BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME N° 099-2016-GTI230-N

ASUNTO : Informe técnico previo de evaluación de software - Servicio de renovación de suscripciones del software HP Webinspect

---

1. NOMBRE DEL ÁREA:

Dpto. de Redes, Telecomunicaciones y Bases de Datos

2. RESPONSABLE DE LA EVALUACIÓN:

Alexander Gamboa Inga

3. CARGO:

Especialista en Redes, Telecomunicaciones y Bases de datos

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.

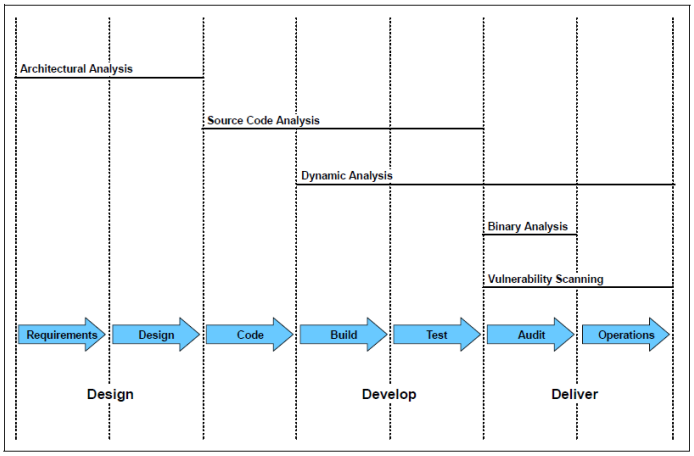

Figura N° 1: The different types of security analysis throughout the software development life cycle
Fuente: *Improving Your Web Application Software Development Life Cycle's Security* (IBM)

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 cuenta con diversas aplicaciones web publicadas hacia Internet, tales como los portales web Institucional, OCN y CID, así como las aplicaciones Carta de Garantía, SICAP, SIBFTP, el módulo web de SIMCTV. Asimismo también se cuenta con la nueva aplicación LBTR la cual está publicada hacia las instituciones financieras a través de una red privada.

Desde el punto de vista de infraestructura 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.

6. ANÁLISIS COMPARATIVO TÉCNICO:

Debido a que es un software con el cual ya cuenta el BCRP, adquirido el año 2012, y el cual ha sido solicitado sea estandarizado, lo que se desea es contratar el servicio de renovación de suscripciones.

7. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

Beneficios:

- Detección de vulnerabilidades en aplicaciones web.

- Generación de reportes especializados (detalle de vulnerabilidades, recomendaciones de solución).

Costos:

- Suscripción a los servicios del fabricante HP
  Mantenimiento de software (incluyendo el suministro de nuevas versiones y patches), soporte técnico del fabricante (escalamiento), por el periodo de un (01) año.

- 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 HP WebInspect fue adquirido por S/. 116 900,00 (ADS-0060-2012-BCRPLIM). Para la renovación del servicio de mantenimiento del presente año se han recibido diversas cotizaciones, siendo la de menor valor por S/. 39 800,00 incluido IGV, que representa el 34,04% del monto de adquisición.

8. CONCLUSIONES:

Considerando la necesidad continua de realizar análisis de vulnerabilidades tanto en los casos de aplicaciones web nuevas como a las modificaciones de las aplicaciones web ya implementadas, se recomienda la contratación del Servicio de renovación de suscripciones del software HP WebInspect, incluyendo el mantenimiento de software y soporte técnico correspondientes, por el periodo de un (01) año.

Departamento de Redes, Telecomunicaciones y Bases de Datos

05 de abril de 2016

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

Alexander John Anthony Gamboa Inga
Especialista en Redes, Telecomunicaciones y Bases de Datos
Departamento de Redes, Telecomunicaciones y Bases de Datos

Leandro Manuel Alvarez Figueroa
Jefe de Departamento de Redes, Telecomunicaciones y Bases de Datos
Departamento de Redes, Telecomunicaciones y Bases de Datos

VISADO POR:

Miguel Ángel 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

Javier Ernesto Olivera Vega
Gerente Central de Administración
Gerencia Central de Administración

Renzo Guillermo Rossini Miñán
Gerente General
Gerencia General

Firmado con certificados digitales emitidos por RENIEC. Los nombres de los firmantes figuran en la última página.
N° sistema008594