telecom

# SEABOARD ENERGIAS RENOVABLES Y ALIMENTOS SRL

## Pentest (Pruebas de Intrusión)

Informe Técnico

25/11/2025

# Tabla de Contenidos

# Objetivos

El objetivo del proyecto consiste en el descubrimiento y posterior ejecución de un **Pentest (Pruebas de Intrusión)** sobre la infraestructura de **SEABOARD ENERGIAS RENOVABLES Y ALIMENTOS SRL** especificada en el alcance, con la finalidad de identificar debilidades y proponer las recomendaciones de remediación

Las actividades fueron realizadas entre el **08/10/2025** y el **25/11/2025**.

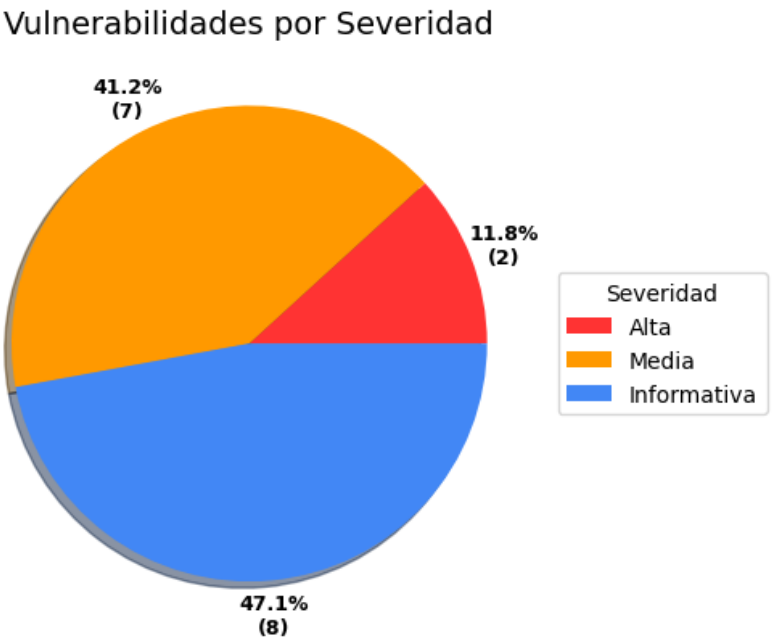
# Alcance

Las siguientes direcciones IP y/o URLs fueron suministradas para realizar una evaluación del tipo Pentest (Pruebas de Intrusión).

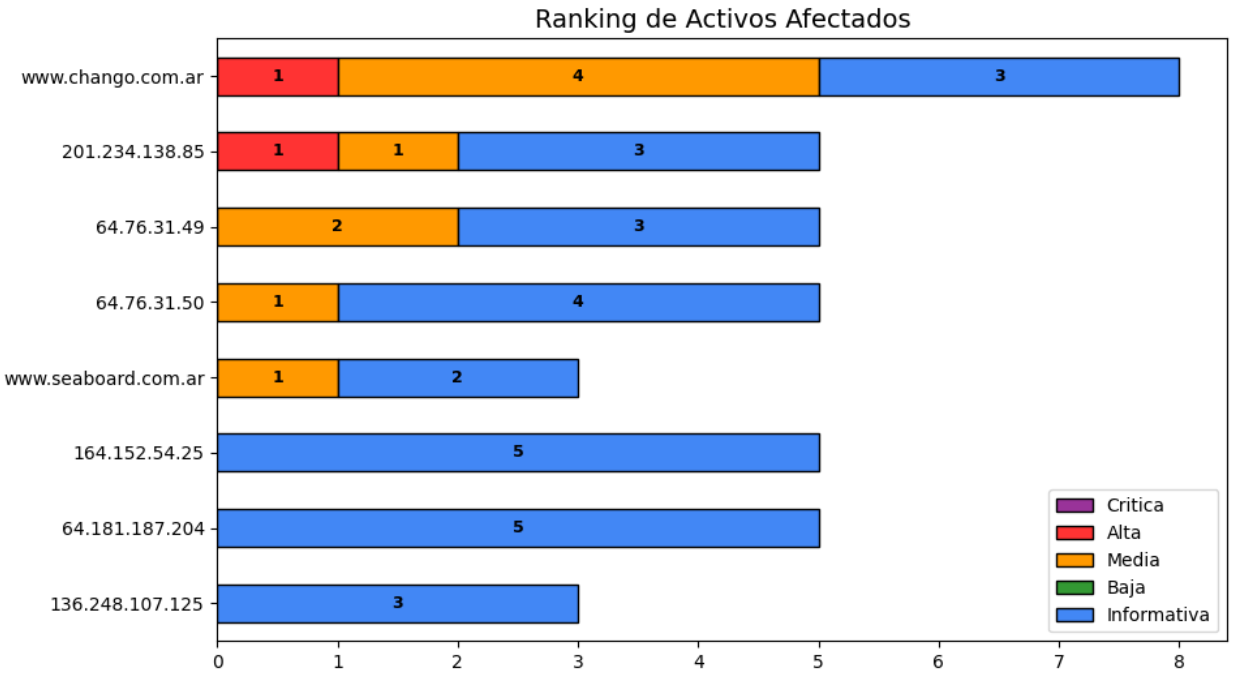
**136.248.107.125**
**164.152.54.25**
**181.80.16.67**
**181.80.16.68**
**200.55.57.197**
**201.234.138.85**
**64.181.187.204**
**64.76.31.49**
**64.76.31.50**
**64.76.31.51**
**64.76.31.52**
**www.apigdesa.seaboard.com.ar**
**www.chango.com.ar**
**www.jdepedidos.seaboard.com.ar**
**www.seaboard.com.ar**

# Resumen de Hallazgos

Como resultado del análisis realizado se han identificado **17** vulnerabilidades, las cuales presentan la siguiente distribución en cuanto a su severidad: **2** de severidad alta, **7** de severidad media y **8** de carácter informativo. Cada vulnerabilidad identificada en el presente informe incluye una breve descripción, los recursos afectados por la misma junto a las evidencias pertinentes, y recomendaciones de solución o mitigación según corresponda.




En el siguiente gráfico se pueden observar los activos afectados que cuentan con mayor cantidad de vulnerabilidades detectadas.



# Hallazgos

En el siguiente listado se pueden visualizar las vulnerabilidades detectadas en el presente análisis clasificadas por Severidad.

| #ID | Nombre | Severidad | Hosts Afectados |
|---|---|---|---|
| **#1** | Information disclosure via api misconfigurations | Alta | 1 |
| **#2** | Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) | Alta | 1 |
| **#3** | SSL Certificate - Expired | Media | 1 |
| **#4** | SSL Certificate - Signature Verification Failed Vulnerability | Media | 1 |
| **#5** | Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0) | Media | 2 |
| **#6** | User enumeration | Media | 1 |
| **#7** | Directory Listing | Media | 1 |
| **#8** | Host Header Injection | Media | 1 |
| **#9** | Frameable response (potential Clickjacking) | Media | 2 |
| **#10** | Robots.txt file | Informativa | 2 |
| **#11** | List of Web Directories Requiring Authentication | Informativa | 1 |
| **#12** | Firewall Detected | Informativa | 6 |
| **#13** | Target Network Information | Informativa | 3 |
| **#14** | Open TCP Services List | Informativa | 6 |
| **#15** | Default Web Page | Informativa | 6 |
| **#16** | HTTP TRACE method is enabled | Informativa | 1 |
| **#17** | WordPress Plugins Detected | Informativa | 1 |

# Pruebas de Intrusión

Durante la ejecución de las pruebas de intrusión, se aplicó una metodología orientada a la detección de vulnerabilidades en servicios expuestos, siguiendo prácticas alineadas con los marcos de referencia de OWASP y OSSTMM. Las actividades fueron desarrolladas sobre los activos definidos en el alcance.

Pruebas realizadas:

1. **Intento de autenticacion con lista de usuarios del sitio sin obtener resultados:**
   - Enumeracion de usuarios:

```
[i] User(s) Identified:

[+] adm-seo
 | Found By: Rss Generator (Aggressive Detection)

[+] adm-valentina
 | Found By: Rss Generator (Aggressive Detection)
```

   - Con dichos usuarios se proceden a guardarlos en un archivo para realizar un ataque por diccionario pero sin obtener resultado satisfactorio:

**Con la lista de usuarios se procedió a realizar un ataque de diccionario con 1000 passwords más comunes sobre el método xmlrpc sin obtener resultado satisfactorio**

```
[+] Performing password attack on Xmlrpc against 2 user/s
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
```

2. **Intento de exlotacion con la lista de plugins del sistema:**
   Se procedió a enumerar los plugins vulnerables y a realizar pruebas sobre algunos de los plugins más comunes:
   - Plugin **duplicator**:

```
msf6 exploit([redacted]/wp_duplicator_code_inject) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Checking if the wp-config.php file already exists ...
[*] All good! Injecting PHP code in the wp-config.php file ...
[-] Failed to inject PHP code in wp-config.php ...
[*] Exploit completed, but no session was created.
```

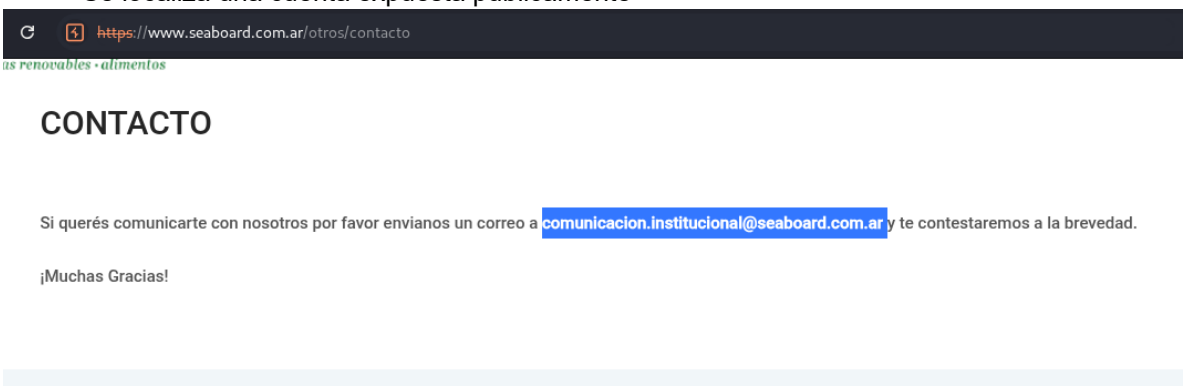
- Plugin **wp_total_cache_exec**:
  Como se ve, el exploit depende de comentarios POST, lo cual no está disponible en el objetivo.

```
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Trying unauthenticated exploitation...
[*] Trying to get posts from feed...
[*] Nothing found. Trying to brute force a valid POST ID...
```

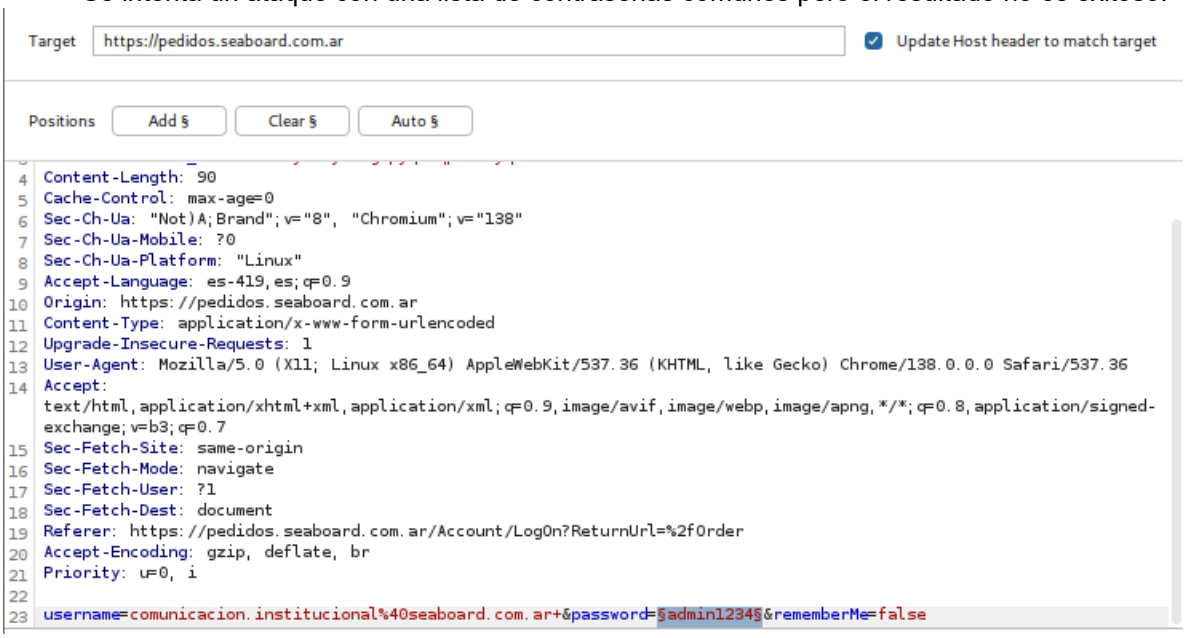
- Plugin **wp_file_manager_rce**:
  Como se ve, no se logró explotar.

