Vulnerability Assessment Report: 127.0.0.1

SECURITY SCORE: 73/100

OVERALL RISK LEVEL: MEDIUM

1. Network Scan Results (Nmap)

Port	Service	Version	State
3000	http		open
5000	upnp		open

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ No web server found on localhost:80
---------------------------------------------------------------------------
+ 0 host(s) tested

[stderr]
+ ERROR: Host maximum execution time of 180 seconds reached
+ ERROR: Host maximum execution time of 180 seconds reached
+ ERROR: Host maximum execution time of 180 seconds reached
+ ERROR: Host maximum execution time of 180 seconds reached
```

3. Crawled Website Endpoints

- No endpoints found

4. Vulnerability Intelligence (CVE Mapping)

Note: Duplicate findings are consolidated for scoring.
Modern Vulnerabilities in Node.js Express framework
- [HIGH 7.5] CVE-2016-10539: negotiator is an HTTP content negotiator for Node.js and is used by many modules and frameworks including Express and Koa. The header for "Accept-Lang...
- [MEDIUM 4.3] CVE-2025-62595: Koa is expressive middleware for Node.js using ES2017 async functions. In versions 2.16.2 to before 2.16.3 and 3.0.1 to before 3.0.3, a bypass to CVE-...

Legacy Vulnerability Intelligence
- ■■ NOTICE: Our engine identified 6 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.