Security Scan Report

Scanned Website: https://kupos.cl
Scan Date: September 3, 2025 at 01:07 PM
Generated by: Ayash Ahmad
Contact: bhatashu666@gmail.com

Comprehensive Security Analysis Report

Generated: September 3, 2025
Scan Target: kupos.cl
Pages Analyzed: 1

Executive Security Assessment

Overall Security Grade: C- (59/100)
Risk Level: MEDIUM

Key Security Metrics

- **Pages Scanned:** 1
- **Total Security Issues:** 11
- **Critical Vulnerabilities:** 0
- **High-Risk Issues:** 3
- **Average Response Time:** 244ms

Critical Findings

HIGH: 3 high-severity issues should be addressed within 48 hours

Immediate Actions Required

No immediate actions required

Business Impact

LOW-MODERATE BUSINESS RISK: Security improvements recommended to maintain good security posture.

Technical Security Analysis

Infrastructure Overview

- **Domains Analyzed:** kupos.cl
- **Technologies Detected:**
- **Total Pages Scanned:** 1

Security Issues by Category

Transport Security

- **Total Issues:** 1
- **Severity Breakdown:**
    - Critical: 0
    - High: 1
    - Medium: 0
    - Low: 0

Top Issues:

- Missing HSTS Header: HTTP Strict Transport Security (HSTS) header is missing, allowing potential downgrade attacks.

Security Headers

- **Total Issues:** 3
- **Severity Breakdown:**
    - Critical: 0
    - High: 1
    - Medium: 2
    - Low: 0

Top Issues:

- Missing Content Security Policy: Content Security Policy (CSP) header is missing, making the site vulnerable to XSS attacks.
- Missing Clickjacking Protection: No X-Frame-Options header or CSP frame-ancestors directive found.
- Missing X-Content-Type-Options: X-Content-Type-Options header is missing or not set to nosniff.

Privacy & Data Protection

- **Total Issues:** 5
- **Severity Breakdown:**
    - Critical: 0
    - High: 0
    - Medium: 0
    - Low: 4

Top Issues:

- Missing Referrer Policy: Referrer-Policy header is missing, potentially leaking sensitive information.
- Missing Permissions Policy: Permissions-Policy header is missing, allowing unrestricted feature access.
- Missing Cross-Origin Resource Policy: CORP header missing, allowing cross-origin resource access.

Content Security

- **Total Issues:** 1
- **Severity Breakdown:**
    - Critical: 0
    - High: 1
    - Medium: 0
    - Low: 0

Top Issues:

- Mixed Content Detected: Found 1 HTTP resources on HTTPS page, creating security vulnerabilities.

Server Configuration

- **Total Issues:** 1
- **Severity Breakdown:**
    - Critical: 0
    - High: 0
    - Medium: 0
    - Low: 1

Top Issues:

- HTTP Error 403: Server returned HTTP 403 error.

Performance Analysis

- **Average Response Time:** 244ms
- **Total Content Size:** 1KB
- **Fastest Page:** 244ms
- **Slowest Page:** 244ms

Security Score Distribution

- A (90-100): 0 pages
- B (80-89): 0 pages
- C (70-79): 0 pages
- D (60-69): 0 pages
- F (0-59): 1 pages

Risk Assessment Matrix

Overall Risk Score: 24

Risk Factors

- **Critical Vulnerabilities:** 0 (Risk Score: 0)
- **High Severity Issues:** 3 (Risk Score: 15)
- **Medium Severity Issues:** 2 (Risk Score: 4)
- **Low Severity Issues:** 5 (Risk Score: 5)

Risk by Category

- **Transport Security:** 1 issues (Max Severity: HIGH)
- **Security Headers:** 3 issues (Max Severity: HIGH)
- **Privacy & Data Protection:** 5 issues (Max Severity: LOW)
- **Content Security:** 1 issues (Max Severity: HIGH)
- **Server Configuration:** 1 issues (Max Severity: LOW)

Risk Timeline

- **Immediate (0-48 hours):** 0 critical issues
- **Short-term (1-4 weeks):** 3 high-priority issues
- **Long-term (1-6 months):** 7 medium/low priority issues

Potential Business Impact

Moderate risk that could impact business operations and customer trust. Prioritize security improvements.

