Guía Docente: Técnicas de auditoría, ataque y programación segura de aplicaciones web

DATOS GENERALES	
Facultad	Facultad de Ciencias y Tecnología
Titulación	Grado en Ingeniería Informática
Plan de estudios	2012
Especialidad/Mención	Criptología y Seguridad de la Información
Materia	Criptología y Seguridad de la Información
Carácter	Optativo
Período de impartición	Segundo Trimestre
Curso	Cuarto
Nivel/Ciclo	Grado
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	Nninguno

DATOS DEL PROFESORADO			
Profesor Responsable	Cristina Romero Tris	**Correo electrónico**	cristina.romero.tris@ui1.es
Área		**Facultad**	Facultad de Ciencias y Tecnología
Perfil Profesional 2.0	Cristina Romero Tris es Doctora en Ingeniería Informática por la Universidad Rovira i Virgili (URV). Posee un título de Máster en Seguridad Informática y Sistemas Inteligentes, que le permitió especializarse en el campo de la seguridad y la privacidad en la sociedad de la información. Asimismo, desarrolló su doctorado y enfocó su actividad investigadora en este mismo campo, centrándose en las aplicaciones prácticas de la criptografía. Tiene más de 20 publicaciones e intervenciones en congresos relacionados. En cuanto a actividad docente, ha impartido varias asignaturas relacionadas con la Seguridad Informática en Universidades tanto presenciales como online desde 2012. En estas asignaturas se aplicaban Técnicas criptográficas a diversos campos, como las Redes de computadores o el Comercio Electrónico. LinKedin		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Auditoría y seguridad avanzada de sistemas y redes de comunicaciones • Autenticación y Sistemas Biométricos • Criptografía y Criptoanálisis • Dirección de Proyectos de Seguridad Corporativos • Técnicas de Análisis Forense • Técnicas de auditoría, ataque y programación segura de aplicaciones web
Contexto y sentido de la asignatura en la titulación y perfil profesional	Esta asignatura forma parte de las asignaturas optativas del itinerario de Criptología y Seguridad de la Información del último año del Grado en Ingeniería Informática. En ella se pretende estudiar las principales técnicas de programación segura y auditoría de aplicaciones Web. Para lograr este objetivo analizaremos en detalle diferentes técnicas de ataque a dichas aplicaciones y los métodos mediante los cuales se puede evitar que estos ataques tengan éxito.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	• CRO6 - Conocimiento y aplicación de los procedimientos algorítmicos básicos de las tecnologías informáticas para diseñar soluciones a problemas, analizando la idoneidad y complejidad de los algoritmos propuestos • CR10 - Conocimiento de las características, funcionalidades y estructura de los Sistemas Operativos y diseñar e implementar aplicaciones basadas en sus servicios. • CT-06 - Capacidad de trabajo en equipo • CT-09 - Capacidad para innovar y generar nuevas ideas • CU2 - Identificar y dar valor a las oportunidades tanto personales como profesionales, siendo responsables de las actuaciones que se pongan en marcha, sabiendo comprometer los recursos necesarios, con la finalidad de realizar un proyecto viable y sostenible para uno mismo o para una organización. • CU3 - Utilizar la expresión oral y escrita de forma adecuada en contextos personales y profesionales. • CU4 - Utilizar las Tecnologías de la Información y la Comunicación (TIC) para poner en marcha procesos de trabajo ajustados a las necesidades de la sociedad actual. • CU6 - Aprender a trabajar individualmente de forma activa • CU17 - Ser capaz de concluir adecuadamente la tesis de la exposición basándose en modelos, teorías o normas, etc • CT-01 - Capacidad de análisis y síntesis: encontrar, analizar, criticar (razonamiento crítico), relacionar, estructurar y sintetizar información proveniente de diversas fuentes, así como integrar ideas y conocimientos • CT-03 - Capacidad de comunicación oral y escrita en el ámbito académico y profesional, con especial énfasis en la redacción de documentación técnica. • CT-04 - Capacidad para la resolución de problemas • CU1O - Reconocer y saber resolver problemas que afecten a derechos fundamentales de las personas y a valores democráticos • CU15 - Utilizar una adecuada estructura lógica y un lenguaje apropiado para el público no especialista y escribir con corrección. • CU16 - Saber transmitir un informe técnico de la especialidad. • CMC-01 - Conocimiento de los métodos matemáticos básicos sobre los que se fundamentan las principales primitivas criptológicas y procedimientos de criptoanàlisis. • CMC-02 - Capacidad para conocer, comprender y utilizar las principales primitivas

