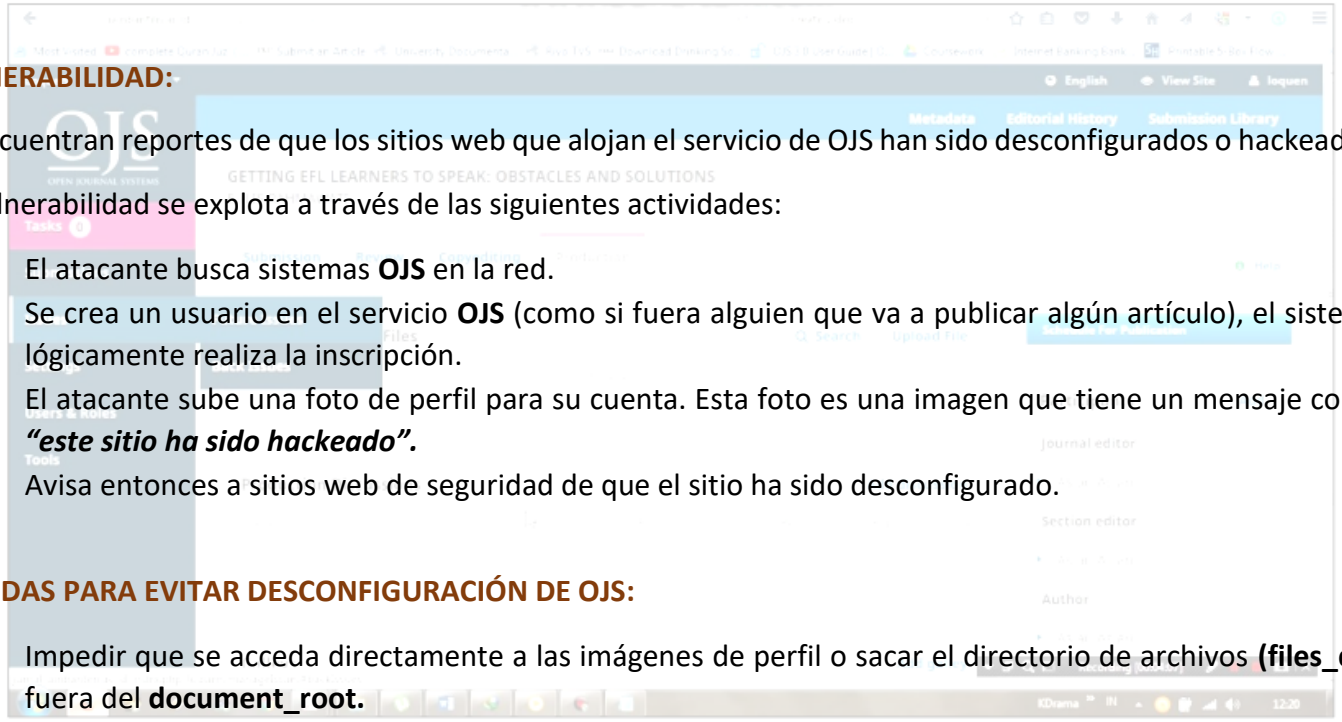
BOLETÍN ESPECIAL DE SEGURIDAD INFORMÁTICA N.- 2020-ESFORSE-TICS-002, SOBRE OLEADA DE DESCONFIGURACIONES A SITIOS CON OJS.

¿Qué es OJS?

Open Journal Systems (OJS) es una aplicación de software de código abierto (sistema de manejo de contenidos y publicaciones desarrollado por Public Knowledge Project) el cual permite a sus usuarios gestionar y publicar revistas académicas, artículos, etc.

Fue desarrollado y lanzado por PKP en 2001 para mejorar el acceso a la investigación, es la plataforma de publicación de revistas de código abierto más utilizada que existe, con más de 10,000 revistas que la utilizan en todo el mundo. Este sistema es bastante popular en las universidades del planeta porque su código es libre.



VULNERABILIDAD:

Se encuentran reportes de que los sitios web que alojan el servicio de OJS han sido desconfigurados o hackeados.

La vulnerabilidad se explota a través de las siguientes actividades:

- El atacante busca sistemas **OJS** en la red.
- Se crea un usuario en el servicio **OJS** (como si fuera alguien que va a publicar algún artículo), el sistema lógicamente realiza la inscripción.
- El atacante sube una foto de perfil para su cuenta. Esta foto es una imagen que tiene un mensaje como ***"este sitio ha sido hackeado".***
- Avisa entonces a sitios web de seguridad de que el sitio ha sido desconfigurado.

MEDIDAS PARA EVITAR DESCONFIGURACIÓN DE OJS:

- Impedir que se acceda directamente a las imágenes de perfil o sacar el directorio de archivos **(files_dir)** fuera del **document_root.**
- Actualizar a la última versión de **OJS** y aplicar todos los parches de la versión.
- Sacar el directorio de archivos fuera de la raíz, por ejemplo: si nuestro sitio está en **/var/www/html/** poner los archivos en **/var/www/** para que el atacante no los pueda ejecutar.
- Activar captcha en el archivo config.inc.php e incluso el captcha para enviar comentarios. Esto evitará desfiguraciones automáticas (no evitará las desfiguraciones manuales).
- Recibir notificaciones automáticas de nuevos registros de usuarios.
- Si es una revista, se sugiere deshabilitar el registro de nuevos usuarios, pues en las revistas no es necesario que se creen nuevos usuarios automáticamente.

REPORTE DE INCIDENTES:

Reporte el incidente al Departamento de TICS, a través de red telefónica interna mediante la ext. 194