Informe obtención de las imágenes del directorio web

Introducción

Como ya sabemos, tras realizar las fotos de las orlas, éstas son subidas a su servidor para que cada usuario pueda descargar su propia imagen. Hasta ahí todo correcto, pero el problema viene cuando se detecta una ligera vulnerabilidad en el servidor que las aloja.

La vulnerabilidad en cuestión reside en que un usuario que esté dado de alta o no en vuestro sitio web puede acceder a todas vuestras imágenes. Por el momento sólo lo he comprobado con las imágenes de las orlas de este año, aunque seguramente se pueda acceder a todas las imágenes disponibles en el servidor.

Vulnerabilidad

Este problema lo detecté cuando fui a ver mi imagen, cuyo acceso se obtiene desde la ruta principal de la imagen (en este caso la mía). Tras suspender el ordenador y volver a entrar, me di cuenta que la sesión no había caducado y que seguía teniendo acceso a la foto sin necesidad de volver a iniciar sesión. Esto me hizo pensar que, si yo podía acceder a mi imagen sin necesidad de iniciar sesión, posiblemente podría acceder a cualquier otra imagen.

Dicho fallo me hizo pensar en la posibilidad de introducir varios números aleatorios con el fin de comprobar si se podría tener acceso a otras posibles imágenes. Tras comprobar que se podía acceder a las citadas imágenes sin necesidad de iniciar sesión, realicé el script que les adjunto y con el que podrán acceder a las imágenes y descargarlas.

Después de realizar un simple estudio a la web puedo informarles de que el directorio donde se encuentran las imágenes está bien protegido porque al realizar una consulta y la posterior descarga de su contenido, se puede observar un error 503.

Al dar este error, el sistema indica que está bien protegido y que no se puede realizar un escaneo del contenido del directorio, pero sí que se puede acceder al contenido de uno en uno.

Solución

La solución que yo les recomendaría es que sólo se tenga acceso a las imágenes con los *token* que se dan al efectuar el login. De esta manera se conseguiría filtrar el acceso a las imágenes, haciendo que el usuario únicamente pueda acceder a las imágenes de su carrera.

Script

El script que he realizado esta programado en Python. Este script va incrementando el valor numérico que representa a la supuesta imagen, realizando una petición a la dirección de la imagen y comprobando si hay una imagen en dicha ruta. Si existe, la descarga.

El script funciona con los límites que se le indiquen. Por motivos de seguridad y para evitar bloqueos por el servidor mediante un ataque automatizado, se realizan esperas cada cierto número de solicitudes.