UNIVERSIDAD SIMÓN BOLÍVAR
DEPARTAMENTO DE PROCESOS Y SISTEMAS
SISTEMAS DE INFORMACIÓN III (LABORATORIO). PS-6117.
Profesor. Tadeo Guerra.

Aplicación de las Pruebas OWASP en el Sistema de Gestión de Servicio Comunitario (SIGESC-USB).

Realizado Por:
Daniel Zeait.
Hetsy Rodríguez.
Iranid Pérez.
Joel Rivas.
Nilver Viera.

Sartenejas, Octubre de 2016.

En este documento se detallará el uso de las pruebas OWASP (acrónimo de Open Web Application Security Project) en el Sistema de Gestión de Servicio Comunitario de la USB (SIGESC-USB). Se procederá a determinar cuáles pruebas aplican de acuerdo a la naturaleza y características del software que se está desarrollando justificando su uso, además de mostrar los resultados de cada test realizado.

Las pruebas a realizar fueron tomadas de la versión 3.0 de las pruebas OWASP, descargadas del enlace: https://www.owasp.org/images/8/80/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf

Primeramente hay que recordar, que el tema de seguridad en estas aplicaciones representa un proceso y no un producto. Es decir, nunca se podrá tener un tipo de scanner de seguridad que proporcione una defensa completa o determine todos los problemas de un software.

En vista de esto, hay que seguir en la línea de lo que aconseja la temática de OWASP de pensar estratégicamente y no tácticamente. Esto pues se ha demostrado recientemente que las vulnerabilidades a las que se somete constantemente un software, no proveen de tiempo suficiente para atacar de forma defensiva y realizar el registro del daño.

Gracias a la elaboración de estas pruebas, se ha comprendido que es necesario evaluar la seguridad del producto que se está desarrollando, independientemente de la fase del SDLC (Ciclo de Vida de Desarrollo del Software) y de la metodología de desarrollo empleada.

Se mostrará entonces, las pruebas que aplican a nuestro sistema, el por qué se emplea la misma y los resultados de cada una.

- Prueba de Reconocimiento mediante motores de búsqueda OWASP-IG-002

Se realiza en este caso pues si la información no está actualizada en los ficheros correspondientes durante la existencia del sitio web, entonces es posible que el contenido no sea incluido al momento de una búsqueda en el navegador.

Resultado: Aplicando la prueba en el sistema correspondiente, se pudo visualizar que el mismo no es mostrado bajo los motores de búsqueda en Google Chrome, Mozilla Firefox ni Opera. Esto es probable debido al certificado de seguridad que hay que añadir para poder acceder a las URLs que pertenecen al dominio de la USB.

- Prueba de Identificación de Puntos de Entrada de la Aplicación (OWASP-IG-003)

En vista de que se hace uso de métodos GET y POST para hacer peticiones y enviar parámetros al sistema, es necesario verificar si se están empleando de la manera correcta bajo los lineamientos de seguridad cuando sea necesario.

Resultado: Efectivamente se pudo corroborar que la transferencia de datos en este sistema es de tipo oculta. Por lo que se puede suponer que se cumple con los parámetros de esta prueba.

- Análisis de Códigos de Error (OWASP –IG-006)

Esta prueba es necesaria pues a menudo ocurren errores que si son visibles mediante peticiones específicas, creadas especialmente mediante herramientas o manualmente, son de gran utilidad para las personas a cargo de las pruebas en vista de que pueden revelar información sobre bases de datos, bugs y otros componentes tecnológicos directamente relacionados con el software desarrollado.

Resultado: Según el listado de errores comunes mostrado por la guía de pruebas de OWASP versión 3.0, se pudo determinar que los resultados del

SIGESC-USB cumple con el formato solicitado. De esta manera se puede verificar que en efecto los mensajes de error, proveen de información útil a los usuarios para detectar de forma eficaz el origen del mismo.

- Pruebas de SSL/TLS (OWASP-CM-001)

Es importante verificar la utilización de un algoritmo de cifrado fuerte y su correcta implementación

Resultado: Actualmente no se cuenta con un algoritmo de cifrado fuerte, sin embargo como el servidor y el dominio del sistema pertenecen a la USB, se confía en que el departamento de sistemas correspondiente, realiza las labores pertinentes para no permitir el ingreso de ataques que vulneren los datos de la institución.

En la siguiente imagen se puede confirmar el reconocimiento de servicios SSL, la versión, el emisor, período de validez, etc.

