## Reporte de Vulnerabilidades para un Servidor Debian con LAMP – CARLOS DUCLAUD

---

**Puerto:** 80/tcp
**Servicio:** HTTP
**Versión:** Apache HTTPD 2.4.62 (Debian)

**Vulnerabilidad: Inyección SQL (SQLi)**

- **Descripción:** La aplicación parece ser vulnerable a inyecciones SQL en ciertos parámetros de URL, lo que podría permitir a un atacante acceder a la base de datos de manera no autorizada, leer o modificar datos.
- **Parámetros afectados:**
    - `http://192.168.1.10:80/?C=N;O=D' OR sqlspider`
    - Variaciones similares como `C=D;O=A' OR sqlspider`, indicando posibles puntos de inyección SQL.
- **Severidad:** Alta, ya que podría permitir a un atacante interactuar con la base de datos.
- **Referencia:** OWASP SQL Injection

---

**Puerto:** 80/tcp
**Servicio:** HTTP
**Versión:** Apache HTTPD 2.4.62 (Debian)

**Vulnerabilidad: Listado de Directorios**

- **Descripción:** El directorio raíz (`/`) está configurado para permitir el listado de directorios, lo que podría exponer archivos sensibles o innecesarios que podrían ser útiles para un atacante. Esto puede proporcionar información sobre la estructura del servidor o generar fugas de información.

- **Severidad:** Media, ya que expone la estructura de archivos del servidor, pero no proporciona directamente datos sensibles.

- **Referencia:** OWASP Directory Listing

---

**Puerto:** 80/tcp
**Servicio:** HTTP
**Versión:** Apache HTTPD 2.4.62 (Debian)

**Vulnerabilidad: Página de Login de WordPress Expuesta**

- **Descripción:** La página de login de WordPress (`/wordpress/wp-login.php`) es accesible públicamente, lo que podría ser objetivo de ataques de fuerza bruta, "credential stuffing" u otros ataques de autenticación.

- **Severidad:** Media, dependiendo de si se implementan controles de acceso y limitación de intentos.

- **Referencia:** OWASP Brute Force