Informe de Análisis de Ataque y Propuesta de Mejora de Ciberseguridad para Kelsoft

Análisis y estrategias para la protección de la infraestructura digital.

Autor: Emanuel Sanchez.

INFORME DE AUDITORÍA DE CIBERSEGURIDAD

CLIENTE: KELSOFT

ID DE INFORME: AUD-2026-001

FECHA: 14 de febrero de 2026

CLASIFICACIÓN: CONFIDENCIAL

---

1. RESUMEN EJECUTIVO

El presente documento detalla los hallazgos de la auditoría de seguridad realizada sobre la plataforma WordPress de **Kelsoft**. Durante el análisis, se identificaron múltiples vectores de exposición de información y configuraciones inadecuadas en el servidor.

Aunque actualmente el servidor procesa correctamente los scripts sensibles (evitando la exposición inmediata de credenciales), la infraestructura presenta una **superficie de ataque abierta** que facilita el reconocimiento y la ejecución de ataques dirigidos. Es imperativo aplicar las medidas de endurecimiento (*hardening*) detalladas en este informe.

---

2. RESUMEN DE RIESGOS

ID	VULNERABILIDAD	RIESGO	ESTADO
V-01	Enumeración de Usuarios (REST API)	🔴 **ALTO**	No Mitigado
V-02	Exposición de Directorios del Núcleo (/wp-includes)	🟠 **MEDIO**	No Mitigado
V-03	Panel de Administración Expuesto (/wp-admin)	🟠 **MEDIO**	No Mitigado
V-04	Acceso a Archivo de Configuración (wp-config.php)	🟡 **BAJO**	No Mitigado

---

3. ANÁLISIS DETALLADO DE HALLAZGOS

3.1 Enumeración de Usuarios vía REST API (V-01)

- **Descripción:** La ruta /wp-json/wp/v2/users se encuentra accesible sin autenticación.
- **Impacto:** Permite a un atacante obtener la lista completa de nombres de usuario reales registrados en el sistema. Esto elimina la necesidad de adivinar el login, permitiendo ataques directos de fuerza bruta o ingeniería social.
- **Recomendación:** Restringir el acceso a los endpoints de la API REST para usuarios no autenticados.

3.2 Exposición y Listado de /wp-includes (V-02)

- **Descripción:** La ruta crítica /wp-includes es accesible. En algunos entornos, permite el listado de archivos (*Directory Browsing*).
- **Impacto:** Revela versiones de bibliotecas, scripts de terceros y la estructura interna del CMS, facilitando la búsqueda de vulnerabilidades específicas (CVEs) para esas versiones.
- **Recomendación:** Deshabilitar la opción Indexes en el servidor y bloquear el acceso HTTP directo a esta carpeta.

3.3 Acceso a Panel Administrativo /wp-admin (V-03)

- **Descripción:** La interfaz de inicio de sesión es accesible públicamente.
- **Impacto:** Exposición constante a ataques de diccionario y ataques de fuerza bruta automatizados por redes de bots.
- **Recomendación:** Implementar una capa de seguridad adicional (2FA), restringir por IP o cambiar la URL de acceso por defecto.

3.4 Acceso a Ruta de Configuración wp-config.php (V-04)

- **Descripción:** El archivo es accesible vía HTTP. Al consultarlo, se muestra una **pantalla en blanco**.
- **Análisis Técnico:** El hecho de que la pantalla sea blanca indica que el motor PHP está funcionando y no está filtrando el código fuente. Sin embargo, el servidor **nunca** debería permitir que este archivo sea consultado externamente.
- **Riesgo Latente:** Si el servidor PHP llegara a fallar o ser desactivado accidentalmente, el archivo se entregaría como texto plano, exponiendo inmediatamente las credenciales de la base de datos de Kelsoft.
- **Recomendación:** Bloquear el acceso a nivel de servidor web (403 Forbidden).

---

4. PLAN DE REMEDIACIÓN TÉCNICA

Se recomienda al equipo de sistemas de Kelsoft aplicar las siguientes reglas en el archivo de configuración principal (.htaccess o configuración de Nginx):

A. Para servidores Apache (.htaccess):

Apache
```
# Bloqueo de archivos sensibles y config
<FilesMatch "^(wp-config\.php|readme\.html|license\.txt)">
   Order allow,deny
   Deny from all
</FilesMatch>

# Deshabilitar el listado de directorios
Options -Indexes

# Bloquear acceso a wp-includes
<IfModule mod_rewrite.c>
   RewriteEngine On
   RewriteRule ^wp-admin/includes/ - [F,L]
   RewriteRule !^wp-includes/ - [S=3]
   RewriteRule ^wp-includes/[^/]+\.php$ - [F,L]
   RewriteRule ^wp-includes/js/tinymce/langs/.+\.php - [F,L]
   RewriteRule ^wp-includes/theme-compat/ - [F,L]
</IfModule>
```

---

5. CONCLUSIÓN

La plataforma de **Kelsoft** presenta una configuración de seguridad estándar que no cumple con los criterios de endurecimiento corporativo. La corrección de estos puntos evitará el 90% de los intentos de intrusión automatizados que sufre el sitio actualmente.

Firma del Auditor:

Emanuel Sanchez , Arx Data.