Pleni

Carlos Eduardo Caballero Burgoa
Gonzalo Nina Mamani
Christian Lima Saravia

17 de julio de 2014

Índice

1. Introducción

Cualquier organización que expone sus servicios informáticos a redes de acceso tendrán que realizar un esfuerzo significativo para asegurar que la información y recursos esten protegidos. Internet es un factor primordial en la comunicación y también un evidente riesgo potencial de acceso y mal uso de los servicios e información disponibles. Obviamente, se catalogan sistemas mas críticos que otros donde su seguridad debe de ser muy significativa, pero en general todas las aplicaciones web deben de estar protegidas y aseguradas ante los principales ataques.

En una aplicación web, dividimos la seguridad en:

Disponibilidad Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

Integridad Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

Confidencialidad Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

2. Antecedentes

Un efecto secundario del crecimiento exponencial que ha tenido el Interneti, es la privacidad de información tanto personal como profesional. En Internet encontramos funcionando a tiendas en línea, negocios que mueven grandes cantidades de dinero, redes de los servicios que habilitan el comercio a nivel internacional así como sitios de redes sociales que contienen información muy delicada de la vida privada de sus miembros.

Mientras más se conecta el mundo, la necesidad de seguridad en los procedimientos usados para compartir la información se vuelve más importante. Desde muchos puntos de vista, podemos creer sin dudar que el punto más crítico de la seguridad del Internet, lo tienen las piezas que intervienen de forma directa con las masas de usuarios, es decir, las aplicaciones web.

Ahora que sabemos que la mayoría de los problemas de seguridad en los sitios web se encuentran a nivel aplicación y que son el resultado de escritura defectuosa de código, debemos entender que programar aplicaciones web seguras no es una tarea fácil, ya que requiere por parte del programador, no únicamente mostrar atención en cumplir con el objetivo funcional básico de la aplicación, sino una concepción general de los riesgos que puede correr la información contenida, solicitada y recibida por el sistema.

3. Definición del problema

Existen muchos problemas que pueden ser identificados rapidamente desde el punto de vista de un usuario normal (cliente) en el sitio web, y asi brindar una solucion rapida y efectiva para asi evitar dañar la imagen de su organización o afectar adversamente a sus clientes, socios y empleados tales como:

Defacement de sitios web Usuarios maliciosos deambulan en Internet específicamente para desfigurar sitios. A menudo esos sitios contienen lenguaje o imágenes ofensivas y el probable resultado es una imagen dañada.

Explotaciones web A menudo, los atacantes comprometen un sitio web e instalan explotaciones para atacar a los visitantes del sitio. Estos son clasificados a menudo como defacement silenciosos ya que el sitio no se ve cambiado visualmente. Sophos señaló que la vasta mayoría de los sitios web que alojan malware (cerca de 80 %) son sitios legítimos que han sido comprometidos.

Fugas de información sensible Los sitios web pueden filtrar información sensible mediante mensajes de error detallados, archivos que no tienen la intención de ser mostrados públicamente.

También existen una serie de problemas

- Fallas de sistema.
- Enlaces rotos.
- Servidores mal configurados o con la configuración por defecto.
- Mensajes de error y advertencia.

4. Objetivo general

Identificar problemas de seguridad de sitios web de manera similar a un motor de búsqueda. Analizar el contenido descubierto mediante el uso de un motor de análisis que es capaz de detectar amenazas tanto conocidas como desconocidas, cambios inusuales y contenido anómalo.

Una vez que se detecta un problema, se invoca el sistema de respuesta a incidentes. La respuesta a incidentes realiza acciones de manera rapida y temprana informando mediante el envío de mensajes (mensajería instantánea, correo electrónico, SMS) al personal encargado de la aplicacion web.

5. Objetivos específicos

- Crear una aplicacion web que permita realizar una copia del sitio web a analizar y almacenarlo en una base de datos.
- Crear un conjunto básico de rutinas que permitan analizar el contenido en busca de codificación sospechosa.
- Crear un conjunto básico de rutinas que permitan verificar de manera periodica la integridad del sitio web, mediante la comparacion de algoritmos de hash (md5 y sha).
- Diseñar los modulos que permitan realizar alertas y/o avisos de los eventos.

6. Herramientas

Las herramientas necesarias para realizar este proyecto es basicamente las siguientes:

- Hosting: Se necesita un espacio donde almacenar el código que soporte las siguientes tecnologias:
  - Base de Datos: PosgreSQL 9.x.

  - PHP 5.3 o superior.
  - Servidor Web: Preferiblemente Apache 2.x.

- Subdominio *pleni.scesi.org-pleni.scesi.memi.umss.edu.bo.*
- Ganas de mejorar y aprender.

7. Justificación

Este proyecto tiene connotaciones de manera academica brindando el aprendizaje de programacion de aplicaciones web a todos los participantes del grupo asi tambien asimilar las medidas para detectar fallos y politicas de seguridad respecto a aplicaciones web.

De manera social la SCESI brindará un servicio a la comunidad universitaria, y entidades externas a la universidad, ayudando a mejorar la seguridad de la sociedad y concientizando sobre lo que esto conlleva.