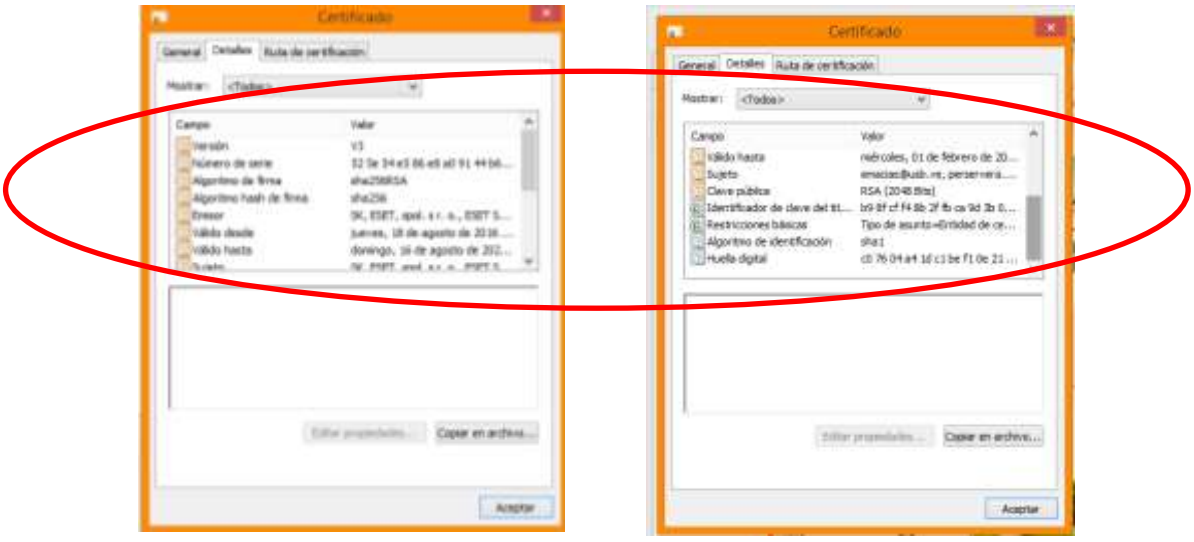

Imagen 1: Características del Certificado SSL.

Fuente: Sistema SIGESC-USB en desarrollo

- Pruebas de Gestión de Configuración de la Aplicación (OWASP-CM-004)

Dado a que en general las aplicaciones web esconden información que no son generalmente considerados durante el desarrollo o la configuración de la

aplicación en sí, es importante determinar dónde se almacena esta información útil para futuros usuarios finales del producto.

Resultado: En efecto previniendo estos detalles de configuración y desarrollo, el SIGESC-USB mantiene la documentación del código y de los artefactos de RUP al día con la implementación del proyecto.

- Pruebas de Gestión de Extensiones de Archivo (OWASP-CM-005)

Es importante poder visualizar las extensiones de los ficheros que se encuentran en el servidor y/o en el software, pues esto hace posible el identificar las tecnologías en las que se basa el producto que se quiere analizar. Además las extensiones de los ficheros también pueden mostrar sistemas adicionales que se conectan a la aplicación.

Resultado: Gracias a la refactorización que se ha realizado en el transcurso de la cadena, del framework (Web2Py) y el lenguaje de programación (Python) empleado, se puede asegurar que se ha logrado una mayor modularización del proyecto, permitiendo visualizar con mayor eficiencia las extensiones de los ficheros para determinar la tecnología utilizada en la implementación del producto.

- Pruebas de Archivos Antiguos, Copias de Seguridad y Sin Referencias (OWASP-CM-006)

Es importante verificar la existencia y el acceso a ficheros redundantes, legibles y descargables de un servidor web, como por ejemplo antiguos, copias de seguridad y renombrados, los cuales son una fuente importante de información. Pueden contener rutas de instalación y contraseñas de la aplicación en general.

Resultado: Actualmente se cuenta con una copia de seguridad almacenada en la nube en el repositorio de Github, adicional a esto, al final del curso se cuenta con los códigos y la documentación almacenada en un CD el cual le es entregado a cliente al finalizar. Sin embargo, las modificaciones que luego de esto realice el

Decanato de Extensión bajo el rol de “Administrador del Sistema”, quedan bajo la garantía de este departamento y no del equipo de desarrollo.

- Pruebas de Interfaces de Administración de la Infraestructura y de la Aplicación (OWASP-CM-007)

Estas pruebas se realizan para buscar interfaces de administración y para comprobar la posibilidad de explotarlos para conseguir acceso a funcionalidades de administración.

