# Documentación de Vulnerabilidades - Apache 2.4.62

## Servicio Detectado:

Puerto: 80/tcp

Servicio: HTTP

Software: Apache HTTP Server

Versión: 2.4.62 (Debian)

## CVE ID: CVE-2023-25690

Descripción: Vulnerabilidad de HTTP Request Smuggling en mod_proxy. Permite a un atacante manipular peticiones HTTP a través de servidores proxy mal configurados.

Impacto: Ejecución de peticiones maliciosas o interferencia en la comunicación entre cliente y servidor.

Gravedad (CVSS): 9.8 (Crítica)

Fuente: https://nvd.nist.gov/vuln/detail/CVE-2023-25690

## CVE ID: CVE-2023-27522

Descripción: Vulnerabilidad en mod_proxy_uwsgi, donde ciertos encabezados pueden ser procesados incorrectamente, permitiendo eludir restricciones de seguridad.

Impacto: Acceso no autorizado a ciertos recursos o funciones.

Gravedad (CVSS): 5.3 (Media)

Fuente: https://nvd.nist.gov/vuln/detail/CVE-2023-27522

## CVE ID: CVE-2023-25699

Descripción: Vulnerabilidad en mod_dav que puede provocar un denial of service (DoS) si se envían ciertas peticiones malformadas.

Impacto: Interrupción del servicio mediante consumo de recursos.

## Documentación de Vulnerabilidades - Apache 2.4.62

Gravedad (CVSS): 7.5 (Alta)

Fuente: https://nvd.nist.gov/vuln/detail/CVE-2023-25699