INDEPENDENT PENETRATION TEST ATTESTATION & REMEDIATION CLOSE-OUT

To: Ateminium Product Owner

Subject: Final Security Assessment of https://ateminium.com

Assessment Period: 6–14 August 2026

Confirmation Review Date: 4 September 2026

I, Atem Manyok, conducted an independent penetration test of Ateminium (https://ateminium.com), a multi-tenant cloud schools management system for South Sudan secondary schools, between 6 and 14 August 2026.

Testing followed a manual-first methodology aligned with OWASP Web Application Security Testing Guide principles, supplemented by automated scanning (OWASP ZAP v2.17.0) and network reconnaissance (Nmap 7.99). The assessment covered authentication, session management, authorization and tenant isolation, input handling, file upload security, security headers, and configuration review.

FINDINGS SUMMARY

I reported findings to the vendor. After analysis against the application's architecture, scanner-reported SQL injection on Next.js _rsc parameters was not confirmed as a database vulnerability; session-fixation and CSRF alerts that referred to the Vercel _vcrcs cookie were not the application session (ateminium_access_token). These scanner findings are not carried forward as confirmed vulnerabilities.

The following verified issues were identified during the assessment:

1. Account enumeration via login error messages — Medium
2. JavaScript-accessible session token in sessionStorage — High
3. No session idle timeout for privileged roles — Medium

4. Weak Content Security Policy (unsafe-eval and unsafe-inline) — Medium
5. No multi-factor authentication for school administrators — Medium

REMEDIATION UNDERTAKEN BY VENDOR

The vendor subsequently addressed all five findings raised during the assessment:

1. Account enumeration via login error messages
   Remediation Implemented: Unified 401 message: "Sign-in details were not accepted"
2. JavaScript-accessible session token in sessionStorage
   Remediation Implemented: JWT now HttpOnly cookie only; no token in client storage
3. No session idle timeout for privileged roles
   Remediation Implemented: 2-hour absolute expiry; 30-minute idle timeout for admins
4. Weak Content Security Policy
   Remediation Implemented: unsafe-eval removed; connect-src restricted
5. No multi-factor authentication for school administrators
   Remediation Implemented: Passkey-based MFA implemented for school administrators

CONFIRMATION PASS

On 4 September 2026, I performed a focused confirmation pass of the remediated items. The following were verified and confirmed effective:

LOGIN ENUMERATION
Invalid credentials return identical "Sign-in details were not accepted" responses.

COOKIE-ONLY SESSION
ateminium_access_token is HttpOnly, Secure, SameSite=Lax; no JWT in client storage.

Session lifetime and idle timeout
Admin sessions: 2-hour absolute expiry; 30-minute idle timeout enforced.

CSP TIGHTENING
unsafe-eval removed; connect-src restricted.

MFA FOR SCHOOL ADMINISTRATORS
Passkey-based MFA implemented and functional.

Controls that held during the original test remain in place, including HTTPS with HSTS, tenant isolation, role-based authorization, brute-force lockout, password-reset token handling, upload restrictions, and clickjacking defences.

RESIDUAL RISK

The following residual risks are acknowledged and accepted:

- CSP unsafe-inline remains pending a nonce-based policy
- SameSite=Lax on the session cookie (intentional for login flows)
- Student and teacher accounts are not required to use MFA in this release
- Public HTML may still present Access-Control-Allow-Origin: * without credentials
- Profile cache in local storage contains display data only; the session secret is not stored there

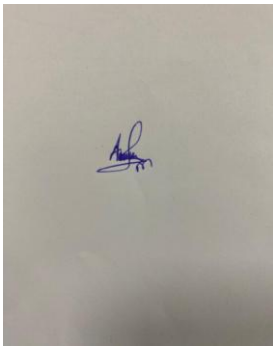
PROFESSIONAL OPINION

I do not represent that Ateminium is free of all defects or cannot be breached. Based on the manual testing performed between 6–14 August 2026, the remediation confirmed on 4 September 2026, and the residual risks noted above, it is my professional opinion that:

Ateminium (https://ateminium.com) implements appropriate technical security controls for a multi-tenant school management platform of this nature. The verified security findings identified during the assessment have

been satisfactorily remediated. The platform is suitable for production use with South Sudan secondary schools.

SIGNED:



ATEM MANYOK

PENETRATION TESTER

4 September 2026

atemmanyok211@gmail.com

+250793225412