Resultado: En efecto SIGESC-USB posee una interfaz de administración de base datos y funcionalidades en generales, la cual es provista a través del framework Web2Py. A menos de que se tenga acceso a la documentación del sistema y/o copias de seguridad, para poder conseguir el acceso deberá ser necesario realizar pruebas de fuerza bruta para poder adivinar la contraseña de acceso. Por lo que se amerita que dicha clave a la hora de entregar el software para ser puesto en producción sea cambiada a un nivel de seguridad mayor que el que posee actualmente.

- Pruebas de Transmisión de Credenciales a Través de un Canal Cifrado (OWASP-AT-001)

Es importante verificar que el transporte de credenciales sea transferido a través de un canal cifrado para evitar ser interceptados por usuarios maliciosos.

Resultado: Dado a que los datos en el sistema son enviados con el método POST a través del protocolo HTTPS, se puede asegurar que la información enviada no es leíble por otras personas incluso si la página pudiera ser alcanzable vía HTTP, pues el cifrado se mantiene.

- Pruebas de Enumeración de Usuarios (OWASP-AT-002)

Es necesario realizar esta prueba para verificar que es posible recolectar un conjunto válido de usuarios simplemente interactuando con los mecanismos de

autenticación del sistema. Pues a menudo, sucede que estas aplicaciones revelan cuando un usuario existe en el sistema, ya sea por consecuencia de una mala configuración o error en el diseño.

Resultado: Se hicieron pruebas interactuando con el mecanismo de autenticación del sistema y se pudo corroborar, que este no aporta ningún tipo de información que permita determinar si un usuario existe o no en la base de datos, pues ya sea que este existe o no, o si su ingreso es inválido el mensaje provisto es *"No se puede determinar que las credenciales proporcionadas sean auténticas".* Esto limita el uso de fuerza bruta para tratar de adivinar alguna contraseña pues se desconoce si en efecto un usuario está registrado en el sistema.

- Pruebas de Cuentas de Usuario Predeterminadas o Adivinables (Diccionario) (OWASP-AT-003)

Estas pruebas se enfocan en interactuar con el mecanismo de autenticación del sistema usando como nombre de usuario y contraseña, aquellas predeterminadas que son ampliamente conocidas, y determinar si a través de esto se puede obtener acceso a la infraestructura de red interna.

Resultado: Se hicieron las pruebas de autenticación bajo los lineamientos de la guía de pruebas de OWASP versión 3.0, y se encontró que ninguno de este par nombre de usuario/contraseña estaba registrado en el sistema. De manera que se puede asegurar que el sistema desarrollado posee un cierto nivel de seguridad.

- Pruebas de Fuerza Bruta (OWASP-AT-004)

Se trata de enumerar sistemáticamente todas las posibilidades candidatas como solución a un problema, que en este caso es la necesidad de disponer de una cuenta de usuario válida para acceder a la parte interna del sistema.

Resultado: Se aplicaron algunas de la pruebas según los lineamientos de la guía de pruebas de OWASP versión 3.0. Dado a que el sistema utiliza una

autenticación basada en formularios HTML sobre una sesión SSL cifrada, se hicieron pruebas de tipo diccionario y ataques de búsqueda basados en patrones. Con lo cual se pudo corroborar que el sistema superó estos mínimos niveles de seguridad.

- Saltarse el Sistema de Autenticación (OWASP-AT-005)

Aunque la mayoría de las aplicaciones requiere autenticación para obtener acceso a información privada o ejecutar tareas, no todos los métodos de autenticación pueden proveer seguridad adecuada. Se quiere entonces, verificar que el sistema de Servicio Comunitario, no posea este tipo de fallas.

Resultado: Se aplicaron pruebas por petición directa de páginas (navegación forzada), para ver si el sistema podía por este método dejar de verificar las credenciales del usuario antes de concederle el acceso, pero los resultados fueron positivos en función de la seguridad, resultando el acceso no permitido.

Se procedió una vez cerrada la sesión del usuario, a realizar la petición de una página diferente vía navegación forzada, lo cual arrojó la siguiente vista.

Imagen 2: Validaciones de Acceso de Sesión.
Fuente: Sistema SIGESC-USB en desarrollo

- Pruebas para Comprobar Sistemas de Recordatorio/Reset de Contraseñas Vulnerables (OWASP-AT-006)

Dado a que este sistema permite a los usuarios reiniciar su contraseña si la han olvidado a través del envío de un email de reset de la contraseña, se pretende verificar si la función está implementada correctamente.

