Credits: 6 CFU.

Lectures mode:

- Before the lecture, the teacher publishes a recorded video illustrating the topics of the incoming lecture. Students have to watch the video before attending the lecture.
- At the start of the lecture, the teacher releases a brief questionnaire to check if the students have understood the main concepts described in the recorded lecture. The questionnaire is administered through the Moodle platform. The teacher, then, answers to any doubt or question.
- The teacher releases a new assignment which will be solved by all groups. For every assignment, a group will be chosen to illustrate the solution through a presentation.
- During the next lecture, the group presents its solution and answers to questions from the teacher and from the other students. Each member of the group can get up to 3 points, which will be summed up with the grade obtained at the final exam.

The course is very practical and it requires a high participation from the students. Thus, even if not mandatory, the participation in the class is strongly recommended to benefit from the interaction with other students and the teacher.

Schedule: II semester (course schedule is published **HERE (https://agendastudentiunipd.easystaff.it/index.php?view=easycourse&_lang=en)**).

Course Content:

"Mobile Security" is a hands-on course. The exercises are in the format of Capture The Flag (CTF) challenges: the students are asked to solve a problem and to find the "flag", which is nothing more than a string located somewhere.
Topics of the course are the following ones:

- Internal architecture of the Android Operating System.
- Mobile app components (Activity, Service, Content Provider, Broadcast Receiver).
- Mobile app analysis techniques.
- Mobile app reverse engineering techniques.
- Mobile app vulnerability assessment.
- Static and dynamic analysis techniques for mobile apps.
- Mobile app vulnerability exploitation.

It is highly recommended to have background knowledge on any object-oriented programming language (e.g., Java).
Knowledge about cybersecurity fundamentals (e.g., cryptography, access control, authentication) can be helpful, but not mandatory.

Grading Criteria:

The final exam will be a set of multiple choice questions covering all the topics of the course.
The exam will have 33 points among which:

- 18 points achievable through theoretical questions (18 questions, each one weighted 1 point)
- 15 points achievable through practical questions