



INFORME SOBRE EL ANÁLISIS DE PROMET

Fecha de análisis: 15/03/2025

Dominio: promet.com.pe



ventas@logosperu.com



Jr. Tauro 883 Urb. Mercurio - Los Olivos



Área de ventas: (+51) 987 038 024



1. Configuración de Seguridad Incorrecta – Directory Listing habilitado

Se revisó el acceso al *directory listing* en algunas rutas. Esto permite visualizar el contenido de directorios que no contienen un archivo index, facilitando el reconocimiento de archivos sensibles o vulnerables.

Solución:

Se agregó una línea de código para limitar el acceso al contenido de carpetas que no cuentan con un archivo index.

```
22  
23 Options -Indexes
```

2. Archivo xmlrpc.php habilitado – Vulnerabilidad a fuerza bruta y DoS

Al tener este archivo habilitado permite realizar múltiples solicitudes para el inicio de sesión o mejor llamados ataques por fuerza bruta. Para ello se limitó el acceso mediante un bloque de código para limitar el acceso al archivo `xmlrpc.php`

```
16  
17 # Deny anyone to access the file  
18 <Files xmlrpc.php>  
19 order deny,allow  
20 deny from all  
21 </Files>  
22
```





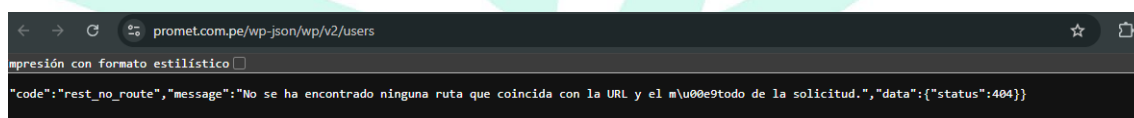
3. Enumeración de Usuarios mediante la API JSON

Se observó que la REST API de WordPress permite enumerar usuarios registrados del sitio, exponiendo nombres de usuario a través de la URL /wp-json/wp/v2/users.

La solución para este problema fue agregar una función dentro de los archivos del tema para evitar el listado de los usuarios y demás informaciones.

```
259 function bloquear_enumeracion_usuarios_rest( $endpoints ) {  
260     if ( isset( $endpoints['/wp/v2/users'] ) ) {  
261         unset( $endpoints['/wp/v2/users'] );  
262     }  
263  
264     if ( isset( $endpoints['/wp/v2/users/(?P<id>[\d]+)'] ) ) {  
265         unset( $endpoints['/wp/v2/users/(?P<id>[\d]+)'] );  
266     }  
267  
268     return $endpoints;  
269 }  
270 add_filter( 'rest_endpoints', 'bloquear_enumeracion_usuarios_rest' );
```

RESULTADO:



4. Ausencia de Cabeceras de Seguridad

Se corrigió la ausencia de cabeceras de seguridad que la falta de ellos hace que el sitio web este expuesto a vulnerabilidades que puede exponer a usuarios y al sitio web a ataques.

Como solución, se implementaron las cabeceras de seguridad adecuadas en el archivo .htaccess, fortaleciendo así la protección general del sitio.






```
26 | Header always set X-Content-Type-Options "nosniff"
27 | Header always set X-Frame-Options "SAMEORIGIN"
28 | Header always set X-XSS-Protection "1; mode=block"
29 | Header always set Referrer-Policy "strict-origin-when-cross-origin"
30 | Header always set Permissions-Policy "geolocation=(), microphone=()"
31 | Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains; preload"
32 | Header always set Content-Security-Policy-Report-Only "default-src 'self'; ..."
33 | </IfModule>
34
```

Resultado:


[Home](#) [About](#) [API](#)