- Pruebas de Gestión del Caché de Navegación y de Salida de Sesión (OWASP-AT-007)

Es necesario comprobar que la función de cierre de sesión está correctamente implementada, y que no es posible reutilizar una sesión. También es importante comprobar que la aplicación automáticamente cierra la sesión de un usuario cuando ha estado inactivo durante un cierto lapso de tiempo, y que ningún dato sensible permanece en el caché del navegador.

Resultado: Efectuando la prueba que sale en la guía de OWASP ya mencionada, se pudo confirmar que la implementación de la función de cierre de sesión fue de forma segura. Pues se procedió a cerrar la sesión y luego pulsar el botón “atrás” del navegador, y el resultado fue que ya no se tenía autenticación válida sobre el sistema.

En el caso de cierre de sesión por tiempo expirado, se pudo determinar que dicho nivel de seguridad no está implementado en el sistema. De hecho si se cierra el navegador una vez realizada la autenticación y luego se abre otra ventana del navegador, la sesión no finaliza. Por lo que se puede decir que existen brechas de seguridad importantes en el sistema.

- Pruebas para Atributos de Cookies (OWASP-SM-002)

Es necesario tener un uso seguro de las cookies, pues estas normalmente son usadas como un identificador de sesión para la autenticación y como un contenedor de datos temporal. De manera que si un atacante fuera capaz de obtener un identificador de sesión, entonces podría usar la cookie para obtener una sesión válida.

Resultado: Dado que las peticiones del sistema están siendo enviadas sobre un canal HTTPS, se puede afirmar que el atributo en este caso es seguro dado a que el envío de la cookie solo se realizará cuando se use este canal (HTTPS).

- Pruebas para Fijación de Sesión (OWASP-SM-003)

Cuando un producto de software no renueva la cookie después de una autenticación de usuario exitosa, podría ser posible encontrar una brecha de vulnerabilidad de fijación de sesión y forzar al usuario a usar una cookie conocida por el atacante.

Resultado: En vista de que parte de la sesión de usuario está desarrollada por la universidad con el acceso del CAS, no se tiene completa certeza de si han cumplido con la implementación de un renovador de identificador de sesión después de que un usuario se autentique exitosamente. Sin embargo se agrega la prueba pues es necesario realizarla por seguridad en el sistema.

- Pruebas para Saltarse el Esquema de Autenticación (OWASP-AZ-002)

Es necesario realizar este tipo de pruebas para verificar cómo ha sido implementado el esquema de autorización para cada perfil/privilegio para obtener acceso a funciones/recursos reservados.

Resultado: Se pudo determinar que la implementación de estas funcionalidades, tienen el nivel de seguridad deseado pues una vez cerrada una sesión, no es posible acceder a algún recurso del sistema. Tampoco se puede acceder si no se está autenticado, y el desarrollo de los privilegios de cada actor está bien delimitado e implementado.

- Pruebas de Comprobación de la Lógica de Negocio (OWASP-BL-001)

Es necesario verificar siempre que el flujo de trabajo y funcionalidades del sistema, cumplan con las reglas que expresan las políticas del negocio.

Resultado: Gracias al uso de la metodología RUP, se puede verificar de manera iterativa, que las funcionalidades y demás características de calidad del SIGESC-USB cumple en cada etapa con las reglas que expresan las políticas del negocio requeridas por la CFCG. Además existe documentación amplia y

actualizada de todos los procesos que componen este sistema para cada uno de los usuarios finales de este producto.

- Pruebas de Validación de Datos. Inyección SQL (OWASP-DV-005)

  Es importante tener una validación adecuada de las entradas procedentes del cliente o del entorno del sistema en general. En este caso se pretende verificar cuando se realiza una consulta SQL a través de las entradas de usuario implementadas en el sistema las validaciones sobre cada una de estas entradas.

  Resultado: Motivados a cumplir con las características de calidad de usabilidad y funcionalidad. Los campos donde los usuario deben ingresar cierta información para generar consultas sobre la Base de Datos, se han implementado con validaciones dinámicas, de manera de que se comentan la cantidad mínima de errores posibles y además el usuario no tenga que enviar todo un formulario para determinar si existen errores o no, sino que se trata de verificar todo durante el ingreso de datos en cada campo.

- Pruebas de Bloqueo de Cuentas de Usuario (OWASP-DS-002)

  Se quiere comprobar si un atacante puede bloquear cuentas de usuario válidas mediante intentos repetidos de registrarse con una contraseña errónea.

Resultado: La implementación con la que cuenta SIGESC-USB a nivel de login, no permite el bloqueo de cuentas de usuario válidas, pues no se tiene un número limitado de ingreso. No estaba modelado en las reglas del negocio y tampoco se consideró relevante agregarle tal nivel de seguridad a esta funcionalidad.