Realizado por equipo de pasantías empresariales (SPE)

Test de pruebas OWASP para Sistema de Servicio Comunitario y Sistema de Planta Física

- Pruebas de gestión del caché de navegación y de Salida de Sesión (OWASP-AT-007)

Se debe comprobar que ningún usuario pueda acceder a los sistemas a través del caché de navegación. También es necesario comprobar que una vez realizado un cierre o salida de sesión por alguno de los usuarios, esta no pueda ser reutilizada, es decir, debemos comprobar que la función de cierre de sesión está bien implementada.

Luego de realizar estas pruebas se pudo comprobar que los cierres de sesión en ambos sistemas están bien implementados; no hay forma de acceder de forma forzada a la sesión de algún usuario cuando este ya cerró sesión.

Por otro lado, respecto a la gestión de caché de la navegación podemos decir que el sistema de la DST provee un buen proceso de cierre de sesión el cual expira las cookies correctamente, es decir, al intentar acceder al sitio correspondiente a cada uno de los sistemas por medio de manipulación de cookies no se logró. Sin embargo, pueden haber brechas de seguridad cuando no se cierra sesión y simplemente se cierra el navegador; ya que cuando esto ocurre y se vuelve a intentar acceder al sitio te abre la sesión previamente iniciada.

- Pruebas de comprobación de la logica de negocio (OWASP-BL-001)

El objetivo de esta prueba es el de verificar que no existan vulnerabilidades en los en los flujos de trabajo definidos por el sistema que permita modificar de forma maliciosa la información que se maneja dentro de ellos. Además, es necesario comprobar que en efecto se lleven a cabo los procesos delimitados por la reglas de negocio y que su alcance sea adecuado con lo previsto en las políticas del negocio.

Primeramente buscamos revisar y comprender cuales son las limitaciones impuestas por el sistema, de entrada nos topamos con que existe implementado un sistema de roles, el cual delimita las funciones que puede tomar cada usuario dentro del sistema y cambia drásticamente su participación dentro de los flujos de los procesos. Esto se observa para ambos sistemas. Luego, comprobamos si en efecto los roles posee las permisologías que requieren por parte de las reglas del negocio para su correcta participación en el flujo.

El siguiente paso corresponde al de realizar corridas de prueba de los flujos principales que corresponden a los procesos críticos de cada sistema. Para esto tomamos los distintos roles y simulamos el input que realizaría cada uno de los usuarios para lograr el camino satisfactorio del proceso.

El resultado de esta fase demostró que en efecto de concreta el flujo positivo de ambos sistemas con éxito.

Luego, requerimos hacer pruebas donde en vez de seguir el flujo positivo, incluimos errores a propósito para revisar cómo reacciona el sistema. En la mayor parte, ambos sistemas logran recuperarse correctamente únicamente conseguimos dos errores:

Para el sistema de servicio comunitario, el error consiste en un error del servidor cuando se intenta consultar una propuesta de servicio comunitario recién creada sin rellenar con datos (salvo el nombre puesto a que es requerido).

Para el sistema de planta física, al realizar las pruebas logramos concluir que el sistema para hacer los backups no está funcionando correctamente, simplemente no está funcionando.

Por último, debemos recomendar que se hagan modificaciones a las interfaces de los usuarios que delimiten de mejor manera cuál es el flujo correcto y como se debe ejecutar, puesto a que en su forma actual resulta muy complicado comprender exactamente cómo se debe proseguir con el flujo a menos de que poseas el conocimiento previo de cómo debe llevarse a cabo.