MÁSTER UNIVERSITARIO EN INGENIERÍA WEB

Guía de Aprendizaje
Información al estudiante

Datos Descriptivos

Centro responsable	Escuela Técnica Superior de Ingeniería de Sistemas Informáticos	
Titulación:	Máster Universitario en Ingeniería Web	
Materia:	Servicios de Internet	
Asignatura:	Seguridad en Aplicaciones Web	
Carácter:	Obligatoria	
Curso académico:	2015/2016	
Curso/semestre:	1º	1º
Créditos Europeos	4	
Idioma impartición:	Español	
Departamento:	Sistemas Informáticos	
Profesorado (c = coordinador)	**Despacho**	**Correo electrónico**
Juan Alberto de Frutos Velasco (C)	D-1223	jafrutos@etsisi.upm.es

Conocimientos previos
Asignaturas previas recomendadas
Back-end con Tecnologías de Libre Distribución (PHP)
Conocimientos previos recomendados
Programación web de back-end

Tutorías					
Profesor	Juan Alberto de Frutos Velasco (C)				
Durante la impartición			Fuera de la impartición		
Día	Inicio	Fin	Día	Inicio	Fin
Martes	15:00	17:00	Martes	11:00	14:00
Viernes	10:00	14:00	Jueves	11:00	14:00

Competencias de la asignatura

Competencias específicas y nivel asignado a la asignatura		
Código	**Descripción**	**Nivel**
CE1	Requisitar, analizar y diseñar en un desarrollo Web bajo las metodologías vigentes en el entorno profesional	2
CE2	Programar y probar en un desarrollo Web con los lenguajes y técnicas vigentes en el entorno profesional	3
CE6	Incorporar seguridad, calidad, usabilidad y persistencia al desarrollo Web vigentes en el entorno profesional	3
CE9	Respetar los marcos legal, social y económico de los desarrollos vigentes en el entorno profesional.	3

Competencias generales	
Código	**Descripción**
CG0	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.
CG1	Que los 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.
CG2	Que los 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.
CG4	Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
CG5	Uso de la lengua inglesa
CG6	Liderazgo de equipos
CG7	Creatividad
CG8	Organización y plantificación
CG9	Gestión de la información
CG10	Gestión económica y administrativa

Contenidos de la asignatura

Resultados de Aprendizajes		
Código	Descripción	Competencias Cubiertas
RA1	Conocer los riesgos de seguridad asociados a las aplicaciones web.	CE1 CE6 CE9
RA2	Configurar el sitio web de forma adecuada con objeto de mitigar riesgos de seguridad	CE1 CE6 CE9
RA3	Utilizar soluciones criptográficas adecuadas para una aplicación web.	CE1 CE6 CE9
RA4	Saber identificar vulnerabilidades en las aplicaciones web.	CE2 CE6 CE9
RA5	Saber desarrollar software seguro para aplicaciones web usando cualquier plataforma.	CE1 CE2 CE6 CE9
RA6	Utilizar herramientas que realicen análisis de vulnerabilidades en las aplicaciones web.	CE2 CE6 CE9

Contenidos Formativos			
Tema	**Título**	**Contenidos**	**RA**
T1	**Introducción: el protocolo HTTP y el servidor Apache**	La seguridad web. El proyecto OWASP y los mayores riesgos en las aplicaciones web. Formatos de request y response. Directivas de configuración de Apache. Virtual Hosting.	RA1 RA2
T2	**Autorización y autenticación**	Autenticación y autorización proporcionadas por el servidor web. Ataques por fuerza bruta y ataques de diccionario. Algoritmos hash. Autenticación y autorización web con formularios: uso de sesiones, uso de captchas.	RA1 RA2 RA3 RA4 RA5
T3	**El protocolo SSL**	Conceptos básicos de cifrado y certificados digitales. Comunicación segura a través de SSL. Autenticación de un servidor web con SSL. Autenticación de clientes con SSL. Configuración de SSL en Apache. Generación de certificados con OpenSSL: autoridad de certificación, servidor web y cliente. SSL y ataques MIM. Firma digital de formularios web.	RA1 RA2 RA3

