UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

MAYO 2019 - SEPTIEMBRE 2019

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERIA EN SISTEMAS

TEMA:

ANÁLISIS DE AMENAZAS Y VULNERABILIDADES DENTRO DEL SISTEMA DE GESTIÓN DEL VOLUNTARIADO EN LA CRUZ ROJA UBICADA EN LA CIUDAD DE BABAHOYO.

EGRESADA:

ROMINA ISABEL CUESTA MORANTE

TUTORA:

ING. NELLY KARINA ESPARZA CRUZ

AÑO 2019

Introducción

En la actualidad las organizaciones tanto públicas como privadas manejan sistemas informáticos para la mejor administración de la información y los datos de usuario, estos sistemas en la mayoría se conectan a la red por lo que son vulnerables a diferentes tipos de amenazas cibernéticas debido en ocasiones a su mala utilización, estas vulnerabilidades pueden poner en peligro la integridad de los datos de una organización.

Una correcta planificación de protección hacia la información de la organización se debe tener en cuenta el análisis de vulnerabilidades como una actividad de gran importancia para estar prevenidos con el progresivo crecimiento de las amenazas hacia los sistemas informáticos.

El presente trabajo de investigación vinculado a un estudio de caso en el análisis del sistema de gestión del voluntariado en la cruz roja el mismo que está involucrado a la sublínea de investigación: Desarrollo de sistemas informáticos. Este sistema cuenta con registros y administración de fichas de voluntarios, administración de cursos, sistema de reportes, entre otros. Por lo que se resalta la importancia de realizar un análisis a profundidad que permita identificar las fortalezas, debilidades y amenazas del sistema.

En los últimos tiempos la programación ha progresado evidentemente los sitios web ahora son más dinámicos ya que existe interacción entre los sistemas web y el usuario beneficiando a la sociedad. La programación tradicional junto con la orientada a

objetos son herramientas esenciales para el desarrollo de sistemas web con ellas podemos tener software de calidad y así reducir la deficiencia de los sistemas existentes.

La seguridad en el sistema informáticos debe ser la primera opción que genere interés prioritario en las organizaciones ya que por medio de la red internet se registran los usuarios y se administran los datos de todos los voluntarios en la ciudad de Babahoyo.

Según la (Unidad Global de ciberseguridad del grupo telefónica Eleven Panths, 2019), afirma que "En la actualidad estamos expuestos a sufrir ataques cada vez más sofisticados y frecuentes que ponen en peligro nuestro negocio, reputación, privacidad y confianza. Por eso, necesitamos ser cada vez más receptivos a las medidas de ciberseguridad y redefinir nuestra estrategia hacia la ciber-resiliencia.", Ningún sistema es completamente seguro ya que existe un alto crecimiento del espionaje informático y cada vez más personas alejadas a las buenas prácticas de la seguridad en los sistemas están en busca de brechas que permitan vulnerar los sistemas produciendo así la filtración de información sensible de la organización.

Para realizar el desarrollo de este estudio de caso se escogió utilizar la metodología MAGERIT ya que esta se acopla a la línea de investigación de los análisis de gestión de riesgos de los sistemas de información. MAGERIT permite mediante sus diferentes fases enumerar los activos asociados al sistema informático como también podemos encontrar las amenazas y vulnerabilidades del sistema el cual permitirá salvaguardar los datos y reducir el impacto de riesgo para la buena utilización del software.

Dentro de las limitaciones de esta investigación acerca del sistema de Gestión del Voluntariado de la Cruz Roja se encuentra la poca información que existe de parte de los desarrolladores del mismo ya que esta problemática afecta a la comprensión del desarrollo de este software.

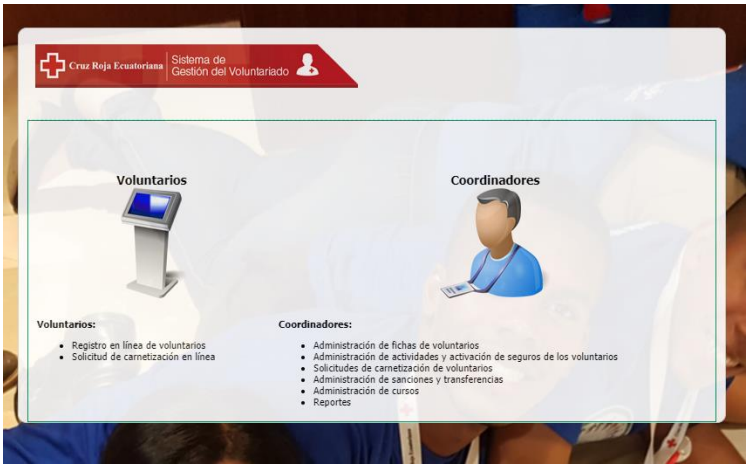
Desarrollo

Las amenazas y vulnerabilidades siempre están presentes en un sistema informático, en este caso en el Sistema de gestión del voluntariado en la cruz roja ubicada en la ciudad de Babahoyo, en la av. 10 de Agosto #1107 entre flores y Martín Icaza. La tecnología ha ido creciendo con el paso del tiempo en el área de la informática y de los sistemas de aplicaciones web, los sistemas informáticos disponen una amplia variedad de beneficios para distintas áreas, ya sea a nivel académicas en empresas públicas o privadas.

La sociedad en la actualidad se está convirtiendo cada vez más en un consumidor virtual debido a la demanda del uso de software por parte de las empresas o clientes. Esto causa un crecimiento de forma exponencial debido a la importancia de implementar el uso de la tecnología para poder agilitar y optimizar procesos de gestión para la administración de información.

El sistema de gestión de voluntariado con el que cuenta la Cruz Roja en la ciudad de Babahoyo permite a los voluntarios tener un perfil de usuario el cual permite sistematizar los tramites correspondiente para el registro en línea del personal y la administración de actividades por parte de las personas encargadas de la coordinación.

