Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Referencia
80	HTTP (Apache)	2.4.65	CNVD-2024-36988	Vulnerabilidad crítica reportada para Apache httpd	https://vulners.com/cnvd/CNVD-2024-36988
80	HTTP (Apache)	2.4.65	CNVD-2024-36989	Fallo crítico relacionado con Apache httpd	https://vulners.com/cnvd/CNVD-2024-36989
80	HTTP (Apache)	2.4.65	B5E74010-A082-5ECE-AB37-62A35B33FE7D	Vulnerabilidad con exploit público disponible	Exploit disponible
80	HTTP (Apache)	2.4.65	541BA8B5-F4B7-5BBD-B106-0800AC961C7A	Explotación disponible para Apache 2.4.x	Exploit disponible
80	HTTP (Apache)	2.4.65	D6E0C57E-9EDB-5F96-A93E-768E2674D8CB	Vulnerabilidad aprovechable mediante exploit	Exploit disponible
80	HTTP (Apache)	2.4.65	CVE-2021-41773	Path traversal que permite acceder a rutas no autorizadas	Vulnerabilidad de path traversal
80	HTTP (Apache)	2.4.65	CVE-2021-42013	Permite ejecución remota de comandos en Apache 2.4.x	Exec de comandos en Apache 2.4.x
80	HTTP (Apache)	2.4.65	CVE-2022-31813	Permite saltarse reglas de seguridad en Apache httpd	Bypass de reglas en Apache httpd
80	HTTP (Apache)	2.4.65	1337DAY-ID-35422	Vulnerabilidad registrada en base de exploits 1337day	Vulnerabilidad listada en 1337day
80	HTTP (Apache)	2.4.65	CVE-2018-1312	Manipulación de encabezados de autenticación	Manipulación de encabezados de autenticación