milo.

Penetration Test Report

Acme Health Services

Report Date: March 4, 2026

Test Period: March 3 – March 4, 2026

Report ID: MILO-2026-03-00847

Classification: CONFIDENTIAL

Prepared By: Milo Security, Inc.

OVERALL RESULT

PASSED

3 findings | 0 critical | 0 high

Table of Contents

1. Executive Summary

What This Means: We tested your website and online systems to see if a hacker could break in. The good news: we found no serious security holes. We did find one moderate issue with your patient portal login system and two minor items that are easy to fix. Overall, your business passed the test. This report contains everything you need for your insurance company, your auditor, or any client who asked for it.

Milo Security was engaged by Acme Health Services to perform a penetration test of their external-facing systems and web applications. The objective was to identify exploitable vulnerabilities that could allow unauthorized access to systems, data, or protected health information (ePHI), and to provide a compliance-ready report suitable for HIPAA audit documentation, SOC 2 evidence, and cyber insurance underwriting requirements.

The assessment was conducted on March 3–4, 2026, targeting 4 web applications and 12 network endpoints. Testing followed industry-standard methodologies including OWASP Testing Guide v4.2, PTES (Penetration Testing Execution Standard), and NIST SP 800-115.

Overall Result **PASSED**

Findings Overview

Severity	Count	Description
Critical	0	No critical vulnerabilities identified
High	0	No high-severity vulnerabilities identified
Medium	1	Session token predictability in patient portal
Low	2	Missing security headers, server version disclosure

Key Takeaways: Acme Health Services maintains a generally strong external security posture. No critical or high-severity vulnerabilities were identified. One medium-severity finding related to session token predictability should be addressed within 30 days. Two low-severity findings represent defense-in-depth improvements. Detailed remediation steps are provided in Sections 4 and 5.

2. Scope & Methodology

2.1 Scope

The following systems were authorized and included in this penetration test:

Asset	Type	Description
www.acmehealth.com	Web Application	Primary public website
portal.acmehealth.com	Web Application	Patient portal (ePHI access)
api.acmehealth.com	REST API	Backend API serving patient portal
mail.acmehealth.com	Mail Server	Email infrastructure
12 IP addresses	Network	External-facing network endpoints

2.2 Methodology

This penetration test followed industry-standard frameworks:

- OWASP Testing Guide v4.2 — web application and API security testing
- PTES (Penetration Testing Execution Standard) — engagement structure
- NIST SP 800-115 — Technical Guide to Information Security Testing
- CVSS v3.1 — vulnerability severity scoring

2.3 Testing Parameters

Parameter	Detail
Test Type	External Penetration Test + Web Application Assessment
Approach	Grey-box (targets provided, no credentials)
Duration	March 3–4, 2026 (24-hour assessment window)
Rules of Engagement	Non-destructive only; no denial-of-service; no data modification

3. Summary of Findings

All findings sorted by severity with CVSS scores and remediation timelines:

ID	Severity	Finding	CVSS	Asset	Remediate By
MIL-001	Medium	**Session Token Predictability**	5.4	portal.acmehealth.com	April 3, 2026
MIL-002	Low	**Missing Content Security Policy Headers**	3.1	www.acmehealth.com	May 4, 2026
MIL-003	Low	**Server Version Disclosure**	2.6	api.acmehealth.com	May 4, 2026

4. Detailed Findings

4.1 Session Token Predictability

ID	Severity	CVSS Score	Affected Asset
MIL-001	**Medium**	5.4 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)	portal.acmehealth.com

What This Means: When your patients log into the patient portal, the system creates a digital "key" to keep them signed in. We found that these keys follow a predictable pattern, which means a sophisticated attacker could potentially guess a valid key and access a patient's session without their password. Think of it like a building where every apartment key is numbered sequentially — if you know one key number, you can guess the next one. This needs to be fixed within 30 days.

Technical Description

The patient portal at portal.acmehealth.com generates session tokens using a partially predictable algorithm. During testing, sequential session tokens shared common prefixes and exhibited low entropy in the final 8 characters. An attacker with knowledge of the token generation pattern could predict valid session tokens and hijack active user sessions, gaining unauthorized access to patient records containing ePHI.