El Sistema de Gestión del Voluntariado de la Cruz Roja fue desarrollado por la Cruz Roja Ecuatoriana en el año 2005, la implementación de este software permite realizar diferentes procesos que permite a los voluntarios y administradores tener una mayor sistematización e interacción de la información logrando tener reportes de las actividades de la institución de una manera fácil y eficaz.



Elaborado por: *Romina Cuesta Morante*

Figura 1. *Login del Sistema de Gestión del Voluntariado*

HTML en inglés HyperTex Markup Languaje (lenguaje de marcas de hipertexto). El hipertexto es un enlace o link que las computadoras poseen para hacer referencias a otro texto. Se interpreta que el hipertexto es un texto que al ejecutar sobre el un clic con el mouse se dirigirá a otro texto cuando usamos internet. Sirve para organizar documentos, pero no para dar una apariencia o diseño a documento. (Equipo Vértice, 2009)

En 1998 se publicó HTML 4 ya que los avances dentro del lenguaje de marcas de hipertexto no se hacen esperar. Esta versión se sigue utilizando hasta el día de hoy y

trae consigo mejoras esenciales como hojas de estilo, tablas, también mejoras en los formularios y da la posibilidad de incorporar scripts. (Casabona & Ceci, 2016)

La versión de HTML 4.01 se publicó el 24 de diciembre de 1999 como último detalle de HTML en esta versión no trae muchas novedades al tratarse de la versión 4.0. Luego de eso W3C se propuso a desarrollar el estándar XHTML. (Alamán, 2017)

Según (Castillo, 2017) afirma que "JavaScript es un lenguaje de programación interpretado. Fue originalmente implementada como parte de los navegadores web para que los Script pudieran ser ejecutados en el lado del cliente e interactuasen con el usuario sin necesidad de que este script pase por el servidor, siendo controlado por el navegador, realizando comunicación asíncrona y modificando el contenido del documento mostrado." JavaScript es un lenguaje de programación que interactúa con los usuarios por lo que no necesita compilarse ya que funciona del lado del cliente el cual permite crear paginas dinámica y los códigos son interpretados por los navegadores y no tiene que pasar por el servidor.

Según (GB Advisors, 2019) afirma que "Nessus es el estándar mundial para la prevención de ataques de red, identificación de vulnerabilidades y detección de problemas de configuración que utilizan los hackers para entrar en la red. Nessus se ha utilizado por más de 1 millón los usuarios en todo el mundo, por lo que es el líder mundial de evaluación de la vulnerabilidad, configuración de seguridad y cumplimiento de las normas de seguridad.", Nessus es un software muy utilizado en la actualidad para hacer pruebas de vulnerabilidades dentro de las empresas u organizaciones, permite identificar las fallas que tienen los sistemas con la finalidad de prevenir amenazas cibernéticas.

Las empresas constantemente están amenazadas con sufrir daños en sus sistemas informáticos, estos daños pueden incitar perdidas de muchos tipos. Las amenazas son mayores cuando en el sistema existen ciertas brechas de seguridad llamados vulnerabilidades que pueden perjudicar de gran manera a las organizaciones. Se obtiene (Urbina, 2016)

Se utilizó el método cuantitativo ya que la información fue obtenida a través de encuestas realizadas a los voluntarios de la cruz roja, recopilando datos concretos estructurados y estadísticos para el desarrollo y respaldo del estudio de caso.

Una de las técnicas de investigación que se utiliza con mayor frecuencia para el análisis de gestión de riesgos dentro de los sistemas informáticos es la metodología MAGERIT. Desarrollada por el Consejo Superior de Administración Electrónica para disminuir los riesgos al momento de manejar información y datos sensibles dentro de una organización para mejorar el uso de los recursos tecnológicos.

La metodología tiene 5 fases:

- **Fase 1 Activos:** Determinar los activos relevantes para la organización.
- **Fase 2 Amenazas:** Determinar a qué amenazas están expuestos dichos activos.
- **Fase 3 Salvaguardas:** Determinar que salvaguardas hay dispuestas y cuan eficaces son frente al riesgo.
- **Fase 4 Impacto residual:** Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- **Fase 5 riesgo residual:** Estimar el riesgo definido como el impacto ponderado con la tasa de ocurrencia de la amenaza. (Molina-Miranda, 2017)

Fase 1. Activos

En la primera fase del desarrollo de la investigación se identifican los activos con mayor relevancia dentro de la organización los cuales forman parte del caso de estudio y se los muestra a continuación:

- Hardware
- Software
- Datos
- Instalaciones
- Personal administrativo
- Personal voluntario

Fase 2. Amenazas

En esta fase se identifican las amenazas y vulnerabilidades que pueden afectar a los activos tecnológicos de la organización, para la identificación de estas amenazas se utiliza la herramienta Nessus la cual consta con una interfaz sencilla y practica para encontrar brechas de seguridad dentro de sistemas informáticos.

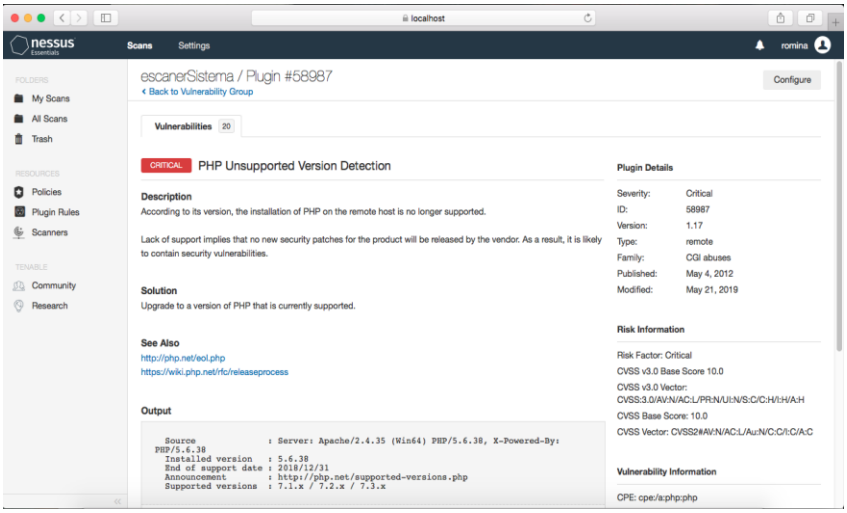
Identificación de amenazas y vulnerabilidades

Se realizó el escaneo de vulnerabilidades con la herramienta Nessus, esta herramienta es la más usada en todo el mundo para realizar hacking ético y comprobar vulnerabilidades en un sistema web.

