S. No.	Vulnerability Name	Severity Level	Host & Port	Description (Brief)	Recommended Fix (Mitigation Steps)
1	SSL/TLS: Report Weak Cipher Suites	High	127.0.0.1 on 443/tcp	The server is using outdated and weak encryption protocols and ciphers (e.g., RC4, 3DES, SSLv2/v3), making it vulnerable to decryption attacks.	Configuration Change: Edit the web server's SSL configuration file (e.g., ssl.conf). Disable all weak ciphers and protocols (SSLv2, SSLv3, TLS 1.0, TLS 1.1). Only enable TLS 1.2 and TLS 1.3 with strong ciphers like AES-256.
2	HTTP Security Headers Detection	Medium	127.0.0.1 on 80/tcp	The web server is missing crucial security headers (X-Frame-Options, X-Content-Type-Options) which increases the risk of attacks like clickjacking and MIME sniffing.	Configuration Change: Add missing security headers to the server's configuration (e.g., using mod_headers in Apache) to instruct browsers on how to handle content securely.
3	Operating System / Software Version Detected	Medium	127.0.0.1 on [Service Port]	A running network service (e.g., Apache, SSH, PHP) is an outdated version that contains publicly known security flaws (CVEs).	Software Update: Update the vulnerable software package to its latest stable version that includes the security patch.