Evidence

Session tokens collected during a 60-second observation window:

Token	Timestamp
`ACME-SESS-2026030314-a8f2c901`	2026-03-03 14:22:01 UTC
`ACME-SESS-2026030314-a8f2c918`	2026-03-03 14:22:14 UTC
`ACME-SESS-2026030314-a8f2c92f`	2026-03-03 14:22:31 UTC

Impact

Exploitation could allow unauthorized access to active patient sessions, resulting in viewing, modification, or exfiltration of ePHI — constituting a potential HIPAA breach under the Breach Notification Rule (45 CFR 164.400-414).

Remediation Steps

- Replace current token generation with a cryptographically secure random number generator (CSPRNG)
- Ensure session tokens contain a minimum of 128 bits of entropy
- Remove predictable components (timestamps, sequential counters) from token values
- Implement session token rotation after authentication state changes
- Consider additional session binding (IP pinning or device fingerprinting) for ePHI sessions

Recommended Timeline: 30 days (by April 3, 2026)

4.2 Missing Content Security Policy Headers

ID	Severity	CVSS Score	Affected Asset
MIL-002	**Low**	3.1 (AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N)	www.acmehealth.com

What This Means: Your main website is missing a security setting that acts like a bouncer for your web pages. This setting (called Content Security Policy) tells web browsers which scripts and content are allowed to run on your site. Without it, if an attacker ever found a way to inject malicious code into your site, the browser wouldn't know to block it. It's like having a building with no guest list at the front desk — anyone could walk in. This is a low-risk issue but an easy fix.

Technical Description

The website at www.acmehealth.com does not implement a Content Security Policy (CSP) header. CSP is a defense-in-depth mechanism that prevents cross-site scripting (XSS), clickjacking, and code injection attacks by specifying permitted content sources.

Impact

Without CSP headers, the site is more vulnerable to XSS attacks if a separate injection vulnerability is discovered. This reduces overall defense posture but does not represent an immediately exploitable risk.

Remediation Steps

- Add Content-Security-Policy header with a restrictive policy whitelisting only trusted sources
- Add X-Content-Type-Options: nosniff
- Add X-Frame-Options: DENY (or SAMEORIGIN if framing is required)
- Add Referrer-Policy: strict-origin-when-cross-origin

Recommended Timeline: 60 days (by May 4, 2026)

4.3 Server Version Disclosure

ID	Severity	CVSS Score	Affected Asset
MIL-003	**Low**	2.6 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)	api.acmehealth.com

What This Means: Your API server is announcing exactly what software it's running and which version, like a house with a sign on the front door saying which brand of lock you use and the model number. This information helps attackers look up known weaknesses for that specific software version. The fix takes about 5 minutes — it's just removing two lines from your server settings.

Technical Description

The API server returns detailed version information in HTTP response headers: "Server: nginx/1.24.0" and "X-Powered-By: Express 4.18.2". This assists attackers in targeting known vulnerabilities for those specific versions.

Remediation Steps

- Configure nginx to suppress version: add 'server_tokens off;' to nginx.conf
- Remove X-Powered-By in Express: add 'app.disable("x-powered-by");' to your application

Recommended Timeline: 60 days (by May 4, 2026)

5. Remediation Roadmap

What This Means: This is your to-do list, in priority order. Fix item #1 first (within 30 days), then items #2 and #3 (within 60 days). Once everything is fixed, contact us for your free re-test — we'll verify the fixes and update this report so you have a clean record for your files.

#	Finding	Action Required	Deadline	Status
1	**MIL-001: Session Token Predictability**	Replace token generation with CSPRNG; ensure 128-bit entropy minimum	April 3, 2026	**Open**
2	**MIL-002: Missing CSP Headers**	Implement Content-Security-Policy and related security headers	May 4, 2026	**Open**
3	**MIL-003: Server Version Disclosure**	Suppress server version headers in nginx and Express	May 4, 2026	**Open**

Free Re-Test: Once all items are remediated, contact support@milosecurity.com or click "Request Re-Test" in your Milo dashboard. Re-test results will be appended as an addendum.

