# Informe de Pentesting – Vulnerabilidad de Indexación Web

**Fecha de elaboración:** 16 de junio de 2025

**Responsable del análisis:** Alan Alvarado Ramírez

## 1. Objetivo

Detectar y demostrar la existencia de una vulnerabilidad en un servicio web expuesto por un servidor Debian (en una VM) y aplicar la mitigación correspondiente. El objetivo principal fue evaluar si el servidor permitía indexación de directorios web, una mala configuración que expone archivos internos, explotarla y remediarla.

## 2. Metodología

La metodología que se suguió en este informe es la siguiente:

1.- Detección

2.- Confirmación

3.- Explotación

4.- Remdiación

### *2.1 Detección de vulnerabilidades con nmap*

Se utilizó la herramienta nmap incorporada en la máquina virtual de kali linux para identificar servicios expuestos y posibles vulnerabilidades:

- Se ejecutó:

  nmap -sV –script=vuln 192.168.1.#

- Se detectó que el puerto 80 (http) estaba abierto con el servidor “Apache2” activo y se identificó como vulnerable a la indexación del directorio.

```
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-phpmyadmin-dir-traversal:
|   VULNERABLE:
|   phpMyAdmin grab_globals.lib.php subform Parameter Traversal Local File Inclusion
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2005-3299
|       PHP file inclusion vulnerability in grab_globals.lib.php in phpMyAdmin 2.6.4 and 2.6.4-pl1 allows r
emote attackers to include local files via the $__redirect parameter, possibly involving the subform array.
|
|     Disclosure date: 2005-10-nil
|     Extra information:
|       ../../../../../etc/passwd not found.
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3299
|_      http://www.exploit-db.com/exploits/1244/
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /readme.html: Wordpress version: 2
|   /wp-includes/images/rss.png: Wordpress version 2.2 found.
|   /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|   /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|   /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|_  /readme.html: Interesting, a readme.
MAC Address: 08:00:27:99:E6:A9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 79.82 seconds
```

*2.2 Confirmación de la vulnerabilidad*

Se utilizó el script “http-enum” para buscar algunas rutas expuestas en donde comenzar la búsqueda de información:

- Se ejecutó:

  nmap -p 80 –script http-enum 192.168.1.101

  El resultado indicó que el servidor estaba permitiendo listar archivos internos de los directorios del servidor web.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -p 80 --script http-enum 192.168.1.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-13 23:18 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00096s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /readme.html: Wordpress version: 2
|   /wp-includes/images/rss.png: Wordpress version 2.2 found.
|   /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|   /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|   /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|_  /readme.html: Interesting, a readme.
MAC Address: 08:00:27:99:E6:A9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.87 seconds
```

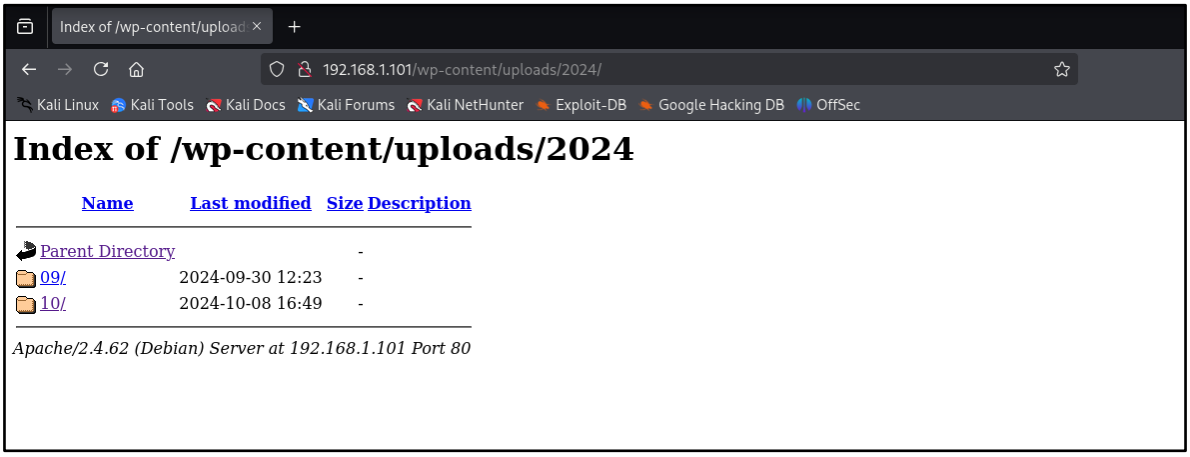
### *2.3 Prueba manual mediante la exploración por el navegador web*

Se accedió a diversas rutas (directorios del servidor) mediante el navegador web hasta que se encontró una ruta con archivos expuestos:

- Se ingresó a:

  http://192.168.1.101/wp-content/

  Se confirmó que el contenido del directorio era visible sin restricciones, evidenciando una vulnerabilidad de indexación habilitada por apache.




# 3. Análisis del impacto

La indexación de directorios puede permitir que un atacante:

- Descubrir archivos sensibles (como respaldos).
- Descargar shells PHP subidos a través de WordPress.
- Analizar la estructura interna del sitio para buscar rutas útiles para otros ataques.
- Encontrar archivos de configuración que contengan credenciales.

# 4. Mitigación

### *4.1 Verificación de la configuración de Apache2*

Se ejecutó el siguiente comando para localizar el archivo de configuración de apache actual:

- Se ejecutó:

sudo apache2ctl -S

Donde se descubre la ruta padre dónde buscar el archivo “.config” (“/etc/apache2/”)

