FICHA TÉCNICA DEL CURSO

Nombre del curso	Hacking y fortificación web
Rama	Ciberseguridad
Lengua en que se imparte	Castellano
Profesor/a responsable	Kike Gandía
Datos de contacto	soporte@mastermind.ac
Modalidad	Online*
Metodología	La metodología empleada se basa en una combinación de: **Clases magistrales**, orientadas a la presentación de conceptos de la materia y a la definición de los objetivos y procedimiento de trabajo. **Tareas, retos y proyectos**, planteándose como técnica de aprendizaje individual tareas que exigen de una trabajo de investigación pretendiendo que el alumno sea autónomo en la resolución de problemas.
Método de aprendizaje	El proceso de enseñanza-aprendizaje se realizará mediante el método de ABP (Aprendizaje Basado en Proyectos) mediante el diseño, programación e implementación de un conjunto de tareas asociadas a una misma temática. Puede ser complejo y transversal. Culmina con una presentación, producto o ejecución de la solución, que refleja lo que el alumnado es capaz de hacer con los aprendizajes que ha adquirido durante el proyecto.
Accesibilidad	• SO: Windows® XP / Vista® / Windows® 7. • Procesador: 1.0 GHz. • Memoria: 512 MB de RAM. • Gráficos: Tarjeta compatible con DirectX y con 64 MB o mas • DirectX®: 8.1 o superior. • Sonido: Compatible con DirectX.

SITUACIÓN/SENTIDO DEL CURSO

Contextualización	Estudiar ciberseguridad es una de las tareas más importantes y necesitadas hoy en día, pues cada vez más están apareciendo nuevas formas de robar y extraer información sensible, datos importantes o cualquier otro tipo de elemento que sea importante para una compañía o persona, por medio del sector digital. El propósito de la fortificación web es conocer en profundidad cada uno de los ataques que se pueden sufrir para su identificación y resolución.
Relación con otras ramas	
Prerrequisitos	Curso Cómo protegerse en la red

OBJETIVOS DEL CURSO

Generales	OG 1- Aprender en profundidad los más importantes ciberataques y sus posibles defensas OG 2- Preparar un entorno de pruebas controlado para la realización de ataques y configuraciones
Específicos	OE 1- Desplegar Wordpress en un entorno controlado OE 2- Realizar ataques contra un entorno controlado con Wordpress OE 3- Conocer las consecuencias de los posibles ciberataques a un servidor web OE 4- Desarrollar la fortificación de un servidor web y un servicio Wordpress ante posibles ciberataques

DEDICACIÓN DEL ESTUDIANTE AL CURSO

Horas teóricas	7h
Horas prácticas (estimadas)	15h

BLOQUES TEMÁTICOS DEL CURSO

Módulo I: Introducción

Objetivos de aprendizaje	• Identificar la estructura de contenidos y los principales objetivos del curso
Número de lecciones	3
Plan de trabajo	Clases teóricas
Evaluación	
Recursos necesarios	Ordenador Acceso a Internet
Duración del módulo	<1h

Módulo II: Creación del entorno de pruebas

Objetivos de aprendizaje	• Preparar nuestro entorno de pruebas controlado para realizar practicas
Número de lecciones	5
Plan de trabajo	Clases combinadas teóricas y prácticas
Evaluación	Tarea
Recursos necesarios	Ordenador Acceso a Internet
Duración del módulo	1h

Módulo III: Ciberataques y fortificación

Objetivos de aprendizaje	• Conocer las consecuencias de los posibles ciberataques a un servidor web
Número de lecciones	29
Plan de trabajo	Clases combinadas teóricas y práctica
Evaluación	6 pruebas
Recursos necesarios	Ordenador Acceso a Internet
Duración del módulo	1h

Módulo IV: Despliegue de WordPress y pentest

Objetivos de aprendizaje	• Realizar ataques contra un entorno controlado con Wordpress
Número de lecciones	16
Plan de trabajo	Clases combinadas de teoría y práctica
Evaluación	
Recursos necesarios	Ordenador Acceso a Internet
Duración del módulo	3h

Módulo V: Conclusión

Objetivos de aprendizaje	• Distinguir de forma resumida cada uno de los puntos necesario para realizar buenas prácticas de protección frente a ciberataques
Número de lecciones	1
Plan de trabajo	Clase teórica
Evaluación	
Recursos necesarios	Ordenador Acceso a Internet

Duración del módulo	<1h

Módulo VI: ¡A practicar!

Objetivos de aprendizaje	• Realizar un proyecto final donde se ponga en práctica el conjunto de conocimientos expuestos a lo largo del curso
Número de lecciones	Proyecto Final
Plan de trabajo	Clase práctica
Evaluación	
Recursos necesarios	Ordenador Acceso a Internet
Duración del módulo	<1h

CONSIDERACIONES FINALES

Este curso no cuenta con ninguna consideración específica más allá de disfrutar aprendiendo.

CERTIFICACIÓN

Con la visualización del 100% del contenido del curso se otorga un certificado de Finalización que consta de la siguiente información: nombre del alumno/a, nombre del curso, fecha de finalización e identificador de certificado.

*El 100% de la formación ofertada en Mastermind Academy es online