	criptográficas, identificar la mas adecuada para cada uso y aplicarlas adecuadamente para garantizar la seguridad del procedimiento. • CMC-03 - Comprensión y capacidad de utilización de los principales métodos y procedimientos de criptoanálisis, aplicando los mismos para la identificación y recuperación de textos cifrados con algoritmos clásicos o débiles. • CMC-04 - Capacidad para plantear, desarrollar y dirigir el análisis forense de un sistema informático comprometido, firmando un informe con conclusiones fundamentadas y razonadas, que pueda ser posteriormente utilizado en un proceso legal • CMC-05 - Capacidad para identificar, comprender y solucionar las principales vulnerabilidades que afectan a las aplicaciones Web, así como para diseñar y programar éstas de forma segura. • CMC-06 - Capacidad para concebir, desarrollar y desplegar proyectos globales y políticas de seguridad corporativas, teniendo en cuenta criterios organizacionales, económicos y aspectos legales. • CMC-07 - Conocimiento y aplicación de los principios fundamentales y técnicas básicas de autenticación de personas físicas y sistemas informáticos, incluyendo los sistemas biométricos y de doble factor. • CMC-08 - Conocimiento sobre los principales tipos de malware, sus vectores de ataque, técnicas de ocultación y de auto-protección más usuales, y capacidad para realizar un correcto análisis del espécimen. • CMC-09 - Capacidad para plantear, desarrollar y dirigir el proceso de auditoría de un sistema en red, de forma manual y a través del uso de herramientas automáticas, generando un informe que resume los resultados.
Resultados de aprendizaje de la asignatura	• Realiza una correcta auditoría de caja negra de una aplicación Web, detectando, identificando y explotando sus principales vulnerabilidades. • Sabe cómo solucionar las principales vulnerabilidades de una aplicación Web, y diseña y codifica éstas de forma segura. • Realiza una correcta auditoría de caja blanca de una aplicación Web, independientemente del lenguaje de programación utilizado, detectando e identificando las principales vulnerabilidades. • Conoce los fundamentos del análisis dinámico y estático de código, y posee experiencia con herramientas que automatizan esta tarea. • Posee experiencia en el uso de escáneres remotos de vulnerabilidades, comprende los informes que éstos generan y es capaz de explicarlos a una audiencia no técnica. • Concibe, desarrolla y despliega proyectos globales y políticas de seguridad corporativas, teniendo en cuenta criterios organizacionales, económicos y aspectos legales.

PROGRAMACION DE CONTENIDOS	
Breve descripción de la asignatura	El objetivo de esta asignatura es introducir al alumno en la programación segura de aplicaciones Web. Para ello, se estudiarán primero conceptos de auditoría de caja negra, destinados a descubrir las principales vulnerabilidades de una aplicación, para analizar posteriormente cómo éstas pueden ser subsanadas y corregidas.
Contenidos	**Unidad Didáctica 1: El modelo de amenazas** • Seguridad • El perímetro de seguridad • Las aplicaciones web • Funcionalidad web • Modelado de amenazas

- El entorno de pruebas

Unidad Didáctica 2: Análisis externo de una aplicación

- Enumerando los contenidos y la funcionalidad
- Recopilación de enlaces
- Search Engine Discovery
- Google Dorks
- Contenido oculto
- Técnicas de fuerza bruta
- Analizando el servidor web
- Aplicaciones web con contenidos por defecto .
- El fichero robots.txt
- Aplicaciones en servidores compartidos
- Puntos de interacción con el usuario
- Tecnologías empleadas por el servidor
- Mapeando la aplicación

Unidad Didáctica 3: Configuración del servidor y despliegue de la aplicación

- Configuraciones vulnerables
- Credenciales por defecto
- Contenido por defecto
- Funciones de depurado
- Funcionalidad por defecto
- Funciones restringidas a los administradores
- Listado de directorios
- Métodos WebDAV
- Problemas de configuración de los Virtual Hosts
- Asegurando la configuración del servidor
- Software de servidor vulnerable
- Encontrar vulnerabilidades en el software de servidor web
- Asegurando el servidor .

