Security Audit Report

Web Application Assessment

Security Team

April 2026

Web Application Security Audit

68

Grade C+

Kurzfazit

Critical security issues must be resolved before production deployment.

Critical	High	Medium
5	12	23

Top Actions

1. Patch XXE vulnerability in XML parser
2. Enable HTTPS 1.3 minimum
3. Implement request rate limiting

Analysis

HIGH **XML External Entity (XXE) Injection**

The /api/parse endpoint accepts untrusted XML without entity expansion protection.

Recommendation

Disable XML entity expansion and validate against whitelist.

HIGH

Missing HTTP Security Headers

CSP, X-Frame-Options, and X-Content-Type-Options headers not configured.

Recommendation

Add security headers to all HTTP responses via WAF.

Impact Assessment

User Impact

Data Exposure

User PII and session tokens at risk

Exploitability

High

Public exploits available

Compliance

Non-Compliant

Violates OWASP Top 10

Recommended Actions

Immediate (24h) 2 actions

Disable XML parsing or validate input

Impact critical
Effort 1h
Role Backend

Blocks XXE attacks

Enable security headers via WAF

Impact critical
Effort 30m
Role DevOps

Mitigates XSS

Short-term (1 week) 2 actions

Upgrade TLS to 1.3 minimum

Impact high
Effort 4h
Role DevOps

Eliminates weak ciphers

Implement rate limiting

Impact high
Effort 2h
Role Backend

Prevents brute force

Schedule Remediation Review

Our team can assist with patch deployment and verification testing.

Book a Session →