| **Modul PSI-ProjectPAD Project Practical Attacks and Defenses**<br>*Project Practical Attacks and Defenses* | 6 ECTS / 180 h |
|---|---|
| (seit SS18)<br>Modulverantwortliche/r: Prof. Dr. Dominik Herrmann | |

**Inhalte:**

Breaking into information systems is exciting, but impractical due to ethical and legal concerns. However, offensive competences and adversarial thinking are essential to build secure systems. In this project students will get the opportunity to acquire practical security skills in a dedicated training environment.

The goal of this project is to build and extend the "Insekta" platform. This web-based tool provides a frontend for virtual machines that can be used to study selected topics in security and privacy on one's own and at one's own pace.

This project is offered together with PSI-ProjectCAD-M, which focuses on conceptually more complex attacks and defenses.

The participants of the project familiarize themselves with security weaknesses in information systems and apply this knowledge to develop vulnerable services which others can use for training. To this end, participants form groups, read about attacks and defenses in textbooks and research papers, and discuss various options to implement them. Instructors will provide extensive and on-demand support to enable the participants to implement a vulnerable service that can be exploited to learn about a particular vulnerability.

Besides implementing vulnerable services, the participants prepare training materials, which consist of questions and tasks to test one's knowledge as well as step-by-step instructions. These training materials may also contain interactive elements for an improved learning experience.

The project also takes into account attacks on privacy, e.g., re-identifying individuals in anonymized datasets and communication networks, tracking users on the Internet, inferring sensitive attributes from seemingly harmless data traces, as well as mitigations, e.g., depersonalization strategies and differential privacy mechanisms. Here, practical activities consist in the preparation of datasets and scripts for analysis.

**Lernziele/Kompetenzen:**

Successful students will be able to describe attacks and defenses from textbooks and research papers in easily understandable form. They will also be able to carry out selected attacks in practice and implement defenses with a programming language of their choice.

**Sonstige Informationen:**

This project is taught in English, unless all participants are fluent in German. The workload of this project is equivalent to 180 hours.

Workload breakdown:

- 10 hrs: Getting familiar with the platform
- 30 hrs: Reading papers and researching security vulnerabilities
- 15 hrs: Preparing the talk (including time for attendance of other talks)
- 70 hrs: Implementing the vulnerable service and defenses
- 55 hrs: Writing training material and documentation

Note that there is another project (PSI-ProjectCAD-M) with a workload equivalent to 270 hours.

**Zulassungsvoraussetzung für die Belegung des Moduls:**
keine

**Empfohlene Vorkenntnisse:**
Students in bachelor and master programs can participate in this project.

Participants should be familiar with basic concepts in information security and privacy, which can be acquired, for instance, by taking the module "Introduction to Security and Privacy" (PSI-IntroSP-B). This includes basic knowledge about the commonly used security terminology, common types of malware and attacks, buffer overflows and related attacks, cryptography, network security, web security, and concepts of privacy.

Moreover, participants should have practical experience with at least one scripting or programming language such as Python or Java. Experience with Linux environments, web technologies, and network protocols is recommended.

**Besondere Bestehensvoraussetzungen:**
keine

| **Angebotshäufigkeit:** WS, SS | **Empfohlenes Fachsemester:** | **Minimale Dauer des Moduls:** 1 Semester |
|---|---|---|

**Lehrveranstaltungen**

**Project Practical Attacks and Defenses** — **4,00 SWS**
**Lehrformen:** Übung
**Sprache:** Englisch/Deutsch
**Angebotshäufigkeit:** WS, SS

**Lernziele:**
cf. module description

**Inhalte:**
Potential topics include:

- web security (injection flaws and other issues mentioned in the OWASP Top 10)
- network security (such as DNS cache poisoning and rebinding attacks)
- security issues in C programs (buffer overflows, etc.)
- cryptography (low-level attacks on ciphers, high-level attacks on protocols, e.g., TLS)
- business logic failures
- misconfigurations
- attacks on availability (denial of service)
- attacks on privacy (such as inference, tracking, re-identification, fingerprinting)
- privacy defenses (such as k-anonymity, related concepts, differential privacy)

**Literatur:**
Literature will be announced at the beginning of the project.

| | |
|---|---|
| **Prüfung**<br>Hausarbeit mit Kolloquium / Prüfungsdauer: 30 Minuten<br>Bearbeitungsfrist: 3 Monate<br>**Zulassungsvoraussetzung zur Modulprüfung:**<br>Regular attendance at project meetings.<br>**zentral organisiert: nein**<br>**Beschreibung:**<br>The module examination consists of two parts: Firstly, the participants submit a written report (in English) that includes the source code of the vulnerable service and the training material. Secondly, the participants give a talk in which they defend their work (in English; in German if all participants are fluent in German) by presenting theoretical and practical aspects of their vulnerable service as well as relevant mitigations. The maximum number of points that can be achieved in the module examination is 100.<br><br>Optionally, participants can submit intermediary results (in English) to collect up to 20 bonus points. If the module examination is passed on its own (generally, this is the case when at least 50 points are obtained), the bonus points will be added to the points achieved in the module examination. The grade 1.0 can be achieved without the bonus points. Details regarding the number of optional submissions during the semester, their type, the points per submission, and the respective deadlines will be announced in the first session of the project. | |