6. Compliance Mapping

What This Means: This section translates our findings into the specific regulatory language your auditor, compliance officer, or insurance company needs to see. You don't need to understand these control numbers — just send the relevant section to whoever is asking.

6.1 HIPAA Security Rule

Finding	HIPAA Control	Requirement	Status
MIL-001	§ 164.312(a)(1)	Access Control — Unique User Identification	**Remediation Required**
MIL-001	§ 164.312(d)	Person or Entity Authentication	**Remediation Required**
MIL-002	§ 164.312(e)(1)	Transmission Security — Integrity Controls	Improvement Recommended
MIL-003	§ 164.312(e)(1)	Transmission Security — Encryption	Improvement Recommended
—	§ 164.308(a)(8)	Evaluation — Technical Security Evaluation	**Satisfied by This Report**

6.2 SOC 2 Trust Services Criteria

Finding	SOC 2 Criteria	Description	Status
MIL-001	CC6.1	Logical and Physical Access Controls	**Remediation Required**
MIL-002	CC6.6	Restricting External Access	Improvement Recommended
MIL-003	CC7.1	Detection of Unauthorized Activities	Improvement Recommended
—	CC4.1	Monitoring — Ongoing Security Evaluations	**Satisfied by This Report**

6.3 Cyber Insurance Summary

This section is formatted for submission to cyber insurance carriers as evidence of annual penetration testing.

Item	Detail
Insured Organization	Acme Health Services, LLC
Testing Provider	Milo Security, Inc.
Test Date	March 3–4, 2026
Test Type	External Penetration Test + Web Application Assessment
Methodology	OWASP v4.2, PTES, NIST SP 800-115, CVSS v3.1
Overall Result	**PASSED — No critical or high-severity findings**
Critical Findings	0
High Findings	0
Medium Findings	1 — Remediation plan in place (30-day timeline)
Low Findings	2 — Remediation recommended (60-day timeline)
Remediation Commitment	All findings to be remediated and verified by May 4, 2026
Re-Test Scheduled	Yes — complimentary re-test upon remediation
Classification	Confidential — for insured and underwriter use only

7. Testing Tools & Techniques

Phase	Tools	Purpose
Reconnaissance	Nmap, Shodan, DNS enumeration, SSL Labs	Service discovery, port scanning, certificate analysis
Web App Testing	Burp Suite Pro, OWASP ZAP, custom scripts	OWASP Top 10, authentication testing, session analysis
API Testing	Postman, Burp Suite, fuzzing tools	Endpoint discovery, input validation, authorization testing
Network Testing	Nmap, Nessus, Metasploit (validation)	Vulnerability ID, fingerprinting, exploit validation
Manual Validation	Expert review, chained attack analysis	Business logic, false positive elimination, exploit proof

8. Appendix: CVSS Severity Scale

Severity	CVSS	Definition	Remediation SLA
Critical	9.0–10.0	Immediate risk; full system compromise or large-scale data breach possible	Immediate (24–48 hrs)
High	7.0–8.9	Significant risk; unauthorized access to sensitive data or systems	14 days
Medium	4.0–6.9	Moderate risk; exploitation requires conditions but could expose data	30 days
Low	0.1–3.9	Minor risk; defense improvement recommended, not immediately exploitable	60 days
Info	0.0	Best practice recommendation with no direct exploitability	Next dev cycle

9. Disclaimer & Confidentiality

Confidentiality Notice

This report is CONFIDENTIAL and intended solely for Acme Health Services and their authorized representatives, including compliance auditors, legal counsel, and cyber insurance underwriters. Distribution to other parties requires written consent from both Acme Health Services and Milo Security, Inc.

Limitations

A penetration test is a point-in-time assessment and cannot guarantee discovery of all vulnerabilities. New vulnerabilities may emerge after testing due to software updates, configuration changes, or newly disclosed threats. Milo Security recommends regular testing (at minimum annually) and continuous vulnerability monitoring.

Liability

Milo Security performed this assessment in accordance with industry best practices. All testing was non-destructive and within authorized scope. Milo Security assumes no liability for actions taken or not taken based on this report. Remediation decisions remain the sole responsibility of the client.

Milo Security, Inc.
support@milosecurity.com | www.milosecurity.com
We do your pentest.