ChalmersGU-KTH-Aarhus CTF Competition
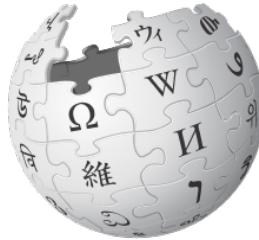
The organization team:
Amir M. Ahmadian, Andrei Sabelfeld, Aslan Askarov, Benjamin Eriksson, Francisco Blas Izquierdo Riera, Ivan Oleynikov, Javier Cabrera Arteaga, John Kristoffersson, Mikhail Shcherbakov, Mohammad M. Ahmadpanah, and Musard Balliu

June 2, 2022

Capture The Flag (CTF)

Capture the flag is a traditional outdoor game often played by children where two teams each have a flag and the objective is to capture the other team's flag.

Capture The Flag (CTF)
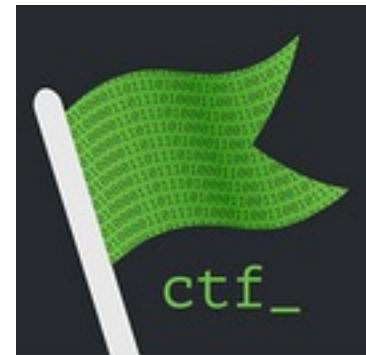
Capture the flag may also refer to:

- "Capture the Flag", a song by the German thrash metal band Sodom from their 1990 album *Better Off Dead*

- "Capture the Flag", a song by Broken Social Scene from their 2002 album *You Forgot It in People*

- *Capture the Flag* (film), a 2015 Spanish 3D computer-animated adventure comedy family film directed by Enrique Gato

- *Capture the Flag* (video game)

- "Capture the Flag", a 1997 tabletop role-playing game scenario published in *Book of Lost Dreams*

- Capture the flag (cybersecurity), a cybersecurity exercise based on the traditional game

ChalmersGU-KTH-Aarhus

- Part of the "*Language-Based Security*" course at the universities
  - 2021: Initiated by ChalmersGU, then KTH engaged
    2022: Aarhus joined
  - *Organization* team: Instructors and TAs
- A *four-hour* competition between groups of students
  - Introducing and expanding students' skills even beyond the syllabi
  - Competition by nature yet the focus is *learning*
  - Improving student teamwork and building network
    - Helped to forget about Covid for a couple of hours in 2021! ☺

ChalmersGU-KTH-Aarhus

Process

- Brainstorming => Concrete challenge ideas => Implementation => Dry-run testing => The competition!

Challenges

- **2022**
  - XSS (basic, advanced)
  - JS sandbox escape
  - GraphQL introspection
  - Shell injection
  - Android decompile
  - Binary WASM (buffer overread, string format, function hijack)
  - Privacy
  - Forensic
  - Machine identifiable code
 - Regex DoS
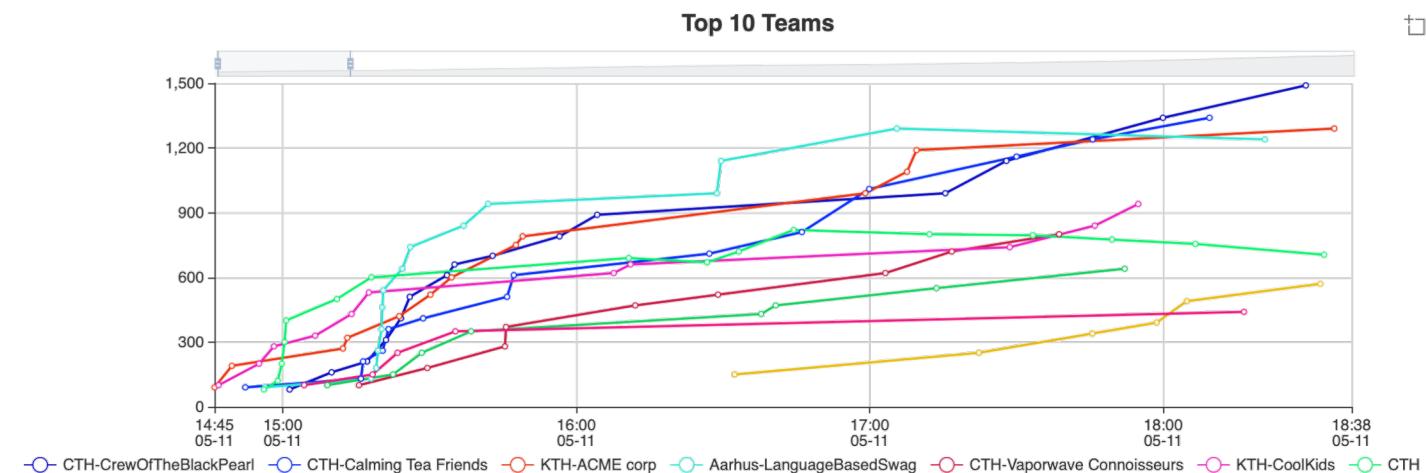
- **2021**
  - XSS (basic, advanced)
  - SQLi
  - Hash cracking
  - Binary WASM
  - Steganography
  - Android (decompile, advanced)

Live Demo

- CTFd
  - Ranking, statistics, hints, and stuff!
- Slack
  - Broadcasting and communication with organizers
  - Behind-the-scene channel
- Writeups

Top 10 Teams

Time for Discussion