

# Review Curso de Hacking y Auditoría Web de Securiters





## INDICE

0-	Introducción.....	2
1-	Experiencia previa .....	2
2-	¿Qué es CHAW? .....	2
3-	El curso.....	2
4-	El examen .....	3
5-	Conclusiones.....	3





## 0- Introducción

Ya está conmigo mi certificado del curso CHAW (Curso de Hacking y Auditoría Web) de Securiters y en esta review, voy a compartir mi experiencia a lo largo de la formación y si la recomiendo a aquellas personas interesadas en hacking orientado a las aplicaciones web.

## 1- Experiencia previa

Mi conocimiento sobre explotación de vulnerabilidades no abarca más que la realización de algunos CTF de Hack The Box y la lectura de libros relacionados con las aplicaciones web pero siempre de forma desordenada. Sin hablar, de que no solo no tenía prácticamente experiencia en “romper” aplicaciones web, sino que también había que realizar un informe, que parece la parte fácil, aunque más adelante veremos que no.

## 2- ¿Qué es CHAW?

CHAW, Curso de Hacking y Auditoría Web es un curso de Securiters donde la tutora y desarrolladora del curso es Marta Barrio Marcos. Es un curso mayoritariamente práctico donde se irán explicando las diversas vulnerabilidades que nos podemos encontrar en una aplicación web, comenzando desde nivel 0.

2

## 3- El curso

El curso lo podemos encontrar en la web de Securiters. Solo necesitas matricularte y obtendrás acceso a todo el contenido.

El contenido del curso lo podemos dividir en varias partes:

- ✓ **Introducción**  
Fundamentos de una auditoría web (tipos, fases de una auditoría, metodología...).
- ✓ **Preparación del entorno**  
Instalación de la máquina virtual para realizar las pruebas (Kali) y las diferentes máquinas vulnerables que se explotarán a lo largo del curso. También se configura Burp para su utilización.
- ✓ **Detección y solución de las vulnerabilidades**  
Este curso trata vulnerabilidades de configuración, inyección, autenticación, autorización, comunicaciones, vulnerabilidades de CSRF y Clickjacking. También se trata como solucionar cada una de las vulnerabilidades tratadas.
- ✓ **Uso de herramientas automáticas**





Se recorren las diferentes soluciones disponibles en el mercado para escaneo automático de aplicaciones web.

✓ **Desarrollo del informe**

Trata como desarrollar el informe posterior a las pruebas de seguridad, desde el informe ejecutivo al informe técnico, pasando por la evaluación de la criticidad de las vulnerabilidades.

Todo esto se presenta mediante videos y diapositivas donde Marta explica todo de forma muy clara, como explotar y solucionar cada una de las vulnerabilidades, como desarrollar el informe a lo que hay que añadir, los diferentes ejemplos prácticos que ejecuta a lo largo del curso, que comienza con la instalación del entorno, las aplicaciones vulnerables que serán utilizadas y la configuración de Burp, continuando con la explotación de cada una de las vulnerabilidades tratadas durante la formación.

#### 4- El examen

El examen del Curso de Hacking y Auditoría Web está dividido en dos partes, por un lado, un cuestionario con 20 preguntas y por el otro, el desarrollo del informe ejecutivo y técnico de una auditoría sobre una aplicación web vulnerable.

3

En primer lugar, hay que desarrollar el informe. Este debe incluir informe técnico y ejecutivo. Este informe debe contener el reporte de al menos 7 vulnerabilidades donde no se repita el tipo de vulnerabilidad.

En este documento se tienen en cuenta el contenido, la presentación y la dificultad y cantidad de vulnerabilidades reportadas.

Esta parte del examen representa el 80% de la nota final de la certificación.

En segundo lugar, tendremos que completar un cuestionario con 20 preguntas sobre el contenido tratado a lo largo de la formación.

Esta segunda parte representa el 20% de la nota total.

#### 5- Conclusiones

¿Merece la pena esta Certificación? Sin dudas, sí. El contenido del curso es simplemente genial, tanto a nivel contenido como por la calidad de las diapositivas y los videos de capacitación.

El hecho de que trate también el desarrollo de la documentación post pruebas, añade otro extra que no tienen muchas certificaciones, que enseñan a vulnerar las aplicaciones, pero





no, como presentar los resultados de esas pruebas a un cliente, algo que puede ser tan importante como saber encontrar y explotar los fallos de una aplicación web.

Por otro lado, el trato de Marta es simplemente sobresaliente y lo tengo que resaltar tanto por la cercanía como por la atención que presta a los alumnos, de verdad.

¿Volvería a realizar otra formación con Securiters o con Marta como tutora? Sin dudarlo.

