PENETRATION TEST REPORT

Asgardian Penetration Analyzer — Authorized Engagement

Scope: 192.168.2.57 (1 hosts)

Date: November 11, 2026 15:30

Operator: Asgardian Penetration Analyzer (SpaceXAI)

AI Provider: SpaceXAI Model: grok-4.7

CLASSIFICATION: CONFIDENTIAL

Metric	Value
Engagement Date	2026-11-11T20:30:46Z
Scope	192.168.2.57
Exclusions	(none)
Live Hosts (inventory rows)	1
Vulnerability Findings	1
Critical / High	0 / 0
Credentials Recovered	None
Overall Risk	MEDIUM
AI Provider	SpaceXAI
AI Model	grok-4.7

Table of Contents

1. Executive Summary
2. Scope & Methodology
3. Host & Service Inventory
4. Vulnerability Findings
5. Exploitation Chain — Best Effort
    5.1 Outcome
6. Recovered Credentials & Hashes
7. Evidence & Artifacts
8. Recommendations
9. Conclusion

1. Executive Summary

Authorized penetration test of scope **192.168.2.57**. Testing was performed autonomously via APA-mcp. Overall residual risk rating: **MEDIUM**.

Host inventory: 192.168.2.57 (Live)

No exploitable vulnerabilities were recorded in the structured findings store.

2. Scope & Methodology

In-Scope: 192.168.2.57
Out-of-Scope: (none)
Authorization: Operator confirmed authorization in Asgardian Penetration Analyzer prior to start.
AI agent: SpaceXAI · grok-4.7 via APA-mcp tools
Working directory: /Users/wraith/Desktop/APA/APA-20261111-151857
Phases: Scoping → Discovery → Enumeration → Vulnerability identification → Exploitation (chained where possible) → Credential recovery → Reporting

3. Host & Service Inventory

Host	Status	OS / Role	Open Services
192.168.2.57	Live	—	80/http Apache httpd, 443/http Apache httpd

4. Vulnerability Findings

Severity	CVE	CWE	Host	Description
Info	N/A	CWE-200	—	No discrete vulnerability records were stored in the APA-mcp findings store. See executive summary and notes for engagement outcome.

5. Exploitation Chain — Best Effort

5.1 Outcome

No chained exploitation

Reconnaissance completed against authorized scope. No attack chain advanced to compromise based on available findings.

Hosts considered

192.168.2.57

Attack Path Diagram

```
Attacker → recon → no foothold
```

Recovered Credentials & Hashes

Cleartext credentials

None recovered during this engagement.

Hashes

None recovered during this engagement.

Attack Path Diagram

```
No credential material recovered.
```

7. Evidence & Artifacts

Artifact	Location / Content
APA findings store	/Users/wraith/Desktop/APA/APA-20261111-151857/findings.json
Engagement prompt	/Users/wraith/Desktop/APA/APA-20261111-151857/prompt.md
Engagement summary	/Users/wraith/Desktop/APA/APA-20261111-151857/summary.md
key-1-of-3.txt	/Users/wraith/Desktop/APA/APA-20261111-151857/key-1-of-3.txt
robots.txt	/Users/wraith/Desktop/APA/APA-20261111-151857/robots.txt
wp-cookies.txt	/Users/wraith/Desktop/APA/APA-20261111-151857/wp-cookies.txt

8. Recommendations

- Remediate Critical and High findings first; apply vendor patches and configuration hardening.
- Disable or restrict unnecessary services discovered during inventory.
- Rotate any credentials recovered during testing and audit reuse across systems.
- Validate fixes with a targeted retest against the same authorized scope.

9. Conclusion

This report documents best-effort testing of the authorized scope using APA-mcp. Live hosts: 1. Vulnerabilities catalogued: 1. Overall risk: **MEDIUM**.