Unidad Didáctica 4: Autenticación del usuario

- Mecanismos de autenticación
- Fallos de diseño
- Ataques de fuerza bruta
- Mensajes de fallo de autenticación
- Transmisión vulnerable de credenciales
- Funcionalidad de cambio de claves
- Contraseña olvidada
- Almacenamiento de credenciales en la aplicación
- Asegurando los mecanismos de autenticación

Unidad Didáctica 5: Validación de entradas de usuario

- Entorno seguro de pruebas
- ¿Qué es la inyección SQL (SQLi)?
- Ejemplo de ataque SQLi

Unidad Didáctica 6: Lógica de negocio

- Vulnerabilidades comunes
- ZAP

METODOLOGÍA	
Actividades formativas	El alumno dispondrá de un espacio dentro del Aula virtual, organizado en seis unidades didácticas. Cada unidad didáctica tendrá un apartado de Contenidos, con los conceptos teóricos sobre la asignatura, y dos actividades por unidad didáctica, de entre las siguientes posibilidades: • **Cuestionario de evaluación:** Cuestionario donde el alumno podrá comprobar si ha asimilado los contenidos explicados en esa unidad. • **Actividades prácticas (Laboratorio práctico):** Incluye el trabajo individual en la resolución de problemas, elaboración de proyectos y actividades similares que permitan aplicar los aspectos conceptuales, procedimentales y actitudinales trabajados en otras partes de la asignatura. • **Trabajo colaborativo**: Los alumnos realizarán un trabajo práctico en grupos de dos o más personas. • **Foros de debate**: Los alumnos expresarán sus opiniones sobre temas de actualidad relacionados con la unidad. • **Estudios de caso**: Los alumnos realizarán un trabajo previo de investigación sobre algún tema clave relacionado con el contenido de la unidad. • **Tutorías:** Se realizarán tres tutorías síncronas a lo largo del trimestre donde se expone la resolución de las dudas presentadas al profesor previamente. Una vez realizadas pueden visualizarse en diferido. • **Lectura crítica, análisis e investigación**: Se trata de actividades en las que el alumno se acerca a los diferentes campos de estudio con una mirada crítica que le permite un acercamiento a la investigación. • **Prueba de Evaluación por Competencias (PEC)**: En el caso de optar por la opción 2 de evaluación (PEC+ examen final), el estudiante tendrá que realizar la prueba de evaluación de competencias (PEC). Esta prueba se define como una actividad integradora a través de la cual el estudiante deberá demostrar la adquisición de competencias propuestas en la asignatura, vinculadas principalmente al «saber hacer». Para ello hará entrega de un conjunto de evidencias en respuesta a los retos propuestos en esta prueba. La entrega se realizará antes de finalizar la asignatura.

EVALUACIÓN	
Sistema evaluativo	El sistema de evaluación se basará en una selección de las pruebas de evaluación más adecuadas para el tipo de competencias que se trabajen. El sistema de calificaciones estará acorde con la legislación vigente *(Real Decreto 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y de validez en todo el territorio nacional)*. El sistema de evaluación de la Universidad Isabel I queda configurado de la siguiente manera: **Sistema de evaluación convocatoria ordinaria** **Opción 1. Evaluación continua** Los estudiantes que opten por esta vía de evaluación deberán realizar el **seguimiento de la evaluación continua (EC)** y podrán obtener hasta un **60 %** de la calificación final a través de las actividades que se plantean en la evaluación continua.

Además, deberán realizar un **examen final presencial (EX)** que supondrá el **40 %** restante. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del trabajo realizado durante la evaluación continua y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación continua.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de evaluación continua, siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Opción 2. Prueba de evaluación de competencias

Los estudiantes que opten por esta vía de evaluación deberán realizar una **prueba de evaluación de competencias (PEC)** y un **examen final presencial (EX)**.

La **PEC** se propone como una prueba que el docente plantea con el objetivo de evaluar en qué medida el estudiante adquiere las competencias definidas en su asignatura. Dicha prueba podrá ser de diversa tipología, ajustándose a las características de la asignatura y garantizando la evaluación de los resultados de aprendizaje definidos. Esta prueba supone el 50 % de la calificación final.

