

# Security Scan Report

Created by: Ayash Ahmad

Email: bhatashu666@gmail.com

---

## Security Scan Summary

### Executive Summary

The security scan of kupos.cl revealed an overall security score of **54%** with a **MEDIUM** risk level. The scan identified 0 critical, 2 high, 2 medium, and 3 low severity issues across 1 URLs.

### Key Findings

- **missing\_hsts** (high): Add Strict-Transport-Security - Found on 1 pages
- **missing\_csp** (high): Add Content-Security-Policy - Found on 1 pages
- **x\_content\_type\_options** (medium): Set X-Content-Type-Options: nosniff - Found on 1 pages
- **clickjacking** (medium): Add X-Frame-Options or frame-ancestors in CSP - Found on 1 pages
- **missing\_referrer\_policy** (low): Add Referrer-Policy - Found on 1 pages

### Top Recommendations

1. Implement a Content Security Policy (CSP) to prevent XSS attacks by specifying which dynamic resources are allowed to load.
2. Enable HTTP Strict Transport Security (HSTS) to ensure that browsers always connect to your site over HTTPS.
3. Prevent clickjacking attacks by implementing X-Frame-Options or frame-ancestors in your Content Security Policy.

### Remediation Steps

1. **Security Headers:** Implement all missing security headers in your web server configuration or application code.
  - Add Content-Security-Policy to restrict resource loading
  - Enable Strict-Transport-Security with a long max-age
  - Set X-Content-Type-Options to nosniff
  - Configure X-Frame-Options or frame-ancestors in CSP
2. **HTTPS Implementation:** Ensure all pages are served over HTTPS.
  - Obtain an SSL certificate (Let's Encrypt offers free certificates)
  - Configure your web server to redirect HTTP to HTTPS
  - Update all internal links to use HTTPS
3. **Cookie Security:** Review and update all cookies with proper security flags.
  - Add Secure flag to ensure cookies are only sent over HTTPS
  - Add HttpOnly flag to prevent JavaScript access to sensitive cookies
  - Set SameSite attribute to Lax or Strict to prevent CSRF attacks

This analysis was generated automatically based on the scan results. For a more comprehensive assessment, consider engaging a security professional.