

Homework Week 2

Your submission should only be your python exploit. Please name your exploit `<matrikelnr>_exploit.py`!

Exploit

To run your exploit I will invoke `docker compose up exploit` and you should print the flag to stdout such that the flag will appear in the log.

As described in the docker files your exploit will be run in a separate docker container from the homework binary. This means your exploit should interact with the `remote` process, which means you should generate your template with `pwn template --host homework --port 1337 ./homework`. You can find the exact way your script will be invoked in the `exploiter.docker` file. Lastly please just print the flag and then exit the script and don't run `io.interactive()`.

Flag

The flag is located in the same directory as the program you are exploiting, so a `cat ./flag.txt` should be enough. The flag format will be `SSL{...}`