Reporte de vulnerabilidades:

Se ha aplicado un escaneo detallado, y búsqueda de vulnerabilidades con el comando “nmap -sV --script=vuln <IP_debian>”, dando el siguiente resultado:

Tabla de vulnerabilidades:

Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Referencia
80	HTTP	Apache 2.4.62	Ninguna conocida		Apache. Sección de vulnerabilidades
80	Wordpress	Versión no determinada	Múltiples vulnerabildades	Dado que no tenemos acceso directo al sistema Debian y no podemos determinar la versión exacta de WordPress, presentamos vulnerabilidades comunes que afectan a varias versiones de WordPress. Se recomienda identificar la versión exacta mediante escaneo o análisis pasivo para precisar las vulnerabilidades aplicables.	WPScan

Posibles Vulnerabilidades en WordPress

A continuación, se describen vulnerabilidades comunes en WordPress, independientemente de la versión específica instalada en el sistema:

Vulnerabilidad	Descripción	Referencia
Inyección de SQL (SQLi)	Permite a atacantes manipular la base de datos mediante consultas SQL maliciosas. Puede llevar al robo de datos o la alteración de información.	CVE Details
Cross-Site Scripting (XSS)	Permite la inyección de código malicioso en las páginas web, afectando a los usuarios que las visitan. Puede usarse para robar credenciales o ejecutar scripts no autorizados.	OWASP XSS
Inyección de archivos (LFI/RFI)	Permite a un atacante incluir archivos locales o remotos en el servidor, lo que puede llevar a la ejecución de código malicioso.	OWASP LFI

Ejecución remota de código (RCE)	Un atacante puede ejecutar código arbitrario en el servidor, obteniendo control total sobre el sitio web y el sistema.	CVE Details
Escalada de privilegios	Usuarios con bajos privilegios pueden obtener acceso de administrador y comprometer la seguridad del sitio.	WPScan
CSRF (Cross-Site Request Forgery)	Obliga a un usuario autenticado a realizar acciones no deseadas en el sitio sin su consentimiento.	OWASP CSRF
Backdoors	Inserción de puertas traseras en los archivos de WordPress que permiten a atacantes acceder sin autorización.	Exploit-DB
Pharma Hack	Inyección de enlaces no autorizados a productos farmacéuticos fraudulentos en el contenido del sitio.	Sucuri Blog
Redirecciones maliciosas	Redirige a los usuarios a sitios web maliciosos sin su conocimiento.	Sucuri Blog
Descargas Drive-by	Inyecta código malicioso en WordPress para descargar malware automáticamente en los dispositivos de los visitantes.	MalwareBytes
Clickjacking	Engaña a los usuarios para que hagan clic en elementos ocultos, activando acciones no deseadas en el sitio.	OWASP Clickjacking

Métodos para Determinar la Versión de WordPress

Dado que estamos operando desde Kali Linux y sólo tenemos acceso a la máquina Debian mediante nmap, podemos intentar identificar la versión de WordPress con las siguientes estrategias:

Escaneo con Nmap:

```
nmap -p80 --script=http-wordpress-enum 10.0.2.4
```

Este script intenta obtener la versión de WordPress a partir de archivos comunes.

Extracción desde los encabezados HTTP:

```
curl -I http:// 10.0.2.4/wordpress/
```

Algunas versiones de WordPress exponen información en los encabezados de respuesta HTTP.

Búsqueda en archivos públicos:

```
curl http:// 10.0.2.4/wordpress/readme.html
```

Muchas instalaciones de WordPress dejan un archivo readme.html accesible con información de la versión.

Uso de WPScan (recomendado en Kali Linux):

```
wpscan --url http://10.0.2.4/wordpress/ --enumerate ap
```

WPScan es una herramienta especializada en la identificación de vulnerabilidades de WordPress.

Recomendaciones de Seguridad

Actualizar WordPress regularmente para aplicar los últimos parches de seguridad.
Eliminar plugins y temas innecesarios que podrían ser vulnerables.
Configurar permisos de archivos y directorios para evitar accesos no autorizados.
Implementar autenticación de dos factores para proteger cuentas administrativas.
Monitorizar el tráfico web en busca de actividades sospechosas.