

Panorama General

El servicio de análisis de vulnerabilidades está diseñado para identificar, cuantificar y evaluar el nivel de riesgo de las debilidades en la infraestructura antes de que estas sean identificadas por un potencial atacante, utilizando herramientas automatizadas y técnicas manuales pueden ser identificadas configuraciones inseguras, ausencia de parches de seguridad, versiones fuera de soporte o con múltiples vulnerabilidades, entre otras.

Este servicio permitirá a “CLIENTE” tener información relacionada con el nivel de riesgo para cada vulnerabilidad identificada, así como recomendaciones para mitigarlas, permitiendo una mejor toma de decisiones a la hora de priorizar o ejecutar un plan de Gestión de Vulnerabilidades, con la finalidad reducir el nivel de exposición de la organización ante un ataque.

Este servicio se ejecuta con una perspectiva de Caja Gris, los escaneos se ejecutan desde un nodo de la red interna, o desde un acceso vía VPN, es posible realizar un descubrimiento o bien, que se asignen segmentos de red específicos para las validaciones.

El presente servicio tiene como alcance la evaluación de seguridad sobre ciertos activos tecnológicos por dirección IP, dicha información será proporcionada por personal de “CLIENTE”.

Este servicio no contempla la explotación o validación a fondo de las vulnerabilidades.

A continuación, se muestran los tiempos de ejecución de acuerdo con el número de activos a considerar:

No. de Activos (IP)	Infraestructura/ Aplicación	C/S Credenciales	Duración aproximada
1-50	Infraestructura	Sin Credenciales	4 días hábiles
51 - 100	Infraestructura	Sin Credenciales	8 días hábiles
101 – 150	Infraestructura	Sin Credenciales	12 días hábiles
1-50	Infraestructura	Sin Credenciales	6 días hábiles
51 - 100	Infraestructura	Sin Credenciales	12 días hábiles
101 – 150	Infraestructura	Sin Credenciales	18 días hábiles

Análisis de Vulnerabilidades a Aplicaciones

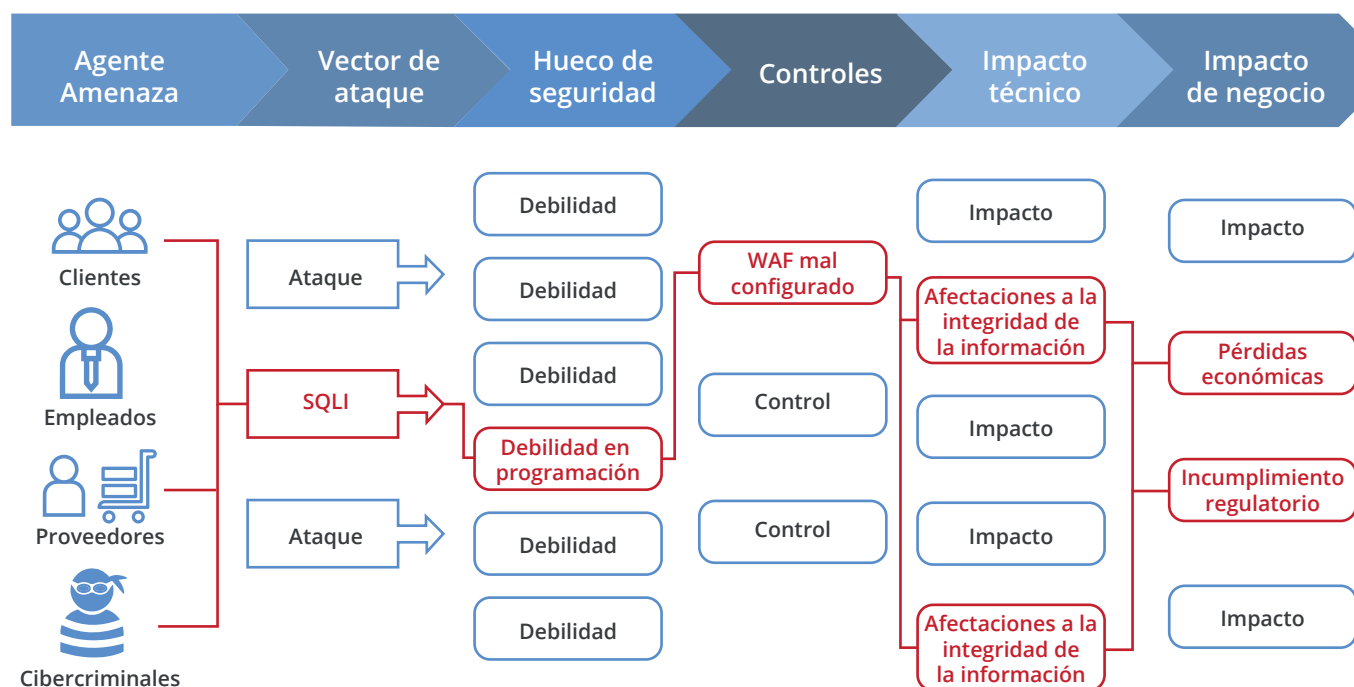
El servicio de análisis de vulnerabilidades está diseñado para identificar, cuantificar y evaluar el nivel de riesgo de las debilidades en las aplicaciones antes de que estas sean identificadas por un potencial atacante, utilizando herramientas y técnicas manuales basadas en las mejores.