El **examen final presencial**, supondrá el **50 %** de la calificación final. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del seguimiento de las actividades formativas desarrolladas en el aula virtual y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Al igual que con el sistema de evaluación anterior, para la aplicación de los porcentajes correspondientes el estudiante debe haber obtenido una puntuación mínima de un 4 en cada una de las partes de las que consta la opción de prueba de evaluación de competencias.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de la prueba de evaluación de competencias siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Características de los exámenes

Los exámenes constarán de 30 ítems compuestos por un enunciado y cuatro opciones de respuesta, de las cuales solo una será la correcta. Tendrán una duración de 90 minutos y la calificación resultará de otorgar 1 punto a cada respuesta correcta, descontar 0,33 puntos por cada respuesta incorrecta y no puntuar las no contestadas. Después, con el resultado total, se establece una relación de proporcionalidad en una escala de 10.

Sistema de evaluación convocatoria extraordinaria

Todos los estudiantes, independientemente de la opción seleccionada, que no superen las pruebas evaluativas en la convocatoria ordinaria tendrán derecho a una convocatoria extraordinaria.

	La convocatoria extraordinaria completa consistirá en la realización de una **prueba de evaluación de competencias** que supondrá el **50 %** de la calificación final y un **examen final presencial** cuya calificación será el **50 %** de la calificación final. Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación de la convocatoria extraordinaria. Los estudiantes que hayan suspendido todas las pruebas evaluativas en convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final) o no se hayan presentado deberán realizar la convocatoria extraordinaria completa, como se recoge en el párrafo anterior. En caso de que hayan alcanzado una puntuación mínima de un 4 en alguna de las pruebas evaluativas de la convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final), se considerará su calificación para la convocatoria extraordinaria, debiendo el estudiante presentarse a la prueba que no haya alcanzado dicha puntuación o que no haya realizado. En el caso de que el alumno obtenga una puntuación que oscile entre el 4 y el 4,9 en las dos partes de que se compone la convocatoria ordinaria (EC o PEC y examen), solo se considerará para la convocatoria extraordinaria la nota obtenida en la evaluación continua o prueba de evaluación de competencias ordinaria (en función del sistema de evaluación elegido), debiendo el alumno realizar el examen extraordinario para poder superar la asignatura. Al igual que en la convocatoria ordinaria, se entenderá que el alumno ha superado la materia en convocatoria extraordinaria si, aplicando los porcentajes correspondientes, se alcanza una calificación mínima de un 5.

BIBLIOGRAFÍA Y OTROS RECURSOS	
Bibliografía básica	D. Stuttard and M. Pinto, "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws," John Wiley & Sons, 2011. Libro muy completo que analiza las aplicaciones web desde el punto de vista de la seguridad ofensiva. Ilustra de manera práctica los ataques que se pueden realizar contra aplicación web y als contramedidas que se han de tomar para mitigar estos ataques. M. Zalewski, "The tangled Web: A guide to securing modern web applications," No Starch Press, 2012. Analiza de forma exhaustiva el modelo de seguridad de la web y nos navegadores actuales y desgrana los conceptos necesarios para que las aplicaciones sean más seguras.
Bibliografía complementaria	Gourley, D. y Totty, B. (2002). *HTTP: the definitive guide*. O'Reilly Media, Inc. Owasp, T. (2013). *Top 10–2013. The Open Web Application Security Project.* Muller, A. Meucci, M. Keary, E. y Cuthbert, D. (2016). *OWASP Testing Guide 4.0*. Publicado por OWASP. Recuperado de https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf Clarke, J. (2009). *SQL injection attacks and defense*. Elsevier. Fogie, S. Grossman, J. Hansen, R. Rager, A. y Petkov, P. D. (2011). *XSS Attacks: Cross Site Scripting Exploits and Defense*. Syngress. Mackman, A. Dunner, M. Vasireddy, S. Escamilla, R. & Murukan, A. (2003). *Improving web application security: threats andcountermeasures*. Redmond, W A: Microsoft.
Otros recursos	D. Gourley and B. Totty, "HTTP: the definitive guide," O'Reilly Media, Inc., 2002. T. Owasp, "Top 10-2013," The Open Web Application Security Project, 2013. A. Muller, M. Meucci, E. Keary, and D. Cuthbert, "OWASP Testing Guide 4.0," Publicado por OWASP. [En línea]. Disponible en: https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf J. Clarke, "SQL injection attacks and defense," Elsevier, 2009. S. Fogie, J. Grossman, R. Hansen, A. Rager, and P. D. Petkov, "XSS Attacks: Cross Site Scripting Exploits and Defense," Syngress, 2011. A. Mackman, M. Dunner, S. Vasireddy, R. Escamilla, and A. Murukan, "Improving web application security: threats and countermeasures," Redmond, WA: Microsoft, 2003.