



Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Aplicación Web para dar seguimiento de revisiones de seguridad

Ignacio Vásquez Oscar
Liberos Sánchez José Angel
Urbina Garrido Mauricio

Ponente:





Contenido



- Introducción
- Descripción del proyecto
- Objetivo
- Herramientas utilizadas
- Metodología de desarrollo
- Demostración
- Problemas que se presentaron
- Oportunidades de mejora
- Conclusiones



Introducción



- ¿Qué es?
 - Aplicativo web para la gestión y control de las pruebas de seguridad realizadas a activos tecnológicos
- Funciones
 - Gestión de sitios y hallazgos
 - Generación de reportes con hallazgos identificados en evaluaciones de seguridad
 - Muestra de resultados en gráficas



Descripción del proyecto



Aplicativo web que ayuda en la gestión de hallazgos identificados durante las pruebas de seguridad realizadas a activos tecnológicos, así como en la generación de reportes con base en a una plantilla con un formato establecido.



Objetivo



Contar con una herramienta que permita dar seguimiento y gestionar las revisiones de seguridad realizadas por las áreas de Seguridad en Sistemas y de Auditoría y Nuevas Tecnologías, contar con un catálogo de hallazgos y sitios, así como la capacidad de obtener estadísticas sobre los problemas más comunes en sitios web de la UNAM.



Herramientas utilizadas



- Debian 10
- Apache 2.4.38
- PostgreSQL 12.6
- Drupal 9
 - Drush
 - Composer
- PHP 7.3.27
- LDAP
- SMTP



Metodología de desarrollo



1. Instalación de entorno de pruebas
 - a. Equipos y servicios
 - b. Software actualizado
2. Descarga de paquetes de software
 - a. Versiones compatibles
3. Instalación de herramientas
 - a. Base de datos
 - b. CMS - Sistema de Gestión de Contenidos (Drupal)
4. Configuración de la aplicación
 - a. Plugins
 - b. Servicios
5. Creación de módulos personalizados para el funcionamiento de la aplicación



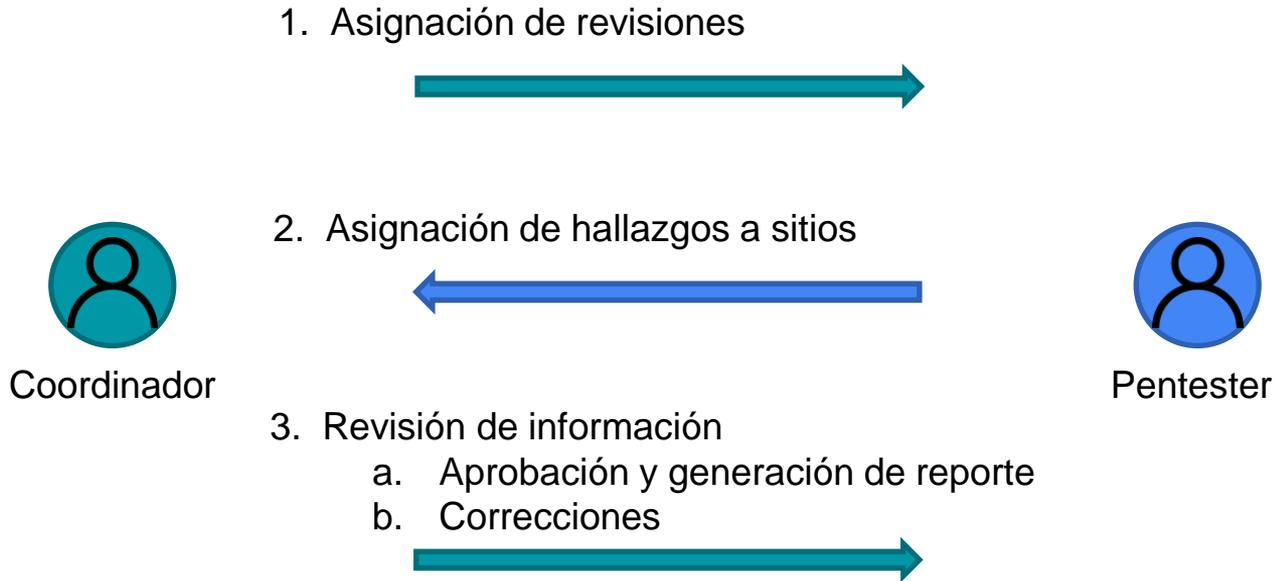
Funciones de la aplicación



- Catálogo de sitios y hallazgos
 - Alta
 - Edición
 - Baja
- Generación de estadísticas
- Clasificación de usuarios
 - Coordinador de revisiones
 - Pentester
 - Auxiliar
- Asignación de revisiones de seguridad
 - Reporte en formato Word



Asignación de revisiones de seguridad





Asignación de revisiones de seguridad (Seguimiento)



4. Asignación de revisiones de seguimiento



Coordinador

5. Verificar hallazgos anteriores o asignar nuevos



Pentester

6. Revisión de información

- a. Aprobación y generación de reporte
- b. Correcciones





DEMOSTRACIÓN





Problemas que se les presentaron



- Nuevas versiones con sintaxis distintas a las anteriores y pocos ejemplos
- Incompatibilidad de módulos con servicios ya instalados
- Diseño de la base de datos



Oportunidades de mejora



- La vista de los catálogos.
- Diseño del sitio.
- El almacenamiento de archivos y la forma de mostrarlos.
- La creación de las gráficas.



Conclusiones



- Control centralizado de revisiones a sitios de la UNAM.
- Crear revisiones y asignarlas a miembros del equipo de forma más automatizada.
- Acorta tiempos en la creación de documentación.
- Creación de documentos word y excel de forma automática.
- Generación de estadísticas mostradas en forma de gráficas.
- Generación de diferentes tipos de gráficas.



Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Gracias por su atención.

¿Preguntas?

