Web Penetration Testing

Un Web Penetration Test es una técnica utilizada para evaluar la seguridad de los recursos y activos de la organización desde el punto de vista de la materia de seguridad a nivel Web.

Esta técnica no solo identifica las vulnerabilidades existentes en la infraestructura web, sino que además ejecuta el análisis con mayor profundidad. Específicamente, se busca además de la identificación, la explotación de las vulnerabilidades y de esa manera se observa el impacto real sobre la organización.

Este tipo de servicio puede llevarse a cabo tanto desde un punto de vista interno como externo de la organización. En el primer caso se busca identificar y explotar las Vulnerabilidades Web que sean visibles desde un escenario con acceso a los recursos y activos de la organización mientras que en el segundo se realiza la evaluación desde el punto de vista de un atacante externo.

Objetivos principales

- ✓ Obtener una fotografía del estado de la seguridad Web que la organización, sistema u host objetivo en un momento determinado.
- ✓ Visualizar su compañía desde el punto de vista del atacante, localizando debilidades, Vulnerabilidades Web y puntos de acceso no autorizados, antes que lo hagan los atacantes.
- ✓ Comprobar el verdadero impacto de las Vulnerabilidades en su entorno particular.
- ✓ Comprobar si el nivel de protección existente se condice con la política de seguridad establecida por la organización.
- ✓ Comprobar la efectividad de sus medidas de protección, políticas y procesos de detección de intrusos y respuesta a incidentes.

¿Por qué realizar un Web Penetration Test?

- ✓ Para conocer el estado de la seguridad Web de una organización (especialmente si nunca se realizó una auditoría de estas características).
- ✓ Para establecer un punto de partida y comenzar a gestionar la seguridad Web de la organización.
- ✓ Está basado en el OWASP TOP TEN 2016 y en el OWASP Testing Guide 4.0, garantizando el mejor desempeño.
- ✓ Para constituir un ciclo de revisión y mejora para la seguridad Web de manera continua, ya sea desde el ciclo de desarrollo o en sus sucesivas iteraciones.

Las etapas asociadas a este servicio son:

- ✓ Reconocimiento Web
- ✓ Análisis y detección de Vulnerabilidades Web
- ✓ Explotación de vulnerabilidades
- ✓ Armado y presentación de reportes

Reportes

En este servicio se generan 2 entregables o reportes que ayudan y guían al cliente en el proceso de remediación de vulnerabilidades.

El primero de ellos, el **Informe Ejecutivo**, describe el nivel de riesgo de la compañía sin entrar en detalles técnicos, evidenciando las problemáticas por medio de conceptos claros y gráficas.

El segundo reporte, el **Informe Técnico**, apunta al área técnica de la empresa, ayudando al personal de TI a solucionar los problemas detectados.

En este reporte se muestran todas las evidencias de los tests ejecutados de manera tal que todas las tareas sean repetibles y transparentes para el cliente. Basado en el OWASP TOP TEN y en el OWASP Testing Guide 4.0.