

Challenge Session 2 – Exercises Instruction

A Google Drive folder containing the exercises will be shared to you at the email you provided during the form registration. The folder will contain:

- 1) got_studentID folder, containing vuln and flag.txt
- 2) freezeTime_studentID
- 3) honeydex_studentID
- 4) SOLUTIONS folder

If you miss some files, please contact us immediately.

For students that did not register, we will release the binaries on Moodle.

In this second challenge, you are asked to solve 3 exercises in the Reverse and Pwn Area:

- GameOfThrones (GoT) – Easy and Short – 11 Points
- FreezeTime – Straightforward but long – 14 Points
- HoneyDex – Easy but tricky – 7 Points

For a total of 32 Points.

For each exercise, we supply two additional hints (available on Moodle), that can help you if you need.

For GoT and FreezeTime, opening a hint will automatically remove 3 points.

For HoneyDex, opening a hint will automatically remove 1 point.

You can open the same hint all the times you want.

To solve an exercise, you need to find a flag in the specific format SPRITZ{...}, and send it to us along a description of what you did to find it (write-up), the eventual code you wrote, and the patched binary if you patched it.

To submit your answer, put all the files you used (python code, patched binaries, ...) , the flags, and the write-ups, in the folder SOLUTIONS that you will find in the Google Drive folder we shared with you.

During the challenge, due to breakout room limitations, we will use a Google Document as a forum chat to make communication easier. Use it if you have questions that might interest everyone. **Please use it properly, otherwise we will invalidate the challenge for everyone:**

<https://docs.google.com/document/d/19ytOpri-zZXQ9NkUdIhQjCgeJU1ePGC6NWxZeQNfzes/edit?usp=sharing>

YOU ARE NOT ALLOWED TO BROWSE THE INTERNET OR CONSULTING COURSE (OR ANY OTHER) MATERIAL.

You have time until 14:30.

NOTES

Note I: DO NOT PATCH GameOfThrones (GoT), otherwise you won't receive points for that exercise.

Note II: The exercises order doesn't matter, you can start from whatever you think is the best.

Note III: If you are stuck, use a hint or move to the next exercise. If you think there is an error in the binary, please contact us!

Note IV: Please submit everything you did, even if you did not fully solved the exercises. You can still gain some precious points.