Coloquio de proyectos
de Becarios en Seguridad Informática

Aplicación Web para seguimiento de revisiones de seguridad

Vasquez Martínez Mario Alejandro
Arteaga Lona Víctor Enrique

UNAM CERT

DGTIC
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Agenda

- Antecedentes
- Necesidades
- Especificaciones del proyecto
- Implementación
- Estructura del sitio
- Conclusiones

Antecedentes

Se hace una solicitud de revisión a un sitio web de la UNAM antes de su liberación.

El auditor encargado se enfoca en aplicar diferentes pruebas de seguridad de aplicaciones web a analizar.

Se genera:

- Reporte con los hallazgos acumulados.
- Recomendaciones.
- Referencias electrónicas.

Necesidades

- Rapidez
- Seguimiento
- Base de conocimientos
- Estadísticas

Especificaciones del proyecto

Objetivo

- Aplicación web que permita la optimización para la creación de documentos la cual genere una base de conocimientos para futuras referencias.

Características solicitadas

- Autenticación
- Gestión y control de usuarios y perfiles
- Listado y manejo de solicitudes
- Generación de reportes
- Estadísticas

Implementación

- Adaptación a tecnologías utilizadas en la CSI/UNAM-CERT.
- Tecnologías con actual crecimiento de uso.
- Amplia documentación por parte de los colaboradores.

Estructura del sitio

- Solicitud para revisión de sitio
- Listado de solicitudes
- Proceso de revisión
- Estadísticas

Solicitud para revisión de sitio

REQUERIMIENTOS

Sistema Operativo

Sistema Operativo: *

GNU/Linux

Version Sistema Operativo: *

6.5

Direccion IP: *

192.168.1.22

Protocolo de acceso remoto: *

SSH

Puerto de acceso remoto *

22

Directorio de aplicacion (Document root) *

/opt/local/webapps

Sitio web

Puerto(s): *

80

Mas de un puerto deben estar separados por comas. Ej: 80,443

URL de las aplicaciones web: *

www.revisiones.unam.mx

Sofware del servidor web: *

Apache httpd

Versión del servidor web: *

7.0.54

Listado de solicitudes

Revisiones de Seguridad

Home | Alta de nueva revisión | Estadisticas | Generar | Lista

Home » Lista » Solicitud detalles

Solicitud detalles

Detalles de solicitud N° 2

Nombre del sitio:	www.revisiones.unam.mx

Organización.

Nombre de organizacion:	CSI/UNAM-CERT	Tipo de organización:	Área de la DGTIC

Fechas de revisión.

Fecha de Solicitud:	2015-10-16	Fecha de disponibilidad:	2015-10-22
Fecha de Inicio de revisión:	2015-10-23	Fecha de Fin de revisión:	2015-10-26

Datos de contacto.

Contacto administrativo - Administrador del proyecto.

Nombre:	Mtro. Marcelo Barreda Plata	Correo:	marcelo@cert.unam.mx	Teléfono:	53695487

