FICHA IDENTIFICATIVA

DATOS DE LA ASIGNATURA

Código: 44835
Nombre: Seguridad
Ciclo: Máster Universitario Oficial
Créditos ECTS: 2
Curso académico: 2026-27

TITULACIONES

Titulación	Centro	Curso	Periodo
2234 - Máster Universitario en Tecnolog. Web, Computación Nube y Aplicac. Móviles	Escola Tècnica Superior d'Enginyeria	1	Primer cuatrimestre

MATERIAS

Titulación	Materia	Carácter
2234 - Máster Universitario en Tecnolog. Web, Computación Nube y Aplicac. Móviles	Producción de software, seguridad y profesión	OBLIGATORIA

COORDINACIÓN

PEÑA ORTIZ RAÚL

RESUMEN

La asignatura introducirá al alumnado en los conceptos de la seguridad en recursos y aplicaciones web del tipo cliente-servidor en las que la comunicaciones se realizan a través de un canal inseguro, como es Internet. Este tipo de aplicaciones es muy amplio y la asignatura trata de recoger las diferentes opciones que aparecen en las aplicaciones web actuales y de analizar los problemas y soluciones de seguridad. El principal objetivo es proveer al alumnado de los mecanismos necesarios para poder incluir la seguridad como un elemento fundamental dentro del desarrollo de aplicaciones web.

CONOCIMIENTOS PREVIOS

RELACIÓN CON OTRAS ASIGNATURAS DE LA MISMA TITULACIÓN

No se han especificado restricciones de matrícula con otras asignaturas del plan de estudios.

OTROS TIPOS DE REQUISITOS

Recomendaciones:

Conocer las tecnologías de programación del lado del servidor.
Conocer las tecnologías de programación del lado del cliente

COMPETENCIAS / RESULTADOS DE APRENDIZAJE

2234 - Máster Universitario en Tecnolog. Web, Computación Nube y Aplicac. Móviles

Capacidad para comprender y aplicar la responsabilidad ética, la legislación y la deontología en el ejercicio profesional.

Capacidad para evaluar el riesgo y los problemas de seguridad en sistemas y aplicaciones y adoptar medidas para mitigarlos en el ámbito de las tecnologías web, computación en la nube y aplicaciones móviles.

Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, siendo capaces de integrar estos conocimientos.

Capacidad para la elaboración, planificación, dirección, coordinación, gestión técnica y económica y la implantación de proyectos Web.

Fomentar en contextos académicos y profesionales, el avance tecnológico, social o cultural dentro de una sociedad basada en el conocimiento y en el respeto a: a) los derechos fundamentales y de igualdad de oportunidades entre hombres y mujeres, b) los principios de igualdad de oportunidades y accesibilidad universal de las personas con discapacidad y c) los valores propios de una cultura de paz y de valores democráticos.

Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.

Que los/las estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo

Que los/las estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.

Que los/las estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

Que los/las estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.

DESCRIPCIÓN DE CONTENIDOS

1. Vulnerabilidades en las aplicaciones web

Aplicaciones web y el coste de la seguridad.
Las vulnerabilidades más críticas en las aplicaciones web.
Guías y recomendaciones de seguridad.
Instalación y uso de una plataforma para pruebas de vulnerabilidad en aplicaciones web.

2. Seguridad en el servidor

Fundamentos del protocolo HTTP.
Mecanismos de Seguridad disponibles en HTTP .
Autenticación en servidores web.
Almacenes de claves, certificados y SSL.
Utilidades de seguridad en el servidor.

3. Seguridad en el cliente

Gestión de sesiones HTTP y Hijacking.
Gestión de Cookies e implicaciones para la seguridad.
Políticas de protección del mismo origen.
Scripts de sitio-cruzado (XSS).
Falsificación de petición en sitios cruzados.
Redirecciones no válidas.
Inyección de datos en la cara del cliente y referencias directas inseguras a recursos.
Herramientas de seguridad a nivel de cliente.null

4. Seguridad a nivel de la aplicación

Autenticación y control de acceso basado en roles y listas de control de acceso.
Validación de formularios: cliente y servidor.
Vulnerabilidades en la capa de datos: acceso a base de datos, inyección SQL, exposición de datos sensibles.
Políticas y buenas prácticas de configuración de los recursos de las aplicaciones web.
Herramientas de seguridad a nivel de aplicación.

VOLUMEN DE TRABAJO (HORAS)

ACTIVIDADES PRESENCIALES

Actividad	Horas
Teoría-Prácticas	14,50
Laboratorio	5,60
Total horas	**20,10**

ACTIVIDADES NO PRESENCIALES

Actividad	Horas
Asistencia a otras actividades	0,00
Elaboración de trabajos individuales o en grupo	0,00
Estudio y trabajo autónomo	22,00
Preparación de clases	6,00
Preparación de actividades de evaluación	2,00
Resolución de casos prácticos	0,00
Total horas	**30,00**

METODOLOGÍA DOCENTE

- Clase de teoría
- Resolución de problemas
- Aprendizaje orientado a proyectos

/ul>

EVALUACIÓN

Los sistemas de evaluación usados en esta asignatura son:

SE1: Evaluación en línea y/o grado de participación

SE2: Evaluación de problemas, trabajos, informes y/o memorias

SE4: Evaluación presencial

SE6: Evaluación de las prácticas de laboratorio

- Primera convocatoria: 0.1*SE1+0.3*SE2+0.2*SE4+0.4*SE6

- Segunda convocatoria: 0.1*SE1+0.3*SE2+0.2*SE4+0.4*SE6

Los trabajos (SE2 y SE6) no superados en la primera convocatoria se podrán enviar. SE1 no es recuperable en la segunda convocatoria.

Las restricciones necesarias que se han de cumplir para que se apliquen los porcentajes indicados anteriormente son las siguientes:

- La nota de SE2, SE4 y SE6 tiene que ser mayor o igual a 5.

El sistema de calificaciones está especificado en el siguiente enlace:

http://www.uv.es/uvweb/universidad/es/estudios-postgrado/informacion-administrativa-postgrado/permanencia-calificaciones/calificaciones-1285897761928.html

La normativas aplicables se encuentran en el siguiente enlace:

http://www.uv.es/uvweb/universidad/es/estudios-grado/informacion-academica-administrativa/normativas/normativas-universidad-valencia-1285850677111.html

BIBLIOGRAFÍA

- 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 crîticos en Aplicaciones Web". 2017. https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/

- Aleksa Vukotic, James Goodwill. Apache Tomcat 7. Apress. 2011.

- Stuart McClure, Saumil Shah, Shreeraj Shah. Web hacking: attacks and defense. 2003