

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	Mención en 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	LinKedin		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA

Asignaturas de la materia	<ul style="list-style-type: none"> • 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	<p>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.</p> <p>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.</p>

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE

Competencias de la asignatura	<ul style="list-style-type: none"> • CMC05: 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. • 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. • CMC06: Capacidad para concebir, desarrollar y desplegar proyectos globales y políticas de seguridad corporativas, teniendo en cuenta criterios organizacionales, económicos y aspectos legales.
Resultados de aprendizaje de la asignatura	<ul style="list-style-type: none"> • 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	<p>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.</p>
---	--

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.

EVALUACIÓN

Sistema evaluativo

En caso de que la situación sanitaria impida la realización presencial de los exámenes con todas las garantías, la Universidad Isabel I celebrará dichas pruebas en modalidad online. Para la realización de dichos exámenes, la universidad incorporará la herramienta de proctoring a nuestra plataforma tecnopedagógica, con el objetivo de garantizar los procesos de autenticación del alumno, como el control del entorno durante el desarrollo de las pruebas de evaluación. A su vez, la Universidad Isabel I pondrá a disposición del alumnado una Unidad de Exámenes Online específica para ofrecer apoyo técnico durante todo el proceso y así solventar todas las incidencias que se puedan presentar.

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.

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

<p>Bibliografía básica</p>	<p>Stuttard, D. y Pinto, M. (2011). <i>The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws</i>. John Wiley & Sons.</p> <p>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 las contramedidas que se han de tomar para mitigar estos ataques.</p> <p>Zalewski, M. (2012). <i>The tangled Web: A guide to securing modern web applications</i>. No Starch Press.</p> <p>Analiza de forma exhaustiva el modelo de seguridad de la web y los navegadores actuales y desgrana los conceptos necesarios para que las aplicaciones sean más seguras.</p>
<p>Bibliografía complementaria</p>	<p>Gourley, D. y Totty, B. (2002). <i>HTTP: the definitive guide</i>. O'Reilly Media, Inc.</p> <p>Owasp, T. (2013). <i>Top 10–2013. The Open Web Application Security Project</i>.</p> <p>Muller, A. Meucci, M. Keary, E. y Cuthbert, D. (2016). <i>OWASP Testing Guide 4.0</i>. Publicado por OWASP. Recuperado de https://www.owasp.org/images/1/19/OTGv4.pdf.</p> <p>Clarke, J. (2009). <i>SQL injection attacks and defense</i>. Elsevier.</p> <p>Fogie, S. Grossman, J. Hansen, R. Rager, A. y Petkov, P. D. (2011). <i>XSS Attacks: Cross Site Scripting Exploits and Defense</i>. Syngress.</p> <p>Mackman, A. Dunner, M. Vasireddy, S. Escamilla, R. & Murukan, A. (2003). <i>Improving web application security: threats and countermeasures</i>. Redmond, WA: Microsoft.</p>
<p>Otros recursos</p>	<p>Web de la agencia del departamento de comercio de EEUU del Instituto Nacional de Estándares y Tecnología http://www.nist.gov/itl/ y de la división de seguridad informática http://csrc.nist.gov/groups/STM/</p> <p>Curphey, M. y Arawo, R. (2006). <i>Web application security assessment tools</i>. <i>Security & Privacy, IEEE</i>, 4(4), 32-41.</p> <p>Meier, J. D. (2006). Web application security engineering. <i>Security & Privacy, IEEE</i>, 4(4), 16-24.</p> <p>La web de OWASP http://www.owasp.org</p> <p>La web de INCIBE (Instituto nacional de ciberseguridad de España) https://www.incibe.es</p> <p>La web del laboratorio de ciberseguridad del MIT http://www.csail.mit.edu</p>