Se hizo el escaneo del Sistema de Gestión del voluntariado de la cruz roja el día viernes 2 de agosto a las 9:47 pm y se encontró 20 vulnerabilidades de las cuales el 5% es crítico, el 29% es de un nivel alto, el 30% medio, el 4% es de nivel bajo y el 32% de

información que no representan riesgos para el sistema. Este análisis se centrará en las más importantes y es detallado a continuación:

Detección de versión no compatible con PHP



Elaborado por: *Romina Cuesta Morante*

Figura 2: *Vulnerabilidad encontrada*

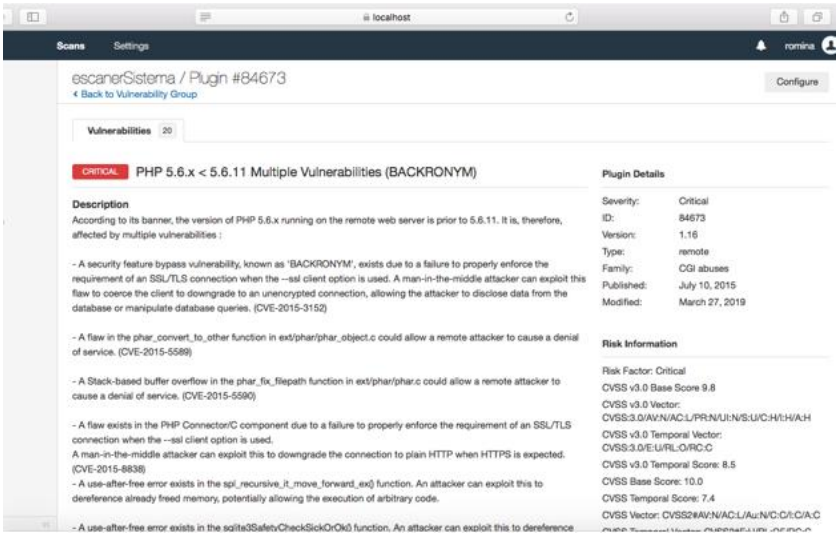
Descripción

La versión que está instalada en el hosting es obsoleta esto implica que el proveedor ya no lanzara nuevas actualizaciones de seguridad esto pone en gran riesgo al sistema y lo deja expuesto a vulnerabilidades de seguridad sin parche.

Solución

Actualizar la versión de PHP a una actualmente compatible.

PHP 5.6.x <5.6.11 Vulnerabilidades múltiples (BACKRONYM)



Elaborado por: *Romina Cuesta Morante*

Figura 3: *Vulnerabilidad encontrada*

Descripción

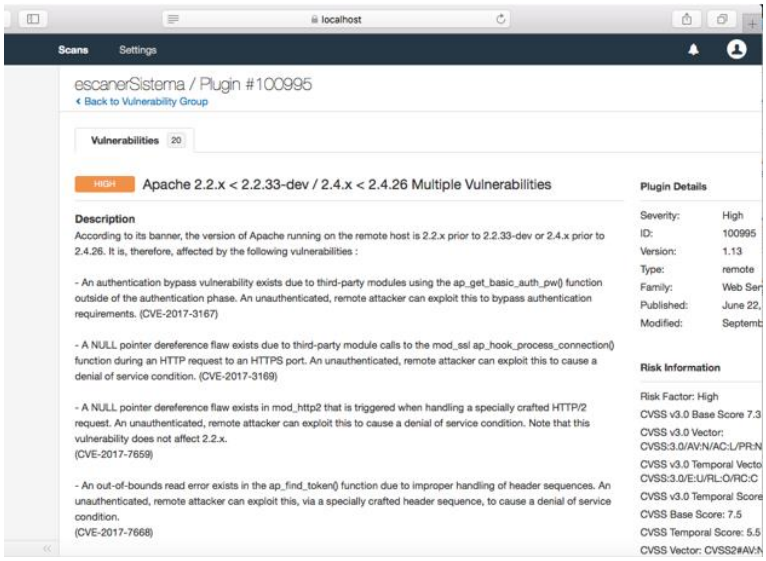
Según la versión que se ejecuta en el servidor web es anterior a 5.6.11 por lo tanto se ve afectado por múltiples vulnerabilidades, una de ellas es conocida como 'BACKRONYM' debido a una falla en hacer cumplir apropiadamente el requisito de una conexión SSL/TLS cuando se usa la opción cliente –ssl. Un atacante man-in-the-middle puede explotar esta falla para obligar al cliente a degradar a una conexión no cifrada, lo que permite al atacante revelar datos de la base de datos o manipular consultas de la base de datos (CVE-2015-3152). Existe otra falla en el componente PHP

Connector / C, el atacante puede aprovechar esto para degradar la conexión a HTTP simple cuando espera HTTPS. (CVE-2015-8838). Otra amenaza identificada es el desbordamiento de búfer basado en la pila en la función phar_fix_filepath en ext / phar / phar.c podría el cual permitir que un atacante remoto cause una denegación de servicio. (CVE-2015-5590)