T4	**Cross Site Scripting (XSS) y robo de sesiones**	Tipos de ataques XSS: Reflected XSS, XSS permanente, Cross Site Request Forgery (CRSF). Mitigar los distintos tipos de XSS. Sesiones y cookies. Robo del identificador de sesión. Ataque por fijación de sesión. Medidas para mitigar el robo de sesión.	RA1 RA4 RA5
T5	**SQL injection y otros riesgos.**	Ataques de SQL injection. Medidas para mitigar SQL injection. SQL injection a través de metadatos del SGBD. SQL injection al sistema de ficheros. Mensajes de error. Blind SQL injection. Validación de los datos de entrada. Parameter tampering. Proteger información sensible. Ataques de Directory Traversal y File Inclusion. Carga de ficheros en el servidor. Referencias directas inseguras a objetos. Inyecciones de código.	RA1 RA4 RA5 RA6
T6	**Análisis de vulnerabilidades en aplicaciones web.**	Hacking con buscadores. Analizadores estáticos de código. Analizadores dinámicos. La herramienta Zen Attcack Proxy (ZAP) de OWASP.	RA1 RA4 RA5 RA6

Breve descripción de las modalidades organizativas utilizadas y métodos de enseñanzas empleados	
Clases de teoría	Se sigue el método expositivo / lección magistral. El profesor expone verbalmente los conceptos de la materia en cada uno de los temas.
Clases problemas	Se sigue el método de resolución de problemas en clase. Se plantea un problema que los estudiantes tienen que resolver desarrollando estrategias nuevas a partir de los conocimientos de la clase magistral.
Trabajos autónomos	Durante el desarrollo o a la finalización de una clase se plantea un problema o cuestión teórica en la que el estudiante tiene que demostrar los conocimientos y competencias adquiridas en la sesión de la clase teórica.
Trabajos en grupos	En esencia, el trabajo en grupo se desarrolla durante las sesiones de las prácticas y en la práctica obligatoria de la asignatura.
Prácticas	Al final de cada unidad, se plantean problemas que el alumno deberá resolver y presentar.
Tutorías	No hay tutorías grupales en la asignatura. Las tutorías son individuales y los estudiantes son atendidos en los horarios establecidos para las tutorías académicas.

Evaluación Continua					
Código	**Descripción**	**Valor en %**	**Calificación mínima**	**Carga**	**RA**
ECA	Asistencia y participación en el aula	10%	70%	39,5	RA1 RA2 RA3 RA4 RA5 RA6
ECT	Evaluación de Test	15%	30%	0,5	RA1 RA2 RA3 RA4 RA5
ECP1	Práctica 1: autenticación y SSL	25%	30%	21,0	RA1 RA2 RA3 RA5
ECP2	Práctica 2: XSS y robo de sesiones	20%	30%	16,0	RA1 RA4 RA5
ECP3	Práctica 3: SQL injection y otros riesgos	15%	30%	12,0	RA1 RA4 RA5
ECP4	Trabajo Teórico	15%	30%	15,0	RA1 RA2 RA3 RA4 RA5 RA6

Criterios de Evaluación					
Código	**Descripción**	**ECP1**	**ECP2**	**ECP3**	**ECP4**
ECA	Completitud y calidad de la asistencia a clases con aprovechamiento				
ECT	Completitud y calidad de las respuestas del test				
CEC1	Cumplimiento y Calidad del resultado de Conocer los riesgos de seguridad asociados a las aplicaciones web. en la solución entregada	**20%**	**20%**	**20%**	**10%**
CEC2	Cumplimiento y Calidad del resultado de Configurar el sitio web de forma adecuada con objeto de mitigar riesgos de seguridad en la solución entregada	**30%**			**10%**
CEC3	Cumplimiento y Calidad del resultado de Utilizar soluciones criptográficas adecuadas para una aplicación web. en la solución entregada	**20%**			**10%**
CEC4	Cumplimiento y Calidad del resultado de Saber identificar vulnerabilidades en las aplicaciones web. en la solución entregada		**40%**	**40%**	**10%**

