Websec practical course — SS 26

Web Application Security

Daniel Kirschten, Carl König, Fabian Franzen

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

January 28, 2026

What we offer

- Exploiting buggy Web Appplications in CTF style
- Real world application: ITSec Scoreboard, TUM Trust Center, Paperless NGX and more (tba)

What you should bring

- Javascript, Python, PHP, SQL, Java
- Necessary? Only basics -
  you can learn it on the way if you are disciplined
- **Willingness to work and learn a lot.**
  Don't say we didn't warn you.

Process

Across entire course: Teams of two

Phase I (∼7 weeks): **Regular challeges**

- "Usual" practical course: weekly meetings and assignments

Phase II (∼3 weeks): **Projects**

- Create your own vulnerable webapp and exploit

Phase III (∼3 weeks): **Real-world pwning**

- Search for vulnerabilities in real-world applications, report your findings

Process — Phase I

Regular challenges

- Every week: Introduction to a new topic
  - **CTF style**: challenge is solved if **flag** is obtained from vulnerable app.[1]
  - Submission of solutions until the following week **before** the meeting
  - Presentation of solution during the meeting - we'll pick teams randomly

[1] "Flag" means `flag\{[0-9a-f]{36}\}`.
Example: `flag{e44314cc2121f285d65bc12ed4ae18a845c1}`

Process — Phase II

Projects

- Create your own vulnerable webapp (including functional exploit)
- Based on some vulnerability / idea / tool / framework / . . . **not covered** in challenge phase
- Details follow when the time has come

Process — Phase III

Real-world pwning

- **Real world application** of the knowledge gained
- Security analysis of two webapps
- Deliverable: **Short writeup** (5-10 pages)
- Details follow when the time has come

Contents

- Injection vulnerabilities
- XSS, CSRF, sandbox escaping
- Include attacks
- Cryptographic attacks
- Upload attacks
- Configuration vulnerabilities
- Advanced bugs
- ...

Time and place

When? tba; 2h slot
Where? tba; probably here (01.08.033)

Registration

- Visit `https://courses.sec.in.tum.de/websec`
- Solve the **qualification challenge**
- Upon solving you'll receive a flag: **flag_[0-9a-f]+**
- 24 slots planned
- **No FCFS** for solves within 48 hours (until **30.01. 16:00**)
  FCFS afterwards
- 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 than this one, and
  - You probably won't have fun in this course.

Questions?

Questions?