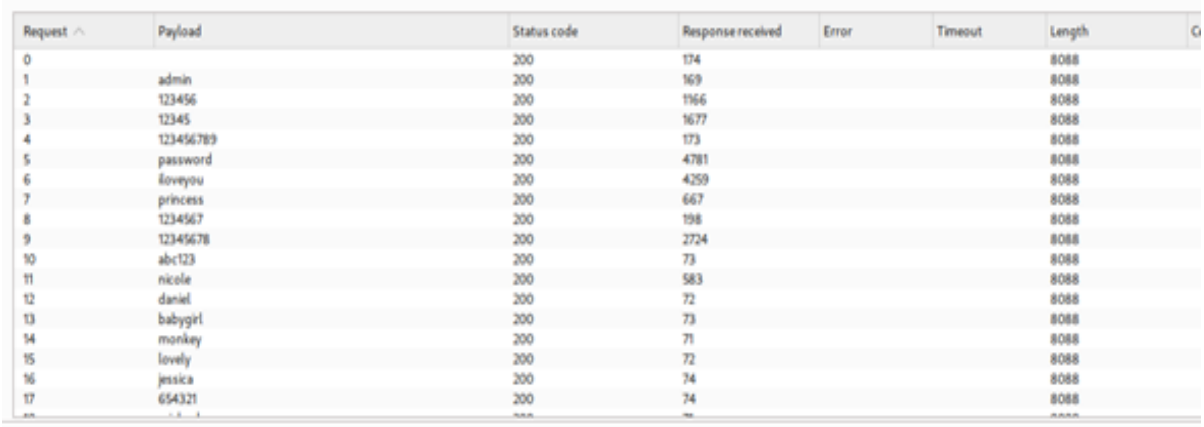
```
msf exploit(multi/http/wp_file_manager_rce) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The target is not exploitable. ForceExploit is enabled, proceeding with exploitation.
[-] Exploit aborted due to failure: unexpected-reply: 190.216.52.124:443 - Unexpected HTTP respo
nse code: 403
```

3. **Intento de autenticacion con cuentas publicas:**
   - Se localiza una cuenta expuesta públicamente




   - Se intenta un ataque con una lista de contraseñas comunes pero el resultado no es exitoso:





| Request | Payload | Status code | Response received | Error | Timeout | Length |
|---|---|---|---|---|---|---|
| 0 | | 200 | 174 | | | 8088 |
| 1 | admin | 200 | 169 | | | 8088 |
| 2 | 123456 | 200 | 1166 | | | 8088 |
| 3 | 12345 | 200 | 1677 | | | 8088 |
| 4 | 123456789 | 200 | 173 | | | 8088 |
| 5 | password | 200 | 4781 | | | 8088 |
| 6 | iloveyou | 200 | 4259 | | | 8088 |
| 7 | princess | 200 | 667 | | | 8088 |
| 8 | 1234567 | 200 | 198 | | | 8088 |
| 9 | 12345678 | 200 | 2724 | | | 8088 |
| 10 | abc123 | 200 | 73 | | | 8088 |
| 11 | nicole | 200 | 583 | | | 8088 |
| 12 | daniel | 200 | 72 | | | 8088 |
| 13 | babygirl | 200 | 73 | | | 8088 |
| 14 | monkey | 200 | 71 | | | 8088 |
| 15 | lovely | 200 | 72 | | | 8088 |
| 16 | jessica | 200 | 74 | | | 8088 |
| 17 | 654321 | 200 | 74 | | | 8088 |

# Detalle de Hallazgos

| #1 Information disclosure via api misconfigurations | | | | |
|---|---|---|---|---|
| Severidad: Alta | **Attack Vector** | Network | **Scope** | Unchanged |
| CVSS: 8.0 | **Attack Complexity** | Low | **Confidentiality Impact** | High |
| Ocurrencias: 1 | **Privileges Required** | None | **Integrity Impact** | None |
| | **User Interaction** | None | **Availability Impact** | None |

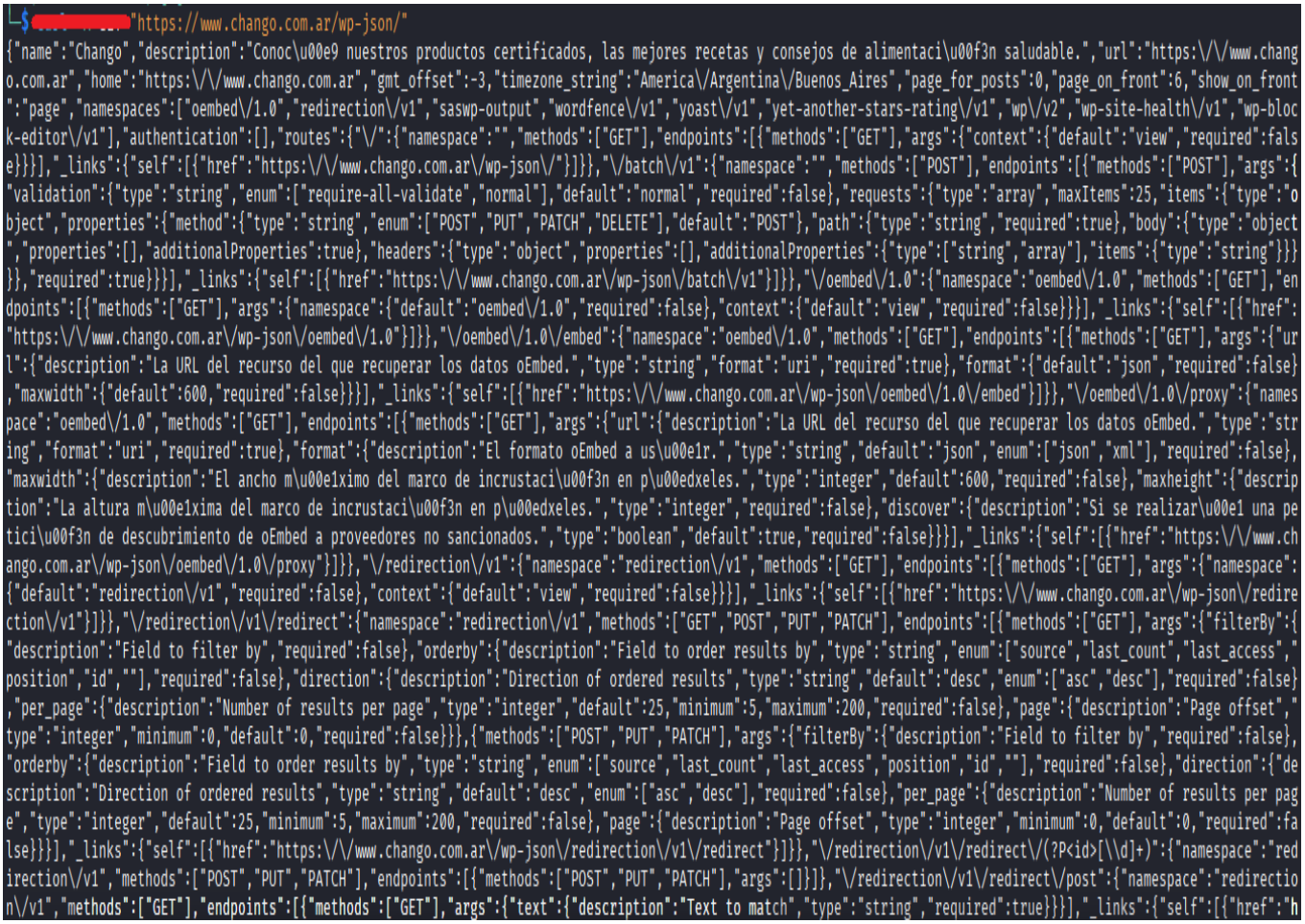
**Recursos Afectados**
www.chango.com.ar

**Descripción**
Se detectó que uno o varios API endpoints revelan información potencialmente sensible a usuarios no autorizados.

**Impacto**
Las vulnerabilidades de divulgación de información pueden tener un impacto tanto directo como indirecto según el propósito del sitio web y, por lo tanto, qué información puede obtener un atacante. En general, el riesgo de este tipo de vulnerabilidad es exponer información que puede ser utilizada para realizar ataques mas elaborados.

**Solución**
Configurar las API para exponer información a usuarios debidamente autorizados y en linea con las necesidades del negocio de manera tal que solo se exponga la información necesaria.

**Evidencias**
Recurso: www.chango.com.ar




{"name":"Chango","description":"Conoc\u00e9 nuestros productos certificados, las mejores recetas y consejos de alimentaci\u00f3n saludable.","url":"https:\/\/www.chango.com.ar","home":"https:\/\/www.chango.com.ar","gmt_offset":-3,"timezone_string":"America\/Argentina\/Buenos_Aires","page_for_posts":0,"page_on_front":6,"show_on_front":"page","namespaces":["oembed\/1.0","redirection\/v1","saswp-output","wordfence\/v1","yoast\/v1","yet-another-stars-rating\/v1","wp\/v2","wp-site-health\/v1","wp-block-editor\/v1"],"authentication":[],"routes":{"\/":{"namespace":"","methods":["GET"],"endpoints":[{"methods":["GET"],"args":{"context":{"default":"view","required":false}}}],"_links":{"self":[{"href":"https:\/\/www.chango.com.ar\/wp-json\/"}]}},"\/batch\/v1":{"namespace":"","methods":["POST"],"endpoints":[{"methods":["POST"],"args":{"validation":{"type":"string","enum":["require-all-validate","normal"],"default":"normal","required":false},"requests":{"type":"array","maxItems":25,"items":{"type":"object","properties":{"method":{"type":"string","enum":["POST","PUT","PATCH","DELETE"],"default":"POST"},"path":{"type":"string","required":true},"body":{"type":"object","properties":[],"additionalProperties":true},"headers":{"type":"object","properties":[],"additionalProperties":{"type":["string","array"],"items":{"type":"string"}}}},"required":true}}}],"_links":{"self":[{"href":"https:\/\/www.chango.com.ar\/wp-json\/batch\/v1"}]}},"\/oembed\/1.0":{"namespace":"oembed\/1.0","methods":["GET"],"endpoints":[{"methods":["GET"],"args":{"namespace":{"default":"oembed\/1.0","required":false},"context":{"default":"view","required":false}}}],"_links":{"self":[{"href":"https:\/\/www.chango.com.ar\/wp-json\/oembed\/1.0"}]}},"\/oembed\/1.0\/embed":{"namespace":"oembed\/1.0","methods":["GET"],"endpoints":[{"methods":["GET"],"args":{"url":{"description":"La URL del recurso del que recuperar los datos oEmbed.","type":"string","format":"uri","required":true},"format":{"default":"json","required":false},"maxwidth":{"default":600,"required":false}}}],"_links":{"self":[{"href":"https:\/\/www.chango.com.ar\/wp-json\/oembed\/1.0\/embed"}]}},"\/oembed\/1.0\/proxy":{"namespace":"oembed\/1.0","methods":["GET"],"endpoints":[{"methods":["GET"],"args":{"url":{"description":"La URL del recurso del que recuperar los datos oEmbed.","type":"string","format":"uri","required":true},"format":{"description":"El formato oEmbed a us\u00e1r.","type":"string","default":"json","enum":["json","xml"],"required":false},"maxwidth":{"description":"El ancho m\u00e1ximo del marco de incrustaci\u00f3n en p\u00edxeles.","type":"integer","default":600,"required":false},"maxheight":{"description":"La altura m\u00e1xima del marco de incrustaci\u00f3n en p\u00edxeles.","type":"integer","required":false},"discover":{"description":"Si se realizar\u00e1 una petici\u00f3n de descubrimiento de oEmbed a proveedores no sancionados.","type":"boolean","default":true,"required":false}}}],"_links":{"self":[{"href":"https:\/\/www.chango.com.ar\/wp-json\/oembed\/1.0\/proxy"}]}},"\/redirection\/v1":{"namespace":"redirection\/v1","methods":["GET"],"endpoints":[{"methods":["GET"],"args":{"namespace":{"default":"redirection\/v1","required":false},"context":{"default":"view","required":false}}}],"_links":{"self":[{"href":"https:\/\/www.chango.com.ar\/wp-json\/redirection\/v1"}]}},"\/redirection\/v1\/redirect":{"namespace":"redirection\/v1","methods":["GET","POST","PUT","PATCH"],"endpoints":[{"methods":["GET"],"args":{"filterBy":{"description":"Field to filter by","required":false},"orderby":{"description":"Field to order results by","type":"string","enum":["source","last_count","last_access","position","id",""],"required":false},"direction":{"description":"Direction of ordered results","type":"string","default":"desc","enum":["asc","desc"],"required":false},"per_page":{"description":"Number of results per page","type":"integer","default":25,"minimum":5,"maximum":200,"required":false},"page":{"description":"Page offset","type":"integer","minimum":0,"default":0,"required":false}}},{"methods":["POST","PUT","PATCH"],"args":{"filterBy":{"description":"Field to filter by","required":false},"orderby":{"description":"Field to order results by","type":"string","enum":["source","last_count","last_access","position","id",""],"required":false},"direction":{"description":"Direction of ordered results","type":"string","default":"desc","enum":["asc","desc"],"required":false},"per_page":{"description":"Number of results per page","type":"integer","default":25,"minimum":5,"maximum":200,"required":false},"page":{"description":"Page offset","type":"integer","minimum":0,"default":0,"required":false}}}],"_links":{"self":[{"href":"https:\/\/www.chango.com.ar\/wp-json\/redirection\/v1\/redirect"}]}},"\/redirection\/v1\/redirect\/(?P<id>[\\d]+)":{"namespace":"redirection\/v1","methods":["POST","PUT","PATCH"],"endpoints":[{"methods":["POST","PUT","PATCH"],"args":[]}]},"\/redirection\/v1\/redirect\/post":{"namespace":"redirection\/v1","methods":["GET"],"endpoints":[{"methods":["GET"],"args":{"text":{"description":"Text to match","type":"string","required":true}}}],"_links":{"self":[{"href":"h

| #2 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) | | | | |
|---|---|---|---|---|
| Severidad: Alta | **Attack Vector** | Network | **Scope** | Unchanged |
| CVSS: 7.5 | **Attack Complexity** | Low | **Confidentiality Impact** | High |
| Ocurrencias: 1 | **Privileges Required** | None | **Integrity Impact** | None |
| | **User Interaction** | None | **Availability Impact** | None |

**Recursos Afectados**
201.234.138.85 Puerto: TCP/8003

**Descripción**
Los cifrados de bloques de 64 bits antiguos son vulnerables a un ataque de colisión práctico cuando se utiliza en modo CBC. Todas las versiones del protocolo SSL/TLS que soporten las suites de cifrado utilizando DES, 3DES, IDEA o RC2 como cifrado simétrico se ven afectadas.
Este CVE está corregido en las siguientes versiones
OPENSSL-0.9.8J-0.102.2
LIBOPENSSL0_9_8-0.9.8J-0.102.2
LIBOPENSSL0_9_8-32BIT-0.9.8J-0.102.2
OPENSSL1-1.0.1G-0.52.1
OPENSSL1-DOC-1.0.1G-0.52.1
LIBOPENSSL1_0_0-1.0.1G-0.52.1
LIBOPENSSL1-DEVEL-1.0.1G-0.52.1
JAVA-1_6_0-IBM-1.6.0_SR16.41-81.1

**Impacto**
Los atacantes remotos pueden obtener datos de texto claro a través de este ataque contra una sesión cifrada de larga duración.

