UNIVERSIDAD SIMÓN BOLÍVAR

DEPARTAMENTO DE PROCESOS Y

SISTEMAS DE INFORMACIÓN

PRUEBAS DE SEGURIDAD DE OWASP EN EL SISTEMA DE GESTIÓN DE SOLICITUDES DE PLANTA FÍSICA (SIAGES)

Por:

Gabriel Álvarez

Amín Arria

Luis Díaz

Manuel Gomes

Francisco Martínez

José Pascarella

Sartenejas, Octubre de 2016

Introducción

Para asegurar la calidad del producto a entregar es de vital importancia realizar una serie de pruebas, que permita garantizar que el producto está libre de fallos, encontrando errores que hayan podido pasar desapercibidos que luego serán corregidos para que el producto cumpla con todos los requerimientos y expectativas del cliente.

Este documento se enfocará en las pruebas de seguridad que se aplicarán a SIAGES. Estas pruebas serán tomadas de la guía de pruebas de OWASP v4.0 que podemos encontrar en el site oficial de OWASP y también para mayor facilidad en este directorio.

Las pruebas serán escogidas tomando en cuenta su importancia y pertinencia con respecto al sistema. Cada prueba escogida vendrá acompañada de la razón por la que se esta haciendo dicha prueba y sus resultados.

Pruebas

Gestión de identidad

1. Definición de roles (OTG-IDENT-001)

En la aplicación existen dos roles principales. El usuario común y el administrador. El usuario común es cualquier individuo perteneciente a la comunidad universitaria, ya sea un estudiante, profesor, obrero o personal administrativo. El rol de administrador es exclusivo del personal de la Unidad de Atención e Inspección de Planta Física. Es imperativo para la lógica del negocio que un usuario común no tenga acceso a las acciones que pueden ser ejecutadas solamente por el administrador.

Resultado: las acciones que puede llevar a cabo un usuario común son:

- Crear solicitudes (limitado a ciertos campos de la solicitud).
- Ver solicitudes creadas por el mismo o solicitudes públicas.

Un administrador puede:

- Crear solicitudes (acceso completo a todos los campos).
- Ver y editar todas las solicitudes.

Actualmente esta es la definición de roles deseada por el cliente y la que funciona en el sistema.

Autenticación

2. Transporte de credenciales a través de un canal cifrado (OTG-AUTHN-001)

La herramienta utilizada para autenticarse en el sistema es el CAS (Servicio Centralizado de Autenticación). Esta herramienta se basa en un USB-ID único para cada individuo perteneciente a la comunidad universitaria y una clave. Debido a que estas credenciales no solo son utilizadas para acceder a este sistema, sino que son utilizadas para todas las acciones y actividades relacionadas con la universidad, se debe asegurar de que estas credenciales se mantengan a salvo.

Resultado: debido a que la aplicación utiliza el protocolo HTTPS para la transferencia de datos entre el cliente y el servidor, podemos asegurar que las credenciales del usuario no serán interceptadas por algún tercero utilizando un sniffer.

3. Saltarse el modelo de autenticación (OTG-AUTHN-004)

Debido a que el sistema solo puede ser utilizado por personas pertenecientes a la comunidad universitaria y también se quiere saber qué usuario ejecutó qué acción debe asegurarse que ningún individuo pueda saltarse la autenticación.

Resultado:

- Mediante una solicitud directa de varias acciones para las que se debe estar autenticado (como ver solicitudes) comprobamos que de esta manera no es posible saltarse la autenticación.
- Mediante el cambio de parámetros en la solicitud tampoco es posible saltarse la autenticación.

Por lo tanto podemos concluir que no es posible usar la aplicación sin autenticarse.

Autorización

4. Saltarse el modelo de autorización (OTG-AUTHZ-002)

Anteriormente se especificaron dos roles en el sistema. Usuario común y administrador. También se especificó que para un correcto funcionamiento de la aplicación el usuario común no debería tener forma de ejecutar acciones que solo pueden ser ejecutadas por el administrador.

Resultado: autenticado como un usuario común se hicieron solicitudes directas mediante el explorador a distintas funciones que solo pueden ser ejecutadas por el administrador. Las respuestas a todas estas solicitudes fue la esperada: un error.

5. Escalación de privilegios (OTG-AUTHZ-003)

Por la importancia que tiene que un usuario común no ejecute acciones que solo pueden ser ejecutadas por un administrador se debe garantizar que un usuario común no tiene manera de cambiar sus privilegios dentro de la aplicación.

Resultado: actualmente la único rol que puede cambiar los privilegios de un usuario (común o administrador) es el administrador a petición del cliente. Se intentó ejecutar esta acción con solicitud directa autenticado como un usuario común y la respuesta fue la esperada: un error.

Manejo de Errores

6. Análisis de errores (OTG-ERR-001)

Durante la navegación en la aplicación es posible encontrarse con errores, como por ejemplo errores del servidor web, errores de la aplicación o errores de la base de datos. Estos errores podrían responder con mensajes que podrían dar información a un usuario malicioso, dejando el sistema vulnerable ante un ataque. Por eso debe asegurarse que esos errores no revelen ninguna información que pueda poner en riesgo el sistema.

Resultado: la herramienta utilizada para desarrollar el sistema (Web2Py) provee un manejo de errores que requiere la autenticación del usuario administrador del servidor para ver información sobre el error recibido, asegurando que ningún usuario externo pueda obtener información valiosa a partir de los errores.