Revista
Española de

Innovación, Calidad e Ingeniería del Software

REICIS

Volumen 5, Número 2 (especial XI JICS), septiembre, 2009

Web de la editorial: www.ati.es
Web de la revista: www.ati.es/reicis
E-mail: calidadsoft@ati.es
ISSN: 1885-4486

Publicado por la Asociación de Técnicos de Informática (ATI), Via Laietana, 46, 08003 Barcelona.

Secretaría de dirección: ATI Madrid, C/Padilla 66, 3º dcha., 28006 Madrid

Revista Española de Innovación, Calidad e Ingeniería del Software (REICIS)

Contenidos

REICIS

Procedimiento para pruebas de intrusión en aplicaciones Web

Delmys Pozo Zulueta, Mairelis Quintero Ríos, Violena Hernández Aguilar, Lisney Gil Loro, Maria Felix Lorenzo Álvarez
Universidad de las Ciencias Informáticas
{dpozo@uci.cu, mquintero, violena, lgil, mflorenzo}@uci.cu

Resumen

Laboratorio Industrial de Pruebas de Software (LIPS) de la empresa cubana Calisoft (Centro para la Excelencia en el Desarrollo de Proyectos Tecnológicos) se encarga de realizar pruebas de liberación a productos entregables de proyectos de exportación e importación. Entre los tipos de prueba que realiza el LIPS están las pruebas de seguridad, específicamente las pruebas de intrusión a aplicaciones Web. La fuerza de trabajo de LIPS son los estudiantes de 1er y 2do año de la UCI (Universidad de las Ciencias Informática). Como estos estudiantes no tienen experiencia y conocimientos en pruebas de seguridad, se decidió elaborar un procedimiento de pruebas de intrusión para aplicaciones Web que guíe a los probadores. Este trabajo presenta las etapas del procedimiento y muestra las pruebas y herramientas de automatización que incluye el procedimiento. También exponen los indicadores de listas de chequeo y plantillas de casos de prueba que se definieron para enseñarle a los probadores que deben probar.

Palabras clave: pruebas de seguridad, procedimiento de pruebas, herramientas de pruebas

Procedure for intrusion testing for Web applications

Abstract

Industrial Testing Laboratory (LIPS) from Cuban Software company Calisoft (Center for the Excellence in Technological Projects's Development) takes upon to accomplish Release Test to produces artefacts of export and importing projects . Among the test types that the LIPS realizes are Security Test, specifically testing of intrusion to Web applications. The students of 1st and 2nd year under grade are LIPS's manpower of the UCI (University of Informatics Sciences). As these students are not experienced and knowledge in Security Test, was decided testers prepare a Intrusion Test Procedure for Web applications to guide to unexperienced tester. This work presents the stages of the procedure and evidences proofs and automatization tools that the procedure includes. Also they expose the indicators of check lists and templates of test cases that were circumscribed to show to the testers what that they should test.

Keywords: security tests, testing procedure, test tools

Pozo D., Quintero M., Hernández V., Gil L., Felix, M. y Álvarez, L.,"Procedimiento para pruebas de intrusión en aplicaciones Web", REICIS, vol. 5, no.2, 2009, pp.70-76. Recibido: 22-6-2009; revisado: 6-7-2009; aceptado: 31-7-2009

1. Introducción

El LIPS constituye uno de los grupos de trabajo de la empresa Calisoft (Centro para la Excelencia en el Desarrollo de Proyectos Tecnológicos). En él se fomenta una correcta instrucción técnica y pedagógica en el desarrollo de habilidades prácticas en los estudiantes a través de las actividades productivas. El LIPS cuenta con un Laboratorio de Pruebas Funcionales con la capacidad de 60 puestos de trabajo a tiempo completo para las pruebas y como fuerza de trabajo parte de los estudiantes de 1ro y 2do año de la UCI (3500 estudiantes aproximadamente). Cuenta además con 21 especialistas de Calidad de Software encargados de dirigir todo el proceso de pruebas en el laboratorio.

En el LIPS se realizan pruebas funcionales, carga y estrés, regresión, exploratorias, volumen y seguridad. Las pruebas de seguridad realizadas son pruebas de intrusión a aplicaciones web debido a la necesidad que existe en la actualidad de evaluar y garantizar la seguridad de estos sistemas. Estudios realizados por CENZIC [1] muestran que en la segunda mitad del 2008 el 80% de las vulnerabilidades encontradas en Internet pertenecían a aplicaciones web. El número de ataques aumenta cada día, ya no basta con garantizar la seguridad durante el proceso de desarrollo, también hay que realizar pruebas de intrusión que evalúen la seguridad del software después de realizado y antes de ser entregado al cliente para su posterior uso.

El proyecto OWASP (*The Open Web Application Security Project*) [2] define la prueba de intrusión o penetración a aplicaciones web como un método de evaluación de la seguridad de un sistema de ordenadores o una red mediante la simulación de un ataque. Una prueba de intrusión está enfocada a evaluar la seguridad de una aplicación web. El objetivo de esta prueba es encontrar las vulnerabilidades de las aplicaciones web y explotarlas para tomar el control del sistema. Como la fuerza de trabajo del LIPS son estudiantes con poco conocimiento y experiencia en pruebas de intrusión surge la necesidad de desarrollar un procedimiento que los guíe en la realización efectiva de las pruebas de intrusión a aplicaciones web.

