemerkungen:**

-