ETHICAL HACKING API

Ethical Hacking API

Descripción

Nuestro servicio de Ethical Hacking API permite evaluar los endpoints de tus aplicativos de manera profesional. Nos enfocamos en entender tu negocio velando siempre por la correcta funcionalidad de este.

Las pruebas realizadas en nuestro servicio de Ethical Hacking API se realizan de forma manual y con herramientas automatizadas.

- ✓ Permite conocer la exposición de las API de las aplicaciones a las amenazas contingentes.
- ✓ Se desarrolla mediante modalidades de caja negra gris o blanca.
- ✓ Se efectúa principalmente a través de técnicas manuales para tener un mayor impacto en la revisión.
- ✓ Considera una fase de verificación de la efectividad de la remediación efectuada por cliente.

Objetivos

- ✓ Obtener posibles riesgos en una los endpoints de tu aplicación web antes de salir a producción.
- ✓ Analizar lógicas de negocios.
- ✓ Entregar un panorama acerca de las vulnerabilidades encontradas para tomar medidas a corto, mediano y largo plazo.
- ✓ Disminuir el tiempo y esfuerzo para afrontar posibles situaciones de riesgo.

Método

- ✓ Metodología OWASP API (Open Web Application Security Project API).
- ✓ La evaluación de la API del aplicativo WEB, se desarrolla a través de herramientas y técnicas manuales, en mayor medida, donde se identifican y descubren vulnerabilidades presentes en la aplicación.
- ✓ Una vez mitigadas las vulnerabilidades descubiertas, se realiza una recertificación de ellas.

Entregables

- ✓ Informe de Ethical Hacking API incluye lo siguiente:
  - identificación de amenazas por nivel de riesgo.
  - Si es necesario, una presentación ejecutiva de resultados.
  - Recomendación de mitigaciones por amenaza detectada.
  - PoC de vulnerabilidades explotadas.
  - Evidencia de componentes afectados.

Alcance

- ✓ Se recomienda los ejercicios de modalidad caja gris debido a que se pueden analizar flujos de los usuarios autenticados.
- ✓ El plazo de ejecución de los servicios será definido por el tamaño y la cantidad de endpoints a revisar.
- ✓ Se ejecutará de forma remota.
- ✓ Se provee un informe de resultados, acciones de mitigación y los detalles de los hallazgos.
- ✓ Una vez mitigadas las vulnerabilidades por parte del cliente, es posible solicitar una revisión de las mitigaciones, donde se prueban las vulnerabilidades nuevamente, para constatar la correcta forma de mitigación. La revisión de las mitigaciones es opcional y a pedido.
- ✓ TENSEN realizará la revisión de las mitigaciones una vez facturada la totalidad del servicio cotizado, dentro de hasta un plazo de 90 días después de entregado el informe de resultados inicial.

Metodología del servicio

Fase I. Modo Pasivo

- ✓ El objetivo de esta fase consiste en comprender la lógica de la API e identificar los posibles vectores de ataque que componen la API de la aplicación WEB, los puntos de acceso, formularios y antecedentes relevantes del sitio bajo análisis.

Fase II. Modo Activo

- ✓ Recolección de Información, Pruebas de: Gestión de configuración, Gestión de Identidad, Autenticación y Autorización, Gestión de Sesión, Validación de Entradas, Pruebas de Lógica de Negocio, Explotaciones de vulnerabilidades previa autorización del cliente, etc.

Fase III. Reporte

- ✓ Se generará un reporte con: Nombre de la API validada, Descripción de las API's, Vectores de ataque, Vulnerabilidades descubiertas, Resultados de la explotación con evidencia de éxito, Impacto de las vulnerabilidades, Medidas de mitigación de vulnerabilidades