

# 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 2ubuntu1.3	None
25	smtp		None
80	http	2.4.7	<b>http-title:</b> 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: 2026-02-24 02:17:27 (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: 2026-02-24 02:17:59 (GMT0) (32 seconds)
-----
+ 1 host(s) tested

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

## 3. Crawled Website Endpoints

- scanme.nmap.org

## 4. Vulnerability Intelligence (CVE Mapping)

*Findings marked as [POTENTIAL] require specific configuration to be exploitable.*

### **Validated Vulnerabilities in Apache httpd 2.4.7**

- [POTENTIAL] CVE-2021-44224: a crafted uri sent to httpd configured as a forward proxy (proxyrequests on) can cause a crash (null pointer d...
- [POTENTIAL] CVE-2025-66200: mod\_userdir+suexec bypass via allowoverride fileinfo vulnerability in apache http server. users with access to...

### **Legacy Vulnerability Intelligence**

- ■■ NOTICE: Our engine identified 1 legacy (pre-2016) vulnerabilities which were filtered.

## 5. Attack Possibilities & Mitigation

**[LOW] Attack:** Missing Anti-Clickjacking Protection

**Mitigation:** The X-Frame-Options header is missing entirely. Implement DENY or SAMEORIGIN to prevent UI redressing.

**[NOTE] Attack:** Missing Content-Security-Policy (CSP)

**Mitigation:** Implement a strict CSP header to prevent unauthorized script execution and data exfiltration.