Características:

* Prebas de vulnerabilidades sobre direcciones Urls.
* Modalidad Black Box y White Box.
* Pruebas de seguridad Dinámicas.
* Verificación de la infraestructura subyacente (Web Application Firewall, Servidores, Bases de Datos, etc).
* Clasifica las vulnerabilidades encontradas por su severidad y potencial impacto.
* Consideraciones y solicitudes para ambos servicios: Url’s, credenciales en caso de corresponder, pruebas programadas según la criticidad y horarios del cliente.
* En caso de tratarse de un servicio sobre Api’s se solicita: Archivo Swagger (OpenAPI Specification), Colección de endpoints, Enviroment’s y métodos soportados.
* Detección de vulnerabilidades que puedan comprometer la confidencialidad, integridad y disponibilidad de los servicios o sistemas de información de una compañía.
* Confidencialidad: se garantiza que toda la información obtenida durante el transcurso de las pruebas será reservada y no se modificará ni divulgará a terceros.
* Entrega de informes ejecutivo y técnico al finalizar las pruebas con el detalle del trabajo realizado, resultado, conclusiones y recomendaciones de mejora.

Beneficios:

* Detección Proactiva: Se identifican vulnerabilidades y fallos de seguridad antes de que sean explotados por atacantes, protegiendo así la integridad y confidencialidad de los datos.
* Recomendaciones de Mitigación: se proporcionan recomendaciones detalladas y prácticas para corregir vulnerabilidades, mejorando continuamente la postura de seguridad.
* Reducción de riesgos de brechas de seguridad que podrían resultar en pérdidas financieras, daño reputacional y problemas legales.
* Reevaluaciones: Se le ofrece la posibilidad de realizar reevaluaciones para asegurarse de que las vulnerabilidades identificadas se han corregido efectivamente

Preguntas e inquietudes Pentest Web:

1. Qué es un pentest web y por qué es necesario?

Un pentest web es una evaluación de seguridad diseñada para identificar y explotar vulnerabilidades en una aplicación web.

Consta de 7 etapas (Planificación y alcance, Reconocimiento, Enumeración, Análisis de Vulnerabilidades, Explotación, Post-Explotación y Reporte).

Las metodologías utilizadas son: Owasp (Open Web Application Security Project) y OSSTMM (Open Source Security Testing Methodology Manual).

1. Qué tipo de vulnerabilidades se busca en un pentest web?

Se buscan vulnerabilidades comunes como inyecciones SQL, XSS, CSRF, fallos en la autenticación y autorización, exposición de datos sensibles, mala configuración de seguridad, entre otros.

1. Qué información necesitas para comenzar?

Se necesita la URL de la aplicación web, credenciales de prueba (si es Graybox) y saber si existe un entorno de prueba disponible.

1. Qué sucede si se encuentra una vulnerabilidad con posible explotación?

Se notificará de inmediato la descripción y su impacto. La continuidad quedará a disposición del cliente si se explota o no.

1. Cómo se realizará la comunicación durante las etapas del pentest?

La comunicación se realizará de manera regular a través de medios me comunicación como correos electrónicos y WhatsApp. Se mantendrá una línea abierta para cualquier pregunta o preocupación que puedas tener durante el proceso.

Preguntas en el caso de incluir Api’s:

1. Tipo de servicios a realizar:
2. BlackBox: Se solicita solo la url y los endpoints
3. Graybox:

* ¿Cuáles son los endpoints disponibles?
* ¿Qué métodos HTTP son soportados por cada endpoint?
* ¿Hay documentación técnica disponible para la API?
* ¿Qué parámetros se utilizan en las solicitudes y respuestas de la API?
* El archivo Swagger que posee descripción de la API y sus endpoints
* ¿Qué sistemas de autenticación y autorización se utilizan?
* ¿Hay entornos de prueba separados del entorno de producción?