




Ejercicio Práctico

 **Título:** Elaboración Estructurada de un Informe Técnico de Hallazgo de Seguridad

Objetivo:

Redactar un informe técnico profesional a partir de un escenario simulado, utilizando estructura modular, lenguaje claro, recomendaciones accionables y evidencia técnica relevante.

Escenario:

Durante una evaluación de seguridad interna, se detectó que la aplicación web de la empresa permite subir archivos sin restricciones adecuadas. Se identificaron los siguientes puntos:

- No se valida el tipo MIME del archivo subido.
- No existe control sobre la extensión del archivo.
- Se pueden subir archivos ejecutables (.php, .jsp, .exe).
- No hay autenticación para realizar la subida.
- El servidor no aísla los archivos subidos del sistema principal.

El hallazgo fue confirmado subiendo un archivo PHP malicioso que, al ser accedido, permitió ejecutar comandos en el servidor.

Actividad:

Redacta un fragmento completo de informe profesional incluyendo las siguientes secciones:

Sección

Instrucciones

| | |
|------------------------------|--|
| Título del hallazgo | Resume la vulnerabilidad detectada en una frase clara |
| Resumen técnico | Describe brevemente el hallazgo y cómo afecta la seguridad del sistema |
| Evidencia técnica | Explica cómo se detectó la vulnerabilidad, qué herramientas se usaron y qué resultados se obtuvieron |
| Impacto potencial | Describe los riesgos que implica esta falla en un entorno real |
| Recomendación técnica | Propón al menos 2 acciones específicas y viables para mitigar el riesgo |



Criterios de calidad esperados:

- Uso de redacción clara, precisa y profesional
 - Contenido bien estructurado y funcional
 - Recomendaciones específicas, accionables y justificadas
 - Conexión directa entre evidencia, análisis e impacto
-



Solución Modelo – Informe Técnico Parcial



Título del hallazgo

Carga de archivos sin validación ni restricciones en endpoint público



Resumen técnico

Se detectó que la aplicación permite la subida de archivos a través del endpoint `/upload` sin validar tipo de archivo, extensión ni usuario autenticado. Esta vulnerabilidad permite al atacante cargar scripts maliciosos capaces de ejecutarse directamente en el servidor.



Evidencia técnica

Durante la auditoría, se utilizó **Burp Suite** para interceptar la solicitud POST al endpoint `/upload`. Se cargó un archivo PHP (`shell.php`) sin ser bloqueado por el servidor. Al acceder a la URL del archivo, fue posible ejecutar comandos arbitrarios mediante el navegador.

Prueba realizada:

Archivo cargado: shell.php

Contenido: `<?php system($_GET['cmd']); ?>`

Resultado: Ejecución exitosa de ``whoami`` → apache

No se detectó validación del tipo MIME ni restricción de extensiones. Tampoco existía autenticación previa para acceder al servicio de carga.



Impacto potencial

Un atacante puede ejecutar código remoto en el servidor web, comprometiendo completamente la infraestructura. Esto incluye robo de datos, instalación de malware, control total del sistema operativo y persistencia en el sistema.

Además, al no requerirse autenticación para subir archivos, el riesgo se amplifica para cualquier usuario externo.



Recomendación técnica

1. **Restringir los tipos de archivo permitidos** a través de filtros en el backend (MIME y extensión) y verificación en el frontend. Rechazar automáticamente archivos con extensiones `.php`, `.jsp`, `.exe`, entre otros.
 2. **Aplicar autenticación obligatoria** y control de roles para acceder al módulo de carga de archivos. Solo usuarios autorizados deben poder utilizar esta funcionalidad.
 3. **Aislar los archivos subidos** en un directorio sin permisos de ejecución y configurar reglas en el servidor web para bloquear la ejecución de archivos desde ese espacio.
 4. **Registrar cada intento de carga** en logs de auditoría con información de IP, nombre de archivo, usuario y timestamp, para su posterior análisis forense.
-

Observaciones finales

Este informe demuestra cómo una redacción técnica clara y modular permite comunicar riesgos complejos de forma comprensible y directamente accionable. La evidencia respalda la recomendación, y la redacción evita ambigüedades, facilitando la toma de decisiones.
