Hacking Ético Web

Curso: HEWEB-01 Nivel: Medio

Ficha técnica

Datos del curso

Duración: 40 horas / 2 meses

Modalidad: E – Learning 100 %

Inicio del curso: Elección personal del alumno

Curso organizado por: SVT Cloud Services (www.svtcloud.com)

Responsable del curso: Miguel Ángel Arroyo

Profesores del curso: Manuel Camacho y Miguel Ángel Arroyo

Contacto para información: formacion@svtcloud.com

Plataforma de formación on-line: https://elearning.svtcloud.com

Objetivos del curso:

Son muy pocas las empresas que no todavía presencia en Internet, aunque sea con una pequeña página Web corporativa con **información** de la empresa; servicios, productos, formas de contacto, etc., sin embargo cada vez son más las organizaciones que si cuentan con esta presencia, y no solo con una página Web de información.

El **comercio electrónico** (E-Commerce) es ya una realidad y cada día aumenta el número de tiendas online disponibles en la red. Si a ello le sumamos que las tecnologías Web han cambiado mucho desde el inicio de la Web y que ahora permiten ser mucho más dinámicas y funcionales, podemos llegar a la conclusión de que estos sitios Web procesan información del día a día de la empresa (**clientes, artículos, proveedores, facturas, presupuestos, etc.**).

Dada la importancia de la información que se procesan, los sistemas de información y las **aplicaciones Web** que la manejan tienen que ser seguros para garantizar la **confidencialidad**, **integridad** y **disponibilidad** de ésta.

Aquí es donde entra en juego la figura del Hacker Ético.

Los objetivos del curso son que el alumno conozca las **técnicas de hacking ético Web** con el fin de poder aplicarlas a la hora de detectar posibles fallos de seguridad en las **aplicaciones Web**, lo que le permitirá a su cliente saber qué contramedidas se deberán implementar para solucionar y mitigar los posibles riesgos. Además para sacar el máximo **provecho** al curso y poder aplicarlo a nivel profesional, se toma como **referencia la metodología OWASP**.

El alumno aprenderá de manera práctica:

- ✓ Entender la metodología OWASP.
- ✓ Fases, categorías y controles de seguridad.
- ✓ Hacer Fingerprinting de servidores y aplicaciones Web.
- ✓ Realizar test de gestión sesiones (CSRF, análisis de sesiones, etc.)
- ✓ Realizar test de autenticación y autorización.
- ✓ Realizar test de manejo de errores y cifrado de comunicaciones
- ✓ Realizar test de validación de datos (XSS, SQLi, File Inclusion, etc.)

Contenido

Hacking Ético Web HEWEB-01
Módulo 1 Introducción a seguridad Web y metodología OWASP **Módulo 2** Fingerprint de servidores Web y aplicaciones **Módulo 3** Test a la gestión de identidades y sesiones **Módulo 4** Test de autenticación y autorización **Módulo 5** Test de manejo de errores y cifrado en comunicaciones **Módulo 6** Test de lado cliente y lógica de negocio **Módulo 7** Test de validación de datos **Módulo 8** Recomendaciones y práctica final de Hacking Ético Web **Clase Magistral** con experto del Sector

Metodología

El proceso de aprendizaje estará basado en las siguientes Actividades:

- ✓ Lectura por parte del alumno de documentación publicada en la plataforma de formación para cada Módulo y Unidad formativa (cada semana se publicará un nuevo Módulo, con una o varias unidades formativas). La documentación consistirá en presentaciones resumen de cada módulo, documento detallado (pdf) y documento con recursos relacionados con la actividad en curso.
- ✓ Visualización por parte del alumno en la plataforma de formación de videos demostrativos o explicativos de la materia tratada en la Unidad o unidades formativas en curso.
- ✓ Tutorías semanales con el tutor asignado en la hora convenida con el tutor para la resolución de dudas (no obligatorias).
- ✓ Realización de un Test o práctica en cada Módulo para evaluar el conocimiento adquirido.
- ✓ Se podrá tener acceso a una clase magistral con expertos en el sector de seguridad, tratando temas sobre una determinada especialidad de hacking ético. Dicha clase podrá ser programada en directo (comunicándole al alumno la fecha y la hora) a través de una plataforma de videoconferencia o en el caso de no poderse realizar la planificación con ningún experto por volumen de trabajo, viajes, etc... se le facilitaría al alumno hasta dos clases magistrales anteriormente grabadas, dependiendo de la disponibilidad de las mismas.

Se estima que cada Módulo (que se liberan semanalmente) requiere un mínimo de 5 horas de dedicación por parte del alumno.

Calendario

Hacking Ético de Sistemas y Redes HESR-02	Fecha inicio
INICIO CURSO	**Elección personal del alumno**
Módulo 1 Introducción a seguridad Web y metodología OWASP	A determinar
Módulo 2 Fingerprint de servidores Web y aplicaciones	A determinar
Módulo 3 Test a la gestión de identidades y sesiones	A determinar
Módulo 4 Test de autenticación y autorización	A determinar
Módulo 5 Test de manejo de errores y cifrado en comunicaciones	A determinar
Módulo 6 Test de lado cliente y lógica de negocio	A determinar
Módulo 7 Test de validación de datos	A determinar
Módulo 8 Recomendaciones y práctica final de Hacking Ético Web	A determinar
Clase Magistral con experto del Sector	A determinar
FIN DEL CURSO. EMISION CERTIFICADOS	**A determinar**

Se podrá realizar una tutoría semanal por cada alumno de 30 minutos. La fecha y hora se establecerá entre el tutor y el alumno a su conveniencia utilizando la plataforma de formación

EVALUACION

Al finalizar el curso, a los alumnos que hayan obtenido una puntuación de más del 50% y de una asistencia de más del 80% de las 40 horas que consta el curso se les entregará un diploma acreditativo de los conocimientos adquiridos, las horas del curso y la puntuación obtenida.

Para la medición de la asistencia se utiliza la plataforma de formación, que mide la dedicación a cada uno de los módulos y actividades.

A continuación se especifican los criterios de evaluación a utilizar para obtener la evaluación final del curso por parte del alumno:

Criterio	% sobre el total
Práctica final	60 %
Actividades evaluación de cada módulo	40 %