1 Introduction

This document describes the "Secure Application Design" KU for the 2025 summer semester. In this course, you will create your own Capture-the-Flag (CTF) challenges, and solve those created by others.

The course is divided into three phases, which will take place over the semester. In order to complete the course, you need to pass all three phases.

1.1 Communication

The following communication channels are available to you.

SEAD Email. The sead.isec@tugraz.at address may be used for individual requests. This address is intended for questions which cannot be discussed publically.

Discord. ISEC uses Discord as our primary means of student communication. You will need to register a Discord account, and join the ISEC server using the invite link `https://discord.gg/mxuUnjP`.

Once you have done so, react with the appropriate emoji in `#getting-started` to gain access to the SEAD course channels. The following channels are available to you:

- `#sead` is a generic channel for all SEAD participants to ask questions in.
- `#sead-looking-for-team` lets you look for (members for) a team to tackle phase 2 with.
- `#sead-ku-announcements` is for information regarding the course.

1.2 Introductory Lectures

An introductory lecture with information and hints regarding the KU and its tasks will take place on 2025-03-07, from 15:15, in HS i11, *(right after the lecture.)*

On 2025-03-21, a kickoff lecture for stage 2 will take place in HS i11, from 14:00. It will contain additional information, guidelines and hints about how to create a good CTF challenge.

Attendance is not mandatory, but highly recommended. A recorded version will be available online, but will not replace the interactive experience.

1.3 Capture the Flag

CTFs are information security competitions, where participants try to earn points by completing various challenges. While there are Attack-Defense style competitions, where teams have to hack their oponents' machines and steal flags while defending their own, the more common format is Jeopardy, where teams solve challenges provided by the organizers.

The challenges can fall into many different categories, most common are reverse engineering (rev), binary exploitation (pwn), cryptography and web.

Most events are time limited and end after a few days. Some of them, like `https://fuzzy.land/` run 24/7 and allow curious people to work on their own time.

2 Your Tasks

2.1 Phase 1: Lay of the Land

In Phase 1, you will be presented with two introductory challenges based on last year's SEAD KU. These tasks are intended to familiarize you with the layout of a Capture-the-Flag challenge. You should be able to solve them based on your pre-existing information security knowledge.

The challenges are available at `https://sead-ctf.student.isec.tugraz.at`. If you have a `https://git.teaching.isec.tugraz.at/` you can log in already. If you don't have an account yet, you will receive one before the deadline. Challenges will be set to public, so you can solve them without an account, and hand in the challenges as soon as you receive one.

For Phase 1, you do not need to submit any written material beyond the flag. Phase 1 accounts for 10 points. Each challenge awards 5 points, and you need 5 points to pass Phase 1. Phase 1 ends on 2025-03-20.

2.2 Phase 2: Build Your Own Challenge

In Phase 2, you will organize yourself into teams of 4 students to design your own Capture-the-Flag challenge. This takes the form of multiple steps.

2.2.1 Form a group

Find other students to form a group and sign up via email to sead.isec@tugraz.at, listing all participating students and their matriculation numbers. You need to do this by 2025-03-28. If you are unable to find a group, please also notify us by 2025-03-29 at latest, and we will assign you to a group. Failing to do so will cause you to be deregistered from the KU without a grade.

2.2.2 Find a challenge idea

Write up a concept for the challenge you would like to design. This typically takes the form of a 1-2 page PDF document.

The document should include the system you want to implement, the planned vulnerability, a rough rundown of the required exploit and a description on how you plan to implement it, including used programming languages and frameworks.

You need to submit this document via sead.isec@tugraz.at by 2025-04-04.

2.2.3 Implement the challenge

Once you have submitted your design, your assigned tutor will review your design and suggest changes. After you received your feedback, you can begin developing your challenge. You also need to create a detailed writeup and an automated solve-script for your challenge, and place it in the respective directory. You should finish development of your challenge by 2025-05-02.

Your tutor will then review your submission and contact you about any issues with the implementation or deployment. Phase 2 accounts for 30 points. Your group needs 15 points to pass Phase 2.

2.3 Phase 3: Hack All Systems

In Phase 3, you will set out to solve the challenges developed by other groups. You will work by yourself on this task.

Challenges will be publicly available at `https://sead-ctf.student.isec.tugraz.at`.

You will have to submit a PDF document containing brief writeups for every challenge you solve. Each write-up should describe the approach you took to solving the challenge. You can also include code snippets that you used for your exploits. You should also include the flag as proof that you completed the challenge. This writeup should typically be around half a page per challenge, but can be up to at most two pages if necessary.

For each challenge you solve, you will receive points. It is not possible to receive partial points for a challenge. Your own challenge will not count towards your points total. Please hand the flag in anyways, as it will be deducted from your points total. If you received the flag, and your document adequately describes how you did so, you will receive points for that challenge.

Phase 3 accounts for up to 60 points. You need 30 points to pass Phase 3. Phase 3 ends on 2025-06-20.

3 Summary

The course is divided into three phases:

- **Phase 1** – solve pre-made challenges
- **Phase 2** – design your own challenge
- **Phase 3** – solve other groups' challenges

Phase 1 awards 10 points, and requires 5 points to pass. Phase 2 awards 30 points, and requires 15 points to pass. Phase 3 awards 60 points, and requires 30 points to pass.

If you pass all three phases, your final grade is determined as follows:

- $\geq 87\frac{1}{2}$ **points**: Sehr Gut (1)
- ≥ 75 **points**: Gut (2)
- $\geq 62\frac{1}{2}$ **points**: Befriedigend (3)
- ≥ 50 **points**: Genügend (4)

3.1 Timeline

- **Intro Lecture** on March 7th
- **Solve intro challenges** by March 20th 23:59
- **Phase 2 Kickoff Lecture** on March 21st
- **Form groups** by March 28th, or **tell us you need a group** by March 29th
- **Submit design concept** by April 4th 23:59
- **Implement your challenge** by May 2nd 23:59
- **Challenge Deployment** around May 9th
- **Solve other groups' challenges** by June 20th 23:59