Scan with nmap					
Port	**Service**	**Version**	**Vulnerability**	**Description**	**Reference**
80	HTTP	Apache 2.4.62	CVE-2024-40898	A partial fix for CVE-2024-39884 in the core of Apache HTTP Server 2.4.61 ignores some use of the legacy content-type based configuration of handlers. "AddType" and similar configuration, under some circumstances where files are requested indirectly, result in source code disclosure of local content. For example, PHP scripts may be served instead of interpreted. Users are recommended to upgrade to version 2.4.62, which fixes this issue.	Link to CVE
80	HTTP	Apache 2.4.62	CVE-2024-40725	A partial fix for CVE-2024-39884 in the core of Apache HTTP Server 2.4.61 ignores some use of the legacy content-type based configuration of handlers. "AddType" and similar configuration, under some circumstances where files are requested indirectly, result in source code disclosure of local content. For example, PHP scripts may be served instead of interpreted. Users are recommended to upgrade to version 2.4.62, which fixes this issue.	Link to CVE