Este servicio permitirá a “CLIENTE” tener información relacionada con el nivel de riesgo para cada vulnerabilidad identificada, así como recomendaciones para mitigarlas, permitiendo una mejor toma de decisiones a la hora de priorizar o ejecutar un plan de Gestión de Vulnerabilidades, con la finalidad de mitigar y reducir el nivel de exposición de la organización ante un ataque.

En esta perspectiva de pruebas, los consultores de HIXSA realizarán la revisión integral de aplicativos web, cliente-servidor o móvil (Servidores de infraestructura, Bases de datos, Servidores web, Componentes middleware).



Es importante mencionar que, dentro de la ejecución de las pruebas se buscan vulnerabilidades específicas de lógica de negocio, elevación de privilegios, referencias inseguras, configuraciones inseguras en servidores o servicios que soportan las aplicaciones, deficiencias en mecanismos de autenticación y controles de acceso, uso de bibliotecas y frameworks vulnerables, o errores de codificación que permitan comprometer la confidencialidad, integridad o disponibilidad de la información, entre otras, con la finalidad de buscar diversos vectores de ataque de acuerdo con las funcionalidades particulares de cada aplicativo.



El set de pruebas a desarrollar por el equipo de HIXSA se encuentra alineado a las buenas prácticas y estándares líderes de la industria.

Como consideraciones a las evaluaciones SPEI se prevé la revisión de la interconexión entre el propio SPEI y las interfaces de usuario. Parte del set de pruebas contempla por ejemplo, la evaluación en el uso de formatos como AMF, el cual, al ser un formato binario, pudiera parecer que dificulta la manipulación de las peticiones; sin embargo, existen plugins que permiten deserializar estas peticiones, modificarlas y volverlas a serializar previo a su envío hacia los servidores de la aplicación, con lo cual es posible llevar a cabo un análisis de vulnerabilidades más completo e identificar desde trazas de ejecución, por medio de las cuales se puede identificar el funcionamiento de la aplicación a nivel de código, hasta inyecciones SQL, o en algunos casos, inyecciones ORM, dependiendo del uso de bases de datos SQL directamente o si se hace uso de algún mapeo objeto-relacional, tal como Hibernate.

Además de las debilidades mencionadas anteriormente, los despachadores web también se suelen ver afectados por vulnerabilidades de lógica de negocio como referencias inseguras a objetos, así como fallos en la verificación de la integridad de las peticiones realizadas, con lo cual es posible evadir restricciones de direcciones IP, e incluso, en fallos a la confidencialidad, los cuales pueden llegar a permitir la recuperación de contraseñas.

Es por ello, que se realizará una revisión a detalle de los siguientes controles:

- Sanitización de campos de entrada
- Gestión adecuada de apertura y cierre de sesiones
- Protección ante ataques de fuerza bruta
- Validación, en cuanto a de lógica de negocio, de los campos de entrada
- Verificación datos expuestos en peticiones
- Revisión de mensajes de error y trazas de ejecución