**CVEs**
https://nvd.nist.gov/vuln/detail/CVE-2016-2183

**Referencias**
Sweet32: https://sweet32.info/
Microsoft Windows TLS:
https://docs.microsoft.com/en-us/windows-server/security/tls/tls-schannel-ssp-changes-in-windows-10-and-windows-server
Configuración del registro de Microsoft Transport Layer Security (TLS):
https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings

**Solución**
Desactivar y dejar de usar los cifrados DES, 3DES, IDEA o RC2.

**Evidencias**
Recurso: 201.234.138.85 Puerto: TCP/8003

```
CIPHER      KEY-EXCHANGE   AUTHENTICATION MAC     ENCRYPTION(KEY-STRENGTH)     GRADE
TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED
DES-CBC3-SHA       RSA     RSA     SHA1    3DES(168)      MEDIUM
TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED
DES-CBC3-SHA       RSA     RSA     SHA1    3DES(168)      MEDIUM
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED
DES-CBC3-SHA       RSA     RSA     SHA1    3DES(168)      MEDIUM
```


| #3 SSL Certificate - Expired | | | | |
|---|---|---|---|---|
| Severidad: Media | **Attack Vector** | Network | **Scope** | Unchanged |
| CVSS: 6.5 | **Attack Complexity** | Low | **Confidentiality Impact** | Low |
| Ocurrencias: 1 | **Privileges Required** | None | **Integrity Impact** | Low |
| | **User Interaction** | None | **Availability Impact** | None |

**Recursos Afectados**
64.76.31.49 Puerto: TCP/443

**Descripción**
Un Certificado SSL asocia una entidad (persona, organización, host, etc.) con una Clave Pública. En una conexión SSL, el cliente autentica el servidor remoto usando el Certificado del servidor y extrae la Clave Pública en el Certificado para establecer la conexión segura.
No se puede confiar en un certificado con fecha de finalización anterior.

**Impacto**
Al explotar esta vulnerabilidad, un atacante puede lanzar un ataque de hombre-en-el-medio (MiTM).

**Referencias**
https://www.crowdstrike.com/en-us/blog/the-risks-of-expired-ssl-certificates/

**Solución**
Instale un certificado de servidor con fechas de inicio y final válidas.

**Evidencias**
Recurso: 64.76.31.49 Puerto: TCP/443

```
Certificate #0 CN=*.seaboard.com.ar  is not valid after Dec 17 15:48:31 2024 GMT.
```

```
Not valid before: Nov 16 15:48:31 2023 GMT
Not valid after:  Dec 17 15:48:31 2024 GMT
```

| #4 SSL Certificate - Signature Verification Failed Vulnerability | | | | |
|---|---|---|---|---|
| Severidad: Media | **Attack Vector** | Network | **Scope** | Unchanged |
| CVSS: 6.5 | **Attack Complexity** | Low | **Confidentiality Impact** | Low |
| Ocurrencias: 1 | **Privileges Required** | None | **Integrity Impact** | Low |
| | **User Interaction** | None | **Availability Impact** | None |

**Recursos Afectados**
64.76.31.49 Puerto: TCP/443

**Descripción**
Un Certificado SSL asocia una entidad (persona, organización, host, etc.) con una Clave Pública. En una conexión SSL, el cliente auténtica el servidor remoto usando el Certificado del servidor y extrae la Clave Pública en el Certificado para establecer la conexión segura. La autenticación se realiza verificando que la clave pública del certificado es firmada por una autoridad de certificado de terceros de confianza.
Si un cliente no puede verificar el certificado, puede abortar la comunicación o incitar al usuario a continuar la comunicación sin autenticación.

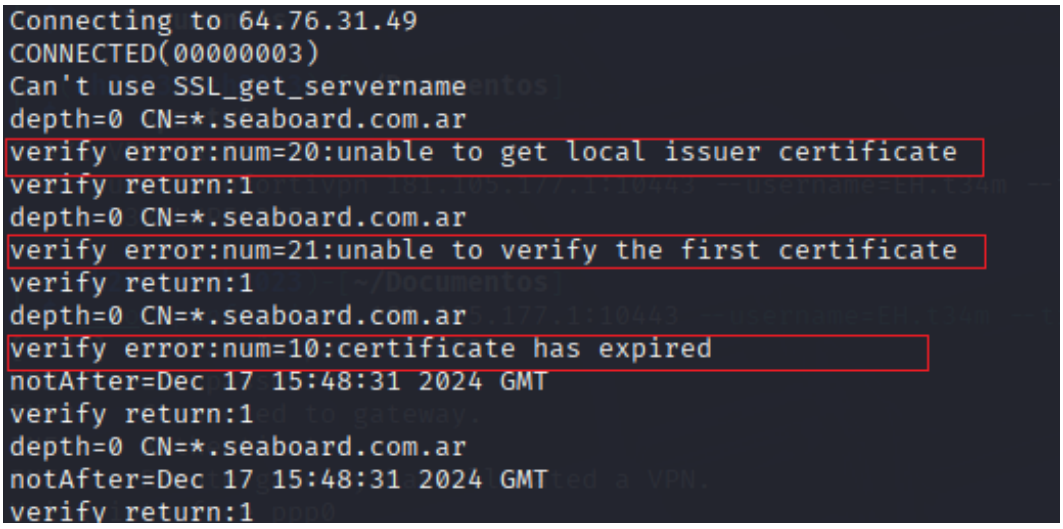
**Impacto**
Aprovechando esta vulnerabilidad, pueden producirse ataques de hombre-en-el-medio (man-in-the-middle) junto con el envenenamiento de la caché DNS.

**Referencias**
https://apidog.com/articles/ssl-certificate-signature-verification-failure-vulnerability/
Mozilla SSL Configuration Guidelines: https://wiki.mozilla.org/Security/Server_Side_TLS
OWASP - Transport Layer Protection Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

**Solución**
Instale un certificado de servidor firmado por una autoridad de certificado de terceros de confianza.

**Evidencias**
Recurso: 64.76.31.49 Puerto: TCP/443

```
Certificate #0 CN=*.seaboard.com.ar ISSUER:_CN=Go_Daddy_Secure_Certificate_Authority_-
_G2,OU=http://certs.godaddy.com/repository/,O=GoDaddy.com\,_Inc.,L=Scottsdale,ST=Arizona,C=U
S certificate has expired
```



| #5 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0) | | | | |
|---|---|---|---|---|
| Severidad: Media | **Attack Vector** | Network | **Scope** | Unchanged |
| CVSS: 6.5 | **Attack Complexity** | High | **Confidentiality Impact** | High |
| Ocurrencias: 2 | **Privileges Required** | None | **Integrity Impact** | Low |
| | **User Interaction** | None | **Availability Impact** | None |

**Recursos Afectados**

201.234.138.85 Puerto: TCP/8003
64.76.31.50 Puerto: TCP/443

**Descripción**

TLS es capaz de utilizar una gran variedad de cifrados (algoritmos) para crear los pares de claves públicas y privadas.
Por ejemplo, TLSv1.0 usa el cifrado de flujo RC4 o un cifrado por bloques en modo CBC. RC4 es conocido por tener sesgos y el cifrado de bloque en modo CBC es vulnerable al ataque POODLE.
TLSv1.0, si está configurado para utilizar las mismas suites de cifrado que SSLv3, incluye un medio por el cual una implementación TLS puede degradar la conexión a SSL v3.0, debilitando así la seguridad.
Esta vulnerabilidad es un PCI FAIL automático de acuerdo con los estándares PCI.
NOTA: El 31 de marzo de 2021 las versiones de TLS 1.0 (RFC 2246) y 1.1 (RFC 4346) fueron oficialmente declaradas obsoletas. Puede consultar más información en las Referencias.

**Impacto**

Un atacante puede explotar fallas criptográficas para realizar ataques de tipo hombre-en-el-medio (man-in-the-middle) o para descifrar comunicaciones.

**Referencias**

Deprecating TLS 1.0 and TLS 1.1 https://tools.ietf.org/html/rfc8996
PCI: ASV Program Guide v3.1 (page 27) https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf
PCI: Uso de los escáneres SSL Early TLS y ASV https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf

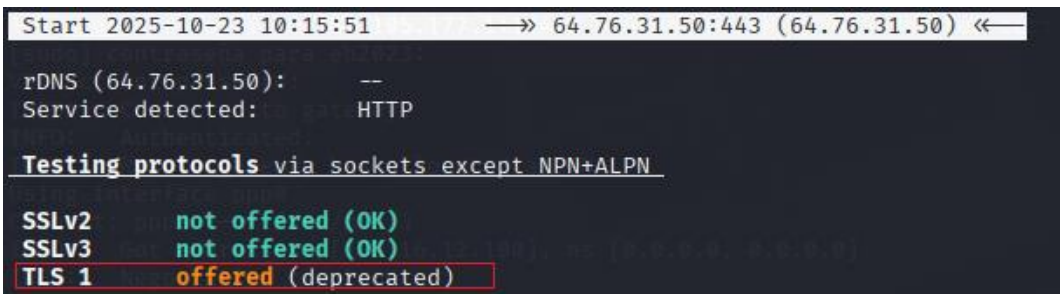
**Solución**

Desactivar el uso del protocolo TLSv1.0 en favor de un protocolo criptográficomente más fuerte como TLSv1.2.

**Evidencias**

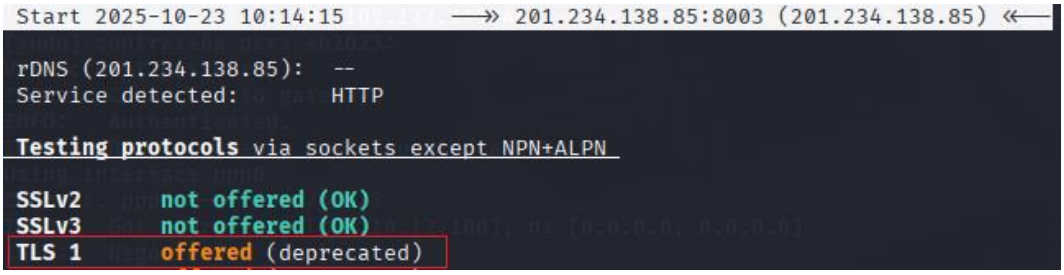
Recurso: 64.76.31.50 Puerto: TCP/443

```
TLSv1.0 is supported
```




Recurso: 201.234.138.85 Puerto: TCP/8003

```
TLSv1.0 is supported
```




| #6 User enumeration | | | | |
|---|---|---|---|---|
| Severidad: Media | **Attack Vector** | Network | **Scope** | Unchanged |
| CVSS: 5.3 | **Attack Complexity** | Low | **Confidentiality Impact** | Low |
| Ocurrencias: 1 | **Privileges Required** | None | **Integrity Impact** | None |
| | **User Interaction** | None | **Availability Impact** | None |

**Recursos Afectados**
https://www.chango.com.ar/

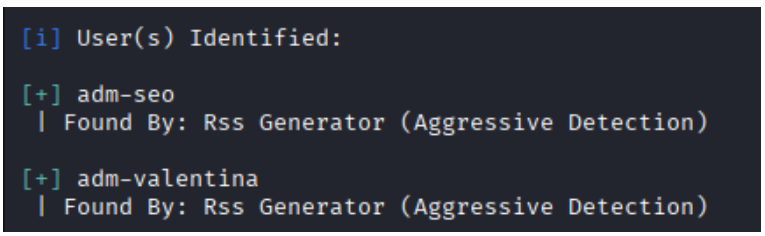
**Descripción**
Durante las pruebas realizadas se observa un comportamiento que permite diferenciar si un usuario existe o no en la aplicación analizada.

**Impacto**
Un atacante podría aprovechar esta vulnerabilidad para obtener una lista de usuarios válidos y utilizarla posteriormente para generar ataques de fuerza bruta.

**Referencias**
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/03-Identity_Management_Testing/README
https://cwe.mitre.org/data/definitions/284.html
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/03-Identity_Management_Testing/04-Testing_for_Account_Enumeration_and_Guessable_User_Account

**Solución**
Se recomienda que la aplicación no revele el nombre de los usuarios válidos, y que no sea posible discernir entre usuarios válidos e inválidos en base a la respuesta emitida por el servidor.

**Evidencias**
Recurso: https://www.chango.com.ar/



**Con la lista de usuarios se procedió a realizar un ataque de diccionario con 1000 passwords más comunes sobre el método xmlrpc sin obtener resultado satisfactorio**

```
[+] Performing password attack on Xmlrpc against 2 user/s
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
Error: Unknown response received Code: 405
```

| #7 Directory Listing | | | | |
|---|---|---|---|---|
| Severidad: Media | **Attack Vector** | Network | **Scope** | Unchanged |
| CVSS: 5.3 | **Attack Complexity** | Low | **Confidentiality Impact** | Low |
| Ocurrencias: 1 | **Privileges Required** | None | **Integrity Impact** | None |
| | **User Interaction** | None | **Availability Impact** | None |

**Recursos Afectados**

https://www.chango.com.ar/wp-content/

**Descripción**

Los servidores web que permiten la lista de directorios se utilizan normalmente para compartir archivos.
La lista de directorios permite al cliente ver una lista simple de todos los archivos y carpetas alojados en el servidor web. Luego, el cliente puede recorrer cada directorio y descargar los archivos.
Los ciberdelincuentes utilizarán la presencia de la lista de directorios para descubrir archivos confidenciales, descargar contenido protegido o simplemente aprender cómo está estructurada la aplicación web.

**Impacto**

Los ciberdelincuentes utilizarán la presencia de la lista de directorios para descubrir archivos confidenciales, descargar contenido protegido o simplemente aprender cómo está estructurada la aplicación web.

