Security Audit Report: A4I Welcome Page

# ✅ Best Practices Implemented

These measures reduce known vulnerabilities and improve overall security posture.

|  |  |  |
| --- | --- | --- |
| **Issue that Needs Attention** | **Risk Level** | **Approach Taken** |
| Cross-site scripting (XSS) | Medium | Content-Security-Policy restricts default sources and limits inline scripts/styles. |
| Clickjacking | High | X-Frame-Options set to DENY. |
| MIME Sniffing | Medium | X-Content-Type-Options set to nosniff. |
| Referrer Leakage | Low | meta name='referrer' set to no-referrer. |
| External Resources | Medium | Google Fonts loaded with crossorigin attribute. |
| Navigation Interception | Medium | Dynamic loader restricts navigation to expected hash links. |
| Subresource Integrity (SRI) | Medium | Use SRI hashes for external fonts/scripts to prevent tampering. |

# 🚨 Recommendations for Improvement

These suggestions highlight areas of potential risk and provide guidance to enhance security.

|  |  |  |
| --- | --- | --- |
| **Issue that Needs Attention** | **Risk Level** | **Recommendations** |
| Use of Inline Scripts | Medium | Move dynamic loader script to an external JS file and disallow 'unsafe-inline' in CSP. |
| Use of Inline Styles | Low | Move <style> blocks to external CSS files to tighten CSP. |
| No HTTPS Enforced | High | Ensure deployment over HTTPS with HSTS headers. |
| Home Link Uses Hash | Low | Consider a fallback strategy to restore full page context for non-JS users. |
| External Navigation Validation | Medium | Add validation or allowlist for hash-based routing targets. |
| Cache Control | Low | Add HTTP headers to control content caching behavior. |

# 📋 Summary

Your A4I Welcome page adheres to several strong security practices such as CSP use, clickjacking protection, MIME sniffing prevention, safe external links, and restrictive default source rules. However, risks remain due to inline scripts/styles, lack of HTTPS enforcement, and absence of Subresource Integrity (SRI). Addressing these can significantly reduce attack surfaces like XSS or MITM.