Solución

Actualizar a la versión 5.6.11 o posterior

Apache 2.2.x <2.2.33-dev / 2.4.x <2.4.26 Vulnerabilidades múltiples



Elaborado por: *Romina Cuesta Morante*

Figura 6: *Vulnerabilidad encontrada*

Descripción

La versión de Apache que se ejecuta en el host remoto es 2.2.x anterior a 2.2.33-dev o 2.4.x anterior a 2.4.26. Por lo tanto, se ve afectado por las siguientes vulnerabilidades:

- Existe una vulnerabilidad identificada como “omisión de autenticación” debido a módulos de terceros que utilizan la función ap_get_basic_auth_pw () fuera de la fase de autenticación. Un atacante remoto no autenticado puede explotar esto para evitar los requisitos de autenticación. (CVE-2017-3167)

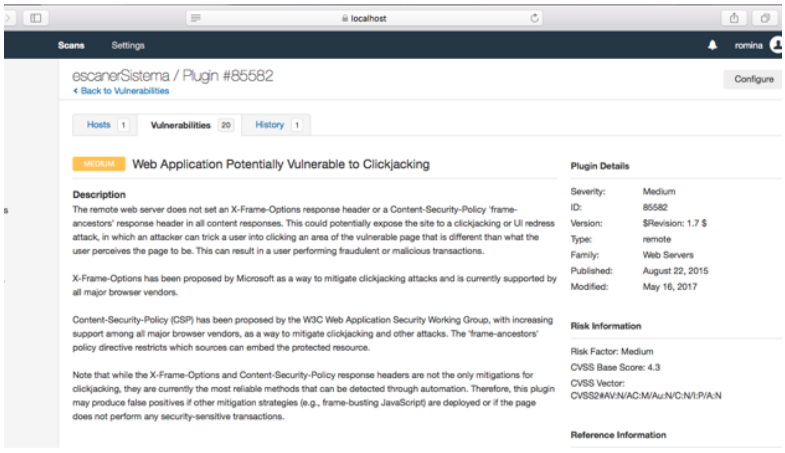
- Existe un defecto de desreferencia de puntero NULL debido a llamadas de módulos de terceros a la función mod_ssl ap_hook_process_connection () durante una solicitud HTTP a un puerto HTTPS. Un atacante remoto no autenticado puede explotar esto para causar una condición de denegación de servicio. (CVE-2017-3169)

- Existe un defecto de desreferencia de puntero NULL en mod_http2 que se activa al manejar una solicitud HTTP / 2 especialmente diseñada. Un atacante remoto no autenticado puede explotar esto para causar una condición de denegación de servicio. (CVE-2017-7659)

Solución

Actualizar la versión a 2.2.33-dev / 2.4.26 o posterior

Aplicación web potencialmente vulnerable a Clickjacking



Elaborado por: *Romina Cuesta Morante*

Figura 7: *Vulnerabilidad encontrada*

Descripción

El servidor web remoto no establece un encabezado de respuesta X-Frame-Options de Content-Security-Policy en todas las respuestas de contenido. Esto podría exponer el sitio a un ataque de clickjacking o reparación de la interfaz de usuario, en el que un atacante puede engañar a un usuario para que haga clic en un área de la página vulnerable que es diferente de lo que el usuario percibe que es la página. Esto puede provocar que un usuario realice transacciones fraudulentas o maliciosas.

X-Frame-Options ha sido propuesto por Microsoft como una forma de mitigar los ataques de clickjacking y actualmente es compatible con todos los principales proveedores de navegadores.

La Política de seguridad de contenido (CSP) ha sido propuesta por el Grupo de trabajo de seguridad de aplicaciones web del W3C, con un apoyo cada vez mayor entre todos los principales proveedores de navegadores, como una forma de mitigar el clickjacking y otros ataques.

Se conoce que los encabezados de respuesta X-Frame-Options y Content-Security-Policy no son las únicas mitigaciones para el clickjacking, actualmente son los métodos más confiables que se pueden detectar a través de la automatización. Por lo tanto, este complemento puede producir falsos positivos si se implementan otras

estrategias de mitigación (por ejemplo, JavaScript que revienta los marcos) o si la página no realiza ninguna transacción sensible a la seguridad. (Cevallos, 2016)

Solución

Escribir el encabezado HTTP X-Frame-Options (con la directiva 'Frame-ancestors') con la respuesta de la página, esto evita que el contenido de la pagina sea representado por otro sitio web cuando se usan las etiquetas HTML de marco o de iframe.

Interpretación del análisis.

Los resultados obtenidos en el análisis a el sistema de gestión del voluntariado de la cruz roja arrojan información que puede ayudar a corregir muchas falencias con las q cuenta el sistema el cual se encuentra en un estado crítico debido a las diversas vulnerabilidades encontradas. Se recomienda poner en practica las sugerencias y políticas que se describen a continuación.

Sugerencias técnicas para las vulnerabilidades encontradas.

- Actualización de los servicios y equipos
- Metodología para el análisis de vulnerabilidades con el objetivo de prevenir amenazas.
- Capacitar al personal administrativo en temas de seguridad de la información.
- Desarrollo de plan de contingencia en caso de riesgos informáticos.
- Hacer copias de seguridad.
- Corregir errores de desarrollo del sistema.

Políticas de seguridad del sistema de gestión de voluntariado de la cruz roja

- Políticas de protección de la información que permita mejorar los intereses de la organización. La falta de protección de los datos de la organización afectara negativamente la reputación y confianza de los usuarios.
- Reducir al mínimo los riesgos de daño mediante la prevención de incidentes de seguridad, asegurando la continuidad de los servicios brindados por la organización.
- Implementar metodología de gestión del riesgo con la finalidad de analizar de forma regular la exposición a vulnerabilidades de los activos.
- Capacitar a los usuarios sobre temas de seguridad de la información.

Estas políticas se establecen con la finalidad de garantizar a que las futuras decisiones que se tomen en la organización estén basadas en preservar la confidencialidad, integridad y la disponibilidad relevante de la empresa.

