CTF Report

Name: René Enjilian

Matrikelnummer: 382229

Contribution:

I developed the service Explotify and its checker with Alejandro Jaramillo and and worked on the CI too. While working on the service I focused on the SSRF (Server Side Request Forgery) vulnerability. Therefore I implemented two databases. The Mongo database stores the song metadata including the name as a flag and the SQLite database was used to store user data including the mobile number as a flag. I also worked on the FFMPEG vulnerability. By extracting html data from web sites I build a model that generates random text using markov chains. We used that random text for our song generation. My main contribution for CI was developing the launcher in order to test the checkers.

Challenges:

In the beginning we focused too much on the service itself and neglected the checker. We underestimated the problems the checker could possibly cause e.g. IPV6 and the stateful design of the checker.

What I learned:

My personal lessons can be divided into two aspects. On the on side I definitely learned many new technologies e.g. Docker, non-relational databases etc. On the other side it was very interesting for me to work on larger project in a team since my experience is mainly limited to mandatory courses in the university.

Next year:

In my opinion we should have started earlier with the CI since most of us had real problems with their checkers, especially at the end of the course. Parts of this year’s CI could therefore be reused next year.