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:	Seguridad en Aplicaciones Móviles y Web
Tipo:	Propia Obligatoria
Créditos ECTS:	4
Curso:	3
Código:	56417
Periodo docente:	Quinto semestre
Tipo de enseñanza:	Presencial
Idioma:	Castellano
Total de horas de dedicación del alumno:	100

Equipo Docente	Correo Electrónico
Tomás Isasia Infante	tomas.isasia@ufv.es
Jaime José López Ruiz	j.lruiz.prof@ufv.es

DESCRIPCIÓN DE LA ASIGNATURA

Actualmente, la mayoría de personas realizan sus operaciones a través de un dispositivo, ya sea utilizando una aplicación móvil o mediante una aplicación web. La mayoría de los datos residen en servidores web que crean contenido dinámico mediante software para presentarlo a los usuarios en sus dispositivos. A pesar de que el canal de transmisión está cifrado, siguen existiendo vulnerabilidades en los extremos, principalmente en el del servidor. Es por ello, que la asignatura Seguridad en Aplicaciones Móviles y Web, permite al alumno conocer los diferentes sistemas existentes a nivel de servidor que deben ser protegidos, donde no solo existe un hardware, sino también una multitud de aplicaciones que pueden ser atacadas. Por otro lado, esta asignatura también introduce al alumno en los vectores de ataque de dispositivos móviles como Android.

Esta asignatura corresponde al título propio de Ciberseguridad y Hacking Ético que complementa los estudios de Grado en Ingeniería Informática. Se imparte en el primer semestre del tercer curso. Requiere una dedicación de 100 horas por parte del alumno.

OBJETIVO

El objetivo de esta asignatura es introducir al alumno en el manejo de herramientas para el análisis de vulnerabilidades en servidores web, servicios web y plataformas móviles además de enseñar los conceptos básicos en torno a la seguridad en aplicaciones web y móviles así como las amenazas y las pruebas que se pueden desarrollar para comprobar dicha seguridad.

CONOCIMIENTOS PREVIOS

Conocimientos básicos de
Sistemas operativos
Programación y desarrollo web
Hacking Ético
Redes y comunicaciones

CONTENIDOS

El contenido básico que se impartirá en la asignatura será el que se explica a continuación, pudiendo sufrir alguna modificación si las circunstancias y/o la operativa de clase lo requiriese.

- Módulo 1 Entendiendo el alcance de la Seguridad.Componentes de la seguridadAmenazas a la seguridadDefensa en profundidadConociendo al enemigo, Perfil y perspectiva de un atacante
- Módulo 2 Construcción de SW Seguro.Ciclo de vida del desarrollo seguro (S-SDLC).Modelos SDLC
- Módulo 3 OWASP OWASP Top Ten 2021Prevención de vulnerabilidad desde el códigoHacking Web Servers y ApplicationsOWASP Top Ten 2018 Controles proactivosOWASP Mobile Security Project: Top 10 Mobile Risk / Hacking Mobile

ACTIVIDADES FORMATIVAS

Prácticas
Resolución de ejercicios sobre máquinas virtuales vulnerables
Planteamiento / exposición / resolución de problemas reales

DISTRIBUCIÓN DE LOS TIEMPOS DE TRABAJO

ACTIVIDAD PRESENCIAL	TRABAJO AUTÓNOMO/ACTIVIDAD NO PRESENCIAL
40 horas	60 horas

COMPETENCIAS

Conocimientos básicos para la recolección de Información

Conocer y entender el top 10 de las vulnerabilidades consideradas críticas por OWASP tanto en aplicaciones web como en móviles.

Entender las amenazas y vulnerabilidades a las que está expuesta cualquier aplicación

Reconocer y detectar de manera proactiva los fallos del desarrollo de las aplicaciones

Identificar vulnerabilidades en aplicaciones en forma manual y con herramientas

Aplicar las contramedidas necesarias para aumentar la seguridad de las aplicaciones

Conocer el conjunto de pruebas y herramientas que se pueden utilizar para probar la fortaleza de una aplicación.