Fase 3. Salvaguardas

Luego de haber identificado las amenazas y vulnerabilidades dentro del sistema de gestión del voluntariado de la cruz roja se reconoce la parte más importante y sensible de la organización a los datos más relevantes recopilados por el sistema. Se destaca la importancia de salvaguardar los datos reduciendo las amenazas con la finalidad de mitigar los riesgos informáticos y tecnológicos de la organización.

Fase final. Impacto y riesgo residual

Los riesgos que se identifican en el análisis pueden implicar perdida o fuga de información importante que pueden poner en peligro los activos y la infraestructura tecnológica de la empresa los cuales se deben corregir para reducir el impacto.

Conclusiones

El presente estudio de caso logra demostrar que el sistema de gestión del voluntariado de la cruz roja presenta varias fallas de seguridad que pueden poner en peligro la integridad de los datos y de su infraestructura tecnológica.

La utilización de herramientas como “Nessus” que permiten analizar el sistema para encontrar vulnerabilidades, proporciona información que puede ser utilizada para corregir y mejorar el funcionamiento para tener un mayor grado de seguridad en la información sensible de la organización.

Los resultados obtenidos en el análisis al sistema informático permiten identificar brechas de seguridad las cuales pueden ser aprovechadas por piratas informáticos para fines no éticos, el objetivo de hacer el análisis al sistema es corregir estas vulnerabilidades para evitar o minimizar los riesgos de fuga de información.

Recomendaciones

Una vez concluido el análisis al sistema de gestión del voluntariado de la cruz roja se interpretan los resultados obtenidos y se recomienda:

Hacer auditorias periódicamente al sistema para minimizar los riesgos que puedan afectar a los datos de la empresa.

Se recomienda el uso de herramientas que permitan identificar posibles amenazas o vulnerabilidades con la finalidad de corregirlas y prevenir cualquier ataque informático

Teniendo en cuenta las vulnerabilidades encontradas en el sistema se recomienda actualizar los servicios que permiten el correcto funcionamiento del mismo.

Bibliografía

1. *Arias, M. Á. (2017). Aprende Programación Web con PHP y MySQL: 2ª Edición. IT campus Academy.*
2. Casabona, E., & Ceci, R. (2016). *Sitios Multiplataforma con HTML5+ CSS3: Domine el nuevo paradigma de la web*. RedUsers.
3. Castillo, A. A. (2017). *Curso de Programación Web: JavaScript, Ajax y jQuery*. IT Campus Academy.
4. *Cevallos Cedeño, V. A. (2016). Diseño e implementación de un portal web para el Consejo Nacional Electoral (CNE) a fin de ayudar en la capacitación a los ciudadanos del Ecuador acerca del código de la democracia aplicando metodología SCRUM para la gestión de proyectos ágiles en la ingeniería de software enfocado a hardening de servidores web y servicios web(Doctoral dissertation, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones).*
5. *Chicaiza Cazar, D. I. (2019). Modelo de gestión de la seguridad de la información para pequeñas empresas (Master's thesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Maestría en Gerencia de Sistemas de información).*
6. Equipo Vértice. (2009). *Diseño básico de páginas web en HTML*. Editorial Vértice.

7. GB Advisors. (2019). *Nessus Escáner de Vulnerabilidad*. Obtenido de gb advisor: https://www.gb-advisors.com/es/gestion-de-vulnerabilidades/nessus-escaner-vulnerabilidad/

8. Gómez, E. F., Duchimaza, J., Holguín, J. R., & Lindao, M. A. (2019). Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. *Revista Científica y Tecnológica UPSE*, *6*(1), 34-41.

9. *Heurtel, O. (2015). PHP 5.6: desarrollar un sitio web dinámico e interactivo. Ediciones ENI.*

10. *Molina-Miranda, M. F. (2017). Análisis de riesgos de centro de datos basado en la herramienta pilar de Magerit. Espirales revista multidisciplinaria de investigación, 1(11).*

11. *Pulido, J. A. M. (2019). Web usage mining aplicado a servidores web apache. Perspectiv@ s, 14(13), 25-30.*

12. Romero Alamán, J. (2017). M-flashcarding como recurso de aprendizaje del HTML.

13. Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. *Polo del Conocimiento*, *3*(4), 230-244.

14. Unidad Global de ciberseguridad del grupo telefónica Eleven Panths. (2019). *Redefiniendo la seguridad hacia la ciber-resiliencia*. Obtenido de Eleven Panths: https://www.elevenpaths.com/es/quienes-somos/nuestra-empresa/index.html

15. *Urbina, G. B. (2016). Introducción a la seguridad informática. Grupo editorial PATRIA.*

Anexos

Encuesta realizada a los voluntarios

1. ¿Conoce el manejo del sistema de gestión del voluntariado?

   Si ( )

   No ( )

2. ¿Usted piensa que el sistema es de fácil manejo?

   Si ( )

   No ( )

3. ¿Conoce usted el manual de usuario del sistema de Gestión de voluntariado?

   Si ( )

   No ( )

4. ¿Tiene una interfaz amigable?

   Si ( )

   No ( )

5. ¿El software se ha detenido inesperadamente en algún momento?

   Si ( )

   No ( )

6. ¿Conoce cuál es el porcentaje de voluntarios o usuarios que han tenido problema en el manejo del sistema?

   Si ( )

   No ( )

7. ¿Cree usted que los sistemas informáticos son completamente seguros?

   Si ( )

   No ( )

8. ¿Usted considera que las informaciones obtenidas a través de la plataforma están seguras?

   Si ( )

   No ( )

9. ¿Cree usted que hacer un análisis periódico para analizar posibles vulnerabilidades dentro del sistema ayudaría a tener una mayor seguridad de los datos?

   Si ( )

   No ( )

10. ¿Cree usted que si se encuentran fallos de seguridad dentro de los sistemas informáticos los administrados tendrían mayor precaución con los datos?

