COURSE DATA

Data Subject

Code	44835
Name	Security
Cycle	Master's degree
ECTS Credits	2.0
Academic year	2018 - 2019

Study (s)

Degree	Center	Acad. year	Period
2234 - M.D. in Web Technology, Cloud Computing and Mobile Apps	School of Engineering	1	Second term

Subject-matter

Degree	Subject-matter	Character
2234 - M.D. in Web Technology, Cloud Computing and Mobile Apps	5 - Production of software, security and profession	Obligatory

Coordination

Name	Department
PEÑA ORTIZ, RAÚL	240 - Computer Science

SUMMARY

The subject introduces students to concepts of security in web applications where communications are performed through an insecure channel as the Internet. This type of application is very broad and the subject tries to pick the options that appear in web applications and analyse current problems and security solutions. The main goal is to provide students with the necessary mechanisms to include security as a fundamental element in the development of web applications.

PREVIOUS KNOWLEDGE

Relationship to other subjects of the same degree

There are no specified enrollment restrictions with other subjects of the curriculum.

Other requirements

Understand the technologies of server-side programming.
Knowing client side programming technologies.

OUTCOMES

2234 - M.D. in Web Technology, Cloud Computing and Mobile Apps

- Students should apply acquired knowledge to solve problems in unfamiliar contexts within their field of study, including multidisciplinary scenarios.
- Students should be able to integrate knowledge and address the complexity of making informed judgments based on incomplete or limited information, including reflections on the social and ethical responsibilities associated with the application of their knowledge and judgments.
- Students should communicate conclusions and underlying knowledge clearly and unambiguously to both specialized and non-specialized audiences.
- Students should demonstrate self-directed learning skills for continued academic growth.
- Students should possess and understand foundational knowledge that enables original thinking and research in the field.
- Ability to apply acquired knowledge and solve problems in new or little-known environments within broader and multidisciplinary contexts, being able to integrate this knowledge.
- Capacity for the elaboration, planning, direction, coordination, technical and economic management and the implantation of Web projects.
- Ability to understand and apply ethical responsibility, legislation and professional ethics in the professional practice.
- To foster, in academic and professional contexts, technological, social or cultural advancement within a society based on In knowledge and respect for: a) fundamental rights and equal opportunities between men and women; b) principles of equal opportunities and universal accessibility of persons with disabilities; and, c) the values of a culture of peace and democratic values.
- Ability to assess risk and security issues in systems and applications and take measures to mitigate them in the fields of Web technologies, cloud computing and mobile applications.

LEARNING OUTCOMES

- Specify and complete computer tasks that are complex, incompletely defined or unfamiliar
- Describe and explain techniques and methods applicable to their particular area of study and identify their limitations
- Organize your own work independently, demonstrating initiative and exercising personal responsibility
- Perform bibliographic searches and reviews using databases and other sources of information
- Learning and improving personal performance as the basis for lifelong learning and professional development
- Communicate effectively both verbally and through other media to a variety of audiences and preferably in a second language
- Appreciate the skills required to work with and lead a team that can consist of different disciplines and different levels of qualification

- Assess risk and information security issues relevant to their area of study.
- Know the main vulnerabilities when developing web applications.
- Develope and evaluate security mechanisms on the server, the client and the application side.
- Demonstrate awareness of the need for ethical professional conduct in information technology.
- Ability to analyse the requirements of a web system based on its functionality, performance, usability, organizational needs and security requirements.
- Ability to transform these requirements into efficient and effective solutions these take into account the needs, the characteristics and the expectations of their users.
- Secure databases and application servers those are used as tools for running web applications.
- Identify and assess the main threats to the security of web applications and the faults that are commonly committed in their programming.
- Analysing and drawing conclusions about security errors that have allowed an intrusion into web servers, and developing new security measures to prevent future attempts to intrude on web servers.

DESCRIPTION OF CONTENTS

1. Vulnerabilities in web applications

Web applications and security cost
Critical vulnerabilities in web applications
Security guides and recommendations
Installation and use of a platform to benchmark vulnerabilities in web applications.

2. Server security

HTTP Basis.
Security mechanisms available in HTTP
Authentication in web servers.
Key stores, certificates and SSL.
Security utilities in the server side.

3. Client security

HTTP session management and Hijacking.
Cookie management and security implications.
Same origin protection policies.
Cross-site scripting (XSS).
Request falsification in cross sites.
Non-valid redirections.
Client-side data injection and insecure direct links to resources.
Security tools in the client side.

4. Application level security

Authentication and role-based access control and ACL.
Form validation: client and server.
Vulnerabilities in the data layer: database access, SQL injection, sensitive data exposure.
Web application resource configuration policies and good practices.
Application level security tools.

WORKLOAD

ACTIVITY	Hours	% To be attended
Theoretical and practical classes	20,00	100
Study and independent work	22,00	0
Preparation of practical classes and problem	6,00	0
Resolution of online questionnaires	2,00	0
TOTAL	50,00	

TEACHING METHODOLOGY

- Theory class
- Problem resolution
- Project-oriented learning

EVALUATION

The assesment modalities used in this subject are:

SE1: Online assessment and/or degree of participation

SE2: Assessment of problems, works, reports and/or memories

SE4: Exam or face-to-face assessment

SE6: Assessment of laboratory

- First call

0.1*SE1+0.3*SE2+0.2*SE4+0.4*SE6

- Second call

0.1*SE1+0.2*SE2+0.4*SE4+0.3*SE6

The necessary restrictions that must be met to apply the percentages shown above are:

- Both final practices and exercises must have been submitted and passed.

In the case of not meeting the above restrictions, will be teacher's decision whether to make a final examination with a weight of 100% of the final grade to the student or require additional work to get pass the course.

The marks and grades system is described in:

http://www.uv.es/uvweb/college/en/postgraduate-courses/postgraduate-administrative-information/continuance-marks/marks-grades-1285897761928.html

The applied regulations are described in:

http://www.uv.es/uvweb/college/en/undergraduate-studies/academic-information/regulations/university-valencia-legislation-1285850677111.html

REFERENCES

Basic

- Simson Garfinkel,Gene Spafford, Web Security, Privacy & Commerce, OReally. 2nd Edition. 2011
- Christoph Kern,Anita Kesavan,Neil Daswani. Foundations of Security: What Every Programmer Needs to Know. 2006. Apress
- Dustin, E., Rashka, J., & McDiarmid, D. "Quality Web Systems: Performance, Security, and Usability". 2002. Addison-Wesley Longman Publishing Co., Inc.
- The Open Web Application Security Project. "OWASP TOP 10: Los diez riesgos más críticos en Aplicaciones Web". Release Candidate. 2017. https://github.com/OWASP/Top10/raw/master/2017/OWASP%20Top%2010%20-%202017%20RC1-English.pdf

Additional

- Aleksa Vukotic, James Goodwill. Apache Tomcat 7. Apress. 2011.
- Stuart McClure, Saumil Shah, Shreeraj Shah. Web hacking: attacks and defense. 2003