SEAD KU 2025

Introduction and General Information

Hannes Weissteiner

07.03.2025

Outline

Organization

Phase 1: Lay of the land

On your own:

- Solve 2 SEAD challenges from last year
- Short intro to CTF challenges
- Just to get you started
- Maximum 10 points
- https://sead-ctf.student.isec.tugraz.at

Phase 2: Build your own challenge

As a group of 4:

- Design a CTF challenge together!
- Think about a cool vulnerability
  - Does not have to be connected with the lecture
- Build a **secure application** around it
- Create an automated solvescript
- Maximum 30 points

Phase 3: Hack the planet!

On your own:

- Solve the challenges of other teams
- Harder challenge -> more points
- 60 points + bonus (TBD)
- **Possible bonus points depend on number and difficulty of challenges**
- Submit a writeup for each solved challenge (half a page per challenge)

Grading

Phase 1: max. 10 points, 5 required

Phase 2: max. 30 points, 15 required

Phase 3: 60+ points, 30 required

Points	Grade
≥ 87.5	Sehr Gut (1)
≥ 75	Gut (2)
≥ 62.5	Befriedigend (3)
≥ 50	Genügend (4)
< 50	Nicht Genügend (5)

Timeline 1/3

- 07.03.2025:
  - Intro lecture (**today**)
  - Start of Phase 1
- 20.03.2025:
  - Deadline for Phase 1 Challenges
- 21.03.2025:
  - Phase 2 Kickoff Lecture

Timeline 2/3

- 28.03.2025:
  - Group registration deadline
- 04.04.2025:
  - Hand in challenge idea
- **Afterwards:** Feedback by tutors
- 02.05.2025:
  - Challenge deadline
  - End of Phase 2

- 09.05.2025:
  - Start of Phase 3
- 20.06.2025:
  - Deadline for writeups
  - End of Phase 3
  - **Freedom!**

What is a CTF?

CTF ⟹ Capture The Flag


Capture The Flag
(Information Security)

- Infosec Competitions
- *“Competitive Hacking”*
- Deliberately vulnerable services
- Solve the challenge → get a flag
  - `LosCTF{this_is_how_a_flag_looks_like}`
  - `glacierctf{Ju57_P0s1X_th1ng5}`
  - `dvCTF{Br4v0K4sP4r0V}`
  - `"$CTFNAME{$some_funny_message}"`

Styles

Attack-Defense

- Teams get their own Server with services
- Attack other teams' services
- Defend your own services
- Usually in a short time-frame
- Traffic analysis, reverse engineering, binary exploitation, web...

Styles

Jeopardy

- All teams get the same challenges
- Usually around 24-48 hours
- Get points by solving different challenges **once**
- Points scale based on difficulty
- rev, pwn, crypto, web, misc
- **This is what we do in this course**

Challenge types

- Reverse Engineering
- Binary Exploitation
- Cryptography
- Web
- Misc

Phase 1 Introduction

- Available now at https://sead-ctf.student.isec.tugraz.at/
- Login through https://git.teaching.iaik.tugraz.at/
  - If you already have an account: Great!
  - If not: Save the flags locally for now
  - Accounts will be created after course registration is done
- 2 Challenges, 5 points each
- Important: Solve all stages of a challenge to get the points!

Tips for Phase 1

- **Google!**
- Discuss challenges with your friends (**No solution/flag sharing**)
- Poke around!
- Where is the flag?
- How can I get to it?
- Maybe you find CTF writeups to similar challenges?

Useful tools

- **Python**: For calculations and automation of repeatable steps
- **pwntools**: For interaction with sockets and local binaries
- **requestbin**: To log HTTP requests, e.g. from a XSS attack
- **Cyberchef**: To quickly translate between encodings and formats
- **Burpsuite**: To intercept and modify web requests by a browser

Any questions?