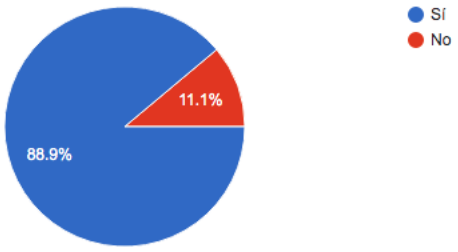
    Si ( )

    No ( )

Se realizó la encuesta a los 54 voluntarios que manejan el sistema en la ciudad de Babahoyo.

RESULTADOS DE LAS ENCUESTAS

1. **¿Conoce el manejo del sistema de gestión del voluntariado?**

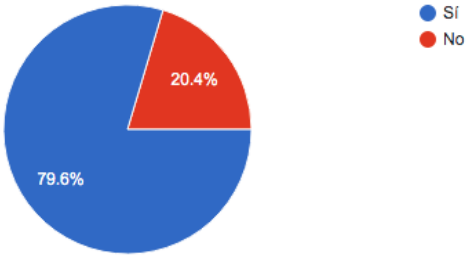


Respuesta	Porcentaje	Frecuencia
Si	88.9%	48
No	11.1%	6
Total	100%	54

Análisis: Los resultados obtenidos en la encuesta realizada dan a conocer que el 88.9% de los voluntarios conocen el manejo del sistema y el 11.1% lo desconoce.

Conclusión: La mayor parte de los voluntarios conocen la existencia del sistema de gestión del voluntariado y pueden ayudar a mejorar su proceso.

2. **¿Usted piensa que el sistema es de fácil manejo?**

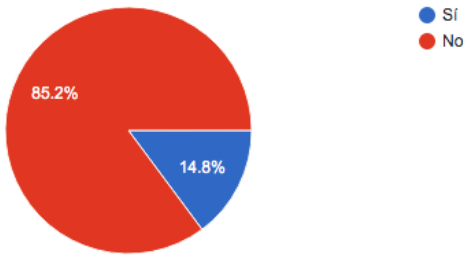


Respuesta	Porcentaje	Frecuencia
Si	79.6%	43
No	20.4%	11
Total	100%	54

Análisis: Al obtener los resultados de la encuesta es evidente que el 79.6% de los voluntarios piensan que el sistema es de fácil manejo y el 20.4% consideran que es dificultoso al momento de manejar dicho sistema.

Conclusión: La mayoría de los voluntarios concuerdan que el sistema de gestión es de fácil manejo.

3. **¿Conoce usted el manual de usuario del sistema de Gestión de voluntariado?**

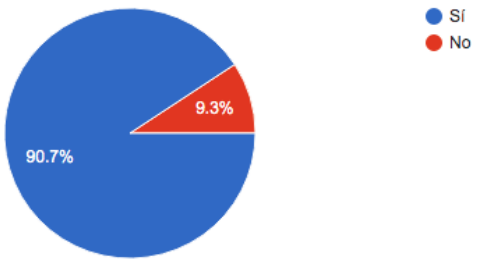


Respuesta	Porcentaje	Frecuencia
Si	14.8%	8
No	85.2%	46
Total	100%	54

Análisis: Los resultados obtenidos muestran que el 85.2% de los voluntarios no tienen conocimiento del manual de usuario del sistema de gestión del voluntariado.

Conclusión: Es conveniente que los voluntarios que manejen el sistema tengan conocimiento de un manual de usuario que les permita tener mayor información detallada de la herramienta.

4. **¿Tiene una interfaz amigable?**

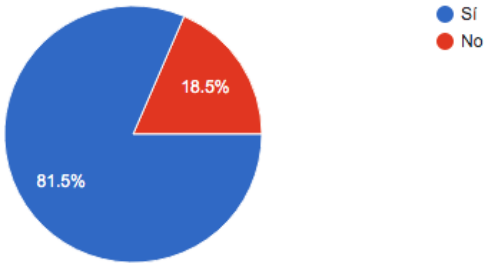


Respuesta	Porcentaje	Frecuencia
Si	90.7%	49
No	9.3%	5
Total	100%	54

Análisis: observando los datos de las encuestas podemos identificar que un 90.7% está de acuerdo con que la interfaz del sistema es amigable y un 9.3% dice lo contrario.

Conclusión: Tener una interfaz amigable hace que a los voluntarios se les haga más fácil manejar el sistema

5. **¿El software se ha detenido inesperadamente en algún momento?**

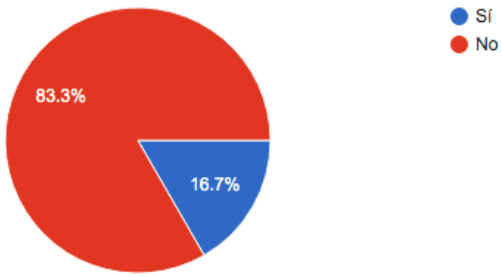


Respuesta	Porcentaje	Frecuencia
Si	81.5%	44
No	18.5%	10
Total	100%	54

Análisis: Un 81.5% de los voluntarios expresa que el sistema ha tenido problemas en algún momento y el 18.5% no lo ha notado.

Conclusión: La mayor parte de los voluntarios dicen que el sistema presenta problemas de conexión con fallas inesperadas del sistema.

6. **¿Conoce cuál es el porcentaje de voluntarios o usuarios que han tenido problema en el manejo del sistema?**

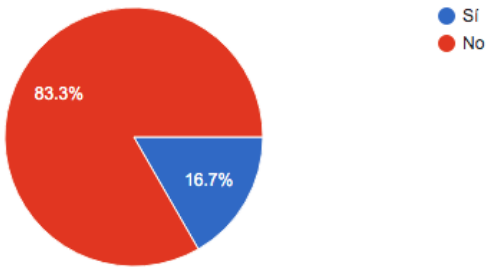


Respuesta	Porcentaje	Frecuencia
Si	16.7%	9
No	83.3%	45
Total	100%	54

Análisis: Los resultados de la encuesta muestran que el 83.3% no han tenido problemas al momento de manejar el sistema y el 16.7% sí.