```
debian@debian:~$ sudo apache2ctl -S
[sudo] password for debian:
VirtualHost configuration:
*:80                   debian.debian (/etc/apache2/sites-enabled/000-default.con
f:1)
ServerRoot: "/etc/apache2"
Main DocumentRoot: "/var/www/html"
Main ErrorLog: "/var/log/apache2/error.log"
Mutex default: dir="/var/run/apache2/" mechanism=default
Mutex mpm-accept: using_defaults
Mutex watchdog-callback: using_defaults
Mutex rewrite-map: using_defaults
PidFile: "/var/run/apache2/apache2.pid"
Define: DUMP_VHOSTS
Define: DUMP_RUN_CFG
User: name="www-data" id=33
Group: name="www-data" id=33
debian@debian:~$
```

### *4.2 Modificación de la configuración de Apache2*

Después de explorar el directorio padre, se encontró el archivo que contiene la configuraciones “apache2.config” y se abre para editar con nao y permisos de superusuario.

- Se ejecutó:

  sudo nano /etc/apache2/apache2.config

  En este archivo se descubre que tiene líneas que permiten la indexación de directorios.

```
# access here, or in any related virtual host.
<Directory />
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>

<Directory /usr/share>
        AllowOverride None
        Options Indexes FollowSymLinks
        Require all granted
</Directory>

<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

Se comentan la líneas que permiten la indexación y se guarda el archivo:

```
# access here, or in any related virtual host.
<Directory />
        #Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>

<Directory /usr/share>
        AllowOverride None
        Options Indexes FollowSymLinks
        Require all granted
</Directory>

<Directory /var/www/>
        #Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

### *4.3 Reinicio del servicio de Apache*

Después de guardar los cambios en el archivo de configuración de apache, se procede a reiniciar el servicio para que los cambios efectuados surtan efecto.

- Se ejecutó:

  sudo systemctl restart apache2

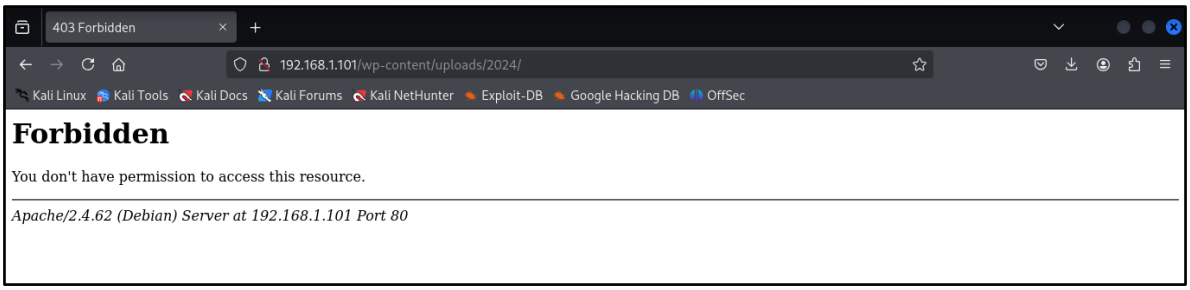
```
debian@debian:/etc/apache2$ sudo systemctl restart apache2
debian@debian:/etc/apache2$
```

### *4.4 Verificación final*

Se intentó acceder de nuevo a la ruta anteriormente vulnerable:

http://192.168.1.101/wp-content/uploads/2024/

Se comprueba que ya no muestra los archivos y muestra un mensaje de “Forbidden”, confirmando que la vulnerabilidad ha sido corregida exitosamente.




# 5. Conclusión

Durante la evaluación se identificó que el servidor permitía la indexación automática de directorios web, exponiendo potencialmente archivos sensibles y abriendo al camino para que los atacantes realizaran su ataques de forma más sencilla. Gracias a la rápida intervención y mitigación, la vulnerabilidad fue corregida con éxito al ajustar la configuración de Apache y reiniciar el servicio correspondiente. Cabe recalcar que este informe solo abarca una vulnerabilidad, pero con la herramienta nmap se encontraron más de 15 vulnerabilidades, por lo cual es necesario atender y mitigar cada una de las demás vulnerabilidades.

# 6. Recomendaciones

- Mitigar las demás vulnerabilidades no abordadas en este informe, pero si presentes en el servidor.
- Aunque algunas de las rutas mostradas como expuestas con la herramienta nmap siguen visibles al público y no son críticas para ciberseguridad, es recomendable hacer una auditoría para validar que tampoco expongan otro tipo de información sensible de la empresa al público.
- Modificar o eliminar las Options -Indexes en todos los directorios web públicos.
- Revisar el resto de la configuración de Apache para detectar otras exposiciones.
- Instalar y configurar un WAF para detectar y bloquear escaneos automatizados.
- Evitar subir archivos confidenciales (backups, archivos de configuración) al directorio web público.
- Monitorizar regularmente los accesos a rutas sensibles mediante herramientas como fail2ban.
- Realizar pentesting de forma recurrente al menos dos veces al año para detectar posibles brechas de seguridad y remediarlas antes de que puedan ser explotadas.