Proceso de revisión

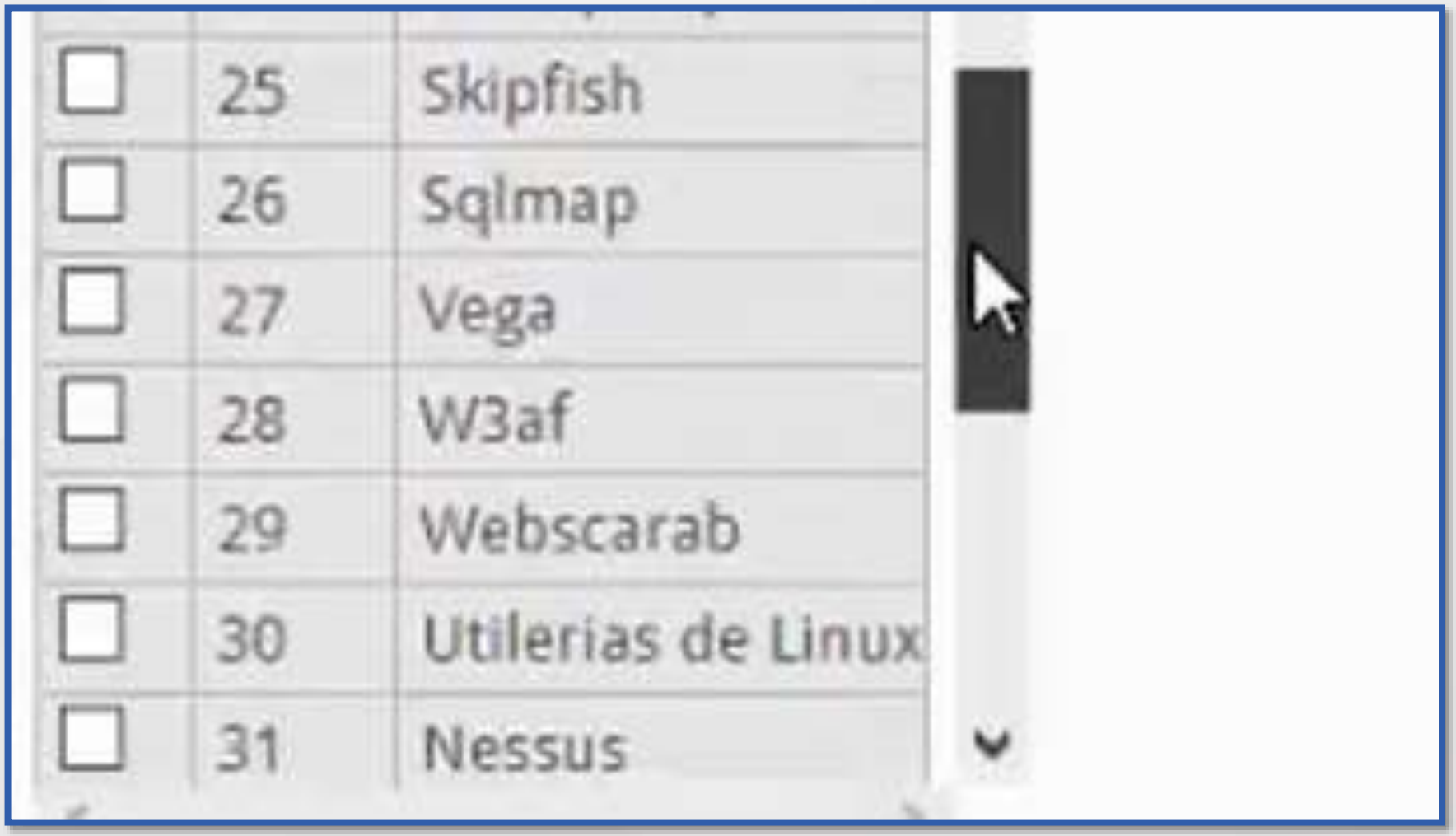

Revisiones de Seguridad
Home
Alta de nueva revisión
Estadisticas
Generar
Lista
Home » Generar » Revision inicial del sitio
Revision inicial del sitio
Solicitud a revisar:
ID
URL_Sitio
Fecha_Inicio
Fecha_Fin
Descargar
Terminar
2
www.revisiones.unam.mx
2015-10-23
2015-10-26
Descargar
Terminar