Conclusión: El mayor porcentaje de los encuestados indican que desconocen el porcentaje de usuarios que tienen problemas con el sistema.

7. **¿Cree usted que los sistemas informáticos son completamente seguros?**

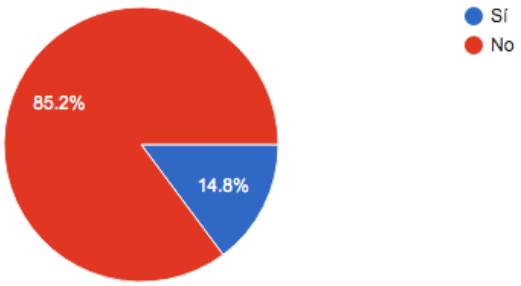


Respuesta	Porcentaje	Frecuencia
Si	16.7%	9
No	83.3%	45
Total	100%	54

Análisis: los resultados obtenidos nos muestran que el 83.3% de los voluntarios creen que los sistemas de información no son seguros y un 16.7% piensa lo contrario.

Conclusión: Una gran cantidad de los voluntarios consideran que los sistemas informáticos no son completamente seguros.

8. **¿Usted considera que las informaciones obtenidas a través de la plataforma están seguras?**

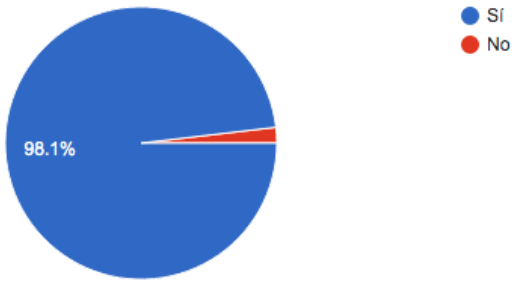


Respuesta	Porcentaje	Frecuencia
Si	14.8%	8
No	85.2%	46
Total	100%	54

Análisis: El 85.2% de los encuestados consideran que las informaciones obtenidas a través de las plataformas no están seguras y el 14.8% piensa que sí.

Conclusión: La mayoría de los encuestados tiene conocimiento de que las informaciones obtenidas desde la plataforma no están seguras y esta propensa a perdida de información.

9. **¿Cree usted que hacer un análisis periódico para analizar posibles vulnerabilidades dentro del sistema ayudaría a tener una mayor seguridad de los datos?**

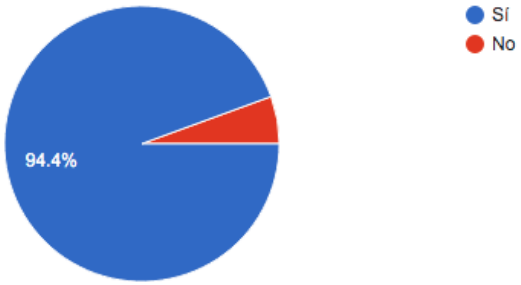


Respuesta	Porcentaje	Frecuencia
Si	98.1%	53
No	1.9%	1
Total	100%	54

Análisis: 53 persona cree que hacer un análisis periódico del sistema ayudaría a tener seguridad de los datos y solo un usuario piensa lo contrario.

Conclusión: La mayoría de los voluntarios tienen conocimiento que si se hace un análisis periódico al sistema ayudaría a tener seguridad de los datos.

10. ¿Cree usted que si se encuentran fallos de seguridad dentro de los sistemas informáticos los administrados tendrían mayor precaución con los datos?



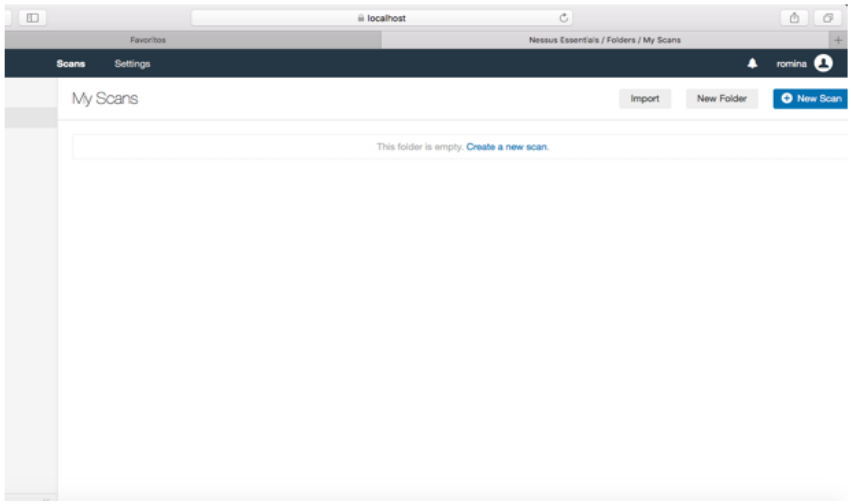
Respuesta	Porcentaje	Frecuencia
Si	94.4%	51
No	5.6%	3
Total	100%	54

Análisis: Los resultados obtenidos en la encuesta muestran que un 94.4% de los voluntarios creen que si se encuentran fallos en los sistemas los administradores tendrían mayor precaución de los datos y el 5.6% cree que no.

