Remediation Checklist

This checklist is for whoever is fixing the issues found in your pentest. It could be your IT person, your MSP, a freelance developer, or your internal team. Each item has step-by-step instructions. Check the box when it's done. Once everything is complete, request your free re-test from Milo to verify the fixes.

Client	Report ID	Test Date	Total Findings
Acme Health Services	MILO-2026-03-00847	March 3–4, 2026	3 (0 Critical, 0 High, 1 Medium, 2 Low)

Priority	Finding	Severity	Deadline
1	**Session Token Predictability**	**Medium**	**April 3, 2026**
2	**Missing Content Security Policy Headers**	**Low**	May 4, 2026
3	**Server Version Disclosure**	**Low**	May 4, 2026

Finding #1: Session Token Predictability

MEDIUM

Affected System: portal.acmehealth.com (Patient Portal)

What's Wrong: The patient portal creates predictable login session keys. An attacker could guess valid keys and access patient accounts without a password.

Deadline: April 3, 2026 (30 days from test date)

☐	Step	Action
☐	1	**Replace session token generator.** Your current code uses a predictable algorithm. Replace it with a cryptographically secure random number generator (CSPRNG). In Node.js: use `crypto.randomBytes(32).toString('hex')`. In Python: use `secrets.token_hex(32)`. In PHP: use `bin2hex(random_bytes(32))`.

☐	2	**Remove predictable components from tokens.** The current tokens include a timestamp prefix (ACME-SESS-YYYYMMDD). Remove all date, time, and sequential components. The entire token should be random.
☐	3	**Ensure minimum 128-bit entropy.** Token length should be at least 32 hex characters (128 bits). The current tokens have approximately 32 bits of effective entropy in the variable portion, which is insufficient.
☐	4	**Add session rotation on auth changes.** Generate a new session token whenever a user logs in, changes their password, or elevates privileges. Invalidate the previous token.
☐	5	**Test your fix.** After deploying, create 10+ sessions in rapid succession and verify that tokens share no common prefixes or patterns. Each token should appear completely random.

Finding #2: Missing Content Security Policy Headers

LOW

Affected System: www.acmehealth.com (Main Website)

What's Wrong: Your website is missing security headers that tell browsers which content is allowed to load. This makes it easier for attackers to inject malicious scripts.

Deadline: May 4, 2026 (60 days from test date)

☐	Step	Action
☐	1	**Add Content-Security-Policy header.** Start with a restrictive policy and loosen as needed. Example starting point: `Content-Security-Policy: default-src 'self'; script-src 'self'; style-src 'self' 'unsafe-inline'; img-src 'self' data:`. Test thoroughly — CSP can break things if too restrictive.
☐	2	**Add X-Content-Type-Options header.** Add to your server config: `X-Content-Type-Options: nosniff`. This prevents browsers from interpreting files as a different type than declared.
☐	3	**Add X-Frame-Options header.** Add: `X-Frame-Options: DENY` (or SAMEORIGIN if your site uses iframes). This prevents clickjacking attacks.
☐	4	**Add Referrer-Policy header.** Add: `Referrer-Policy: strict-origin-when-cross-origin`. This limits how much URL information is shared with other sites.

☐	5	**Verify headers are present.** After deploying, check your headers at `securityheaders.com` — enter your URL and confirm all four headers appear correctly.

Finding #3: Server Version Disclosure

LOW

Affected System: api.acmehealth.com (API Server)

What's Wrong: Your server is broadcasting exactly what software and version it runs. This helps attackers target known vulnerabilities for that version.

Deadline: May 4, 2026 (60 days from test date)

☐	Step	Action
☐	1	**Suppress nginx version.** Open your nginx configuration file (usually `/etc/nginx/nginx.conf`) and add `server_tokens off;` inside the `http { }` block. Save and restart nginx: `sudo nginx -t && sudo systemctl reload nginx`.
☐	2	**Remove Express X-Powered-By header.** In your main Express application file (usually `app.js` or `server.js`), add this line near the top: `app.disable("x-powered-by");`. Redeploy the application.
☐	3	**Verify headers are suppressed.** Run: `curl -I https://api.acmehealth.com` and confirm that the response no longer includes `Server: nginx/1.24.0` or `X-Powered-By: Express`. The Server header may still say "nginx" without the version — that is acceptable.

All items fixed? Request your free re-test.

Once you've completed all the steps above, Milo will re-test your systems at no additional cost to verify everything is resolved. Your report will be updated with a clean addendum confirming all findings have been remediated.

Email: support@milosecurity.com
Subject line: Re-Test Request — MILO-2026-03-00847

Or visit **www.milosecurity.com/retest** and enter your Report ID.

This checklist corresponds to Milo Penetration Test Report MILO-2026-03-00847. For full technical details, evidence, and compliance mappings, refer to the complete report.