Guía Docente

DATOS DE IDENTIFICACIÓN

Titulación:	Diploma en Ciberseguridad y Hacking Ético (Título Propio asociado a Ingeniería Informática)
Rama de Conocimiento:	Ingeniería y Arquitectura
Facultad/Escuela:	Escuela Politécnica Superior
Asignatura:	Desarrollo Seguro S-SDLC - OWASP
Tipo:	Propia Obligatoria
Créditos ECTS:	1,50
Curso:	2
Código:	56416
Periodo docente:	Cuarto semestre
Tipo de enseñanza:	Presencial
Idioma:	Castellano
Total de horas de dedicación del alumno:	37,50

Equipo Docente	Correo Electrónico
Jorge Antonio Cisneros González	j.cisneros.prof@ufv.es

DESCRIPCIÓN DE LA ASIGNATURA

Esta asignatura proporciona un conocimiento de los conceptos del desarrollo seguro desde el punto de vista de la ingeniería del software, incidiendo en los ciclos de vida de desarrollo seguro (S-SLDC) y atendiendo al proyecto abierto de seguridad en aplicaciones Web (OWASP por sus siglas en inglés).

Esta asignatura corresponde al título propio de Ciberseguridad y Hacking Ético que complementa los estudios de Grado en Ingeniería Informática. Se imparte en el segundo semestre del segundo curso. Requiere una dedicación de 35 horas por parte del alumno.

OBJETIVO

El objetivo principal de esta asignatura es dar a conocer al alumno cuáles son los fallos de software más comunes según la clasificación elaborada anualmente por OWASP, y en la medida de lo posible, explicar cómo se pueden evitar desde el punto de vista del desarrollador.

Los fines especficos de la asignatura son:

Que el alumno obtenga las herramientas necesarias para evaluar la calidad del software desde el punto de vista de la seguridad informática

CONOCIMIENTOS PREVIOS

Es recomendable que el alumno haya aprobado las asignaturas del primer curso del título propio así como las asignaturas de Introducción a la Programación y Programación Orientada a Objetos.

CONTENIDOS

Estudio de las vulnerabilidades más frecuentes según la clasificación de OWASP, utilizando la herramienta Juice Shop. Concretamente:
https://owasp.org/www-project-top-ten/

A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures
A10:2021-Server-Side Request Forgery

ACTIVIDADES FORMATIVAS

El alumno resolverá los distintos retos integrados en la herramienta Juice Shop, desde el nivel 1 al nivel 3 obligatoriamente, y de nivel 4 a 6 de forma voluntaria.

En clase se resolverán conjuntamente varios de ellos para que sepan cómo funciona y cómo se utilizan las herramientas más comunes de análisis de seguridad en el desarrollo de software.

Además, para apoyar el trabajo individual del alumno, en el Aula Virtual de la Universidad (Canvas) los alumnos cuentan con una resolución de esos retos iniciales grabados en video, que pueden consultar cuando quieran.

Las actividades de carácter no presencial previstas incluyen el estudio individual, que permitirá trabajar en la fijación de los conceptos teóricos abordados en las clases expositivas correspondientes a todas las materias del módulo y adquirir la destreza práctica que se persigue con las clases prácticas y los laboratorios, que aplicarán el aprendizaje por descubrimiento. El estudio y trabajo realizado por el alumno será supervisado y guiado por el profesor mediante tutorías, individuales o en grupo. En algunos casos, el alumno tendrá que realizar en clase la exposición de las principales conclusiones de su estudio o trabajo, lo que permitirá el intercambio de conocimientos y experiencias entre alumnos

DISTRIBUCIÓN DE LOS TIEMPOS DE TRABAJO

ACTIVIDAD PRESENCIAL	TRABAJO AUTÓNOMO/ACTIVIDAD NO PRESENCIAL
19 horas	18,50 horas
Lección expositiva 15h Tutorías 2h Evaluación 2h	Estudio y trabajo individual 11,50h Trabajo en grupo 7h

COMPETENCIAS

Conocer y poner en práctica técnicas y herramientas de análisis de las vulnerabilidades del software.

Evaluar si un programa está correctamente desarrollado siguiendo estándares de seguridad.

RESULTADOS DE APRENDIZAJE

El alumno conoce y pone en práctica técnicas y herramientas de análisis de las vulnerabilidades del software más frecuentes.