Security Compliance Assessment

OWASP Top 10 2021 Compliance

Score: 78%
⚠ Needs improvement

General Data Protection Regulation (GDPR)

Score: 75%
⚠ Privacy improvements needed

Payment Card Industry (PCI DSS)

Score: 100%
Good compliance

ISO 27001 Security Controls

Score: 83.5%
Good compliance

Compliance Summary

- **Overall Compliance Score:** 78%
- **Standards Met:** 39/50
- **Critical Gaps:** 0

Security Remediation Roadmap

Phase 1: Immediate Actions (0-48 hours)

Priority: CRITICAL

Phase 2: Short-term Improvements (1-4 weeks)

Priority: HIGH

1. **Missing HSTS Header**
    - Category: Transport Security
    - Impact: HIGH
    - Action: Add Strict-Transport-Security header with max-age of at least 31536000 seconds (1 year).
2. **Missing Content Security Policy**
    - Category: Security Headers
    - Impact: HIGH
    - Action: Implement a strict Content Security Policy to prevent XSS and data injection attacks.
3. **Mixed Content Detected**
    - Category: Content Security
    - Impact: HIGH
    - Action: Replace all HTTP resources with HTTPS equivalents.

Phase 3: Long-term Enhancements (1-6 months)

Priority: MEDIUM/LOW

1. **Missing Clickjacking Protection**
    - Category: Security Headers
    - Impact: MEDIUM
    - Action: Add X-Frame-Options: DENY or SAMEORIGIN, or use CSP frame-ancestors directive.
2. **Missing X-Content-Type-Options**
    - Category: Security Headers
    - Impact: MEDIUM
    - Action: Set X-Content-Type-Options: nosniff to prevent MIME type sniffing.
3. **Missing Referrer Policy**
    - Category: Privacy & Data Protection
    - Impact: LOW
    - Action: Set Referrer-Policy to strict-origin-when-cross-origin or stricter.
4. **Missing Permissions Policy**
    - Category: Privacy & Data Protection
    - Impact: LOW
    - Action: Implement Permissions-Policy to control browser feature access.
5. **Missing Cross-Origin Resource Policy**

- Category: Privacy & Data Protection
- Impact: LOW
- Action: Set Cross-Origin-Resource-Policy to same-site or same-origin as appropriate.

6. **Missing Cross-Origin Embedder Policy**

   - Category: Privacy & Data Protection
   - Impact: INFO
   - Action: Consider setting Cross-Origin-Embedder-Policy if using advanced features.

7. **Missing Cross-Origin Opener Policy**

   - Category: Privacy & Data Protection
   - Impact: LOW
   - Action: Set Cross-Origin-Opener-Policy to same-origin for better isolation.

8. **HTTP Error 403**

   - Category: Server Configuration
   - Impact: LOW
   - Action: Investigate server configuration and fix the underlying issue.

Implementation Timeline

Week 1-2: Address all critical security vulnerabilities
Week 3-4: Implement high-priority security improvements
Month 2-3: Deploy medium-priority enhancements
Month 4-6: Complete long-term security initiatives

Resource Requirements

Estimated Effort: 44 hours
Team Requirements: Security engineer, DevOps engineer, Developer
Budget Considerations: SSL certificates, security tools, potential consulting
Timeline: 3-6 months for complete implementation

Security Trend Analysis

Current Security Posture

- **Security Maturity Level:** Initial
- **Most Common Issue Type:** Privacy & Data Protection
- **Security Hotspots:** https://kupos.cl (11 issues)

Recommendations for Improvement

• Consider adopting modern security frameworks and tools
• Implement continuous security monitoring
• Establish regular security training for development team

Industry Benchmark Comparison

Security Score Comparison

- **Your Score:** 59
- **Industry Average:** 75
- **Performance:** ⚠ Below Average

Issue Density Comparison

- **Your Issues per Page:** 11.0
- **Industry Average:** 3.2
- **Performance:** ⚠ Worse than Average

Performance Comparison

- **Your Response Time:** 244ms
- **Industry Average:** 1200ms
- **Performance:** Faster than Average

Appendix

Methodology

This security assessment was conducted using advanced automated scanning techniques combined with AI-powered analysis. The scan evaluated multiple security domains including:

- Transport Layer Security (HTTPS/TLS)
- Security Headers Implementation
- Content Security Policies
- Authentication and Session Management
- Input Validation and Output Encoding
- Information Disclosure Prevention
- Server Configuration Security
- Privacy and Data Protection Measures

Limitations

- This is an automated assessment and may not identify all security vulnerabilities
- Manual penetration testing is recommended for critical applications
- Results are based on publicly accessible information only
- Some issues may require additional context for accurate assessment

Next Steps

1. Review and prioritize identified security issues
2. Implement immediate fixes for critical vulnerabilities
3. Develop a comprehensive security improvement plan
4. Schedule regular security assessments
5. Consider professional penetration testing for critical systems

---

Report generated by AI Security Agent v2.0
For questions or support, contact: bhatashu666@gmail.com