RESULTADOS DE APRENDIZAJE

Reconocer el top 10 de vulnerabilidades web

Reconocer el top 10 de vulnerabilidades móviles

Use de herramientas de seguridad

SISTEMA DE EVALUACIÓN DEL APRENDIZAJE

Si los exámenes no se pudieran realizar de forma presencial, se realizarán de forma remota mediante las herramientas que determine la Universidad Francisco de Vitoria, garantizando siempre la evaluación de las competencias y resultados de aprendizaje de la asignatura.
Las prácticas NO son reevaluables, la nota obtenida durante el curso es la que se traslada entre las convocatorias ordinaria y extraordinaria.
La asignatura se evaluará mediante las notas de un máximo de dos exámenes, de la asistencia y la participación en clase y de las prácticas correspondientes con la ponderación descrita en este apartado.
A) En la convocatoria ordinaria,
Él alumno será susceptible de ser evaluado por curso (evaluación continua) si asiste a un mínimo del 80% de las clases.
Para que la asignatura se considere superada en la convocatoria ordinaria será necesario obtener una nota igual o superior a 5.0 puntos sobre 10.0 aplicando la ponderación que describiremos más adelante, la asistencia contará como una práctica más.
B) En la convocatoria extraordinaria,
Consistirá en un único examen de todo el temario, pudiendo incluir cuestiones de teoría, ejercicios y prácticas de laboratorio.
La nota total se calculará junto a la calificación obtenida en las prácticas durante la evaluación ordinaria.
Para aprobar será necesario obtener una nota total igual o superior a 5.0 puntos sobre 10.0.
Ponderación
Si no asiste a ese mínimo el alumno solo se puede presentar a la convocatoria ordinaria y en caso de no superar la asignatura a la extraordinaria.
En la convocatoria ordinaria:
A) Si el alumno asiste más de un 80%
A.1) Si obtiene una puntuación media de 75 / 100 en las prácticas se considerará aprobada la asignatura sin necesidad de presentarse al examen.
La calificación final será 100% prácticas / ejercicios clase / participación
A.2) Si no obtiene 75/100 puntos
A.2.1) Si la nota es mayor a 70 puntos, se le dará la opción de repetir la práctica con la nota más baja.
Si una vez entregada esa práctica la nota media de las mismas es de 75 o más puntos se ponderará como dice el apartado A1
A.2.2) Si la nota es menor a 70 puntos, tendrá que realizar el examen y la ponderación de la nota será: 40% prácticas y asistencia + 60% examen. Considerando la participación/asistencia como una práctica más.
B) Si el alumno asiste a menos del 80%
Se calificara con la fórmula de la ponderación escrita en el apartado A.2.2
En la convocatoria extraordinaria:
Examen 60% + Practicas 40%
Respecto a los posibles ensayos, informes o trabajos que hubiera que entregar para superar la asignatura, hay que tener en cuenta que el profesor penalizará en las evaluaciones a los alumnos que cometan faltas de ortografía en sus escritos. No se admitirán entregas que no se realicen por el aula virtual. No se permiten entregas por correo electrónico ni fuera de plazo.
Es necesario conseguir al menos una nota de 5 puntos en cada una de las pruebas para hacer media.
Para aprobar la asignatura es necesario aprobar tanto las pruebas y como las prácticas.
Las notas de las pruebas no aprobadas tendrán un valor de 0 a la hora de hacer la media.
Queda a discreción del docente guardar las partes aprobadas entre convocatorias que decidirá dependiendo del alumno y las circunstancias específicas.
Plagio
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. El autoplagio NO está permitido.

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

OWASP OWASP Top 10 2021
OWASP Top 10:2021 -> https://owasp.org/Top10/es/

OWASP OWASP Top 10 Mobile 2024
OWASP Mobile Security Project: Top 10 Mobile Risk / Hacking Mobile