
Security Audit Report

Web Application Assessment

Web Application Security Audit

68

Grade C+



Kurzfazit

Critical security issues must be resolved before production deployment.

Critical

5

High

12

Medium

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

Short-term (1 week) 2 actions

Disable XML parsing or validate input

Impactcritical

Effort1h

RoleBackend

Blocks XXE attacks

Upgrade TLS to 1.3 minimum

Impacthigh

Effort4h

RoleDevOps

Eliminates weak ciphers

Enable security headers via WAF

Impactcritical

Effort30m

RoleDevOps

Mitigates XSS

Implement rate limiting

Impacthigh

Effort2h

RoleBackend

Prevents brute force

Schedule Remediation Review

Our team can assist with patch deployment and verification testing.

Book a Session →