El presente trabajo muestra las etapas del procedimiento elaborado, además de las pruebas y herramientas incluidas en el mismo. La sección 2 presenta las pruebas y herramientas del procedimiento, la sección 3 muestra sus etapas y la 4 las conclusiones.

2. Pruebas y herramientas que incluye el procedimiento.

La realización de las pruebas se separó en dos niveles siguiendo la filosofía de la compañía Above Security. El primer nivel consiste en la evaluación de las vulnerabilidades de la aplicación, donde se recopilan las debilidades encontradas mediante la utilización de herramientas automatizadas y poca intervención manual, en este nivel las pruebas son realizadas por los estudiantes debido a la poca intervención manual que se requiere. En este nivel es donde se aplica el procedimiento desarrollado.

El segundo nivel consiste en la recopilación de evidencias objetivas que demuestren la explotación de las vulnerabilidades detectadas en el primer nivel. Como este nivel requiere de mayor tiempo, esfuerzo y conocimiento por parte de los probadores para llevar a cabo su ejecución el LIPS contrata los servicios del Grupo de Seguridad (GS) de la UCI, el cual cuenta con probadores expertos en temas de seguridad de sistemas informáticos.

Para la realización del procedimiento se utilizó la Guía de Pruebas del proyecto OWASP. Esta guía define varias categorías de prueba de intrusión, de estas el procedimiento contempla 4. También se seleccionaron dentro de estas categorías las pruebas más fáciles de aplicar por los probadores. Las herramientas automatizadas que se utilizan son el escáner de vulnerabilidades Nessus y el excelente software para extraer parejas de usuario / contraseña de contraseñas remoto Brutus.

Las categorías de prueba del procedimiento son:

- Recopilación de Información: El objetivo de esta categoría es comprobar si la aplicación brinda datos sensibles utilizables por cualquier atacante. Los tipos de prueba incluyen comprobación de firma digital, descubrimiento de aplicaciones, análisis de códigos de error y pruebas de SSL/TLS.
- Comprobación de las reglas del Negocio (CRN): Las pruebas de esta categoría es la comprobación de las reglas del negocio definidas para la aplicación.
- Comprobación de la autenticación (CA): Esta categoría pone a prueba el sistema de autenticación de la aplicación mediante prueba de fuerza bruta y pruebas al recordatorio de contraseñas del sistema.
- Validación de datos (VD): Verifica que todas las entradas de datos estén validadas realizando pruebas de inyección SQL, ORM, LDAP, XML, SSI, procedimientos almacenados y código.

3. Procedimiento de Pruebas de Intrusión

El procedimiento define los pasos para llevar a cabo las pruebas de intrusión desde su planificación hasta la documentación de los hallazgos encontrados, haciendo uso de diferentes plantillas de apoyo.

2.1. Etapa 1: Planificación de las Pruebas

En esta fase el EP planifica las pruebas, para ello utiliza la platilla de Plan de Prueba definida por RUP donde se establecen las especificaciones necesarias para las pruebas, como hardware, recursos del sistema, la estrategia de prueba, cronograma planificado, cronograma real, los roles y responsabilidades.

2.2. Etapa 2: Diseño de las Pruebas

Para guiar a los probadores en la ejecución las pruebas se elaboraron plantillas de listas de chequeo (LCH) y de caso de prueba (CP) que serán rediseñados por el EP en esta etapa según las características de la aplicación. Para probar las categorías de prueba CRN y VD se definieron CP y para las categorías de prueba RI y CA se definieron LCH.

Las LCH recogen los indicadores a evaluar, su descripción, la herramienta que se utilizará, el resultado esperado y el resultado real. Los indicadores a evaluar definidos para la categoría RI de forma general recogen si puede obtenerse la firma digital (tipo y versión) del servidor web, los puertos abiertos en el IP del servidor y los servicios asociados a esos puertos, las aplicaciones web instaladas en el servidor, la existencia cifrados débiles y si el código de error de la aplicación muestra información sobre el sistema operativo o base de datos del servidor web. Los indicadores a evaluar definidos para la categoría CA contemplan si se logra mediante el ataque de fuerza bruta obtenerse el usuario y la contraseña de un usuario privilegiado en la aplicación, si puede saltarse el sistema de autenticación y el del recordatorio contraseña.

Para realizar el CP de la categoría CRN primero se debe realizar una matriz de privilegios que contenga las funcionalidades de la aplicación y los roles que tienen permiso para realizarla. Luego se crea un CP por rol y en él se coloca un escenario para cada funcionalidad donde el rol no tenga permisos, para comprobar si esta funcionalidad puede

ser ejecutada ilegalmente por un rol sin privilegios, o con privilegios mínimos. La estructura del CP se muestra en la tabla 1.

