



SAPIENZA
UNIVERSITÀ DI ROMA

Security in Software Applications

Master degree in Cybersecurity
A.A. 2022/2023

Tue 17-19

Fri 8-11



Info

- Dr. Daniele Friolo
 - **Office hours** by appointment
 - usually Tue/Fri 14-16
 - **Email** friolo@di.uniroma1.it
- All the material and announcements can be found on
 - Google Classroom course code: vo6mu6q (w. recorded lessons)
 - My webpage: <https://danielefriolo.github.io/teaching/>
 - The course will follow the same blueprint of last year.

Attendance Tracking!!

- Please fill out the following form after following each class
 - <https://forms.gle/oh7oegAWFeSBMWUt5>



Outline

- **Improving Existing Code**
 - Known vulnerabilities: Buffer overflow, SQL/code injection, TOCTOU
 - Static and Dynamic Code Analysis and Tools
 - Common Vulnerability Scoring System CVSS
- **Evaluating Security**
 - Principles
 - OWASP
 - Testing
- **Develop Secure Software**
 - Secure code development / defensive coding
 - Java security
 - Cryptography
- **Current Approaches**
 - Language-based security
 - Information Flow Control
 - Proof-Carrying Code
 - Code Obfuscation



References

- R. Anderson, **Security Engineering: a guide to building dependable distributed systems**, 2nd ed., John Wiley and Sons 2008
- J.Viega, G.McGraw, **Building Secure Software**, Addison- Wesley 2002
- G.McGraw, **Software Security: Building Security in**, Addison- Wesley 2006
- G.Hoglung, G.McGraw, **Exploiting Software: how to break code**, Addison-Wesley 2004
- G.McGraw, E.Felten, **Securing Java**, John Wiley and Sons 1999,
- D.A.Wheeler, **Secure Programming for Linux and Unix HOWTO**



Course Evaluation

- **Three individual project (20% each)**
 - Static Analysis of C fragment
 - Analysis of Java Code with assertions
 - Testing/Evaluating given application
- **One final written exam OR paper presentation (to decide) (40%)**
- Need to pass **all** of them
- Submission of projects by deadline necessary to take exams in first session (January and February)