Vulnerability Assessment Report

Objective

To identify outdated or vulnerable software running on the website testphp.vulnweb.com using nmap -sV, and research known security flaws (CVEs) in the detected services.

Why This Matters

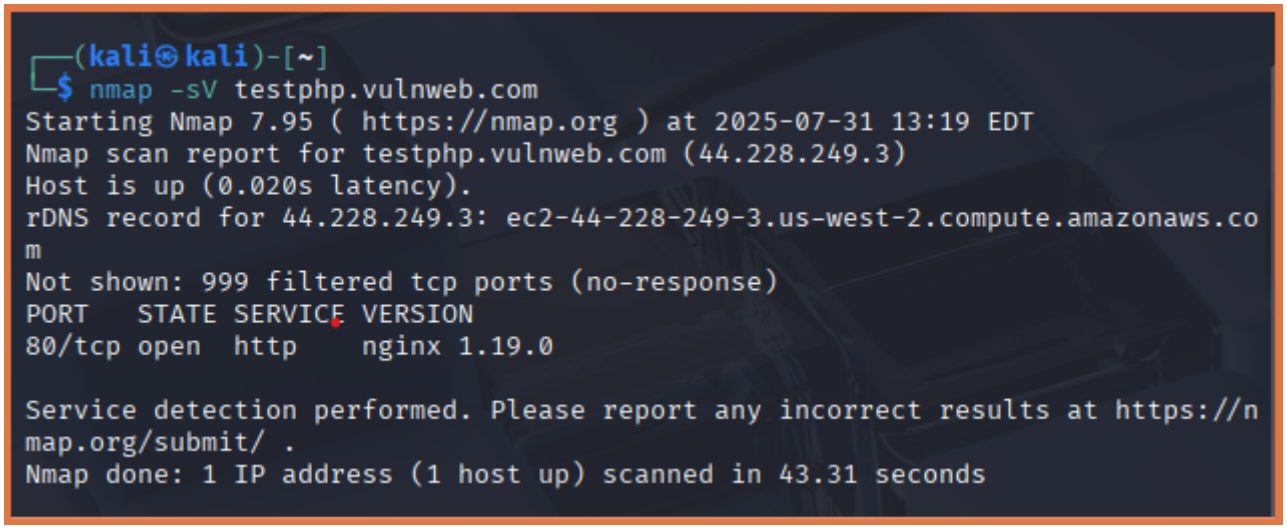
Outdated software often contains known security vulnerabilities that are publicly documented as CVEs (Common Vulnerabilities and Exposures). These flaws:
- Can be exploited by attackers
- Allow unauthorized access or denial of service
- May lead to data theft, defacement, or complete system compromise

Routine scanning and patching are essential to reduce the risk of attacks.

Julius B. Thomas
2462095

Nmap Scan Result

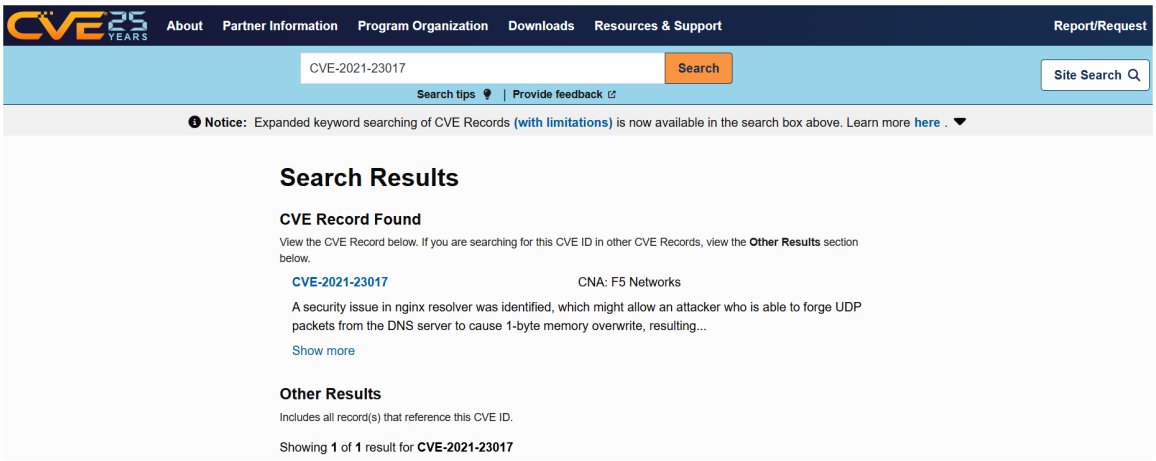
Command Used:
nmap -sV testphp.vulnweb.com



Output Summary:
- Target Domain: testphp.vulnweb.com
- IP Address: 44.228.249.3
- Detected Service:
  -> Port: 80/tcp
  - >Service: HTTP
  - >Software Version: nginx 1.19.0

Julius B. Thomas
2462095

What is a CVE?