El alumno es capaz de evaluar distintos programas desde el punto de vista de los estándares de seguridad.

SISTEMA DE EVALUACIÓN DEL APRENDIZAJE

El sistema de evaluación contempla cuatro tipos de pruebas:
•[1] Práctica obligatoria sobre los niveles 1 a 3: presenta un peso del 30% en la nota final.
•[2] Práctica voluntaria sobre los niveles 4 a 6: presenta un peso del 35% en la nota final.
•[3] Examen tipo test: presenta un peso del 30% en la nota final.
•[4] Participación en clase e implicación en la asignatura: presenta un peso del 5% en la nota final, siendo requisito imprescindible haber asistido como mínimo al 80% de las sesiones. En caso contrario este tipo de prueba se calificará con 0 puntos.
En la prueba [1] es necesario obtener un mínimo de 5 puntos sobre 10 para poder aprobar la asignatura.
En la prueba [2] NO es necesario obtener un mínimo de 5 puntos sobre 10 para poder aprobar la asignatura.
En la prueba [3] es necesario tener un mínimo de 5 puntos para poder aprobar la asignatura.
Aquellos alumnos que estén exentos de la obligación de asistir a clase, bien por segunda matrícula en la asignatura o sucesivas, bien por contar con autorización expresa de la Dirección del Grado, serán evaluados por el mismo tipo de pruebas. El 5% de la participación en clase podrán obtenerlo asistiendo al menos a tres tutorías con el profesor responsable de la asignatura o entregando las prácticas que el profesor les asigne.
Recuperación en convocatoria extraordinaria: Los alumnos que no hayan alcanzado la nota mínima en el examen, habiendo suspendido por tanto en la convocatoria ordinaria, podrán optar a una recuperación en la convocatoria extraordinaria.
En convocatoria extraordinaria el alumno se presentará solo a las partes que tenga evaluadas por debajo de 5 .
La nota ponderada de la evaluación continua será un valor entre 0 y 10 y se calculará como sigue: 0,30*[1] + 0,35*[2] + 0,30* [3] + 0,05*[4].
A efecto de cómputo de convocatorias en una asignatura, solamente se contabilizarán como consumidas aquellas en las que el alumno se haya presentado a todas las pruebas de evaluación, o a una parte de las mismas, siempre que su peso en la nota final supere el 50%, aunque no se presente al examen final. Se entenderá que un alumno

se ha presentado a una prueba aunque la abandone una vez comenzada la misma. La condición de No Presentado en la convocatoria extraordinaria estará ligada a la no asistencia o entrega de ninguna prueba, práctica o trabajo que esté pendiente.

Cualquier tipo de fraude o plagio por parte del alumno en una actividad evaluable, será sancionado según se recoge en la Normativa de Convivencia de la UFV. A estos efectos, se considerará "plagio" cualquier intento de defraudar el sistema de evaluación, como copia en ejercicios, exámenes, prácticas, trabajos o cualquier otro tipo de entrega, bien de otro compañero, bien de materiales o dispositivos no autorizados, con el fin de hacer creer al profesor que son propios.

_____

[1] Grabación de la resolución de varios retos de nivel 1 a 3, explicando cómo se resuelven (justificándolo) y cómo se podría evitar desde el punto de vista del desarrollador de software.
[2] Grabación de la resolución de varios retos de nivel 4 a 6, explicando cómo se resuelven (justificándolo) y cómo se podría evitar desde el punto de vista del desarrollador de software.
[3] Examen tipo test sobre la teoría alojada en Canvas. 50 preguntas tipo test, sólo una respuesta correcta a elegir entre 5, restan las incorrectas.
[4] Participación e implicación: 5% de la calificación final. Se evaluarán los ejercicios y otras actividades en grupo, el interés mostrado por el alumno, concretamente se computará el índice de asistencia a tutorías tanto individuales o grupales, el grado de participación activa en las clases mediante la respuesta a preguntas del profesor, el estudio de temas avanzados no vistos en clase, la recopilación de noticias aparecidas en los medios de comunicación relacionadas con la asignatura, etc. La calificación de este apartado será un valor numérico entre 0 y 10. Aunque esta nota sea inferior a 5, no se podrá optar a recuperación.

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

Björn Kimminich Pwning OWASP Juice Shop
https://pwning.owasp-juice.shop/companion-guide/latest/