BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME Nº 0187-2023-GTI230-N

ASUNTO : Informe técnico previo de evaluación de software - Renovación de servicios del software tipo DAST (Dynamic Application Security Testing) del BCRP de la marca Open Text/ Micro Focus Fortify WebInspect

---

1. NOMBRE DEL ÁREA:

Dpto. de Ciberseguridad y Redes.

2. RESPONSABLE DE LA EVALUACIÓN:

Christian Manuel García Cerna.
Alexander Gamboa Inga.
Miguel Tejada Malaspina.
Marco Granadino Cáceres.

3. CARGO:

Especialista en de Ciberseguridad y Redes.
Jefe del Dpto. de Ciberseguridad y Redes (i).
Subgerente de Servicios de Tecnologías de Información.
Subgerente de Riegos de Tecnologías de Información.

4. JUSTIFICACIÓN:

Las vulnerabilidades de seguridad en las aplicaciones son resultado de defectos de calidad, que pueden ocurrir durante el proceso de desarrollo de la aplicación, por tanto las organizaciones requieren de herramientas que les permitan identificar y solucionar estas vulnerabilidades como parte de las prácticas estándar de gestión del ciclo de vida de la aplicación, incluyendo las fases de diseño, desarrollo y entrega.

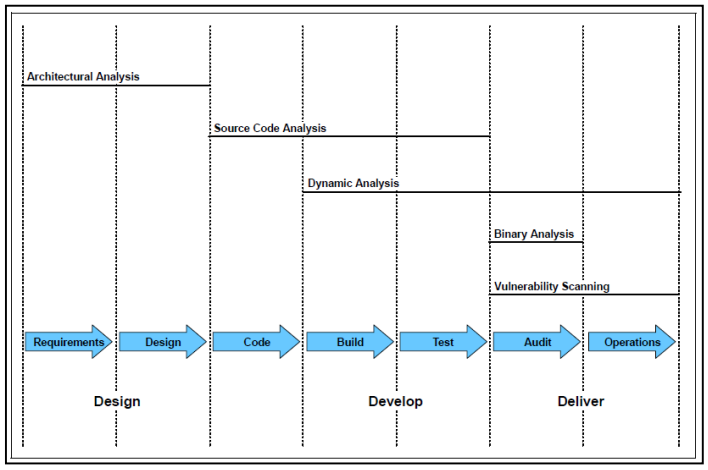

Figura N° 1: The different types of security analysis throughout the software development life cycle

Fuente: *Improving Your Web Application Software Development Life Cycle's Security* (IBM)

Las herramientas utilizadas para analizar la seguridad de las aplicaciones web se pueden agrupar en tres categorías:

Análisis White box: Toda la información relevante sobre el sistema o el software, incluyendo el código fuente, se conoce y está disponible para el responsable del análisis. Comprende las denominadas pruebas estáticas (*Static Aplication Security Testing – SAST*). SAST es de naturaleza amplia, pues simula todos los resultados posibles e inspecciona cada línea de código, y se pueden identificar más tipos de vulnerabilidades que con otros métodos de análisis.

Análisis Black box: Consiste en examinar el software o el sistema sin el conocimiento previo del medio ambiente. Este tipo de análisis es similar a lo que un atacante externo podría hacer. Cuando una organización es sensible a amenazas externas, el análisis Black box es generalmente el primer método de análisis, y los riesgos encontrados del mismo son priorizados porque reflejan con mayor precisión el riesgo expuesto al exterior. Comprende las denominadas pruebas dinámicas (*Dynamic Application Security Testing* – DAST). DAST trabaja atacando la aplicación mediante el uso de técnicas similares a las que un hacker podría emplear, usando muchos escenarios de ataque y monitoreando las respuestas de la aplicación con el fin de diagnosticar las vulnerabilidades. DAST es ideal para llevar a cabo una prueba del sistema de extremo a extremo. Con herramientas automatizadas de este tipo, en sólo minutos se pueden intentar miles de ataques en contra de una aplicación, descubriendo automáticamente los puntos de entrada (superficie de ataque) de la misma.

Análisis Gray box: Combina los beneficios de los análisis de tipo White box y Black box, lo que se logra correlacionando los resultados. Se recomienda aplicarlo a través del ciclo de vida de la aplicación para maximizar los resultados.

El BCRP tiene implementadas diversas aplicaciones web, entre ellas: Portal Web Institucional (www.bcrp.gob.pe), Portal de Series Estadísticas, Biblioteca, Fondo de Empleados, SICAP, SIBFTP, Tienda virtual, LBTR, SACWeb, entre otras, por lo cual es necesario contar con herramientas tecnológicas que permitan detectar las vulnerabilidades de las aplicaciones web previo a su puesta en producción y ante modificaciones que se realicen a las mismas.