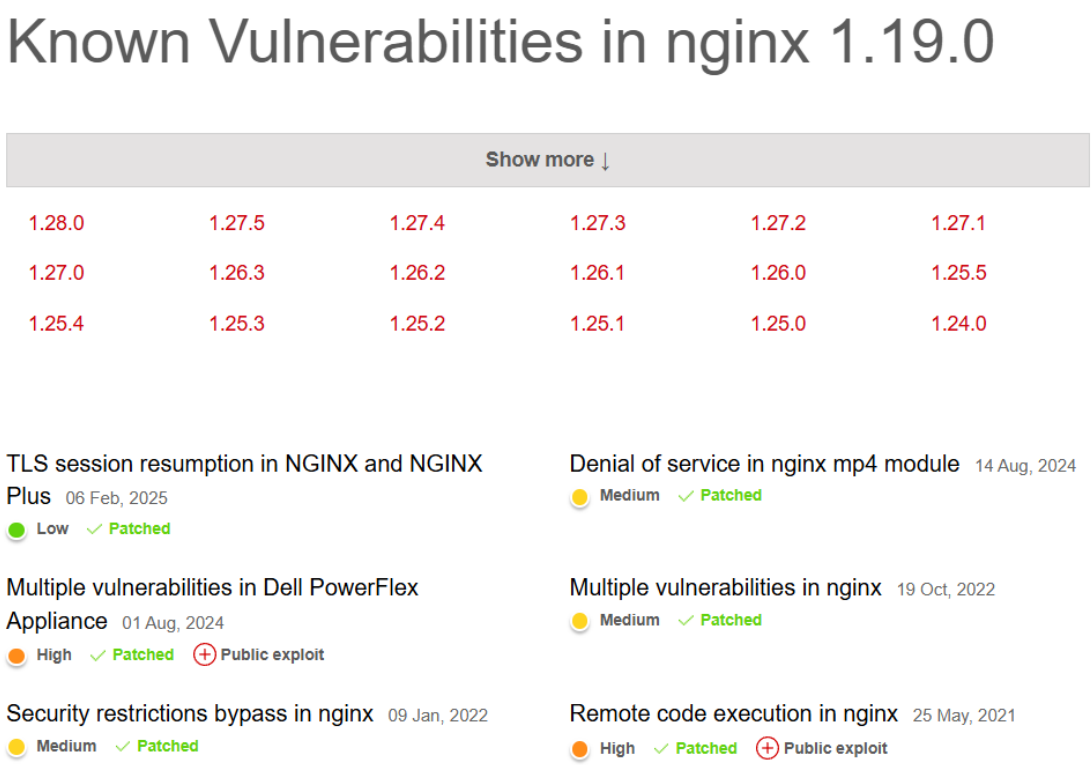


CVE (Common Vulnerabilities and Exposures) is a unique identifier for publicly known cybersecurity vulnerabilities. Each CVE contains:
- A unique ID (e.g., CVE-2021-23017)
- A description of the issue
- Its severity (Low/Medium/High)
- Its potential impact (DoS, RCE, bypass, etc.)

CVE information is published by trusted databases such as CVE.org, NVD, and Vulmon.

Julius B. Thomas
2462095

CVEs for nginx 1.19.0



Detected Service: nginx 1.19.0

- CVE-2021-23017: 1-byte memory overwrite in resolver (High Severity, RCE, Patched)
- DoS in nginx mp4 module: Denial of service via malformed MP4 requests (Medium Severity, Patched)
- Security bypass in nginx: Restriction bypass using crafted headers (Medium Severity, Patched)

Risk Analysis

The detected version, nginx 1.19.0, contains critical vulnerabilities:

1. CVE-2021-23017 can allow attackers to execute arbitrary code remotely by exploiting DNS resolver logic — a serious threat.
2. Denial of Service (DoS) vulnerabilities can cause the web server to become unresponsive.
3. Security bypass bugs might let attackers access restricted areas or functions.

These risks highlight the need to upgrade to a secure version (e.g., 1.21+).

Julius B. Thomas
2462095

Conclusion

- The Nmap scan found nginx 1.19.0 running on the target.
- This version has multiple known vulnerabilities, including CVE-2021-23017, which can lead to serious exploitation.
- Keeping the nginx version updated is essential to eliminate these threats.

Sources Used

1. https://www.cybersecurity-help.cz/vdb/SB2021052543
2. https://vulmon.com/vulnerabilitydetails?qid=CVE-2021-23017
3. https://www.cve.org/CVERecord?id=CVE-2021-23017

Julius B. Thomas
2462095