Nombre del Rol	**Escenarios**	**Descripción de la funcionalidad a probar**	**URL**	**Resultado esperado**	**Respuesta del sistema**
< Nombre del Rol>	<Funcionalidad a probar>	<Descripción de la funcionalidad.>	<URL de acceso a la funcionalidad>	< Resultado que se espera al realizar la prueba.>	<Resultado que se obtiene al realizar la prueba.>

Tabla 1. Estructura del CP de la categoría CRN

La tabla 2 muestra el CP elaborado para la categoría VD. Se diseñará un CP por cada funcionalidad reflejando todos los campos de entrada que tiene.

Funcionalidad:	<Nombre de la funcionalidad>		**Herramienta:**	<Nessus>
Campos de Entrada	**Clasificación**	**Resultado Esperado**	**Respuesta del Sistema**	**Flujo Central**
<Nombre del campo de entrada>	<La clasificación es según el componente de diseño utilizado][ejemplo: campo de texto, lista desplegable o campo de selección.>	<Resultado que se espera al realizar la prueba, específicamente si el campo de entrada es vulnerable a inyección SQL, ORM, LDAP, XML, SSI, código o procedimientos almacenados.>	<Resultado que se obtiene al realizar la prueba>	<Pasos a desarrollar para probar la Funcionalidad que se indicó>

Tabla 2. Estructura del CP de la categoría VD

2.3. Etapa 3. Ejecución de la pruebas

En esta etapa los probadores ejecutan las categorías de pruebas definidas haciendo uso de las LCH y los CP diseñado por el EP. La ejecución de las pruebas se realiza comenzando por la categoría RI, luego se pueden realizar las categorías CA, CRN y VD en paralelo o en el orden que se decida. Cuando finalizan las pruebas se eliminan de las vulnerabilidades encontradas los falsos positivos.

2.4. Etapa 4. Documentación e Informe de los resultados

A la vez que los probadores ejecutan las pruebas van registrando las no conformidades (NC) en el registro de defectos y dificultades (RDD), estas NC no son más que las vulnerabilidades detectadas. El RDD refleja la descripción de las NC y la etapa de

detección. El EP al concluir la jornada de prueba realiza un informe diario del RDD donde recoge todas las NC encontradas. Luego este informe es entregado al equipo de desarrollo y cuando se terminan todas las iteraciones se le entrega el informe final al GS.

4. Conclusiones

Para evaluar el aporte que traería la utilización del procedimiento se encuestaron 7 expertos del GS, de los encuestados 2 evaluaron el procedimiento de regular (Suficientemente bueno con reservas) y los 5 restantes lo evaluaron de bueno (Aplicable con resultados destacados).Este procedimiento además de ser utilizado por probadores de poca experiencia, también puede emplearse en equipos de desarrollo que deseen evaluar las vulnerabilidades de las aplicaciones web que construyen.

El LIPS ha realizado pruebas de seguridad a varias aplicaciones web de la UCI después de aplicado el procedimiento, las NC detectadas fueron entregadas al GS. El proceso de pruebas del GS es muy largo y trabajoso, hasta la fecha ha culminado la revisión de tres aplicaciones. La gráfica 1 muestra la comparación de las NC detectadas por los probadores a tres aplicaciones web antes y después de la utilización del procedimiento, además muestra el tamaño de las aplicaciones en casos de uso. Antes las NC detectadas durante la evaluación de las vulnerabilidades eran inferiores a las detectadas en el GS y después esa cantidad están más igualadas. Analizando estos datos puede concluirse que el procedimiento es útil para los probadores porque después de su uso la cantidad de NC o vulnerabilidades encontradas se asemejan más a las vulnerabilidades explotadas por el GS.

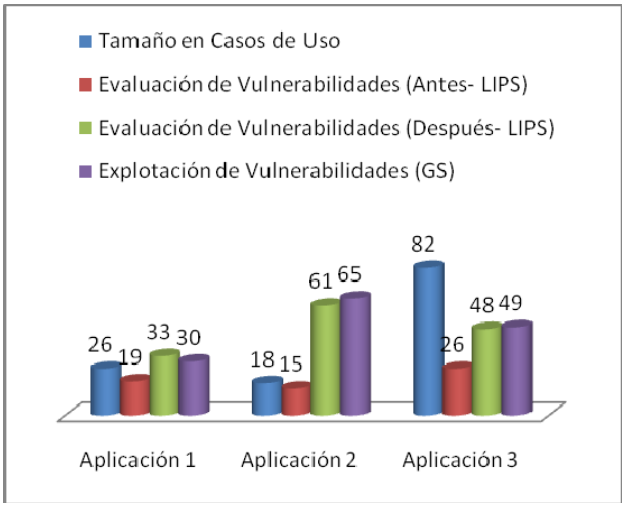

Figura 1. Cantidad de NC antes y después del uso del procedimiento

Referencias

[1] Cenzic, “Web Application Security Trends Report Q3-Q4, 2008”, Cenzic, 2009.

[2] OWASP**.** *Owasp testing guide V2.0,* OWASP, 2007.