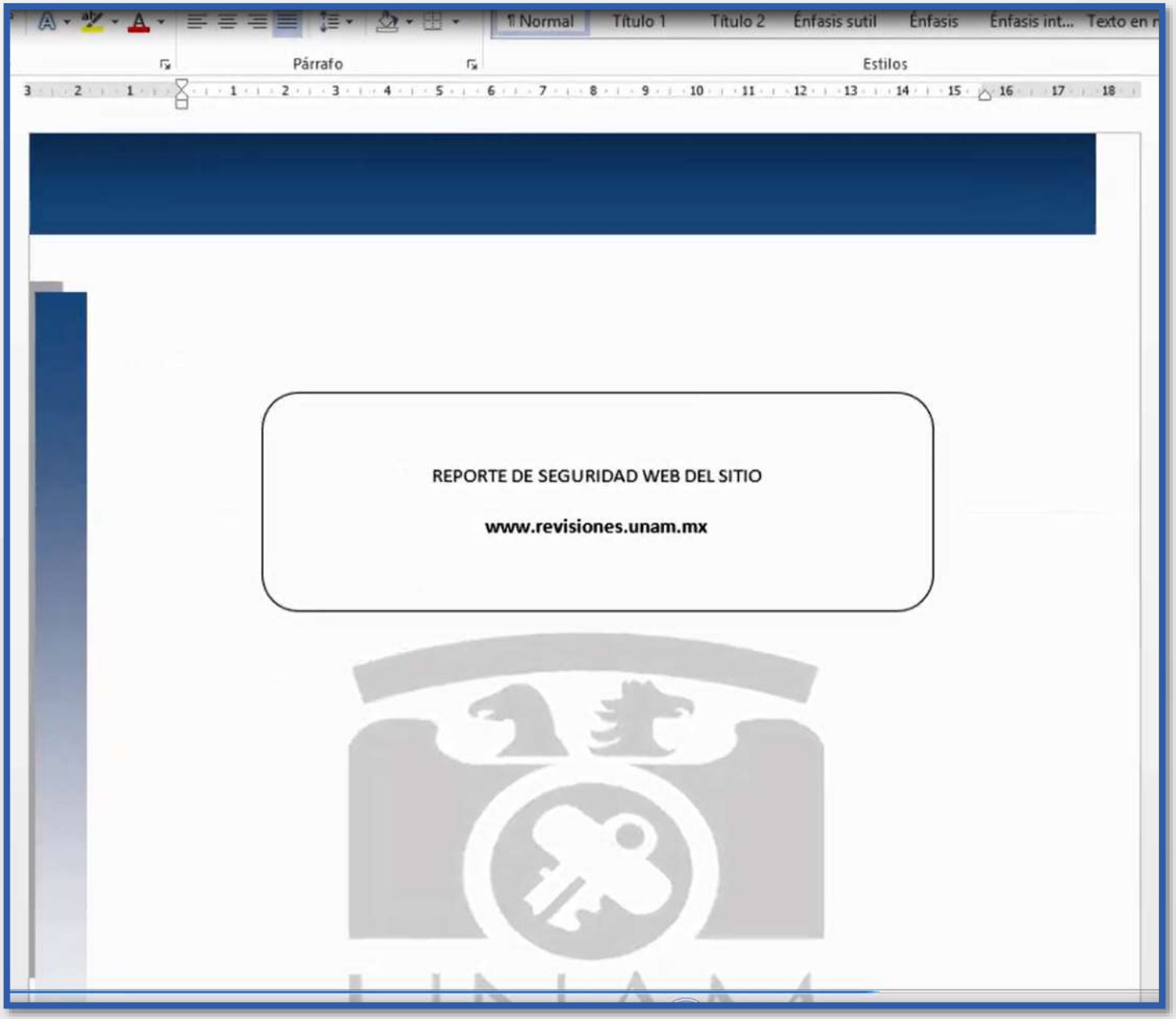
Auditor titular que realizará la revisión:

Marcelo Daniel Barrera Plata

Hallazgos que se encontraron en la revisión:

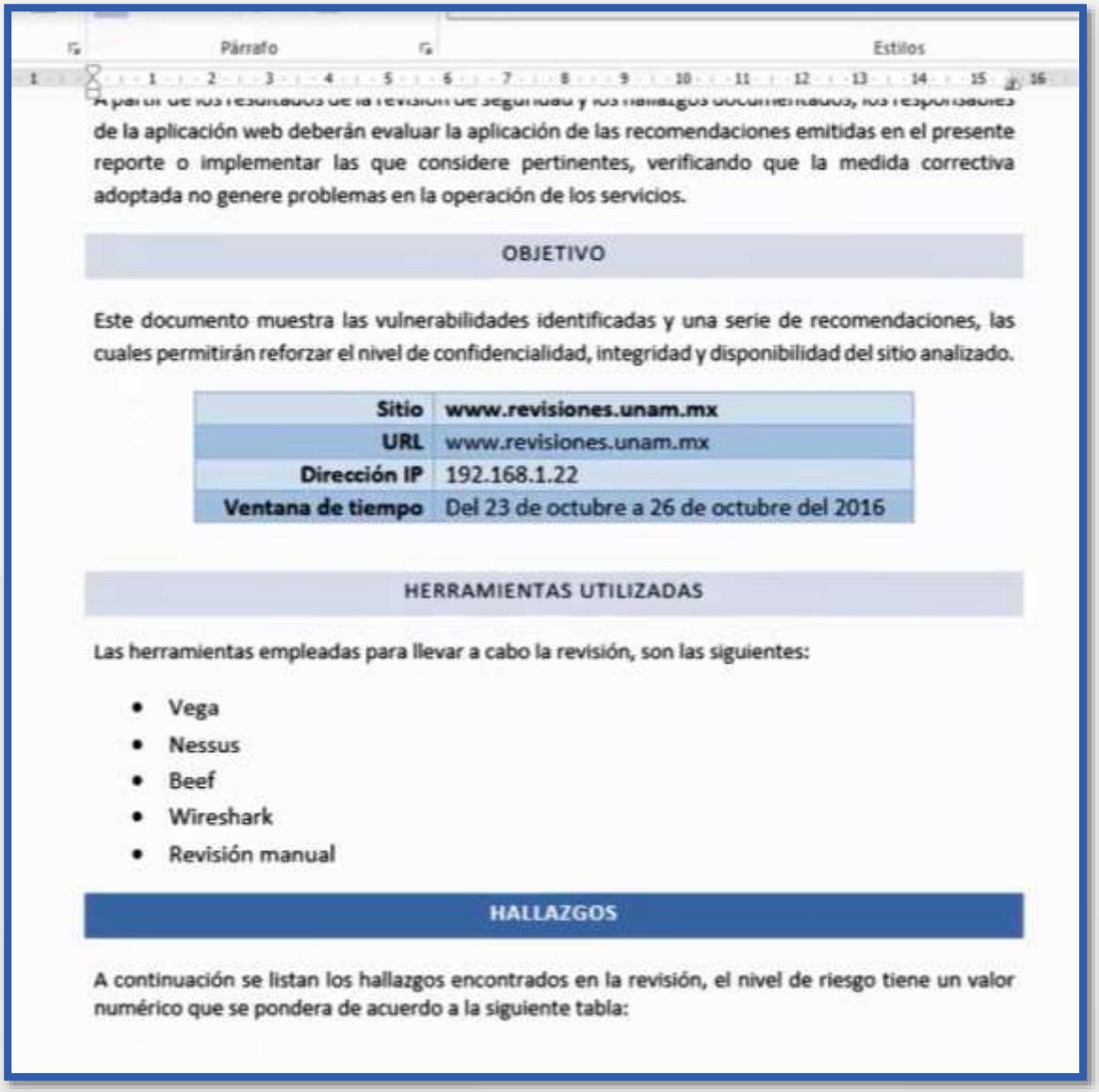
	NID	Titulo	Descripcion	Nivel	Tipo Objetivo
☐	45	XSS CROSS SITE SCRIPTING REFLECTED	A través de la URL es posible la inserción de código JavaScript, el cual interpreta el navegador dando lugar a ataques de Cross Site Scripting.	Medio - 4.2	Aplicación Web
☐	49	INCLUSIÓN DE CÓDIGO EXTERNO	Se encontró la inclusión de código JavaScript de un sitio diferente al que aloja la aplicación web.	Bajo - 0.6	Aplicación Web
☐	51	VISUALIZACIÓN DE CONTENIDO DE PRUEBAS	Es posible observar un archivo con contenido de pruebas, este contiene una re dirección a , también al interceptar la respuesta es posible ver contenido similar al de la página principal.	Bajo - 0	Aplicación Web
☐	54	VISUALIZACIÓN DE ERRORES FRAMEWORK	Al acceder a ciertas URL se muestran errores del Framework de desarrollo y de PHP.	Medio - 4.3	Aplicación Web
☐	58	XSS CROSS SITE SCRIPTING STORED	El sitio es vulnerable a ataques Cross-Site Scripting Stored, al ingresar código JavaScript, este es almacenado en la base de datos a través del formulario para comentarios e interpretado por el navegador web cada vez que se carga la página.	Alto - 7	Aplicación Web
☐	61	FALLO DE CONFIGURACIÓN - HTTPS	No se ha establecido una página de índice por defecto para la aplicación web y se muestra la que proporciona por defecto el servidor Apache.	Medio - 4	Aplicación Web
☐	66	ERRORES POR DEFECTO DE LA APLICACIÓN	Al solicitar un recurso al que no se tiene acceso o no existente, se muestra la página de error que tiene el servidor de aplicaciones web Apache por defecto.	Medio - 4	Aplicación Web
☐	71	DIVULGACIÓN DE INFORMACIÓN - PHPINFO()	Se puede obtener información sobre el procesador de hipertexto a través del archivo info.php.	Medio - 4	Aplicación Web


25 Skipfish
26 Sqlmap
27 Vega
28 W3af
29 Webscarab
30 Utilerias de Linux
31 Nessus


¶ Normal
Título 1
Título 2
Énfasis sutil
Énfasis
Énfasis int...
Texto en r
Párrafo
Estilos
REPORTE DE SEGURIDAD WEB DEL SITIO
www.revisiones.unam.mx

Actualizar tabla...

