Master's Degree Title: Computer Security.
Semester: S3.
Teaching Unit (UE): UEF322.
Course Title: Web and Mobile Application Security.
Credits: 4.
Coefficient: 3.

Course Objectives: Understand the fundamental principles and concepts of secure Web browsing, Web development architecture, the main Web-specific vulnerabilities and attacks, as well as the mechanisms and best practices for developing and configuring Web applications. Understand the role of encryption in the security of mobile applications and devices, and describe common scenarios in which encryption is applied.
Recommended prior knowledge: Network security and digital vulnerability analysis.

Course content:

Chapter 1: Vulnerabilities and attack methods.

- Different types of hackers.
- Organisation and objectives of hacker teams.
- The phases of an intrusion.
- Vulnerability analysis and Zero-Day vulnerabilities.
- Malicious code attacks.
- Social engineering attacks.
- Application attacks.

Chapter 2: The Web security model.

- The Web browser as an operating system and execution platform.
- Permission-based access control.
- Protocols, isolation and communication.

Chapter 3: Web application security.

- OWASP - Top 10 attacks.
- Web application protection techniques.

Chapter 4: Goals and problems of HTTPS.

- SSL/TLS protocol: review.
- Strengthening security with HTTPS.
- HTTPS problems: forged certificates, mixed http/https traffic, etc.

Chapter 5: Content Security Policy (CSP: Content Security Policy).

- Web workers.
- Content security policies. - Frame isolation (Sandboxed iFrames).

Chapter 6: Session tracking and authentication.

- How to authenticate a website.
- Secure mechanism for tracking state between client and server.
- Cookies and session integrity.

Chapter 7: XML and Web services security.

- Review of Web services.
- Security in XML.
- Overview of AJAX technology.
- Attacks against AJAX and defence mechanisms.

Chapter 8: Mobile security.

- Mobile computing technologies.
- Overview of mobile computing security.

Assessment method: Continuous assessment and examination.

Bibliography:

1. Mavoungou S., Kaddoum G., Taha M., and Matar G., Survey on threats and attacks on mobile networks, https://ieeexplore.ieee.org/document/8272037.
2. Papageorgiou A., Strigkos M., Politou E., Alepis E., Solanas A., and Patsakis C., Security and privacy analysis of mobile health applications: the alarming state of practice, https://ieeexplore.ieee.org/document/8272037.
3. M. Oltrogge, E. Derr, C. Stransky, Y. Acar, S. Fahl, C. Rossow, G. Pellegrino, S. Bugiel, and M. Backes, “The rise of the citizen developer: Assessing the security impact of online app generators,” in 2018 IEEE Symposium on Security and Privacy, SP 2018, Proceedings, 21-23 May 2018, San Francisco, California, USA, May 2018, pp. 634–647. [Online]. Available: https://doi.org/10.1109/SP.2018.00005.
4. M. Zalewski, The Tangled Web: A Guide to Securing Modern Web Applications, 1st ed. San Francisco, CA, USA: No Starch Press, 2011.