**Referencias**

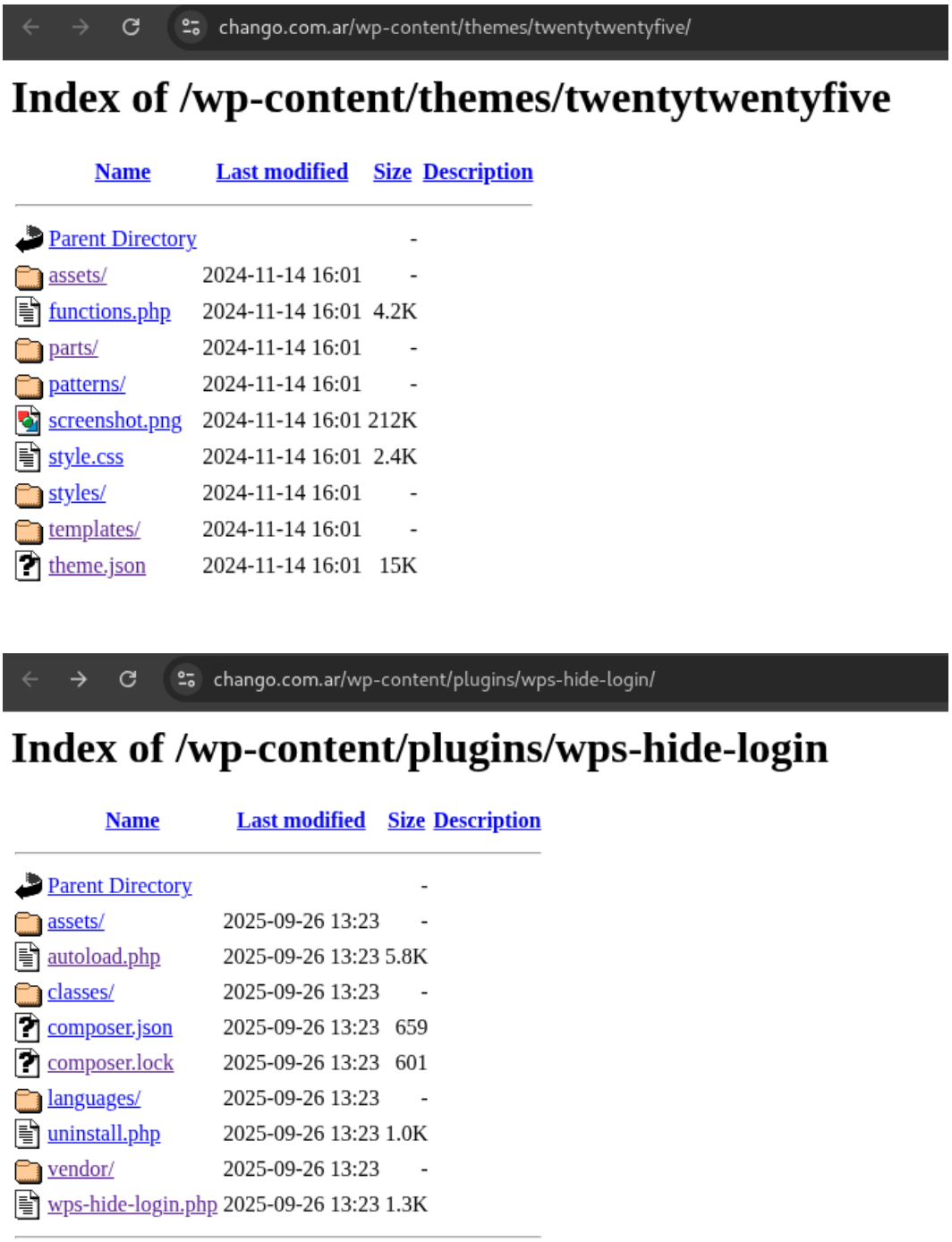
https://portswigger.net/kb/issues/00600100_directory-listing

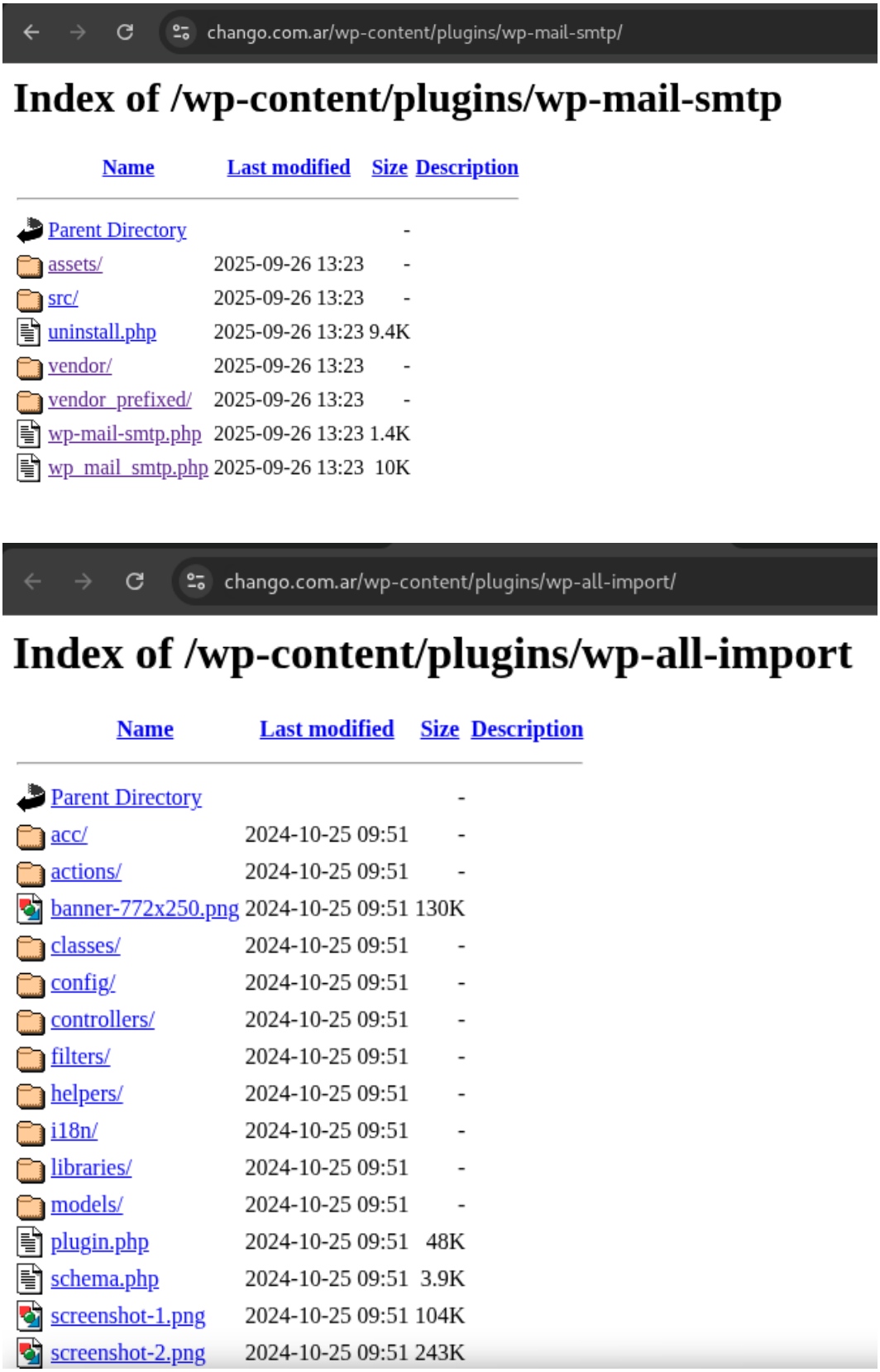
**Solución**

A menos que el servidor web se utilice para compartir archivos estáticos y no confidenciales, habilitar la lista de directorios se considera una mala práctica de seguridad.
Esto generalmente se puede hacer con un simple cambio de configuración en el servidor. Los pasos para deshabilitar la lista de directorios diferirán según el tipo de servidor que se utilice (IIS, Apache, etc.). Si se requiere y se permite el listado de directorios, se deben tomar medidas para garantizar que se reduzca el riesgo

de dicha configuración.
Estos pueden incluir:
1. Requerir autenticación para acceder a las páginas afectadas. 2. Agregar la ruta afectada al archivo `robots.txt` para evitar que los motores de búsqueda puedan buscar el contenido del directorio. 3. Asegurarse de que los archivos confidenciales no se almacenen en la web o en la raíz del documento. 4. Eliminar cualquier archivo que no sea necesario para que la aplicación funcione.

**Evidencias**
Recurso: https://www.chango.com.ar/wp-content/





chango.com.ar/wp-content/plugins/wp-mail-smtp/

# Index of /wp-content/plugins/wp-mail-smtp

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| assets/ | 2025-09-26 13:23 | - | |
| src/ | 2025-09-26 13:23 | - | |
| uninstall.php | 2025-09-26 13:23 | 9.4K | |
| vendor/ | 2025-09-26 13:23 | - | |
| vendor_prefixed/ | 2025-09-26 13:23 | - | |
| wp-mail-smtp.php | 2025-09-26 13:23 | 1.4K | |
| wp_mail_smtp.php | 2025-09-26 13:23 | 10K | |

chango.com.ar/wp-content/plugins/wp-all-import/

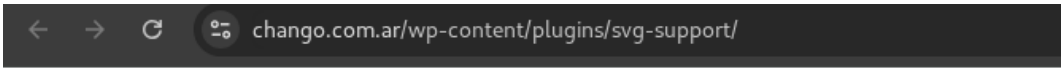
# Index of /wp-content/plugins/wp-all-import

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| acc/ | 2024-10-25 09:51 | - | |
| actions/ | 2024-10-25 09:51 | - | |
| banner-772x250.png | 2024-10-25 09:51 | 130K | |
| classes/ | 2024-10-25 09:51 | - | |
| config/ | 2024-10-25 09:51 | - | |
| controllers/ | 2024-10-25 09:51 | - | |
| filters/ | 2024-10-25 09:51 | - | |
| helpers/ | 2024-10-25 09:51 | - | |
| i18n/ | 2024-10-25 09:51 | - | |
| libraries/ | 2024-10-25 09:51 | - | |
| models/ | 2024-10-25 09:51 | - | |
| plugin.php | 2024-10-25 09:51 | 48K | |
| schema.php | 2024-10-25 09:51 | 3.9K | |
| screenshot-1.png | 2024-10-25 09:51 | 104K | |
| screenshot-2.png | 2024-10-25 09:51 | 243K | |


# Index of /wp-content/uploads

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| 2024/ | 2024-12-01 00:00 | - | |
| 2025/ | 2025-11-01 00:00 | - | |
| wp-file-manager-pro/ | 2024-11-19 10:37 | - | |
| wpallimport/ | 2024-10-24 09:27 | - | |

*Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.1.25 Server at www.chango.com.ar Port 443*




# Index of /wp-content/plugins/svg-support

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| admin/ | 2025-09-26 13:24 | - | |
| composer.json | 2025-09-26 13:24 | 1.2K | |
| config.codekit3 | 2025-09-26 13:24 | 80K | |
| css/ | 2025-09-26 13:24 | - | |
| functions/ | 2025-09-26 13:24 | - | |
| includes/ | 2025-09-26 13:24 | - | |
| integrations/ | 2025-09-26 13:24 | - | |
| js/ | 2025-09-26 13:24 | - | |
| languages/ | 2025-09-26 13:24 | - | |
| scss/ | 2025-09-26 13:24 | - | |
| svg-support.php | 2025-09-26 13:24 | 6.1K | |
| svg-support.png | 2025-09-26 13:24 | 37K | |
| uninstall.php | 2025-09-26 13:24 | 531 | |
| vendor/ | 2025-09-26 13:24 | - | |

| #8 Host Header Injection | | | | |
|---|---|---|---|---|
| Severidad: Media | **Attack Vector** | Network | **Scope** | Unchanged |
| CVSS: 4.3 | **Attack Complexity** | Low | **Confidentiality Impact** | Low |
| Ocurrencias: 1 | **Privileges Required** | None | **Integrity Impact** | None |
| | **User Interaction** | Required | **Availability Impact** | None |

**Recursos Afectados**
www.chango.com.ar

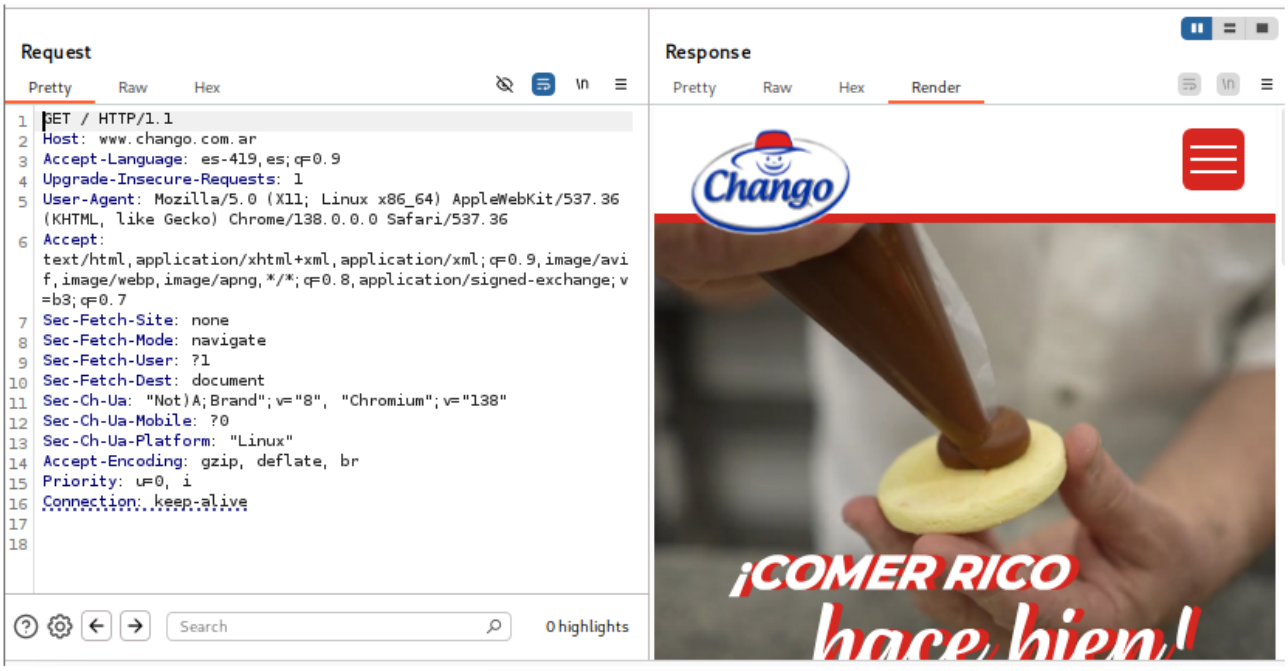
**Descripción**
Al crear URI para enlaces en aplicaciones web, los desarrolladores a menudo recurren al encabezado de host HTTP disponible en la solicitud HTTP enviada por el lado del cliente.

**Impacto**
Un atacante remoto puede explotar esto enviando un encabezado falso con un nombre de dominio bajo su control, lo que le permite envenenar el caché web o los correos electrónicos de restablecimiento de contraseña, por ejemplo.