CEC5	Cumplimiento y Calidad del resultado de Saber desarrollar software seguro para aplicaciones web usando cualquier plataforma. en la solución entregada	**30%**	**40%**	**40%**	**10%**
CEC6	Cumplimiento y Calidad del resultado de Utilizar herramientas que realicen análisis de vulnerabilidades en las aplicaciones web. en la solución entregada				**50%**

Evaluación Final				
Código	**Descripción**	**Valor en %**	**Calificación mínima**	**RA**
EFE	Examen final escrito	35%	30%	RA1 RA2 RA3 RA4 RA5 RA6
EFT	Evaluación de Test	15%	30%	RA1 RA2 RA3 RA4 RA5
EFP1	Práctica Final	35%	30%	RA1 RA2 RA3 RA4 RA5
EFP2	Trabajo Teórico	15%	30%	RA1 RA2 RA3 RA4 RA5 RA6

Criterios de Evaluación			
Código	**Descripción**	**EFP1**	**EFP2**
EFE	Completitud y calidad de las respuestas de los supuestos prácticos del examen		
EFT	Completitud y calidad de las respuestas del test		
CEF1	Cumplimiento y Calidad del resultado de Conocer los riesgos de seguridad asociados a las aplicaciones web. en la solución entregada	**20%**	**10%**
CEF2	Cumplimiento y Calidad del resultado de Configurar el sitio web de forma adecuada con objeto de mitigar riesgos de seguridad en la solución entregada	**10%**	**10%**
CEF3	Cumplimiento y Calidad del resultado de Utilizar soluciones criptográficas adecuadas para una aplicación web. en la solución entregada	**10%**	**10%**
CEF4	Cumplimiento y Calidad del resultado de Saber identificar vulnerabilidades en las aplicaciones web. en la solución entregada	**25%**	**10%**
CEF5	Cumplimiento y Calidad del resultado de Saber desarrollar software seguro para aplicaciones web usando cualquier plataforma. en la solución entregada	**35%**	**10%**
CEF6	Cumplimiento y Calidad del resultado de Utilizar herramientas que realicen análisis de vulnerabilidades en las aplicaciones web. en la solución entregada		**50%**

Cronograma de Trabajo de la Asignatura		
Evaluación Continua para Grupo de Mañana		
Día	**Actividades aula**	**Actividades Evaluación**
1	T1	ECA
2	T2	ECA
3	T3	ECA
4	T3	ECA
5	T4	ECA
6	T4 T5	ECA
7	T5	ECA
8	T6	ECA
(lunes)		ECT ECP1 ECP2 ECP3 ECP4

Cronograma de Trabajo de la Asignatura		
Evaluación Continua para Grupo de Fin de Semana		
Día	**Actividades aula**	**Actividades Evaluación**
1 (viernes)	T1 T2	ECA
2 (sábado)	T3	ECA
3..6 (L - J)	Realización de prácticas (asistencia no obligatoria	
7 (viernes)	T4 T5	ECA
8 (sábado)	T5 T6	ECA
9..12 (L - J)	Realización de prácticas (asistencia no obligatoria	
(viernes)		ECT ECP1 ECP2 ECP3 ECP4

Recursos didácticos

Recursos didácticos	
Equipamiento	Aula 7 del Centro de Informática y Comunicaciones con 30 puestos dotados con PC en red, Pizarra y cañón de video
Recursos Web	http://moodle.upm.es/titulaciones/oficiales/course/view.php?id=3269
Bibliografía	http://www.owasp.org
	Chris Snider, Thomas Myer, Michale Southwell "Pro PHP Security", 2nd Edition, Apress, 2010
	Bryan Sullivan, Vincent Liu, "Web application security", Mc Graw Hill, 2012
	Chris Shiflett, "Esential PHP Security", O'Really, 2005
	Ivan Ristic, "Bulletproof SSL and TLS", Feisty Duck, 2014