TABLA DE CONTENIDO


Párrafo
Estilos
A partir de los resultados de la revisión de seguridad y los hallazgos documentados, los responsables de la aplicación web deberán evaluar la aplicación de las recomendaciones emitidas en el presente reporte o implementar las que considere pertinentes, verificando que la medida correctiva adoptada no genere problemas en la operación de los servicios.

OBJETIVO

Este documento muestra las vulnerabilidades identificadas y una serie de recomendaciones, las cuales permitirán reforzar el nivel de confidencialidad, integridad y disponibilidad del sitio analizado.

Sitio	**www.revisiones.unam.mx**
URL	www.revisiones.unam.mx
Dirección IP	192.168.1.22
Ventana de tiempo	Del 23 de octubre a 26 de octubre del 2016

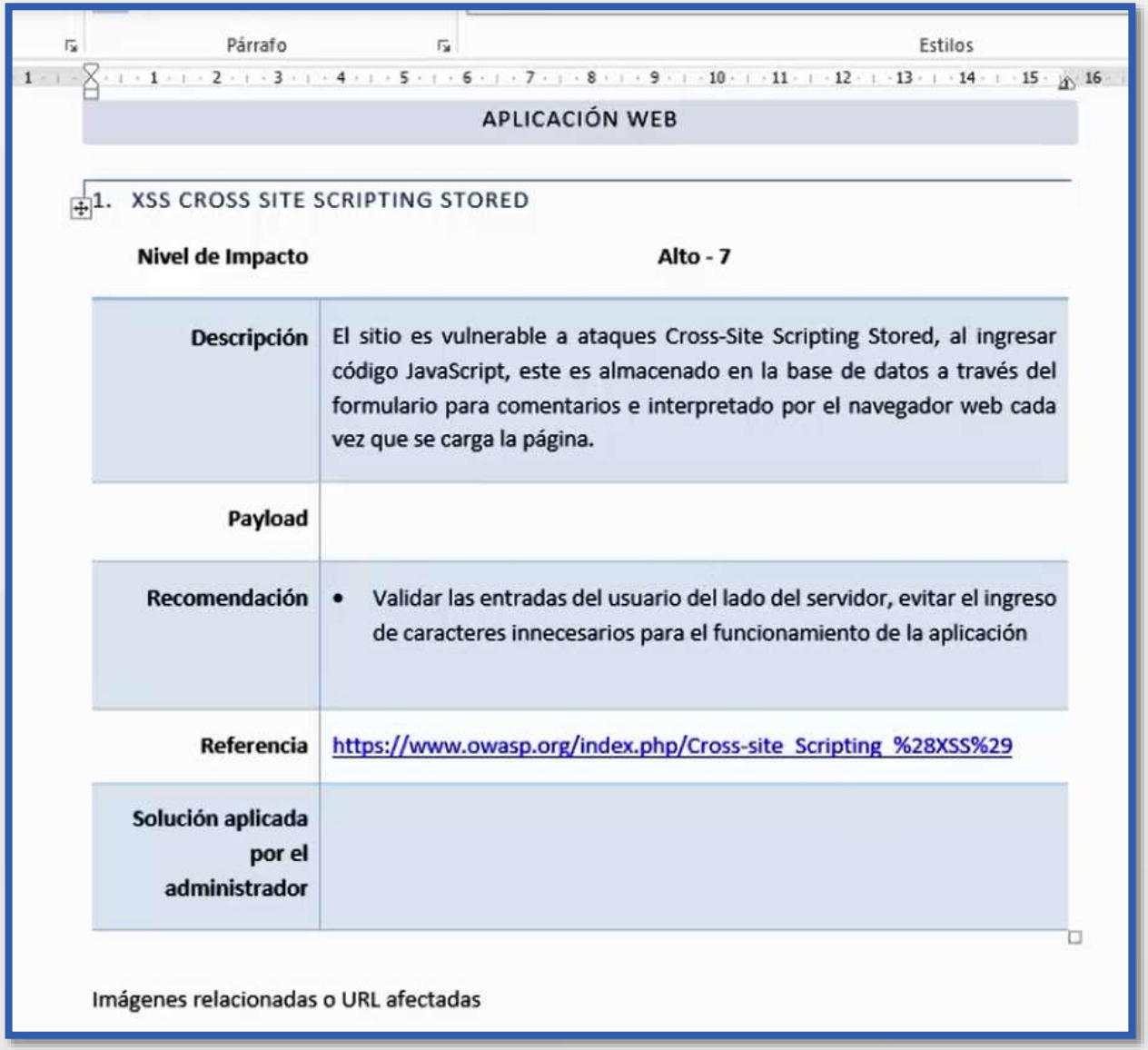
HERRAMIENTAS UTILIZADAS

Las herramientas empleadas para llevar a cabo la revisión, son las siguientes:

- Vega
- Nessus
- Beef
- Wireshark
- Revisión manual

HALLAZGOS

A continuación se listan los hallazgos encontrados en la revisión, el nivel de riesgo tiene un valor numérico que se pondera de acuerdo a la siguiente tabla:



Párrafo Estilos

APLICACIÓN WEB

1. XSS CROSS SITE SCRIPTING STORED

Nivel de Impacto **Alto - 7**

