Gamification of Digital Labs:
Towards a Multipurpose and Collaborative Virtual Platform

Objectives of the Project

- Design of an extensible plug-in architecture which will be used by all new functionalities
- Integration of a virtualization infrastructure within the existing platform
- Development of an automated plagiarism detection system
- Implementation of federated authentication using the university credentials and revision of the existing access control system

Infobox .dcall 2020

Laufzeit
1.10.2020 – 31.8.2021

Themenbereich
.dcall Lehre

Projektleiter
Marco Squarcina
marco.squarcina@tuwien.ac.at

Project results

The virtual lab of the *Introduction to Security*- lectures at TU Wien relies on an open-source, in-house platform that has been developed to provide a safe, remotely accessible environment, where students can interact with realistic applications containing ad-hoc vulnerabilities. The activities are organized as a computer security contest, an educational exercise to give participants hands-on experience in the sort of attacks and protections found in the real world. One of the key concepts of the platform is "learning by doing": students are challenged to fill the gap between theory and practice and develop out of the box skills to solve the problems presented in the course. Furthermore, the gamification of learning approach leveraged in the lab, increases the engagement and overall satisfaction levels among the students, as shown in recent evaluation surveys. To simplify teaching activities and to offer advanced practical exercises needed, the platform has some features to integrate. These advanced exercises are especially valuable for new courses developed as part of the recently approved specialization on security in the Software Engineering & Internet Computing Master programs, which will further increase the demand for this virtual lab. The project reached the expected goals stated in the original proposal. The aim to create a future-proof, easy to maintain, and extensible framework, mandated a complete rewrite of the entire code base. The planned functionalities, i.e., virtualization support, federated authentication, and plagiarism detection, have been integrated into the platform as core plugins, taking advantage of the new architecture. At the same time, it is clear that these components will benefit from an extended testing phase, embodying the feedback of other lecturers, before being considered production-ready.

Possible follow-up topics

Investigate the requirements of other courses to support them with this platform.