Cybersecurity (module 3 CFU)
Web Security and Privacy (module 3 CFU)

a.y. 2022-23
Outcomes will be sent via email within two weeks

1. ***TEXT IN NON-ENGLISH: 2 penalty points***
2. ***UNREADABLE WRITING will be skipped***
3. ***TEXT WRITTEN WITH A PENCIL will be skipped***
4. ***All questions of an exercise QX must be answered with no more than one page of text. Be concise and focus on what a question is asking.***

Q0: **Write on your paper (or in Exam.net)**

- First name
- Last name
- Student ID

Q1: **Email systems [7.5 points]**

- Q1.1 [3.5 points]: You are setting up a new web portal at bazinga.com and you want to avoid that a third party may be able to spoof or alter email messages from your domain, what do you have to do in practice? Which guarantees will you get?
- Q1.2 [2 points]: What are the benefits offered by DMARC if we are already using SPF and DKIM?
- Q1.3 [2 points]: What are the limitations of DMARC?

Q2: **Web attacks and mitigations [7.5 points]**

- Q2.1 [2 points]: If we log all HTTP(S) requests, can we always identify when an attacker is targeting our website or the users of our website? If not, can you make concrete examples of attacks that could go unnoticed?
- Q2.2 [2 points]: Why a website should configure a CORS policy? Can CORS protect the website from attacks?
- Q2.3 [3.5 points]: Describe **in detail** the strategies that an attacker can use to perform a blind SQL injection.