El defacement (o desfiguración) es un tipo de ataque que involucra cambiar el contenido visual de una página web sin autorización, generalmente modificando su apariencia para mostrar mensajes, imágenes o contenido no autorizado por los propietarios del sitio. Una de las vulnerabilidades comunes que pueden conducir a defacements es la vulnerabilidad en la función de carga de archivos (File Upload) de un sitio web.

**Vulnerabilidad en File Upload**

1. **Validación Inadecuada**: Si un sitio web permite a los usuarios cargar archivos sin una validación adecuada, esto puede ser explotado para subir archivos maliciosos que pueden ser utilizados para defacement u otros ataques.
2. **Ejecución de Código**: Si el sitio web no verifica correctamente el tipo de archivo o contenido del archivo cargado, un atacante podría subir un archivo que contenga código malicioso, como scripts JavaScript o código PHP, que luego pueden ser ejecutados en el servidor para modificar el contenido del sitio.
3. **Acceso no Autorizado**: Un atacante podría cargar archivos que reemplacen o modifiquen archivos legítimos del sitio web, como páginas HTML, imágenes o archivos de configuración, para cambiar la apariencia del sitio o incluso causar daños al funcionamiento del mismo.

**Medidas de Mitigación**

Para protegerse contra este tipo de vulnerabilidades, es importante implementar las siguientes prácticas de seguridad:

* **Validación Rigurosa**: Verificar el tipo y tamaño del archivo subido, así como su contenido utilizando filtros de tipo MIME y extensiones de archivo.
* **Almacenamiento Seguro**: Asegurarse de que los archivos cargados se almacenen en ubicaciones seguras y restringidas, fuera del directorio raíz del sitio web.
* **Renombrar Archivos**: Cambiar el nombre del archivo cargado para evitar la ejecución accidental de scripts o archivos maliciosos.
* **Ejecución de Contenido**: Deshabilitar la ejecución de archivos cargados en el servidor, especialmente para tipos de archivos que no deberían ser ejecutados (como PHP en un directorio de carga de imágenes).
* **Auditorías Regulares**: Realizar auditorías de seguridad periódicas para detectar y corregir posibles vulnerabilidades de carga de archivos y otras vulnerabilidades de seguridad en el sitio web.

Implementar estas medidas puede ayudar a proteger un sitio web contra ataques de defacement y otros tipos de explotaciones que podrían surgir a través de vulnerabilidades en la función de carga de archivos.

3.5