Desde el punto de vista de Ciberseguridad de TI, se necesita contar con herramientas del tipo DAST, que automaticen la detección de vulnerabilidades en aplicaciones web para su uso en las etapas de puesta en producción de nuevas aplicaciones y cambios en aplicaciones existentes (incluyendo tanto las aplicaciones que son de desarrollo propio como los productos adquiridos) y auditorías periódicas ante nuevas vulnerabilidades que puedan ser descubiertas.

5. ALTERNATIVAS:

Consideramos las siguientes marcas que brindan soluciones del tipo DAST (Dynamic Application Security Testing).

- Open Text/Micro Focus Fortify WebInspect.
- Qualys Web Application Scanning (WAS).

6. ANÁLISIS COMPARATIVO TÉCNICO:

El análisis técnico ha sido realizado de conformidad con la metodología establecida en el documento "Guía Técnica sobre evaluación de software en la administración pública" (Resolución Ministerial NO 139-2004-PCM), tal como se exige en el reglamento de la Ley N° 28612.

a. Propósito de evaluación

Comparar alternativas de productos existentes en el mercado.

b. Propósito de evaluación

Solución DAST (Dynamic Application Security Testing).

c. Identificación del modelo de calidad

Se aplicará el Modelo de Calidad de Software descrito en la Parte I de la Guía de evaluación de software aprobado por RM NO 139-2004-PCM.

d. Selección de métricas.

Las métricas fueron seleccionadas en base a las características técnicas descritas en el Anexo N° 1.

Según el análisis realizado, la única marca que cumple lo requerido es Open Text/ Micro Focus Fortify WebInspect.

7. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

Beneficios:

- Detección de vulnerabilidades en las aplicaciones web de la institución.
- Pruebas de black box (DAST).
- Generación de reportes especializados (detalle de vulnerabilidades, recomendaciones de solución) que son analizados por el Departamento de Ciberseguridad y Redes para luego ser derivado hacia el Departamento de Gestión y Calidad para su subsanación o compensación de acuerdo con el hallazgo encontrado.
- Soporte con OWASP (Open Web Application Security Project).
- Resultados exportables a soluciones de WAF (Web Application Firewall) que la institución también dispone.

Costos:

Las prestaciones requeridas corresponden al periodo de un (01) año de servicio:

- Prestación principal: Implementación del servicio

Licenciamiento, actualizaciones de software (incluyendo el suministro de nuevas versiones y patches), soporte técnico del fabricante (escalamiento).

- Prestación accesoria: Servicios del partner (proveedor local)
  Mesa de ayuda y soporte presencial, en el esquema 24x7x2 y mantenimiento técnico preventivo anual.

En base a las cotizaciones referenciales obtenidas se estima que el costo del servicio se encuentra dentro del margen presupuestado en PAC 2023.

8. CONCLUSIONES:

Por lo expuesto anteriormente, se solicita la contratación de la renovación de servicios del software tipo DAST (Dynamic Application Security Testing) de la marca Open Text/Micro Focus Fortify WebInspect por el periodo de (01) año.

ANEXO N° 1

ATRIBUTOS Y MÉTRICAS

N°	Atributos	Puntaje máximo	Open Text/Micro Focus Fortify WebInspect	Qualys Web Application Scanning (WAS)
1	Detección de vulnerabilidades en las aplicaciones web de la Institución	10	10	10
2	Pruebas de black box (DAST)	10	10	10
3	Generación de reportes especializados (detalle de vulnerabilidades, recomendaciones de la solución)	10	9	9
4	Soporte con OWASP (Open Web Application Security Project)	10	10	10
5	Resultados exportables a soluciones de WAF (Web Application Firewall)	10	8	8
6	Integración nativa con soluciones de Gestión del Ciclo de Vida de Aplicaciones	10	10	10
7	Permitir programar escaneos para que se realice en fechas y horas programadas	10	10	10
8	Ejecución de escaneos hacia aplicaciones ilimitadas	10	10	0
9	Consola de gestión centralizada	10	0	10
10	Solución con licenciamiento perpetuo	10	10	0
Puntaje Total		100	87	77

Lima, 18 de octubre de 2023

cc.

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

Christian Manuel GARCIA CERNA
Especialista en Ciberseguridad y Redes
Departamento de Ciberseguridad y Redes

Alexander John Anthony GAMBOA INGA
Jefe de Departamento de Ciberseguridad y Redes Interino
Departamento de Ciberseguridad y Redes
Firma como encargado.

Miguel Angel TEJADA MALASPINA
Subgerente de Servicios de Tecnologías de Información
Subgerencia de Servicios de Tecnologías de Información

Marco Antonio GRANADINO CACERES
Subgerente de Riesgos de Tecnologías de Información
Subgerencia de Riesgos de Tecnologías de Información

Silvia Elizabeth MEDINA MORENO
Gerente de Tecnologías de Información
Gerencia de Tecnologías de Información

VISADO POR:

Javier Ernesto OLIVERA VEGA
Gerente Central de Administración
Gerencia Central de Administración