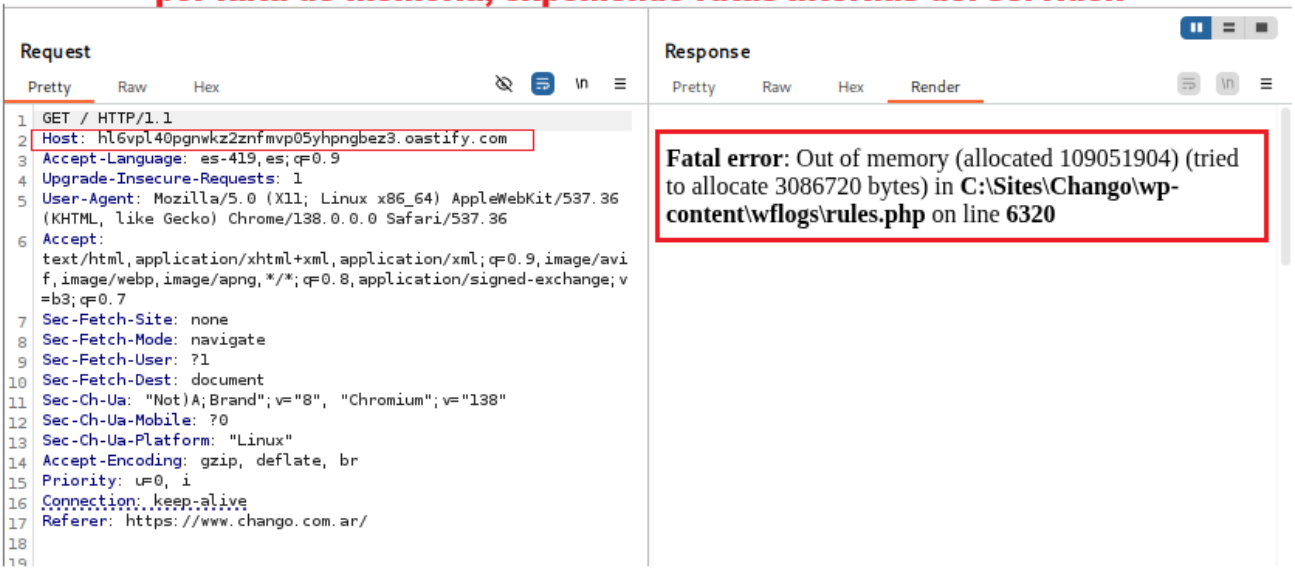
**Solución**
La aplicación web no debe confiar en Host y X-Forwarded-Host y debe usar un SERVER_NAME seguro en lugar de estos encabezados.
Referencia:
https://fr.slideshare.net/DefconRussia/http-host-header-attacks
https://www.skeletonscribe.net/2013/05/practical-http-host-header-attacks.html
https://www.linkedin.com/pulse/host-header-injection- depth-utkarsh-tiwari/

**Evidencias**
Recurso: www.chango.com.ar

## Responde correctamente




**Si se modifica el encabezado Host, la aplicación genera un error fatal por falta de memoria, exponiendo rutas internas del servidor.**



| #9 Frameable response (potential Clickjacking) | | | | |
|---|---|---|---|---|
| Severidad: Media | **Attack Vector** | Network | **Scope** | Unchanged |
| CVSS: 4.3 | **Attack Complexity** | Low | **Confidentiality Impact** | Low |
| Ocurrencias: 2 | **Privileges Required** | None | **Integrity Impact** | Low |
| | **User Interaction** | Required | **Availability Impact** | None |

**Recursos Afectados**
https://www.chango.com.ar/
https://www.seaboard.com.ar/

**Descripción**
Si una página no establece un encabezado HTTP adecuado X-Frame-Options o Content-Security-Policy, puede ser posible que una página controlada por un atacante la cargue dentro de un iframe. Esto puede permitir un ataque de secuestro de clicks, en el que la página del atacante superpone la interfaz de la aplicación de destino con una interfaz diferente proporcionada por el atacante.
Tenga en cuenta que algunas aplicaciones intentan evitar estos ataques dentro de la propia página HTML, utilizando el código "framebusting". Sin embargo, este tipo de defensa es normalmente ineficaz y generalmente puede ser eludido por un atacante.
Usted debe determinar si cualquier función accesible dentro de páginas enmarcables puede ser utilizado por los usuarios de aplicaciones para realizar cualquier acción sensible dentro de la aplicación.

**Impacto**
Al inducir a los usuarios a realizar acciones tales como clicks de ratón y pulsaciones de teclas, el atacante puede hacer que realicen involuntariamente acciones dentro de la aplicación que está siendo apuntada. Esta técnica permite al atacante eludir las defensas contra la falsificación de solicitud inter-sitio, y puede resultar en acciones no autorizadas.

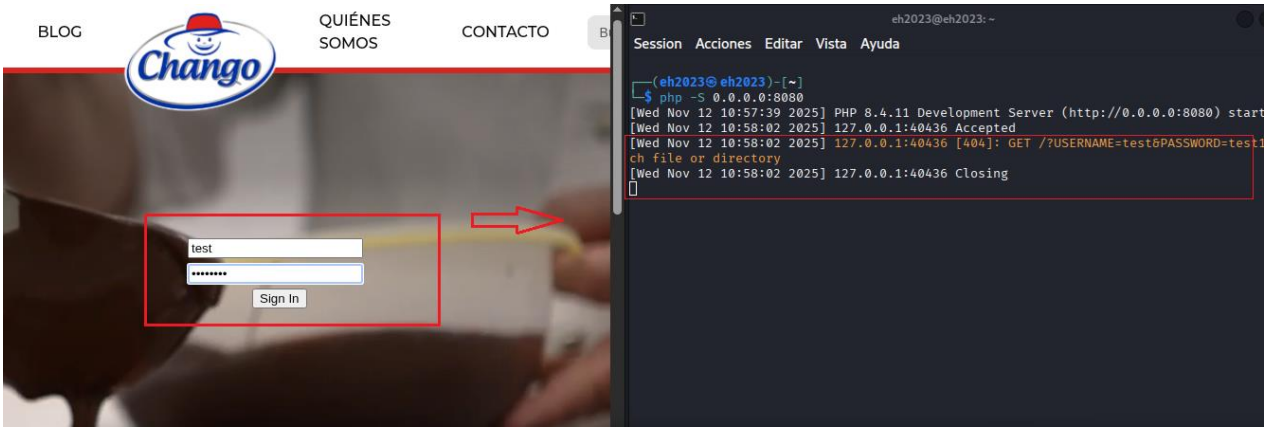
**Referencias**
* [Web Security Academy: Clickjacking](https://portswigger.net/web-security/clickjacking)
* [X-Frame-Options](https://developer.mozilla.org/en-US/docs/Web/HTTP/X-Frame-Options)

**Solución**
Para prevenir eficazmente los ataques de framing, la aplicación debe devolver un encabezado de respuesta con el nombre **X-Frame-Options** y el valor **DENY** para evitar el encuadre total, o el valor **SAMEORIGIN** permitir el encuadre sólo por páginas en el mismo origen que la respuesta misma. Tenga en cuenta que el encabezado SAMEORIGIN puede ser eliminado parcialmente si la aplicación en sí puede ser hecha para enmarcar sitios web no confiables.

**Evidencias**
Recurso: https://www.chango.com.ar/

Como se muestra en la imagen, un ejercicio que ejemplifica la explotación de esta vulnerabilidad consiste en la captura de credenciales mediante el montaje de un frame (iframe) malicioso sobre la interfaz legítima. En un entorno de red local (LAN), esto podría permitir que un atacante conectado a la misma red intercepte o recolecte credenciales de usuarios sin su conocimiento, demostrando la importancia de mitigar este tipo de fallos mediante políticas de encabezados como X-Frame-Options

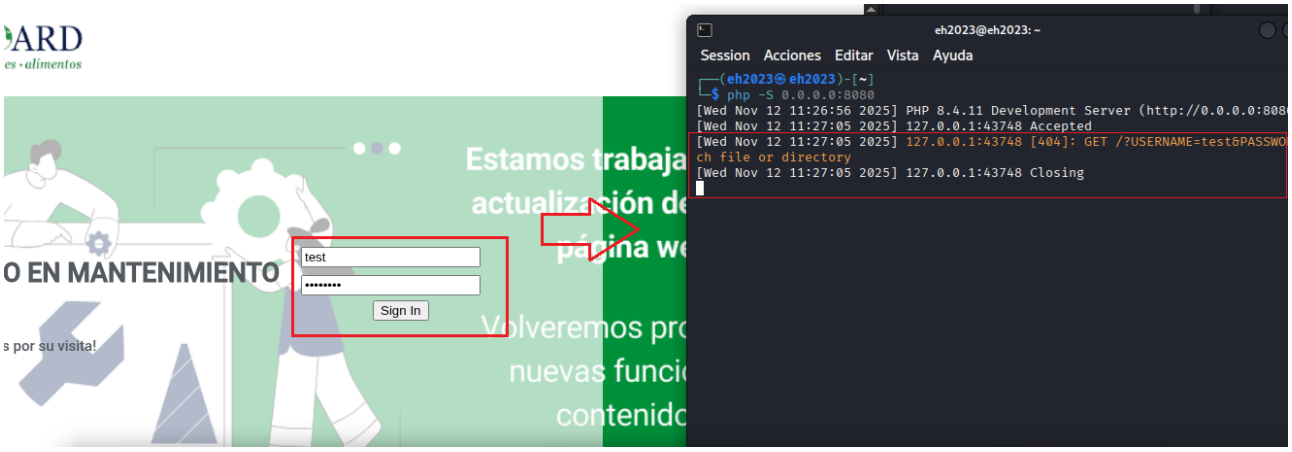
```
[!] Headers analyzed for https://www.chango.com.ar/
[+] There are 0 security headers
[-] There are not 9 security headers
```




Recurso: https://www.seaboard.com.ar/

Como se muestra en la imagen, un ejercicio que ejemplifica la explotación de esta vulnerabilidad consiste en la captura de credenciales mediante el montaje de un frame (iframe) malicioso sobre la interfaz legítima. En un entorno de red local (LAN), esto podría permitir que un atacante conectado a la misma red intercepte o recolecte credenciales de usuarios sin su conocimiento, demostrando la importancia de mitigar este tipo de fallos mediante políticas de encabezados como X-Frame-Options

```
[*] Analyzing headers of https://www.seaboard.com.ar/
[*] Effective URL: https://www.seaboard.com.ar/
[!] Missing security header: X-Frame-Options
[!] Missing security header: X-Content-Type-Options
[!] Missing security header: Strict-Transport-Security
[!] Missing security header: Content-Security-Policy
[!] Missing security header: Referrer-Policy
[!] Missing security header: Permissions-Policy
[!] Missing security header: Cross-Origin-Embedder-Policy
[!] Missing security header: Cross-Origin-Resource-Policy
[!] Missing security header: Cross-Origin-Opener-Policy
```



| #10 Robots.txt file |
| --- |
| Severidad: Informativa |
| CVSS: 0.0 |
| Ocurrencias: 2 |

**Recursos Afectados**

http://www.chango.com.ar/robots.txt
https://www.seaboard.com.ar/robots.txt

**Descripción**

Los robots de archivos. txt se utiliza para dar instrucciones a robots web, como los rastreadores del motor de búsqueda, acerca de ubicaciones dentro del sitio web que los robots se permiten, o no se permiten, arrastrar e indexar.
La presencia de los robots. txt no presenta en sí mismo ningún tipo de vulnerabilidad de seguridad. Sin embargo, a menudo se utiliza para identificar áreas restringidas o privadas del contenido de un sitio. Por lo tanto, la información en el archivo puede ayudar a un atacante a mapear el contenido del sitio, especialmente si algunos de los lugares identificados no están vinculados desde otros lugares del sitio. Si la aplicación se basa en robots.txt para proteger el acceso a estas áreas, y no impone un control de acceso adecuado sobre ellas, esto presenta una grave vulnerabilidad.

**Impacto**

* [CWE-200: Exposición de información](https://cwe.mitre.org/data/definitions/200.html)

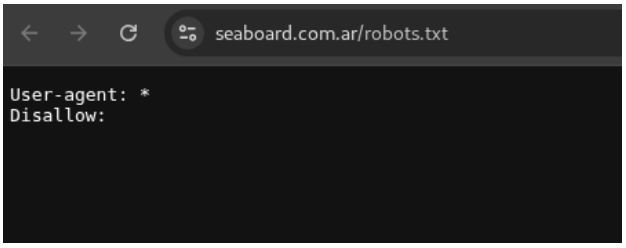
**Solución**

Los robots. txt file no es en sí mismo una amenaza de seguridad, y su uso correcto puede representar una buena práctica por razones de no seguridad. Usted no debe asumir que todos los robots web honrarán las instrucciones del archivo. Más bien, asuma que los atacantes prestarán mucha atención a cualquier lugar identificado en el archivo. No confíes en robots. txt para proporcionar cualquier tipo de protección sobre el acceso no autorizado.

**Evidencias**

Recurso: https://www.seaboard.com.ar/robots.txt

```
The web server contains a robots.txt file.
```




Recurso: http://www.chango.com.ar/robots.txt

```
The web server contains a robots.txt file.
```


| #11 List of Web Directories Requiring Authentication |
|---|
| Severidad: Informativa |
| CVSS: 0.0 |
| Ocurrencias: 1 |

**Recursos Afectados**

64.181.187.204 Puerto: TCP/8003

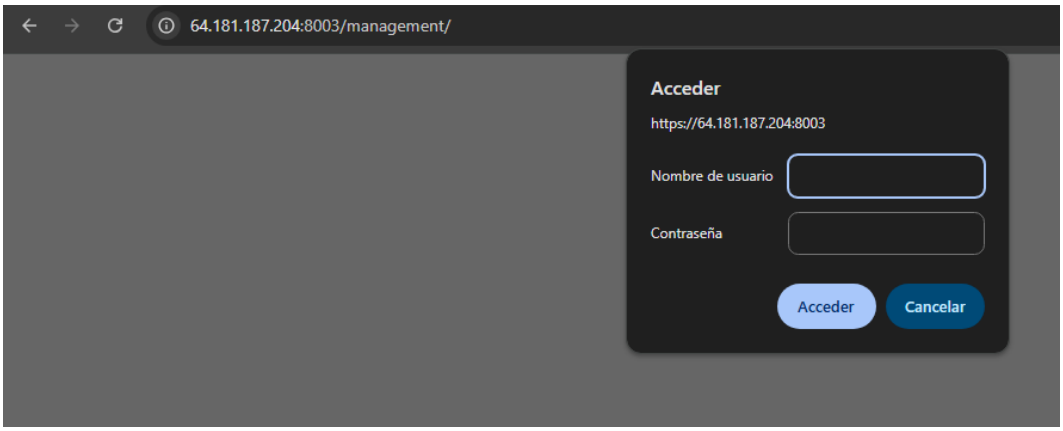
**Descripción**

El servicio ha identificado una lista de directorios Web que requieren autenticación para acceder.

