Xerago SecureScan Report

Target URL: https://www.xerago.com/

Risk Level: HIGH

Summary:

Risk Level: HIGH

SQL Injection scan inconclusive

Missing Content-Security-Policy header

Missing Permissions-Policy header

Server header present: cloudflare

CSP missing frame-ancestors directive (clickjacking risk)

No CSRF token found in forms

security.txt missing

Findings & Recommendations:

- SQL Injection scan inconclusive

  Recommendation: Sanitize and parameterize all database queries.

- Missing Content-Security-Policy header

  Recommendation: Add a Content-Security-Policy header.

- Missing Permissions-Policy header

  Recommendation: Add Permissions-Policy header.

- Server header present: cloudflare

  Recommendation: Remove or obfuscate X-Powered-By/Server headers.

- CSP missing frame-ancestors directive (clickjacking risk)

  Recommendation: Review this issue and apply best security practices.

- No CSRF token found in forms

  Recommendation: Implement CSRF protection for all forms.

- security.txt missing

  Recommendation: Review this issue and apply best security practices.