Sentra.AI - Security Audit Report

Target: localhost

Date: 2026-02-02 01:31:47

Scan ID: 8df6a219-f19e-467e-a40b-62349cead8bc

Executive Summary (AI Analysis)

1. Summary:

Localhost is running a Windows-based host (MSRPC/135, SMB/445) alongside dual HTTP services (ports 80 and 8000). The web server is Apache 2.4.25 (Debian) hosting a PHP application (evidenced by `login.php` and PHPSESSID cookies). The target appears to be a Docker container or WSL2 environment (`host.docker.internal`). Sensitive directories (`/config/`, `/docs/`) allow directory indexing, and an admin login portal is exposed at `/login.php`.

2. Risks:

- Outdated Software: Apache 2.4.25 (2017) has known CVEs (e.g., CVE-2017-7679, CVE-2018-1312).
- Information Disclosure: Directory indexing on `/config/` (likely sensitive files) and `/docs/`; ETag headers leak server inode numbers; `robots.txt` reveals hidden paths.
- Session Hijacking: PHPSESSID and "security" cookies lack the `HttpOnly` flag, making them vulnerable to XSS theft.
- Clickjacking: Missing `X-Frame-Options` header allows the site to be embedded in malicious iframes.
- Network Exposure: SMB (445) and MSRPC (135) are open; if unpatched, these expose the host to lateral movement and exploits like EternalBlue.
- Administrative Exposure: `/login.php` is directly accessible, facilitating brute-force attacks.

3. Recommendations:

- Patch: Upgrade Apache to the latest 2.4.x stable release immediately.
- Harden Web Config:
  - Disable directory indexing: `Options -Indexes` for `/config/`, `/docs/`, and root.
  - Remove default files (`/icons/README`) and restrict/block access to `/config/`.
  - Add security headers: `X-Frame-Options: DENY`, `X-Content-Type-Options: nosniff`, and set `HttpOnly; Secure; SameSite=Strict` flags on all cookies.
- SMB/MSRPC: If not required, close ports 135/445 at the host firewall; if required, ensure latest Windows patches are applied and restrict access via IP whitelisting.
- ETags: Configure `FileETag None` or `FileETag MTime Size` to prevent inode leakage.

- Authentication: Implement rate-limiting/fail2ban on `login.php` and consider moving the admin panel to a non-standard path or VPN-restricted interface.

Technical Details (Nmap)

```
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-02 01:30 +0800
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 96 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
8000/tcp open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

Sentra.AI - Security Audit Report

Web Vulnerabilities (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          192.168.65.254
+ Target Hostname:    host.docker.internal
+ Target Port:        80
+ Start Time:         2026-02-01 17:30:45 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.25 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ Cookie PHPSESSID created without the httponly flag
+ Cookie security created without the httponly flag
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x1a 0x5780ba3955700
+ File/dir '/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ OSVDB-3268: /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ OSVDB-3268: /docs/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 6544 items checked: 0 error(s) and 11 item(s) reported on remote host
+ End Time:           2026-02-01 17:30:58 (GMT0) (13 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```