**Evidencias**

Recurso: 64.181.187.204 Puerto: TCP/8003

```
Directories Requiring Authentication
/management/
```



## #12 Firewall Detected

Severidad: Informativa

CVSS: 0.0

Ocurrencias: 6

**Recursos Afectados**

136.248.107.125
164.152.54.25
201.234.138.85
64.181.187.204
64.76.31.49
64.76.31.50

**Descripción**

Se identificó la presencia de un dispositivo de filtrado de paquetes (firewall) que afecta el comportamiento de los paquetes enviados a ciertos puertos o protocolos. Esto se evidenció por la falta de respuesta o por respuestas inconsistentes en comparación con puertos cerrados convencionales, lo que permite inferir que un sistema de seguridad está procesando o bloqueando activamente el tráfico.

**Impacto**

Aunque es una medida defensiva, su detección permite inferir la existencia de políticas de filtrado y facilita el reconocimiento de red por parte de un atacante.

**Solución**

Configurar el firewall para no distinguir entre puertos cerrados y filtrados (usar DROP en lugar de REJECT), y aplicar políticas de mínimo privilegio sobre los puertos expuestos.

**Evidencias**

Recurso: 64.76.31.50

```
Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 111, 135, 445, 1.
Firewall responded to TCP probes sent to port 113 with RST packets (hopcount to firewall 6
vs hopcount to target 7).

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-79,81-112,114-442,444-6128,6130-65535
```

Recurso: 64.76.31.49

```
Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 445.
Firewall responded to TCP probes sent to port 113 with RST packets (hopcount to firewall 6
vs hopcount to target 7).

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-112,114-178,180-442,444-6128,6130-65535
```

Recurso: 201.234.138.85

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-112,114-178,180-1705,1707-1999,2001-2146,2148-2512,2514-2701,2703-3388,
3390-5630,5632-6128,6130-8002,8004-42423,42425-65535
```

Recurso: 136.248.107.125

```
Some of the ports filtered by the firewall are: 20, 21, 23, 25, 53, 80, 111, 135, 445, 1.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-21,23-381,383-442,444-1521,1523-6128,6130-65535
```

Recurso: 164.152.54.25

```
Some of the ports filtered by the firewall are: 20, 21, 23, 25, 53, 80, 111, 135, 445, 1.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-21,23-381,383-442,444-4432,4434-6128,6130-65535
```

Recurso: 64.181.187.204

```
Some of the ports filtered by the firewall are: 20, 21, 23, 25, 53, 80, 111, 135, 445, 1.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-21,23-381,383-442,444-6128,6130-8002,8004-65535
```

## #13 Target Network Information

| |
|---|
| Severidad: Informativa |
| CVSS: 0.0 |
| Ocurrencias: 3 |

**Recursos Afectados**

136.248.107.125
164.152.54.25
64.181.187.204

**Descripción**

La información mostrada en la sección Resultado fue devuelta por la infraestructura de red responsable del tráfico de enrutamiento desde nuestra plataforma cloud a la red de destino (donde se encuentra el aparato del escáner).
Esta información fue devuelta de: 1) el servicio WHOIS, o 2) la infraestructura proporcionada por el servidor de gateway más cercano a nuestra plataforma cloud. Si su ISP está descomponiendo el tráfico, el servidor de la puerta de entrada de su ISP devolvió esta información.

**Impacto**

Esta información puede ser utilizada por usuarios maliciosos para reunir más información sobre la infraestructura de red que puede ayudar a lanzar ataques contra ella.

**Solución**

N/A

**Evidencias**

Recurso: 136.248.107.125

```
The network handle is: ORACLE-4
Network description:
Oracle Corporation
```

Recurso: 164.152.54.25

```
The network handle is: ORACLE-4
Network description:
Oracle Corporation
```

Recurso: 64.181.187.204

```
The network handle is: ORCL-SLDC-1
Network description:
Oracle Corporation
```

## #14 Open TCP Services List

| |
|---|
| Severidad: Informativa |
| CVSS: 0.0 |
| Ocurrencias: 6 |

**Recursos Afectados**

136.248.107.125
164.152.54.25
201.234.138.85
64.181.187.204
64.76.31.49
64.76.31.50

**Descripción**

Se identificaron servicios accesibles mediante conexiones TCP en el perímetro de red, visibles durante el reconocimiento activo. La sección de Resultados muestra el número de puerto (Port), el servicio predeterminado que escucha en el puerto (IANA Assigned Ports/Services), la descripción del servicio (Descripción) y el servicio que el escáner detectó mediante el descubrimiento del servicio (Service Detected).

**Impacto**

La exposición de servicios TCP permite a un atacante ampliar la superficie de ataque y buscar vulnerabilidades asociadas a cada servicio detectado.

**Solución**

Limitar la exposición solo a los servicios necesarios, aplicar hardening y monitoreo sobre los puertos abiertos, y cerrar aquellos que no estén en uso.

**Evidencias**

Recurso: 64.76.31.50

```
Port IANA Assigned Ports/Services Description    Service Detected      OS On Redirected Port
80   www-http       World Wide Web HTTP   http
443  https   http protocol over TLS/SSL   http over ssl
```

```
64.76.31.50      80    tcp    http           open      Citrix NetScaler https redirect
64.76.31.50      179   tcp    bgp            filtered
64.76.31.50      443   tcp    https          open
64.76.31.50      1522  tcp    rna-lm         filtered
64.76.31.50      2000  tcp    cisco-sccp     filtered
64.76.31.50      4443  tcp    pharos         filtered
64.76.31.50      5060  tcp    sip            filtered
64.76.31.50      8003  tcp    mcreport       filtered
```

Recurso: 64.76.31.49

```
Port IANA Assigned Ports/Services Description    Service Detected      OS On Redirected Port
179  bgp     Border Gateway Protocol      unknown
443  https   http protocol over TLS/SSL   http over ssl
```

```
64.76.31.49      80    tcp    http            filtered
64.76.31.49      179   tcp    bgp             filtered
64.76.31.49      443   tcp    https           open
64.76.31.49      1522  tcp    rna-lm          filtered
64.76.31.49      2000  tcp    cisco-sccp      filtered
64.76.31.49      4443  tcp    pharos          filtered
64.76.31.49      5060  tcp    sip             filtered
```

Recurso: 201.234.138.85

```
Port IANA Assigned Ports/Services Description    Service Detected      OS On Redirected Port
179 bgp     Border Gateway Protocol      unknown
8003 unknown unknown http over ssl
```

```
201.234.138.85   80    tcp    http            filtered
201.234.138.85   179   tcp    bgp             filtered
201.234.138.85   443   tcp    https           filtered
201.234.138.85   1522  tcp    rna-lm          filtered
201.234.138.85   2000  tcp    cisco-sccp      filtered
201.234.138.85   4443  tcp    pharos          filtered
201.234.138.85   5060  tcp    sip             filtered
201.234.138.85   8003  tcp    mcreport        open
```

Recurso: 136.248.107.125

```
Port IANA Assigned Ports/Services Description    Service Detected      OS On Redirected Port
1522 ricardo-lm     Ricardo North America License Manager      oracle over ssl
```

```
136.248.107.125  80    tcp    http            filtered
136.248.107.125  179   tcp    bgp             filtered
136.248.107.125  443   tcp    https           filtered
136.248.107.125  1522  tcp    ssl/oracle-tns  open      Oracle TNS Listener unauthorized
136.248.107.125  2000  tcp    cisco-sccp      filtered
136.248.107.125  4443  tcp    pharos          filtered
136.248.107.125  5060  tcp    sip             filtered
136.248.107.125  8003  tcp    mcreport        filtered
```

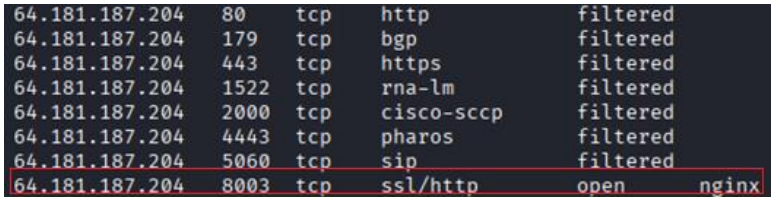
Recurso: 164.152.54.25

```
Port IANA Assigned Ports/Services Description    Service Detected      OS On Redirected Port
443 https  http protocol over TLS/SSL   http over ssl
4433 unknown unknown http over ssl
```

```
164.152.54.25    80    tcp    http            filtered
164.152.54.25    179   tcp    bgp             filtered
164.152.54.25    443   tcp    ssl/https       open
164.152.54.25    1522  tcp    rna-lm          filtered
164.152.54.25    2000  tcp    cisco-sccp      filtered
164.152.54.25    4433  tcp    vop             open
164.152.54.25    4443  tcp    pharos          filtered
164.152.54.25    5060  tcp    sip             filtered
164.152.54.25    8003  tcp    mcreport        filtered
```

Recurso: 64.181.187.204

```
Port IANA Assigned Ports/Services Description    Service Detected      OS On Redirected Port
8003 unknown unknown http over ssl
```



```
64.181.187.204   80    tcp    http           filtered
64.181.187.204   179   tcp    bgp            filtered
64.181.187.204   443   tcp    https          filtered
64.181.187.204   1522  tcp    rna-lm         filtered
64.181.187.204   2000  tcp    cisco-sccp     filtered
64.181.187.204   4443  tcp    pharos         filtered
64.181.187.204   5060  tcp    sip            filtered
64.181.187.204   8003  tcp    ssl/http       open       nginx
```

## #15 Default Web Page

| |
|---|
| Severidad: Informativa |
| CVSS: 0.0 |
| Ocurrencias: 8 |

**Recursos Afectados**

164.152.54.25 Puerto: TCP/443
164.152.54.25 Puerto: TCP/4433
201.234.138.85 Puerto: TCP/8003
64.181.187.204 Puerto: TCP/8003
64.76.31.49 Puerto: TCP/443
64.76.31.50 Puerto: TCP/443
64.76.31.50 Puerto: TCP/80
www.seaboard.com.ar Puerto: 443

**Descripción**

Se muestra la página Web predeterminada para el servidor Web.

**Solución**

Restringir o bloquear cualquier servicio expuesto que no se esté usando o sea desconocido.

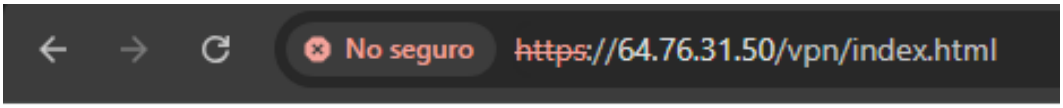
**Evidencias**

Recurso: 64.76.31.50 Puerto: TCP/443

```
GET / HTTP/1.1
Host: 64-76-31-50.static.impsat.net.ar
Connection: Keep-Alive



<html><head><META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=UTF-8"><script
type="text/javascript" src="/vpn/resources.js"></script><script type="text/javascript"
src="/vpn/init/redirection_body_resources.js"></script></head><body><span id="This object
may be found "></span><a href="/vpn/index.html"><span id="here"></span></a><span
id="Trailing phrase after here"></span></body></html>
```




**Http/1.1 Internal Server Error 43531**

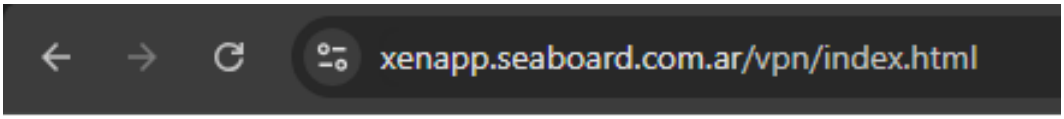
Recurso: 64.76.31.50 Puerto: TCP/80

```
GET / HTTP/1.1
Host: 64-76-31-50.static.impsat.net.ar
Connection: Keep-Alive



HTTP/1.1 302 Object Moved
Location: https://xenapp.seaboard.com.ar/
Content-Type: text/html
Cache-Control: private
Connection: close

<head><body> This object may be found <a HREF="https://xenapp.seaboard.com.ar/">here</a>
</body>
```



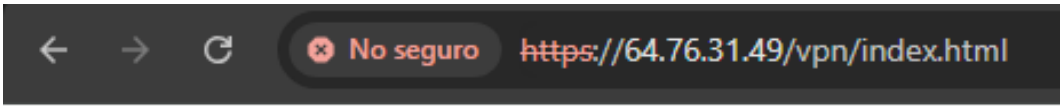

**Http/1.1 Internal Server Error 43531**

Recurso: 64.76.31.49 Puerto: TCP/443

```
GET / HTTP/1.1
Host: 64-76-31-49.static.impsat.net.ar
Connection: Keep-Alive



<html><head><META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=UTF-8"><script
type="text/javascript" src="/vpn/resources.js"></script><script type="text/javascript"
src="/vpn/init/redirection_body_resources.js"></script></head><body><span id="This object
may be found "></span><a href="/vpn/index.html"><span id="here"></span></a><span
id="Trailing phrase after here"></span></body></html>
```




**Http/1.1 Internal Server Error 43531**

Recurso: 201.234.138.85 Puerto: TCP/8003

```
GET / HTTP/1.1
Host: 201.234.138.85:8003
Connection: Keep-Alive



<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Bad Request</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Bad Request - Invalid Hostname</h2>
<hr><p>HTTP Error 400. The request hostname is invalid.</p>
</BODY></HTML>
```


**Bad Request - Invalid Hostname**

HTTP Error 400. The request hostname is invalid.

Recurso: 164.152.54.25 Puerto: TCP/443

```
GET / HTTP/1.1
Host: 164.152.54.25
Connection: Keep-Alive



{"code":404,"message":"Not Found"}
```


Recurso: 164.152.54.25 Puerto: TCP/4433

```
GET / HTTP/1.1
Host: 164.152.54.25:4433
Connection: Keep-Alive



{"code":404,"message":"Not Found"}
```


Recurso: 64.181.187.204 Puerto: TCP/8003

