What we offer

▶ Exploiting buggy Web Applications in CTF style
▶ Real world application: Artemis
What you should bring

- Java, Javascript, PHP, SQL
- Necessary? You can learn it on the way if you are disciplined
- **Willingness to work and learn a lot**
Process

Phase I (≈10 weeks):
- “Usual” practical course (weekly meetings and assignments)

Phase II (≈4 weeks):
- Final project (short paper and presentation)
Process — Phase I

- **Teams of two**
- Every week: Introduction to a new topic
  - Submission of solutions until the following week **before** the meeting
  - Private explanation of solution during the meeting
Contents

- Injection vulnerabilities
- XSS, CSRF, sandbox escaping
- Include attacks
- Cryptographic attacks
- Upload attacks
- Configuration vulnerabilities
- Advanced bugs
- ... own suggestions?
Process — Phase II

Final project

▷ **Real world application** of the knowledge gained
▷ **Specialisation** in one/two topics
▷ Security analysis of **Artemis**
▷ Short paper (about 5 pages)
▷ **Presentation** (about 15 minutes)
▷ Details follow when the time has come
Artemis - interactive learning with individual feedback

**Programming exercises**

**Modeling exercises**

**Text exercises**

**Quiz exercises**

**Scalability:** handle > 200 submissions per second

**Usability:** beginners are able to use it

**Instant feedback:** provide feedback in real-time

Team exercises  | Lectures  | Presentations  | Exam mode  | Questions and answers  | Learning analytics
Automatic assessment of programming exercises

1. Student submit
2. Version Control Server notify
3. Continuous Integration Server compile, run tests
4. Notify student with feedback
Artemis architecture

Remote Build Agent

Local Build Agent

Continuous Integration Server

Version Control Server

User Management System

Student Computer

Version Control Client

Artemis Application Client

Artemis Application Server

University Infrastructure

REST + WS

git

LTI Interface
Time and place

When?  Montag, 14:00 - 15:30
Where?  https://bbb.in.tum.de/lud-r9f-drd
Registration

- Solve the **qualification challenge**
- Visit honeynet.sec.in.tum.de
- Upon solving you’ll receive a flag: `websec{[0-9a-f]*}`
- Submit until **22.02.2021, 23:59**
- **$2^4$** slots planned
- **FCFS**, but solving the challenge usually is sufficient for joining
- Don’t forget to register in the **matching system**!
Why is there a challenge?

- **Option 1: You’re already a ”l33t” hacker**
  - You will be fast and
  - Will not have problems with this course.

- **Option 2: You are a beginner but determined**
  - You’ll probably take some time, but
  - This will give you a good impression on the course.

- **Option 3: You can’t solve the challenge**
  - Tasks in this course may be a fair bit harder than this one, and
  - This course is probably not for you.
Questions?