Descripción	El sitio es vulnerable a ataques Cross-Site Scripting Stored, al ingresar código JavaScript, este es almacenado en la base de datos a través del formulario para comentarios e interpretado por el navegador web cada vez que se carga la página.
Payload	
Recomendación	• Validar las entradas del usuario del lado del servidor, evitar el ingreso de caracteres innecesarios para el funcionamiento de la aplicación
Referencia	https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29
Solución aplicada por el administrador	

Imágenes relacionadas o URL afectadas

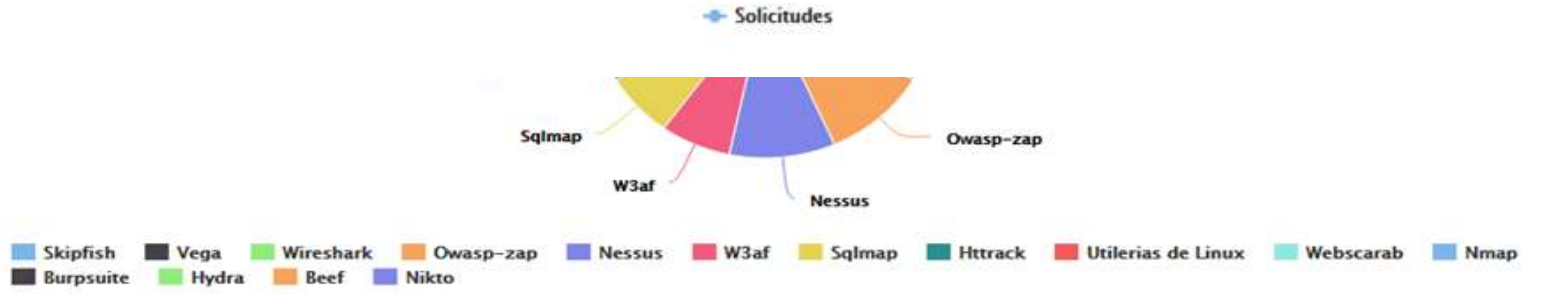
Estadísticas

Revisiones de Seguridad

Home | Alta de nueva revisión | Estadisticas | Generar | Lista

Numero total de revisiones por año.

Año	Total de revisiones
2015	1
2016	1



Conclusiones

- Mejora en tiempos.
- Generación inicial de la base de conocimientos.
- Creación de un histórico.
- Estadísticas descriptivas.
- Modular, versátil, centralizado, intuitivo.
- Oportunidades de mejora.

GRACIAS

Mario Alejandro Vasquez Martínez
Víctor Enrique Arteaga Lona

Coordinación de Seguridad de la Información / UNAM-CERT

56628169

mario.vasquez@cert.unam.mx
victor.arteaga@cert.unam.mx