```
GET / HTTP/1.1
Host: 64.181.187.204:8003
Connection: Keep-Alive



<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Draft//EN">
<HTML>
<HEAD>
<TITLE>Error 404--Not Found</TITLE>
</HEAD>
<BODY bgcolor="white">
<FONT FACE=Helvetica><BR CLEAR=all>
<TABLE border=0 cellspacing=5><TR><TD><BR CLEAR=all>
<FONT FACE="Helvetica" COLOR="black" SIZE="3"><H2>Error 404--Not Found</H2>
</FONT></TD></TR>
</TABLE>
<TABLE border=0 width=100% cellpadding=10><TR><TD VALIGN=top WIDTH=100% BGCOLOR=white><FONT
FACE="Courier New"><FONT FACE="Helvetica" SIZE="3"><H3>From RFC 2068 <i>Hypertext Transfer
Protocol -- HTTP/1.1</i>:</H3>
</FONT><FONT FACE="Helvetica" SIZE="3"><H4>10.4.5 404 Not Found</H4>
</FONT><P><FONT FACE="Courier New">The server has not found anything matching the Request-
URI. No indication is given of whether the condition is temporary or permanent.</p><p>If the
server does not wish to make this information available to the client, the status code 403
(Forbidden) can be used instead. The 410 (Gone) status code SHOULD be used if the server
```

```
knows, through some internally configurable mechanism, that an old resource is permanently
unavailable and has no forwarding address.</FONT></P>
</FONT></TD></TR>
</TABLE>

</BODY>
</HTML>
```


**Error 404--Not Found**

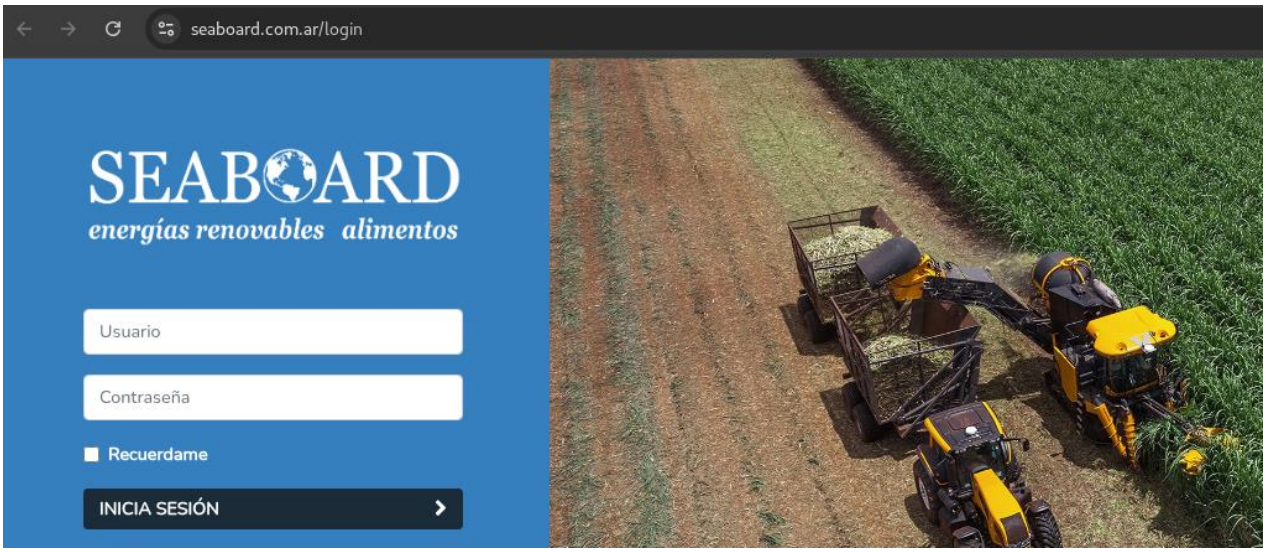
**From RFC 2068 *Hypertext Transfer Protocol -- HTTP/1.1*:**

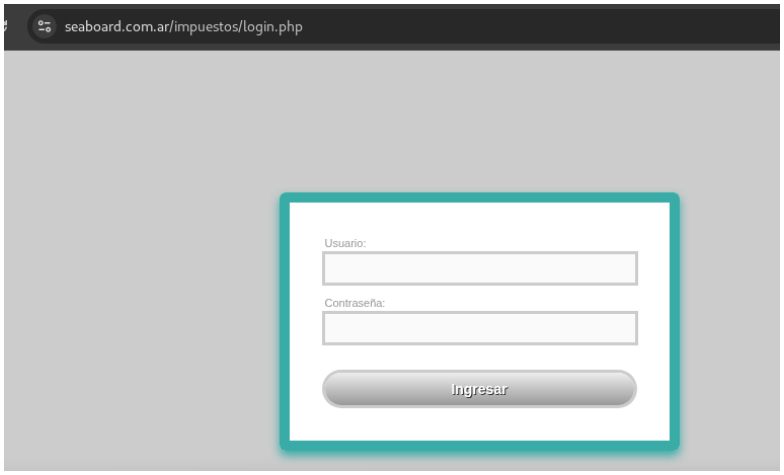
**10.4.5 404 Not Found**

The server has not found anything matching the Request-URI. No indication is given of whether the condition is temporary or permanent.

If the server does not wish to make this information available to the client, the status code 403 (Forbidden) can be used instead. The 410 (Gone) status code SHOULD be used if the server knows, through some internally configurable mechanism, that an old resource is permanently unavailable and has no forwarding address.

Recurso: www.seaboard.com.ar Puerto: 443




seaboard.com.ar/impuestos/login.php
Usuario:
Contraseña:
Ingresar


https://pedidos.seaboard.com.ar/Account/LogOn?ReturnUrl=%2fOrder
SEABOARD
energías renovables · alimentos
Ingreso de Pedidos
Inicio de Sesión
Información de la Cuenta
Usuario
Contraseña
Recordar Usuario
Aceptar
Ingreso de Pedidos - ver. 4.5 | Dirmod Copyright © 2015

| #16 HTTP TRACE method is enabled |
| --- |
| Severidad: Informativa |
| CVSS: 0.0 |
| Ocurrencias: 1 |

**Recursos Afectados**
https://www.chango.com.ar/

**Descripción**
El método HTTP TRACE está diseñado para fines de diagnóstico. Si está habilitado, el servidor web responderá a solicitudes que utilizan el método TRACE haciendo eco en su respuesta de la solicitud exacta recibida.

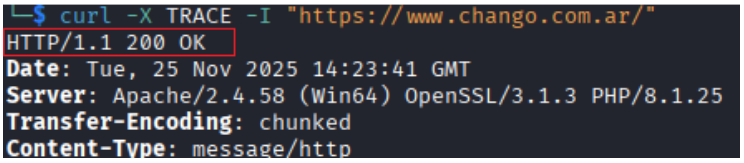
Este comportamiento es a menudo inofensivo, pero ocasionalmente conduce a la divulgación de información sensible como los encabezados de autenticación interna aprehendidos por proxies inversos. Esta funcionalidad podría utilizarse históricamente para evitar la bandera de cookies HttpOnly en las cookies, pero esto ya no es posible en los navegadores web modernos.

**Impacto**
* [CWE-16: Configuration](https://cwe.mitre.org/data/definitions/16.html)

**Referencias**
* [Web Security Academy: Information disclosure via TRACE method](https://portswigger.net/web-security/information-disclosure/exploiting#information-disclosure-due-to-insecure-configuration)

**Solución**
El método TRACE debe desactivarse en servidores web de producción.

**Evidencias**
Recurso: https://www.chango.com.ar/



| #17 WordPress Plugins Detected |
| --- |
| Severidad: Informativa |
| CVSS: 0.0 |
| Ocurrencias: 1 |

**Recursos Afectados**

www.chango.com.ar

**Descripción**

Este es un aviso informativo que el escáner fue capaz de detectar uno o más plugins de WordPress instalados.

**Evidencias**

Recurso: www.chango.com.ar

```
add-search-to-menu [!] The version is out of date, the latest version is 5.5.12

custom-post-type-ui [!] The version is out of date, the latest version is 1.18.1

duplicator [!] The version is out of date, the latest version is 1.5.14

ewww-image-optimizer [!] The version is out of date, the latest version is 8.3.0

google-authenticator  [!] Google Authenticator <= 0.47 - Two Factor Authentication Bypass

mw-wp-form [!] Titles: MW WP Form < 4.4.3 - Unauthenticated Path Traversal, MW WP Form <
5.0.0 - Missing Authorization, MW WP Form < 5.0.2 - Unauthenticated Arbitrary File Upload,
MW WP Form < 5.0.4 - Improper Limitation of File Name to Unauthenticated Arbitrary File
Deletion, MW WP Form < 5.1.0 - Editor+ Stored XSS

schema-and-structured-data-for-wp [!] Title: Schema & Structured Data for WP & AMP < 1.52 -
Authenticated (Contributor+) Stored Cross-Site Scripting

updraftplus Titles: UpdraftPlus < 1.24.12 - Unauthenticated PHP Object Injection,
UpdraftPlus - Backup/Restore < 1.25.1 - Reflected XSS

w3-total-cache Titles: W3 Total Cache < 2.8.2 - Subscriber+ Server-Side Request Forgery, W3
Total Cache < 2.8.2 - Information Exposure via Log Files, W3 Total Cache < 2.8.2 -
Unauthenticated Plugin Deactivation and Extensions Activation/Deactivation, W3 Total Cache <
2.8.13 - Unauthenticated Command Injection

wordpress-seo [!] The version is out of date, the latest version is 26.4

wp-all-import [!] Titles: Import any XML, CSV or Excel File to WordPress < 3.9.4 - Admin+
Limited Unsafe File Upload, Import any XML, CSV or Excel File to WordPress < 4.0.0 - Admin+
Remote Code Execution via Conditional Logic

wp-crontrol [!] The version is out of date, the latest version is 1.19.3

wp-file-manager [!] Title: Multiple elFinder Plugins - Arbitrary File Deletion via Traversal

