BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME Nº 0235-2022-GTI230-N

Informe técnico previo de evaluación de software - Renovación de mantenimiento y soporte del software Micro Focus Fortify WebInspect

1. NOMBRE DEL ÁREA:

Dpto. de Ciberseguridad y Redes.

2. RESPONSABLE DE LA EVALUACIÓN:

Christian Manuel García Cerna.

3. CARGO:

Especialista en de Ciberseguridad y Redes.

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.

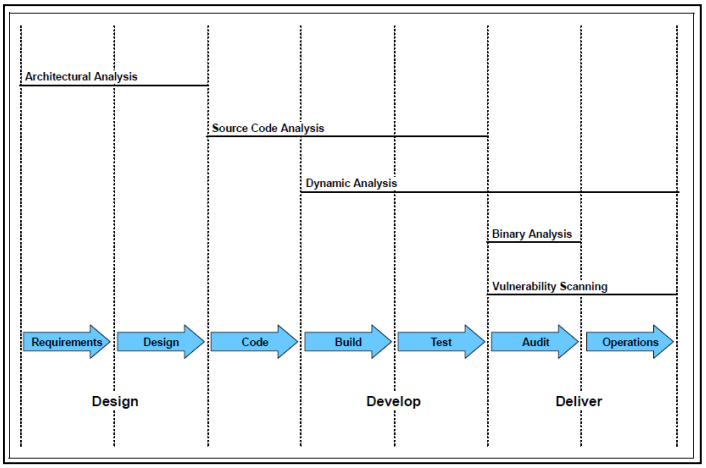

Figura N° 1: The different types of security analysis throughout the software development life cycle
Fuente: *Improving Your Web Application Software Development Life Cycle's Security* (IBM)

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 Banco tiene diversas aplicaciones web publicadas hacia Internet tales como: Portal Web Institucional (www.bcrp.gob.pe), Portal de Series Estadísticas, OCN, Biblioteca, aplicaciones de carta de garantía, SICAP, SIBFTP, Tienda virtual, el módulo web de SIMCTV, entre otros. Asimismo, también se dispone con la aplicación web del sistema LBTR la cual solo está publicada hacia las instituciones financieras a través de una red privada (extranet).

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:

En el año 2012 a través del proceso ADS-0060-2012-BCRPLIM – "*Adquisición de licencias de software para detección de vulnerabilidades en aplicaciones web*", el BCRP adquirió el software HP WebInspect, el cual se aplica en el análisis de tipo Black box (DAST).

En el año 2017 Micro Focus adquirió la línea de soluciones HPE (Hp Enterprise), y renombró el producto como Micro Focus Fortify WebInspect.

El software Fortify WebInspect detecta vulnerabilidades susceptibles de ataques en aplicaciones web y API mediante un análisis dinámico automatizado (DAST). El software genera reportes de sus hallazgos que son revisados por el Departamento de Ciberseguridad y Redes para evaluar la criticidad de las vulnerabilidades web encontradas. Este reporte con recomendaciones es derivado al Departamento de Gestión y Calidad para su subsanación o compensación de acuerdo al hallazgo encontrado.

De la revisión de información relevante en estudios actuales sobre las mejores soluciones de DAST (*Dynamic Application Security Testing* – DAST), la marca Fortify Micro Focus se mantiene dentro de lideres del cuadrante mágico de Gartner del año actual 2022.

Figura N° 2: Lideres en soluciones de Pruebas de Seguridad de Aplicación
Fuente: *Magic Quadrant for Application Security Testing* (*Gartner*)

Entre otras alternativas, la brindada por el fabricante Veracode también cumple con los requerimientos actuales de la institución para el análisis de seguridad de las aplicaciones web; sin embargo, el software Fortity WebInspect adquirido e implementado en el Banco desde el año 2012 es un bien perpetuo de la institución, por lo cual dentro del análisis realizado la recomendación es estandarizar su renovación de mantenimiento y soporte técnico para continuar recibiendo actualizaciones de seguridad y disponer de soporte local y del fabricante.

6. ANÁLISIS COMPARATIVO TÉCNICO:

Debido a que el software Fortify WebInspect es de propiedad del Banco por su licenciamiento perpetuo adquirido en el año 2012, el cual ha sido solicitado sea estandarizado, lo que se desea es contratar el servicio de renovación de mantenimiento y soporte para la solución.

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: Renovación de soporte y mantenimiento a los servicios del fabricante Micro Focus

  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 lo que respecta a los costos asociados, el software Fortify WebInspect fue adquirido por S/. 116 900,00 (ADS-0060-2012-BCRPLIM). En los años 2020 y 2021 se realizó la renovación de las suscripciones por los montos de S/. 49 000,00 incluido IGV (0047-2020-BCRPLIM), S/. 55 000,00 incluido IGV (AS-0069-2021-BCRPLIM), respectivamente. Estos montos representan un 41.92% y 47.05% respectivamente del precio de la adquisición.

La renovación del mantenimiento y soporte de la solución actual Fortify WebInspect garantiza su funcionalidad y actualización tecnológica reduciendo la posibilidad de obsolescencia, lo cual preserva el valor económico de la inversión realizada.

8. CONCLUSIONES:

De acuerdo con el análisis realizado en el presente informe y con la necesidad continua por seguridad de realizar análisis de vulnerabilidad a las aplicaciones web de la Institución para reducir las exposiciones a ciberataques, se recomienda la renovación del mantenimiento y soporte técnico del software Micro Focus Fortify WebInspect por el periodo 2023 (un año).

Lima, 7 de octubre de 2022

cc.

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

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

Leandro Manuel ALVAREZ FIGUEROA
Jefe de Departamento de Ciberseguridad y Redes
Departamento de Ciberseguridad y Redes

VISADO POR:

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

Felipe Ernesto ROEL MONTELLANOS
Gerente de Tecnologías de Información
Gerencia de Tecnologías de Información