 **Security Headers**
by Probely, a **snky** Business

Scan your site now

Scan

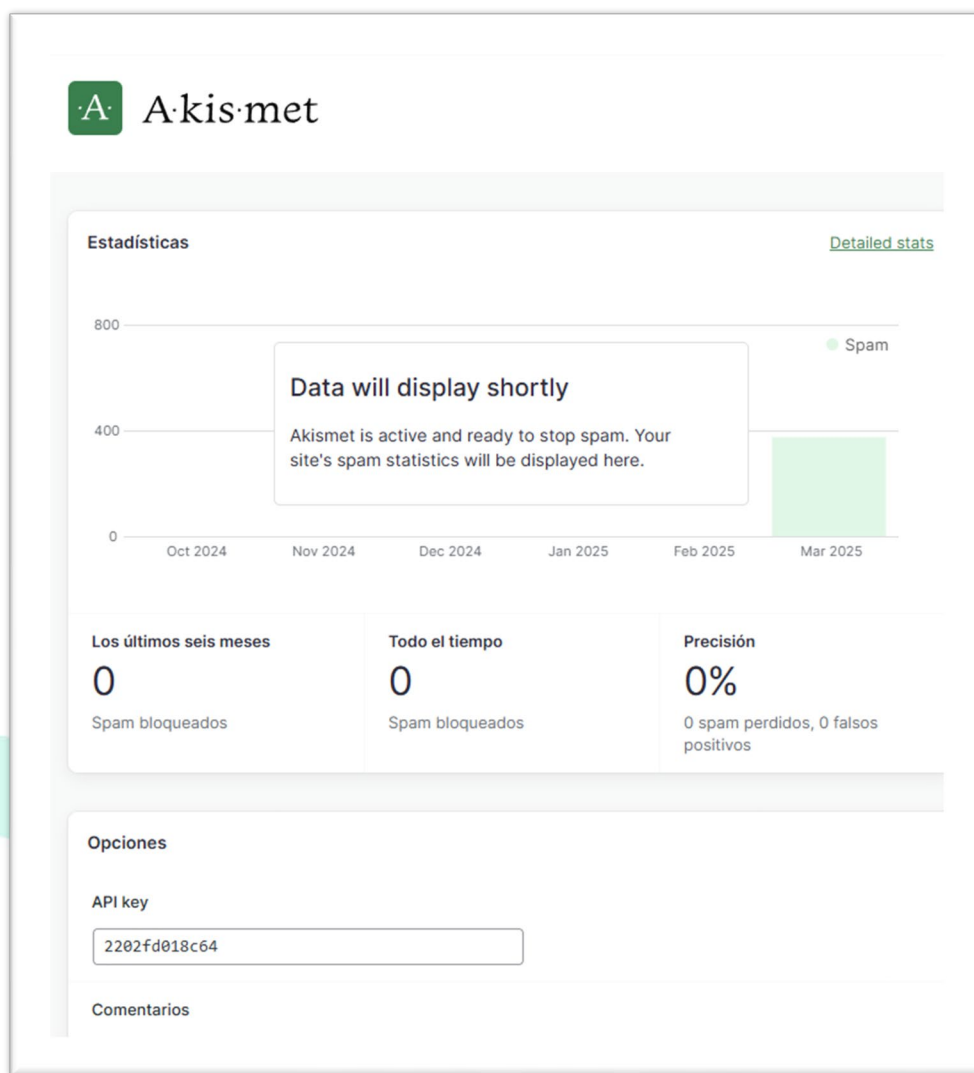
☐ Hide results ☒ Follow redirects

Security Report Summary	
	Site: https://promet.com.pe/
	IP Address: 69.10.40.98
	Report Time: 18 Mar 2025 18:44:58 UTC
	Headers: ✔ X-Content-Type-Options ✔ X-Frame-Options ✔ Referrer-Policy ✔ Permissions-Policy ✔ Strict-Transport-Security ✖ Content-Security-Policy
	Advanced: Great grade! Perform a deeper security analysis of your website and APIs: Try Now



5. Activación del Plugin Akismet (Antispam)

Se activó el plugin Akismet para agregar una capa de defensa contra spam en comentarios de su sitio web.




6. Búsqueda de Malware

Se realizó un escaneo en busca de archivos maliciosos o modificaciones sospechosas en el código fuente. No se encontraron archivos maliciosos ni que perjudiquen al sitio web.





 Escáner de malware

Escáner de malware


[MALICIOSOS](#) [ESCANEO A DEMANDA](#) [HISTORIAL](#)

Maliciosos
Malware detectado por Imunify

Plazo Estado

Plazo: Últimos 30 días x

<input type="checkbox"/>	Detectado	Tipo	Malicioso	Motivo	Estado	Acciones
NINGÚN RESULTADO						



 Escáner de malware

Escáner de malware

[MALICIOSOS](#) [ESCANEO A DEMANDA](#) [HISTORIAL](#)

Plazo

Plazo: Últimos 30 días x

Fecha	Tipo	Ruta	Total	Resultado	Acciones
28 de febrero de 2025 13:12		/var/spool/cron/promet	1	No se encontró malware	
28 de febrero de 2025 11:16		/home/promet	33789	No se encontró malware	

