Vulnerability Assessment Report: scanme.nmap.org

SECURITY SCORE: 91/100

OVERALL RISK LEVEL: LOW

1. Network Scan Results (Nmap)

Port	Service	Version	Evidence
22	ssh	6.6.1p1 Ubuntu 2ubuntu2.13	None
25	smtp		None
80	http	2.4.7	**http-title:** Go ahead and ScanMe!...
135	msrpc		None
139	netbios-ssn		None
179	bgp		None
445	microsoft-ds		None
9929	nping-echo		None
31337	tcpwrapped		None

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 45.33.32.156
+ Target Hostname: scanme.nmap.org
+ Target Port: 80
+ Start Time: 2026-02-23 18:09:16 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ 26 items checked: 0 error(s) and 2 item(s) reported on remote host
+ End Time: 2026-02-23 18:09:43 (GMT0) (27 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

[stderr]
+ ERROR: Host maximum execution time of 600 seconds reached
```

3. Crawled Website Endpoints

- http://scanme.nmap.org/
- http://scanme.nmap.org/#menu
- [FORM] http://scanme.nmap.org/search/

4. Vulnerability Intelligence (CVE Mapping)

Findings marked as [POTENTIAL] require specific configuration to be exploitable.
Modern Vulnerabilities in Apache httpd 2.4.7
- [HIGH 8.2] [POTENTIAL] CVE-2021-44224: a crafted uri sent to httpd configured as a forward proxy (proxyrequests on) can cause a crash (null pointer dereference) or, for configurations mixin...
- [MEDIUM 5.4] [POTENTIAL] CVE-2025-66200: mod_userdir+suexec bypass via allowoverride fileinfo vulnerability in apache http server. users with access to use the requestheader directive in htac...
Modern Vulnerabilities in Apache 2.4.7
- [HIGH 8.2] [POTENTIAL] CVE-2021-44224: a crafted uri sent to httpd configured as a forward proxy (proxyrequests on) can cause a crash (null pointer dereference) or, for configurations mixin...
- [MEDIUM 5.4] [POTENTIAL] CVE-2025-66200: mod_userdir+suexec bypass via allowoverride fileinfo vulnerability in apache http server. users with access to use the requestheader directive in htac...
Legacy Vulnerability Intelligence
- ■■ NOTICE: Our engine identified 2 additional legacy vulnerabilities (pre-2016) associated with these services. These have been filtered to prioritize current threats.

5. Attack Possibilities & Mitigation

[LOW] Attack: Clickjacking / Cross-Site Scripting (XSS)
Mitigation: Implement X-Frame-Options and Content-Security-Policy headers.