wp-mail-smtp [!] The version is out of date, the latest version is 4.7.0

yith-woocommerce-compare [!] Titles: YITH WooCommerce Compare < 2.1.0 - Unauthenticated PHP
Object injection,  YIT Plugin Framework < 3.3.13 - Subscriber+ Settings Updatem, Multiple
YITH WooCommerce plugins - Cross-Site Scripting via shortcode ajax, YITH WooCommerce Compare
< 2.38.0 - Cross-Site Request Forgery
```

# Conclusiones

En base a las vulnerabilidades detectadas y el análisis de las mismas, se puede determinar el siguiente nivel de severidad general, dada la existencia de **2** vulnerabilidades con dicha severidad.

| Nivel de Severidad | Alta |
|---|---|

A continuación se ofrece un listado de acciones recomendadas para mejorar la postura de seguridad del sistema y reducir los riesgos de explotación:

| Acciones Recomendadas |
|---|
| Priorizar la remediación según la clasificación de riesgo. |
| Desarrollar un plan de acción para implementar la recomendación o remediación. |
| Realizar un análisis de la causa raíz. |
| Realizar entrenamiento de concientización. |
| Realizar el manejo de excepciones y la aceptación de riesgos para las vulnerabilidades que no se pueden remediar. |
| Volver a realizar el análisis de vulnerabilidades para identificar si las soluciones aplicadas son eficaces para remediar las vulnerabilidades expuestas. |
| Tener en cuenta las soluciones y referencias recomendadas en cada vulnerabilidad expuesta en este informe. |

En base a los resultados obtenidos durante el análisis, se ofrecen las siguientes sugerencias de remediación para abordar y mitigar las vulnerabilidades identificadas:

| Sugerencia de Remediación | Vulnerabilidad Abordada |
|---|---|
| Es necesario revisar la configuración de la API para garantizar que únicamente se exponga la información estrictamente necesaria para su funcionamiento. Se debe implementar un control adecuado de autenticación y autorización en cada endpoint, evitando respuestas que incluyan datos sensibles o internos del sistema. | **#1 Information disclosure via api misconfigurations** |
| Deshabilitar el uso de protocolos (SSLv3, TLS1.0, TLS1.1) y algoritmos de cifrado considerados débiles o vulnerables (DES, 3DES, IDEA, CBC, RC2, RC4, MD5, SHA1), en favor de protocolos criptográficamente más fuertes. | **#2 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)** |
| | **#5 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)** |
| Instalar un certificado de servidor con fechas de inicio y final válidas. | **#3 SSL Certificate - Expired** |
| Instalar un certificado de servidor firmado por una autoridad de certificado de terceros de confianza. | **#4 SSL Certificate - Signature Verification Failed Vulnerability** |
| Asegurar que los mensajes de errores de acceso, o al intentar recuperar la contraseña, no permitan diferenciar si el usuario existe o no en la aplicación | **#6 User enumeration** |
| Revisar la configuración de los servidores web y deshabilitar la funcionalidad de listado de directorios en los mismos. | **#7 Directory Listing** |

| Sugerencia de Remediación | Vulnerabilidad Abordada |
|---|---|
| Es fundamental validar el encabezado Host recibido en cada solicitud, asegurando que coincida únicamente con el dominio legítimo de la aplicación. Para ello, se recomienda implementar una lista blanca de dominios permitidos en el servidor o en la lógica de la aplicación, evitando confiar en valores proporcionados por el cliente. | **#8 Host Header Injection** |
| Verificar la correcta implementación de los atributos de seguridad en los Headers HTTP. | **#9 Frameable response (potential Clickjacking)** |
| Revisar la configuración del firewall aplicando el principio de mínimo privilegio, unificando respuestas a puertos no autorizados y complementando con monitoreo y registros de intentos de escaneo. | **#12 Firewall Detected** |
| Restringir la exposición de puertos a los estrictamente necesarios, asegurando que los servicios asociados estén actualizados, correctamente configurados y monitoreados frente a accesos no autorizados. | **#14 Open TCP Services List** |
| Deshabilitar las páginas por defecto que pueden otorgar más información a un atacante, incluyendo aquellas características útiles en entornos de desarrollo que divulgan información. | **#15 Default Web Page** |

# Recomendaciones Generales

Más allá de los hallazgos obtenidos a través del análisis realizado, resulta crucial establecer un enfoque holístico y multicapa en ciberseguridad. Las recomendaciones que proponemos buscan reforzar su infraestructura de TI y promover una cultura de seguridad resiliente, alineada con las tendencias y prácticas avanzadas del sector, adaptándose así a las dinámicas de un panorama digital que no cesa de cambiar. Recomendamos:

- **Visibilidad, detección y respuesta :** La habilidad para detectar y responder con celeridad a los incidentes de seguridad es fundamental. Contar con un servicio de SOC asegura que esté siempre un paso adelante de los riesgos potenciales.
- **Fortalecimiento de la Infraestructura de Red :** Los puntos débiles identificados en su red pueden fortalecerse de manera significativa a través de Firewalls de última generación y soluciones de seguridad para endpoints. Estas tecnologías son cruciales para una defensa perimetral robusta y ofrecen una protección proactiva contra una variedad de amenazas.
- **Capacitación y Conciencia de Seguridad :** Fomentar la conciencia sobre seguridad entre el personal es esencial, ya que los usuarios informados son la primera línea de defensa. Los programas de formación pueden disminuir de manera significativa el riesgo de brechas de seguridad al educar a los usuarios sobre las mejores prácticas y políticas de seguridad.
- **Análisis Continuo de Vulnerabilidades :** Es vital realizar análisis de vulnerabilidades y pruebas de penetración de forma regular para identificar y mitigar proactivamente las nuevas vulnerabilidades. Esta práctica garantiza la solidez y la adaptabilidad de su infraestructura frente a las amenazas emergentes.
- **Evaluaciones regulares :** Es vital realizar evaluaciones regulares, mantener la seguridad operativa de las plataformas y hardening de los firewalls para protección contra intrusiones. El cumplimiento de los estándares de seguridad es esencial, al igual que revisar los controles de seguridad IT y practicar una gobernanza y gestión de riesgos efectivas. Además, planes de crisis preparados son clave para una respuesta ágil y minimizar impactos en el negocio. Finalmente, tener planes de gestión de crisis bien desarrollados y probados asegura una respuesta rápida y eficaz ante incidentes imprevistos, mitigando los daños y preservando la continuidad del negocio.

Estas recomendaciones están pensadas para ser integradas dentro de un enfoque estratégico de seguridad, garantizando que no solo se atiendan los puntos débiles actuales, sino que también se establezca una base sólida para la seguridad futura. Nuestro equipo de expertos en ciberseguridad está listo para asesorar y apoyar la implementación de estas soluciones, asegurando que su empresa se mantenga a la vanguardia en protección y cumplimiento.

En Telecom, entendemos los desafíos intrincados de la ciberseguridad y estamos equipados para apoyar su empresa en cada paso del camino. Con nuestro portafolio integral y un equipo de profesionales experimentados, nos dedicamos a ayudarlo a alcanzar y mantener una postura de seguridad que no solo responda a las amenazas actuales, sino que también se anticipe y adapte a los riesgos del mañana.

# Actividades Realizadas

Las actividades que se realizaron para el presente análisis se separaron en las etapas descriptas a continuación:

**Etapa 1: Reconocimiento y Enumeración**

En esta etapa se recopiló información sobre los activos informados en el alcance, incluyendo la identificación de rangos de IP, dominios, servidores, y cualquier información pública disponible. La enumeración implica descubrir y mapear activos, servicios y aplicaciones en la red para conformar la superficie de ataque. También se utilizó inteligencia de fuentes abiertas (OSINT) para complementar y ampliar la información obtenida.

Durante el proceso, se detectó que algunos hosts no respondieron a las pruebas iniciales, por lo que no fue posible realizar un análisis detallado sobre ellos.

**Etapa 2: Análisis de Vulnerabilidades**

Se utilizaron diferentes herramientas automatizadas para identificar y evaluar los servicios brindados y el tráfico de red en el sistema objetivo. Este proceso puede incluir análisis de código, escaneo de vulnerabilidades, y evaluación de configuraciones de seguridad. El objetivo es identificar debilidades que podrían ser explotadas por un atacante.
A continuación se listan algunas de las debilidades buscadas, sin ser el presente un listado exhaustivo:

- Detección de vulnerabilidades conocidas asociadas a la versión de software de los servicios instalados.
- Verificación de vulnerabilidades conocidas sobre el sistema operativo de base instalado.
- Detección de falta de actualizaciones (parches).
- Detección de errores de configuración o configuraciones predeterminadas.
- Utilización de algoritmos de cifrado inseguros, o ausencia de cifrado.
- Exposición de información.
- Tratamiento incorrecto de entradas manipuladas por el usuario (XSS, Inyección de comandos o código, etc)
- Detección de falencias en el proceso de autenticación.
- Errores en manejo de sesiones de usuario.
- Posibilidad de generar ataques de fuerza bruta.
- Credenciales predeterminadas o conocidas.
- Control de acceso inadecuado o inexistente.

**Etapa 3: Modelado de Amenazas**

Se utilizaron todos los datos recopilados en las fases anteriores para determinar la posibilidad de explotación. Se determinó el riesgo de las vulnerabilidades descubiertas durante esta fase utilizando principalmente la National Vulnerability Database (NVD), creada y mantenida por el gobierno de EE.UU. que analiza las vulnerabilidades de software publicadas en la base de datos Common Vulnerabilities and Exposures (CVE). La NVD clasifica la gravedad de las vulnerabilidades utilizando el Sistema de Puntuación de Vulnerabilidades Comunes (CVSS). Esta etapa se complementó con verificaciones manuales sobre estos equipos a fin de eliminar los “falsos positivos” y corroborar las detecciones.

**Etapa 4: Explotación**

En esta etapa se intentaron explotar las vulnerabilidades identificadas para evaluar la resistencia del sistema a ataques reales. Se buscó determinar si las contramedidas de seguridad eran efectivas y si las vulnerabilidades podían ser explotadas con éxito para validar la profundidad y el alcance de las mismas.

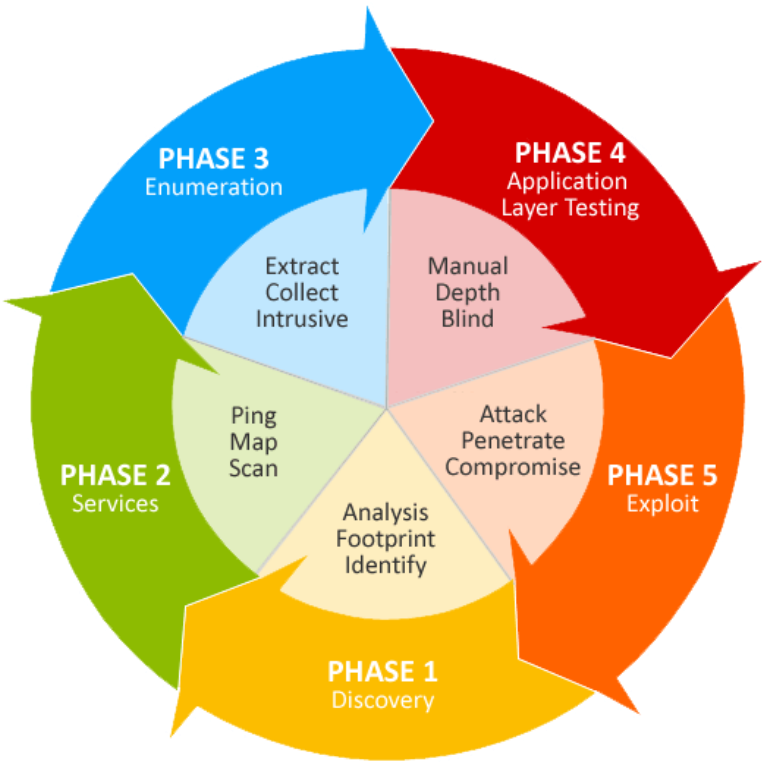
**Etapa 5: Informes**

Una vez finalizadas las etapas de análisis, se generó un informe ejecutivo con un resumen gerencial de los hallazgos y equipos detectados, junto a un informe técnico donde se describen las vulnerabilidades, detallando el nivel de riesgo asociado, el impacto que estas pudieran tener en la seguridad, las recomendaciones de

solución correspondientes, evidencia de las mismas y toda información adicional que fuera considerada útil para su identificación y corrección.

# Anexo 1: Metodología

El enfoque utilizado se basa en el Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM), e incluye una combinación de pruebas automatizadas (cuando es posible) y de inspección manual (cuando sea necesario) de los servicios expuestos. El OSSTMM es un estándar ampliamente reconocido y utilizado en la industria de la seguridad informática. Fue desarrollado y publicado inicialmente por el ISECOM (Institute for Security and Open Methodologies) en el año 2001. Proporciona un marco completo y estructurado para llevar a cabo pruebas de penetración y evaluación de la seguridad en sistemas, redes y aplicaciones.




OSSTMM proporciona una serie de escenarios de prueba, técnicas y herramientas para realizar evaluaciones exhaustivas de seguridad. Está diseñado para ser utilizado por profesionales de la seguridad, equipos de pruebas de penetración y auditores de seguridad para identificar vulnerabilidades, evaluar la efectividad de las políticas de seguridad y proporcionar recomendaciones para fortalecer la infraestructura de una organización. Gracias a su enfoque cuantitativo y en detalle, el OSSTMM ha sido adoptado por muchas empresas y organizaciones como una metodología confiable para mejorar la seguridad informática y proteger los activos críticos.

Si bien se trata de un proceso mayoritariamente manual, durante el análisis se utilizaron una serie de herramientas automatizadas que permitieron disminuir los tiempos necesarios para la finalización de las tareas, como así también permitieron la manipulación del tráfico enviado a los servicios analizados.

# Anexo 2: Herramientas

Durante el presente análisis se utilizó un amplio conjunto de herramientas especializadas que nos permiten evaluar la seguridad de sistemas y redes. Se presenta un listado no exhaustivo de las mismas:

- Qualys: Scanner de vulnerabilidades utilizado para la detección de parches faltantes, errores de configuración y configuraciones por defecto en el sistema operativo y servicios que corren en los servidores analizados. Posee más de 55.000 plugins que detectan cada uno una vulnerabilidad en particular.
- Tenable Web App Scanning: plataforma de pruebas de seguridad de aplicaciones dinámicas (DAST). Rastrea una aplicación web en ejecución a fin de crear un mapa del sitio para luego identificar cualquier vulnerabilidad en la aplicación o vulnerabilidades conocidas en los componentes de terceros.
- Burp Suite: Suite de herramientas para pruebas de seguridad de aplicaciones web, incluyendo escaneo de vulnerabilidades y manipulación de solicitudes y respuestas.
- Metasploit: Framework para pruebas de penetración que proporciona módulos de explotación y post-explotación para diversas vulnerabilidades.
- SQLMap: Herramienta para explotar y detectar vulnerabilidades de inyección SQL en aplicaciones web y bases de datos.
- Nmap: Herramienta de escaneo de red utilizada para descubrir hosts y servicios, así como para evaluar la seguridad y configuración de los dispositivos conectados.
- ZAP Proxy: Software de código abierto desarrollado por el proyecto OWASP, diseñado para realizar pruebas de penetración y análisis exhaustivo de vulnerabilidades en aplicaciones web.
- Programas internos: Scripts desarrollados por el área de Ethical Hacking para efectuar el análisis de determinadas configuraciones y confirmar vulnerabilidades encontradas.

# Anexo 3: Clasificación del Riesgo

La evaluación de cada vulnerabilidad se calcula a través del CVSS (Common Vulnerability Scoring System). CVSS es un sistema estandarizado y de código abierto utilizado para evaluar y clasificar la gravedad de las vulnerabilidades informáticas. Fue desarrollado para proporcionar una medida cuantitativa y objetiva de la severidad de una vulnerabilidad, ayudando a los equipos de seguridad a priorizar las acciones de mitigación, lo que permite una respuesta más efectiva y coordinada ante posibles amenazas.
El CVSS se compone de un conjunto de métricas que consideran diferentes aspectos de la vulnerabilidad:

**AV: Attack Vector**
Representa cómo un atacante podría explotar la vulnerabilidad

- AV:N (Network) : El ataque se realiza a través de la red (por ejemplo Internet).
- AV:A (Adjacent) : El ataque se realiza desde una red adyacente (por ejemplo, una red local).
- AV:L (Local) : El ataque se realiza de manera local en el sistema afectado.
- AV:P (Physical) : El atacante necesita acceso físico al sistema para explotar la vulnerabilidad.

**AC: Attack Complexity**
Describe la complejidad del ataque necesario para explotar la vulnerabilidad.

- AC:L (Low) : El ataque es sencillo y no requiere condiciones especiales.
- AC:H (High) : El ataque es complicado y puede requerir condiciones adicionales o conocimientos técnicos específicos.

**PR: Privileges Required**
Indica los privilegios previos necesarios para explotar la vulnerabilidad.

- PR:N (None) : No se requieren privilegios adicionales para explotar la vulnerabilidad.
- PR:L (Low) : Se requieren privilegios limitados (por ejemplo, acceso de usuario).
- PR:H (High) : Se requieren privilegios elevados (por ejemplo, acceso de administrador).

**UI: User Interaction**
Describe si la explotación de la vulnerabilidad requiere la interacción de un usuario del sistema afectado.

- UI:N (None) : No se requiere interacción de un usuario para explotar la vulnerabilidad
- UI:R (Required) : Se requiere la interacción activa de un usuario para que el ataque tenga éxito.

**S: Scope**
Indica el alcance de la vulnerabilidad.

- S:U (Unchanged) : La vulnerabilidad solo afecta a los recursos directamente afectados por la explotación.
- S:C (Changed) : La vulnerabilidad afecta a componentes adicionales o recursos controlados por el mismo autor del ataque.

**C: Confidentiality Impact**
Describe el impacto de la vulnerabilidad en la confidencialidad de los datos.

- C:N (None) : No hay impacto en la confidencialidad. La vulnerabilidad no afecta la confidencialidad de los datos.
- C:L (Low) : El impacto en la confidencialidad es bajo. La explotación de la vulnerabilidad podría resultar en la divulgación limitada de información sensible o datos confidenciales.
- C:H (High) : El impacto en la confidencialidad es alto. La explotación de la vulnerabilidad podría resultar en la divulgación significativa o completa de información sensible o datos confidenciales.

**I: Integrity Impact**
Indica el impacto de la vulnerabilidad en la integridad de los datos.

- I:N (None) : No hay impacto en la integridad. La vulnerabilidad no afecta la integridad de los datos.
- I:L (Low) : El impacto en la integridad es bajo. La explotación de la vulnerabilidad podría resultar en una alteración limitada o superficial de los datos o información del sistema.
- I:H (High) : El impacto en la integridad es alto. La explotación de la vulnerabilidad podría resultar en una alteración significativa o completa de los datos o información del sistema.

**A: Availability Impact**
Describe el impacto de la vulnerabilidad en la disponibilidad de los recursos.

- A:N (None) : No hay impacto en la disponibilidad. La vulnerabilidad no afecta la disponibilidad de los recursos o servicios.
- A:L (Low) : El impacto en la disponibilidad es bajo. La explotación de la vulnerabilidad podría resultar en una degradación temporal o parcial de los recursos o servicios.
- A:H (High) : El impacto en la disponibilidad es alto. La explotación de la vulnerabilidad podría resultar en una interrupción completa o prolongada de los recursos o servicios, afectando significativamente su disponibilidad.