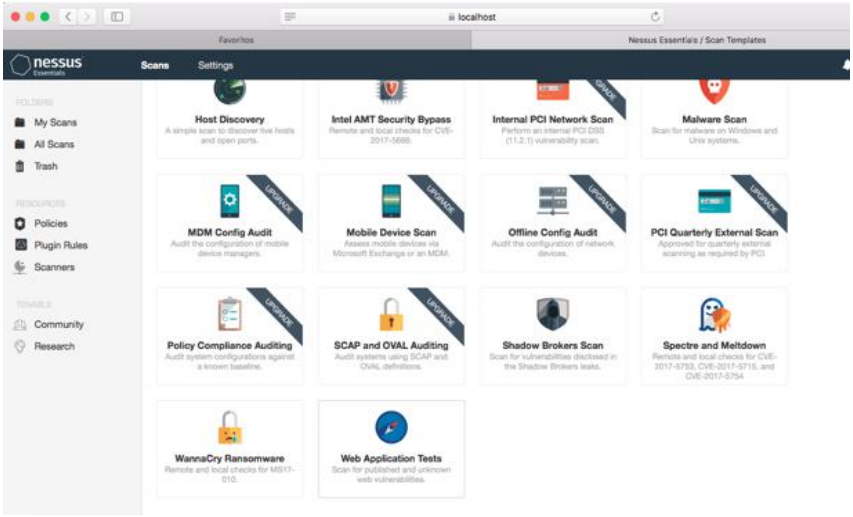
Conclusión: La mayor parte de los voluntarios creen que si se encuentran fallos en los sistemas tendrían más precaución con los datos.

ANÁLISIS DEL SISTEMA EN NESSUS

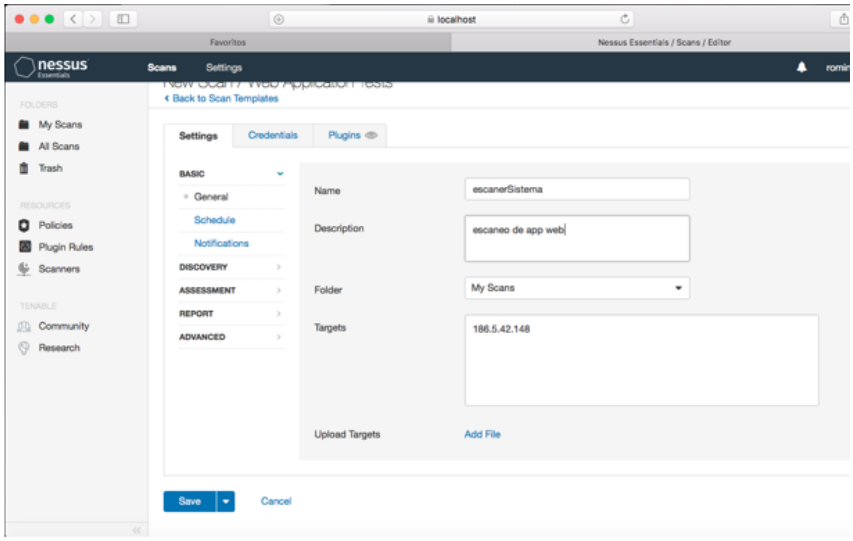
1. Dar clic en nuevo escáner



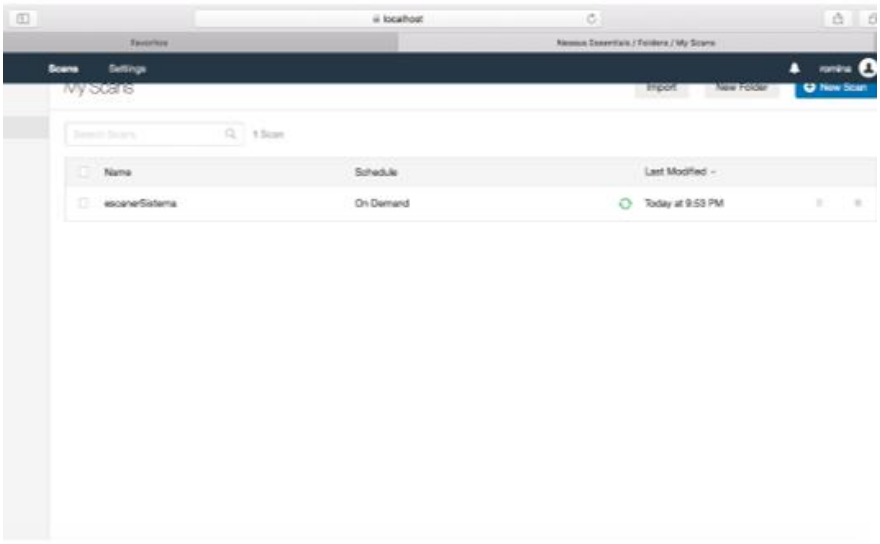
2. Escoger la opción Web Application Test



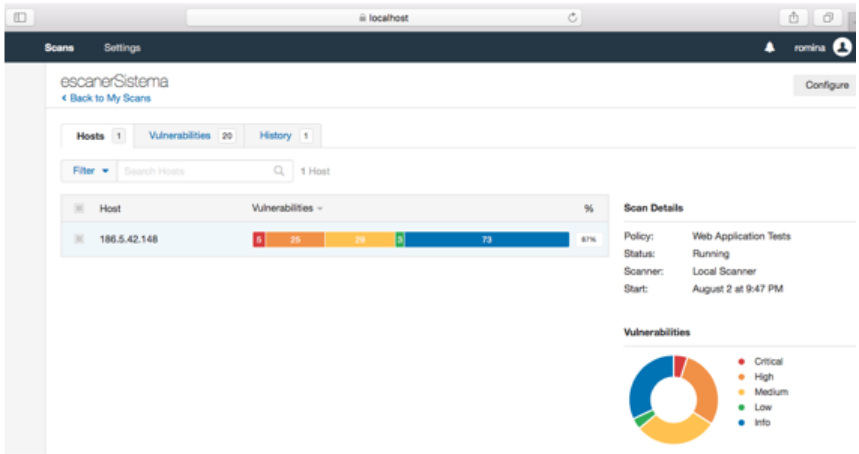
3. Darle un nombre a nuestro primer escaneo, poner una descripción, la dirección ip del sistema y darle clic en guardar.



4. Aparecerá nuestro primer escaneo y damos clic en ejecutar



5. Esperar a que cargue todo



6. Observamos las vulnerabilidades existentes