CMHW – Certificado MILE-SEC Hacking Web

Temario

- Pruebas Actuales de Seguridad contra Aplicaciones Web
- Pruebas Estáticas y Dinámicas de Seguridad (SAST) y (DAST)
- Metodologías para Prueba de Penetración contra Aplicaciones
- Guía de Pruebas para Seguridad Web
- OWASP Zed Attack Proxy
- DNSRecon y OSINT
- Google Dorks
- Shodan para Pruebas de Penetración
- Metadatos
- Maltego, TheHarvester
- Encriptar HTTP en Tránsito, SSL / TLS
- Perfilar el Servidor y Versión del Servidor
- Configuración del Software
- Nikto
- Spidering al Sitio Web
- Páginas por Defecto
- Detección de Tecnologías utilizando ZAP
- Navegación Forzada con ZAP
- Fuzzing con Zed Attack Proxy
- Fuga de Información
- Diferentes tipos de Autenticación
- Recolectar Nombres de Usuario
- Escáneres de Vulnerabilidades
- Tipos de Vulnerabilidades en Aplicaciones Web
- Descubrimiento y Explotación
- Escaneo Activo con Zed Attack Proxy
- Rastreo de Sesión
- Fallas o Defectos de Sesión
- Inyección de Comandos
- Inclusión de Archivo Local y Archivo Remoto
- Recorrido de Directorios
- Inyección SQL
- Meta Información de Base de Datos
- Explotación In-band /Inline
- SQLMap
- XML External Entity (XXE)
- Server Side Request Forgery (SSRF)
- DOM
- Cross Site Scripting (XSS)
- XSS Reflejado, Almacenado y DOM
- Descubrir XSS
- Inyección HTML
- BeEF
- Cross-Site Request Forgery (CSRF)
- Fallas Lógicas

Presentación

Las aplicaciones web modernas tienen un rol muy importante en todas las organizaciones. Pero si la organización no tiene la capacidad de evaluar y asegurar adecuadamente sus aplicaciones web, los ciberatacantes podrían comprometer estas aplicaciones, afectando el funcionamiento normal de la empresa, como también robar datos sensibles. Desafortunadamente muchas organizaciones operan bajo la errónea percepción, de un escáner de seguridad para aplicaciones web es la manera más fiable de descubrir fallas en sus sistemas. Las ciberdefensas modernas requieren una comprensión realista y profunda de los problemas de seguridad relacionadas con la aplicación web. Cualquiera puede aprender a realizar algunos tipos de ataques contra la web, pero una prueba de penetración efectiva contra aplicaciones web requiere un conocimiento más profundo.

CMHW
CERTIFICADO MILE-SEC
HACKING WEB

Objetivos

Este curso enseña a los participantes a entender las principales fallas encontradas en las aplicaciones web, como también a identificar y explotarlas con el propósito de demostrar el potencial impacto hacia la empresa. Los profesionales en seguridad de la información frecuentemente se esfuerzan en ayudar a las organizaciones a entender su riesgo en términos de la empresa. Ejecutar elaborados e impresionantes ataques tiene poco valor si la organización no toma en serio su riesgo, y despliega las medidas correctivas adecuadas. El propósito de este curso es mejorar la seguridad de las organizaciones a través de una prueba de penetración, y no solo demostrar las habilidades de Hacking. Este curso ayuda a los participantes a demostrar el verdadero impacto de las fallas en las aplicaciones web, no únicamente a través de la explotación, sino también a través de una adecuada documentación y reporte.