Websec-Practicum — SS 25

Web Application Security

Fabian Franzen and Daniel von Kirschten

Chair for IT Security / I20
Prof. Dr. Claudia Eckert
Technische Universität München

January 30, 2025

What we offer

- **Exploiting** buggy **Web Appplications** in **CTF style**
- Real world applications: **Artemis**, **ASTRA**, **ITSec Scoreboard**, **Paperless NGX**, ...

What you should bring

- Java, Javascript, PHP, Python, Go, SQL, CSS, HTML, ...
- Necessary? You can learn it on the way if you are disceplined
- **Willingness to work and learn a lot**

Process

Phase I (∼8 weeks):

- "Usual" practical course (weekly meetings and assignments)

Phase II (∼2 weeks):

- Build your own WebSec challenge!

Phase III (∼4 weeks):

- Final project. Analyze one (or two) of the aforementioned tools (short report 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
- ...

Process — Phase II

- Create your **own** challenge
  - Maybe there is something we overlooked content-wise?
- Solve the challenges of the other teams the week after

Process — Phase III

Final project

- **Real world application** of the knowledge gained
- **Specialisation** in one/two topics
- Security analysis of aforementioned tools
- Short report (about 5 pages)
- **Presentation** (about 15 minutes)
- Details follow when the time has come

Time and place

When? ???
Where? 01.08.033 (this meeting room)

Registration

- Solve the **qualification challenge**
- Visit courses.sec.in.tum.de
- Uppon solving you'll receive a flag: **flag{...}**
- Submit untill **19.02.2025, 23:59**
- **16** slots planned
- **FCFS**, but solving the challange 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 probaply 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 then this one, and
  - This course is probably not for you.

Questions?

Questions?