Pleni
Sistema para la recolección de información orientado a la mejora en la evaluación de seguridad

Carlos Eduardo Caballero Burgoa
Gonzalo Nina Mamani
Cristhian Lima Saravia

25 de febrero de 2015

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 estén protegidos. Internet es un factor primordial en la comunicación, pero 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 Internet, es la privacidad de información tanto personal como profesional. En Internet encontramos funcionando 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 de 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. Justificación

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

4. Planteamiento del problema

Existen muchos problemas que pueden ser identificados rápidamente desde el punto de vista de un usuario normal (cliente) en el sitio web, y así brindar una solución rápida y efectiva para así evitar dañar la imagen de su organización o afectar adversamente a sus clientes, socios y empleados.

En el área de la seguridad se podrían detallar varios tipos de ataque 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.

Fallos del sistema También existen una serie de problemas:

- Enlaces rotos.
- Mensajes de error y advertencia.
- Servidores mal configurados o con la configuración por defecto.
- Certificados SSL expirados.
- Errores de servidor.

Por lo mencionado se define el problema como:
"El elevado numero de sitios web que no poseen las características mínimas de seguridad conduce a la obtención de información privilegiada."

5. Objetivos

5.1. Objetivo general

Desarrollar una herramienta de seguridad para la detección temprana de actividades sospechosas de modo que pueda garantizarse un mínimo de seguridad aceptable.

5.2. Objetivos específicos

- Registrar toda la información disponible del sitio web para el análisis posterior.
- Crear un conjunto básico de rutinas que permitan verificar de manera periódica la integridad del sitio web.
- Analizar la información registrada para encontrar algún tipo de código malicioso.

- Diseñar las rutinas que permitan realizar avisos y/o alertas de los eventos para el correcto mantenimiento del sitio.

6. Hipótesis o idea a defender

Se pretende concientizar a la sociedad acerca de los peligros de la mala administración de los sistemas y su información, para así no tener perdidas importantes para cualquier organización. De esta manera se quiere brindar soluciones a los problemas de seguridad mas comunes.

7. Aporte científico

A partir de la información registrada podrían proyectarse errores frecuentes referentes al proceso de desarrollo, y administración de forma que estos puedan ser previstos en etapas mas tempranas.

8. Diseño metodológico y teórico

Para el proceso de creación de esta herramienta, se han seguido algunos lineamientos fundamentales del desarrollo ágil, a pesar de eso, se fundamentan muchos de los procedimientos creados basados en la experiencia en seguridad informática de los componentes del equipo.

9. Desarrollo del proyecto

El desarrollo del proyecto se realizó en las siguientes etapas:

9.1. Captación de la información

Se procedieron a crear los métodos necesarios para absorber la mayor cantidad de información disponible de forma publica del sitio a analizar.

También se crearon algunos otros métodos para el aprovechamiento del buscador google en lo referente a la obtención de información.

9.2. Análisis de la información

Con toda la información captada en las anteriores etapas, se crearon herramientas para probar las distintas técnicas de vulneración del sitio web, de forma que estas pudiesen ser mas automatizadas.

9.3. Herramientas utilizadas

Las herramientas necesarias para realizar este proyecto fueron básicamente las siguientes:

- Base de Datos NoSQL: CouchDB.
- Node.js.
- Express.js (framework para el desarrollo web).

- Servidor web para el despliegue: nginx.

10. Conclusiones y recomendaciones

Pudo observarse con la herramienta desarrollada, que la gran mayoría de sitios desarrollados a nivel local carecen de políticas apropiadas de seguridad de su información, todo esto a causa de la dejadez de los encargados de administración. Los cuales velan mas por el despliegue rápido que por el mantenimiento continuo del sistema.

Creemos que la solución debe pasar por la especialización de las funcionalidades de un sistema, en lugar de desear una solución que tenga muchas funcionalidades y no cumpla con las especificaciones deseadas.

Referencias

[1] ThreatFactor NSIA.
Extraído el 17 de Julio del 2014, de
http://threatfactor.com/Products/NSIA/Features.

[2] UNAM-CERT: Equipo de Respuesta a Incidentes UNAM.
Aspectos básicos de la seguridad en aplicaciones web.
Extraído el 17 de Julio del 2014, de
http://www.seguridad.unam.mx/documento/?id=17

[3] Marco de desarrollo de la Junta de Andalucia.
Conceptos de seguridad en aplicaciones WEB.
http://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/212