VulnSightAI Scan Report

Target: **scanme.nmap.org**

Scan Date: 2025-07-09 17:53:10

AI-Powered CVE Suggestions

Okay, based on the limited technologies detected (Apache 2.4.7 being the most prominent), here are some critical potential CVEs to be aware of. Keep in mind that Apache 2.4.7 is extremely old, so it's likely *severely* vulnerable. This list assumes the Apache installation hasn't been patched since its release. A more complete scan would reveal more accurate vulnerabilities.

Important Note: Since the information is limited to Apache 2.4.7, these CVEs focus on that. The presence of Google Analytics, HTML5, HTTPServer, etc., don't directly translate to critical vulnerabilities without further context (like knowing the specific JavaScript libraries used or versions of the HTTPServer).

Here are 3 critical potential CVEs to consider for Apache 2.4.7:

1. **CVE-2015-3183: Apache HTTP Server mod_proxy vulnerability**
    *   **Description:** A vulnerability in mod_proxy in Apache HTTP Server 2.2.x before 2.2.30 and 2.4.x before 2.4.16 allows remote attackers to cause a denial of service (memory consumption) via a crafted request. Specifically involves connection reuse.
    *   **Severity:** High (Denial of Service)
    *   **Why Critical in this Context:** Denial of service is often a first step in a larger attack. Since this version is vulnerable to many other problems this could be used as a diversion.

2. **CVE-2015-0253: Apache HTTP Server mod_lua buffer overflow**
    *   **Description:** mod_lua in Apache HTTP Server 2.4.x before 2.4.12 is vulnerable to a buffer overflow in the r:parsebody function. This may allow remote attackers to execute arbitrary code or cause a denial of service.
    *   **Severity:** Critical (Remote Code Execution, Denial of Service)
    *   **Why Critical in this Context:** Remote Code Execution (RCE) allows an attacker to completely take over the server, making it the highest severity threat.

3. **CVE-2013-5704: Apache HTTP Server mod_rewrite bypass**
    *   **Description:** mod_rewrite in the Apache HTTP Server 2.2.x before 2.2.26 and 2.4.x before 2.4.7, when used in conjunction with proxypass and ProxyPassReverse directives, can allow attackers to bypass intended rewrite rules and access restricted resources.
    *   **Severity:** Medium (Information Disclosure/Access Bypass)
    *   **Why Critical in this Context:** While listed as medium severity, because of the age of 2.4.7 it is listed as critical because it could allow someone access to internal resources that are unpatched.

Important Considerations:

*   **Outdated Software:** Apache 2.4.7 is ancient. Upgrading is absolutely the *highest* priority. The number of vulnerabilities present is astronomical.
*   **Scanning is Crucial:** A proper vulnerability scan with a tool like Nessus, OpenVAS, or Qualys is essential to get an accurate picture of the vulnerabilities present. This limited analysis is only a starting point.
*   **Configuration Matters:** The specific configuration of Apache will significantly impact the actual risk. For example, if `mod_lua` isn't loaded, CVE-2015-0253 isn't relevant.
*   **Country/IP:** The country and IP addresses are threat intelligence and geolocation data. These are indicators for investigation, but not vulnerabilities in themselves. Knowing the country allows you to apply threat models for threat actors in that area.

In short, the server *must* be upgraded immediately. Followed by a thorough vulnerability scan. The information above represents a fraction of the potential issues with such an outdated version of Apache.

Subdomain Enumeration

- Koi subdomain nahi mila.

Nmap Port Scan Results

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-09 17:51 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.27s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 91 closed tcp ports (reset)
PORT     STATE    SERVICE      VERSION
21/tcp   open     tcpwrapped
22/tcp   open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp   filtered smtp
80/tcp   open     http         Apache httpd 2.4.7 ((Ubuntu))
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
554/tcp  open     rtsp?
1723/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 103.33 seconds
```

Technology Stack

- **Apache:** 2.4.7
- **Country:**
- **Google-Analytics:** Universal
- **HTML5:**
- **HTTPServer:**
- **IP:**
- **Script:**
- **Title:**