

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To identify outdated or vulnerable software running on the website testphp.vulnweb.com using nmap -sV, and research known security flaws (CVEs) in the detected services.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Outdated software often contains known security vulnerabilities that are publicly documented as CVEs (Common Vulnerabilities and Exposures).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.

Nmap Scan Result

Command Used:

nmap -sV testphp.vulnweb.com

```
(kali㉿kali)-[~]  
$ nmap -sV testphp.vulnweb.com  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 13:19 EDT  
Nmap scan report for testphp.vulnweb.com (44.228.249.3)  
Host is up (0.020s latency).  
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com  
Not shown: 999 filtered tcp ports (no-response)  
PORT      STATE SERVICE VERSION  
80/tcp    open  http    nginx 1.19.0  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 43.31 seconds
```

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

What is a CVE?

The screenshot shows the CVE.org website interface. At the top, there's a navigation bar with links like 'About', 'Partner Information', 'Program Organization', 'Downloads', 'Resources & Support', and 'Report/Request'. Below this is a search bar containing 'CVE-2021-23017' and a 'Search' button. A notice below the search bar states: 'Notice: Expanded keyword searching of CVE Records (with limitations) is now available in the search box above. Learn more here.' The main content area is titled 'Search Results' and shows a 'CVE Record Found' section. It includes a description of the vulnerability: 'A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting...'. It also mentions 'CNA: F5 Networks' and a 'Show more' link. Below this is an 'Other Results' section stating 'Showing 1 of 1 result for CVE-2021-23017'.

Remote code execution in nginx

Published: 2021-05-25 | Updated: 2022-07-31

Risk	 High
Patch available	 YES
Number of vulnerabilities	1
CVE-ID	CVE-2021-23017
CWE-ID	CWE-193
Exploitation vector	Network
Public exploit	Public exploit code for vulnerability #1 is available.
Vulnerable software	nginx Server applications / Web servers
Vendor	NGINX

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.

CVEs for nginx 1.19.0

Known Vulnerabilities in nginx 1.19.0

Show more ↓					
1.28.0	1.27.5	1.27.4	1.27.3	1.27.2	1.27.1
1.27.0	1.26.3	1.26.2	1.26.1	1.26.0	1.25.5
1.25.4	1.25.3	1.25.2	1.25.1	1.25.0	1.24.0
TLS session resumption in NGINX and NGINX Plus 06 Feb, 2025 Low ✓ Patched			Denial of service in nginx mp4 module 14 Aug, 2024 Medium ✓ Patched		
Multiple vulnerabilities in Dell PowerFlex Appliance 01 Aug, 2024 High ✓ Patched + Public exploit			Multiple vulnerabilities in nginx 19 Oct, 2022 Medium ✓ Patched		
Security restrictions bypass in nginx 09 Jan, 2022 Medium ✓ Patched			Remote code execution in nginx 25 May, 2021 High ✓ Patched + Public exploit		

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+).

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>