Procedimiento para pruebas de intrusión en Aplicaciones Web

Autor Principal:
Ing. Delmys Pozo Zulueta
Universidad de las Ciencias Informáticas
dpozo@uci.cu

Ambiente de trabajo

Recursos

LIPS

- 60 puestos de trabajo.
- Estudiantes de 1ro y 2do año de la UCI (3500 estudiantes aproximadamente)
- 21 especialistas de Calidad de Software

Pruebas

- Funcionales
- Farga y estrés
- Regresión
- Exploratorias
- Volumen
- Seguridad

"La prueba de intrusión o penetración a aplicaciones web es un método de evaluación de la seguridad de un sistema de ordenadores o una red mediante la simulación de un ataque"

OWASP (The Open Web Application Security Project)

CALISOFT ©Carretera San Antonio Km 2 1/2 Torrens, Ciudad de La Habana, Cuba. Teléf: (537) 8372427

Niveles de realización:

Nivel 1: Evaluación de vulnerabilidades

- Necesita utilización de herramientas automatizadas y poca intervención manual
- Realizado por los probadores del LIPS

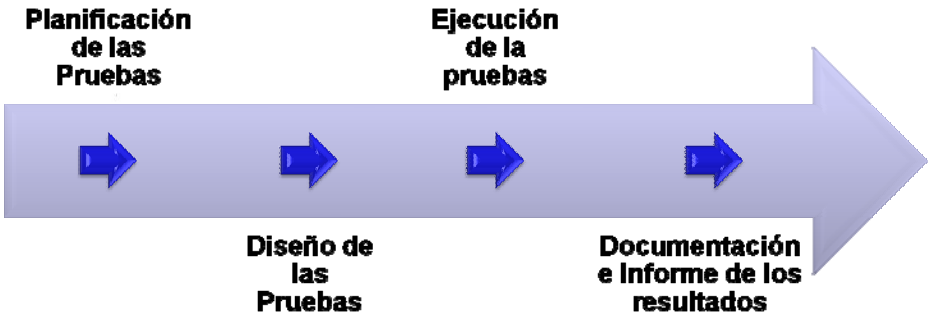
Nivel 2: Explotación de vulnerabilidades

- Necesita mayor tiempo, esfuerzo y conocimiento por parte de los probadores
- Realizado por el Grupo de Seguridad de la UCI

Pruebas y herramientas

Categoría	Objetivos	Herramientas
Recopilación de Información (RI)	Comprobar si la aplicación brinda datos sensibles que puedan ser utilizados por cualquier atacante	Nessus
Comprobación de la autenticación (CA)	Poner a prueba el sistema de autenticación	Brutus
Comprobación de las reglas del Negocio (CRN)	Comprobar las reglas del negocio definidas para la aplicación	Nessus
Validación de datos (VD)	Verificar que todas las entradas de datos estén validadas	Nessus

Etapas del procedimiento



Etapa 2: Diseño

Lista de Chequeo

- Recopilación de Información
- Comprobación de la autenticación

Caso de Prueba

- Comprobación de las reglas del Negocio
- Validación de datos

Indicadores de RI

- ✓ Firma digital.
- ✓ Puertos abiertos.
- ✓ Aplicaciones web instaladas en el servidor.
- ✓ Existencia cifrados débiles.
- ✓ Análisis delcódigo de error de la aplicación.

Indicadores de CA

- ✓ Ataque de fuerza.
- ✓ Sistema de autenticación.
- ✓ Recordatorio contraseña.

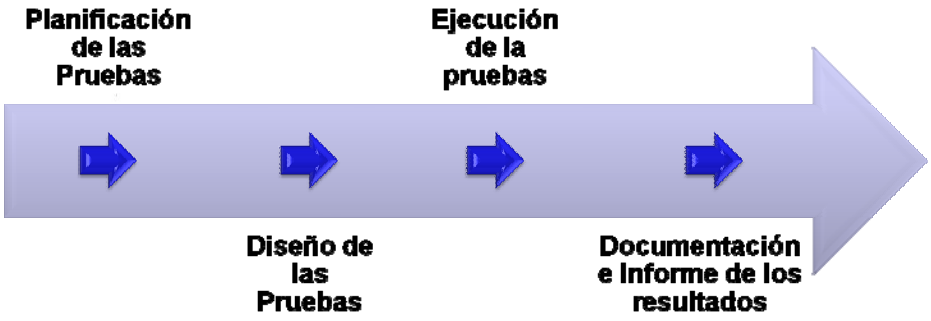
Estructura del CP de CRN

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.>

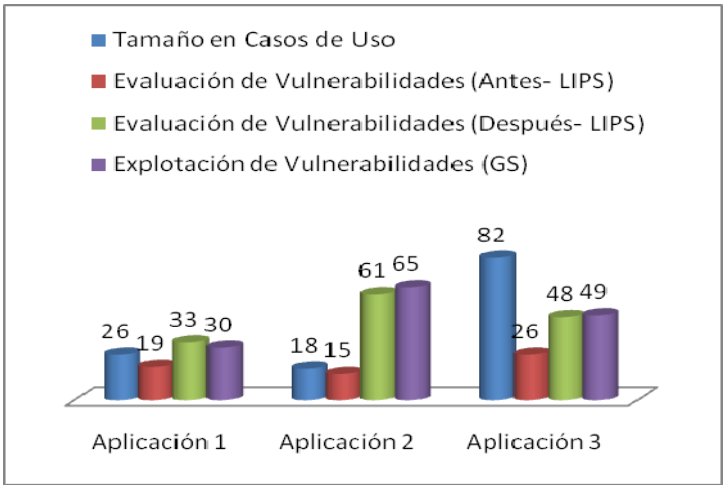
Estructura del CP de VD

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 que se indicó>

Etapas del procedimiento



Comprobación



Procedimiento para pruebas de intrusión en Aplicaciones Web

Autor Principal:
Ing. Delmys Pozo Zulueta
Universidad de las Ciencias Informáticas
dpozo@uci.cu