esse

CTF Contests: Hands-On Experience of the IT Security Culture – UE 03: Writeups

Clemens Hlauschek, Daniel Marth, Florian Fankhauser

INSO – Industrial Software
Institute of Information Systems Engineering | Faculty of Informatics | TU Wien

Task Writeups

- Explanation of how a task was solved
- List available resources
  - Code, binary files, network services, ...
- Explain analysis steps, mention used tools
- Solution / exploit, compare different approaches

Example Writeups

- Google CTF 2021, Filestore
  - `https://www.proggen.org/doku.php?id=security:ctf:writeup:google:2021:filestore`
- hxp 36C3 CTF (2019), file magician
  - `https://ctftime.org/writeup/17892`
- hxp 36C3 CTF (2019), WriteupBin
  - `https://ctftime.org/writeup/17891`

Course Writeups

- Document **your** contribution to the team
  - Solved / attempted tasks
  - Team coordination
  - Infrastructure setup
  - ...
- Mention other collaborators, distinguish individual contributions
- English or German

Writeup Structure

- TL;DR / short summary
- Description of the task
- Detailed analysis steps (e.g., used tools, commands)
- Description of vulnerability / exploitable issue(s)
- Solution, including description of steps to get there
- Tried, but failed solutions
- Possible alternative solutions (if available)
- Lessons learned

Upcoming Event: PlaidCTF

PlaidCTF 2022

- https://plaidctf.com/
- 08 April 2022, 23:00 - 09 April 2022, 23:00
- Submit your writeup in TUWEL until 01 May 2022, 23:55
- Organizers will use Discord for communication
- We will meet 09 April at 08:30 at the Inflab
  - Favoritenstraße 9-11
  - https://www.inflab.tuwien.ac.at/
- Please respect the COVID-19 measures of TU Wien!
  - https://www.tuwien.at/en/tu-wien/corona

Further Preparation

- Memory corruptions
  - `https://www.proggen.org/doku.php?id=security:memory-corruption:start`
- pwntools
  - `https://docs.pwntools.com/`
- Brush up your Linux and scripting (e.g., Python) skills!

Exercises

Writeup Exercise

- Form groups
- Search online for writeups
- Read them, try to understand the solution
- Create a text channel on Discord in the “training” section
- Document your insights and what was missing in the chat

Known plaintext - XOR

- https://www.root-me.org/en/Challenges/Cryptanalysis/Known-plaintext-XOR
- Cryptanalysis, 20 points

RSA - Factorisation

- https://www.root-me.org/en/Challenges/Cryptanalysis/RSA-Factorisation
- Cryptanalysis, 25 points

Pixel Madness

- https://www.root-me.org/en/Challenges/Cryptanalysis/Pixel-Madness-86
- Cryptanalysis, 15 points

Thank you!

https://security.inso.tuwien.ac.at/ctf-2022s/