# Sentra.AI - Security Audit Report

Target: localhost

Date: 2026-02-23 16:53:31

Scan ID: 1f049205-2457-4b58-a997-5b44545f645a

**Risk Score: 9.0/10 - CRITICAL**

## Executive Summary (AI Analysis)

1. Summary:
The target is running Apache 2.4.25 (Debian) hosting a PHP application (redirecting to `login.php`) on port 80, with an additional HTTP service on port 8000. The underlying host also exposes Windows/SMB services (MSRPC on 135 and Microsoft-DS on 445). The environment appears to be a Docker container or WSL instance (`host.docker.internal`).

2. Risks:
- Outdated Software: Apache 2.4.25 (2016) is EOL and vulnerable to multiple CVEs (e.g., CVE-2017-15710, CVE-2018-1312).
- Information Disclosure: Directory indexing enabled on `/config/` and `/docs/`; inode leakage via ETags; `/config/` may expose sensitive configuration files.
- Session Weakness: `PHPSESSID` and `security` cookies lack `httponly` flags, increasing XSS impact.
- Clickjacking: Missing `X-Frame-Options` header.
- Attack Surface: Admin login page (`/login.php`) exposed; SMB ports (135/445) present on localhost (risk if bridged to network).

3. Recommendations:
- Patch: Upgrade Apache to latest stable 2.4.x branch immediately.
- Harden Web App: Disable directory indexing (`Options -Indexes`); restrict or remove `/config/` from web root; implement rate limiting on `login.php`.
- Secure Cookies: Set `httponly`, `secure`, and `samesite` flags for all session cookies.
- Headers: Add `X-Frame-Options: DENY` (or `SAMEORIGIN`), `X-Content-Type-Options: nosniff`, and remove ETags (`FileETag None`).
- SMB: If unnecessary, disable ports 135/445; if required, ensure SMB signing is enforced and access is restricted by firewall.
- Cleanup: Remove default Apache files (`/icons/README`) and review `robots.txt` entries for sensitive paths.

## Technical Details (Nmap)

```
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-23 16:52 +0800
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000012s 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 0.25 seconds
```

## Web Vulnerabilities (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ ERROR: Host maximum execution time of 60 seconds reached
+ Target IP:          192.168.65.254
+ Target Hostname:    host.docker.internal
+ Target Port:        80
+ Start Time:         2026-02-23 08:52:13 (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:           2026-02-23 08:52:29 (GMT0) (16 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

## Remediation Playbooks (OS: WINDOWS)

### Fix #1 [LOW]: HTTP - Unencrypted web traffic

*Source: Nmap - Port 80/tcp*

```
Redirect HTTP to HTTPS (IIS)
Install URL Rewrite module, then add redirect rule
Or enforce HTTPS-only in application
```

### Fix #2 [MEDIUM]: MSRPC - Used for DCOM, potential for RPC exploits

*Source: Nmap - Port 135/tcp*

```
Block RPC from external networks
netsh advfirewall firewall add rule name="Block RPC Inbound" dir=in
action=block protocol=tcp localport=135
```

### Fix #3 [HIGH]: SMB (Windows File Sharing) - High risk for ransomware/lateral movement

*Source: Nmap - Port 445/tcp*

```
Disable SMBv1 (EternalBlue mitigation)
Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force
Block SMB from external networks
netsh advfirewall firewall add rule name="Block SMB Inbound" dir=in
action=block protocol=tcp localport=445
```

### Fix #4 [MEDIUM]: Directory listing enabled - exposes file structure

*Source: Nikto - directory indexing*

```
Disable directory browsing in IIS
Set-WebConfigurationProperty -pspath 'IIS:\Sites\Default Web Site' -filter
/system.webServer/directoryBrowse -name enabled -value false
```

### Fix #5 [MEDIUM]: Missing X-Frame-Options header - clickjacking risk

*Source: Nikto - x-frame-options*

```
Add header in IIS via web.config
<customHeaders><add name="X-Frame-Options" value="SAMEORIGIN"
/></customHeaders>
```

### Fix #6 [HIGH]: Known vulnerability in OSVDB database

*Source: Nikto - osvdb*

```
Update the affected software to the latest version
```