0.0 SCOPE OF REVIEW

This runbook is based on a forensic review of 15 rendered pages from the domain [redacted]. Its purpose is to identify material AI-readiness, indexability, technical SEO, and governance signals that may affect how the site is interpreted by search engines and AI systems.

The findings in this document should be read as:

- confirmed observations for the audited sample, and
- directional indicators of broader governance patterns that may also exist elsewhere on the site.

Without a wider crawl or page-set validation, these findings should not be treated as full-site confirmation.

---

[1] Evidence: Audit scope details (JSON: audit_scope.sampled_pages_count=15, audit_scope.primary_url=[redacted])

0.1 EXECUTIVE SUMMARY

On the audited sample of 15 pages, we observed a critical issue where AI crawlers like GPTBot and Gemini were unable to access content due to non-success HTTP status codes[1]. This represents a fundamental barrier to how AI systems can process and understand the site's content, potentially impacting visibility and data utilization by advanced AI models.

This runbook highlights several core signals:

- **AI Crawler Accessibility**: Key AI crawlers are currently blocked from accessing content, hindering AI-driven discovery and processing[1].
- **Missing Structured Data**: No structured data was detected on the audited pages, limiting the site's ability to provide rich results and context to search engines and AI systems[2].
- **Suboptimal Mobile Performance**: Mobile PageSpeed scores are low, with critical metrics like Largest Contentful Paint (LCP) and Total Blocking Time (TBT) failing thresholds, impacting user experience and search ranking[3].

- **Incomplete Security Headers**: Several important security headers are missing, potentially exposing the site to vulnerabilities and impacting trust signals[4].

This runbook serves as an entry diagnostic to prioritize immediate actions and validate broader patterns before scaling remediation efforts.

---

[1] Evidence: AI crawler access status for GPTBot and Gemini (JSON: snapshots.web_ai_crawler_readiness_snapshot.robots.parsed.gptbot.allowed=false, snapshots.web_ai_crawler_readiness_snapshot.robots.parsed.gemini.allowed=false)

[2] Evidence: Schema analysis coverage (JSON: snapshots.web_ai_crawler_readiness_snapshot.rendered_pages_sample[*].schema_analysis.coverage_ratio=0)*

[3] Evidence: PageSpeed mobile performance score (JSON: snapshots.web_ai_crawler_readiness_snapshot.pagespeed_min.normalized.pagespeed_score_mobile=40)

[4] Evidence: Missing security headers (JSON: snapshots.web_ai_crawler_readiness_snapshot.crawl_raw.pages[*].headers.missing_headers=["Strict-Transport-Security","X-Frame-Options","Referrer-Policy"])*

0.2 HOW TO READ THIS RUNBOOK

This document is designed as a decision-support diagnostic, not as a full-site inventory. It should be used to answer three questions:

1. Which risks are already confirmed on the audited page?
2. Which of those risks are likely to originate from broader governance or template patterns?
3. Which items should be validated on a wider page sample before remediation is scaled?

The practical purpose of this runbook is to reduce decision uncertainty early and to convert a limited audit surface into a prioritized next-step plan.

0.3 BUSINESS IMPACT

Current State

On the audited sample of 15 pages, several critical issues were observed:

- **AI Crawler Access**: AI crawlers like GPTBot and Gemini received non-success HTTP status codes, preventing content access[1]. This may indicate a fundamental misconfiguration impacting how AI systems can discover and process the site's content.
- **Structured Data**: No structured data was detected on any of the 15 audited pages[2]. This limits the site's ability to appear in rich search results and provide contextual information to AI models.
- **Performance**: The mobile PageSpeed score was 40, with key metrics like Largest Contentful Paint (LCP) at 8.7 seconds and Total Blocking Time (TBT) at 520 milliseconds, both failing established thresholds[3]. This can lead to poor user experience and negatively impact search engine rankings.
- **Security**: Several critical security headers, including `Strict-Transport-Security`, `X-Frame-Options`, and `Referrer-Policy`, were missing from the audited pages[4]. This may expose the site to various security vulnerabilities.
- **Canonical Tags**: 3 out of 15 audited pages were missing canonical tags[5]. This can lead to indexation issues and dilute search authority.

Governance Implication

Even when identified on a limited audited sample of 15 pages, these signals matter because they often originate in shared templates, publishing workflows, governance gaps, or missing implementation standards. Addressing these issues at their root can prevent their recurrence across the site and ensure consistent quality. Broader site-wide pattern should be validated separately.

Decision Support

This runbook supports management decisions in two ways: (a) highlights what is demonstrably visible on the audited sample of 15 pages, (b) identifies which issues justify broader validation before company-wide remediation is commissioned.

What is Required to Quantify

- **AI Crawler Access Impact**: Requires analysis of server logs for AI crawler traffic and potential content indexing by AI models.
- **Structured Data Impact**: Google Analytics 4 (GA4) to measure rich result impressions and clicks, and Google Search Console (GSC) data for schema coverage.
- **Performance Impact**: Google Analytics 4 (GA4) for user engagement metrics (e.g., bounce rate, conversion rate) correlated with page load times, and GSC data for Core Web Vitals performance.
- **Security Impact**: Requires security incident reports and vulnerability scans to quantify potential risks.
- **Canonical Tag Impact**: Requires GSC data for index coverage and canonicalization issues.

---

[1] Evidence: AI crawler access status for GPTBot and Gemini (JSON: snapshots.web_ai_crawler_readiness_snapshot.robots.parsed.gptbot.allowed=false, snapshots.web_ai_crawler_readiness_snapshot.robots.parsed.gemini.allowed=false)

[2] Evidence: Schema analysis coverage (JSON: snapshots.web_ai_crawler_readiness_snapshot.rendered_pages_sample[*].schema_analysis.coverage_ratio=0)*

[3] Evidence: PageSpeed mobile performance metrics (JSON: snapshots.web_ai_crawler_readiness_snapshot.pagespeed_min.normalized.pagespeed_score_mobile=40, snapshots.web_ai_crawler_readiness_snapshot.pagespeed_min.normalized.lcp_seconds=8.7, snapshots.web_ai_crawler_readiness_snapshot.pagespeed_min.normalized.tbt_ms=520)

[4] Evidence: Missing security headers (JSON: snapshots.web_ai_crawler_readiness_snapshot.crawl_raw.pages[*].headers.missing_headers=["Strict-Transport-Security","X-Frame-Options","Referrer-Policy"])*

[5] Evidence: Canonical tag coverage (JSON: snapshots.web_ai_crawler_readiness_snapshot.rendered_pages_sample[*].indexability.pages_missing=3)*

0.4 COMPETITIVE CONTEXT

What the Audit Does and Does Not Contain

This diagnostic provides a forensic snapshot of AI readiness and technical health based on a representative page sample. It does not include a competitive benchmark against specific rivals, nor does it quantify market share or revenue impact. Its primary goal is to identify internal technical and governance risks.

First-Mover Window

The rapid evolution of AI models and their increasing role in content discovery and synthesis creates a strategic window for businesses. Early adoption of AI-friendly web practices can lead to enhanced visibility, better content understanding by AI systems, and potential advantages in future search and content platforms. Conversely, neglecting these foundational elements can result in a competitive disadvantage as AI-driven content consumption grows.

Technical Debt Context

Data not available for this audit scope.

0.5 DELIVERY OVERVIEW

Timeline Summary

Detailed time estimates are not available within this audit scope and will be confirmed during implementation planning.

Resource & Access Requirements

Successful remediation will require collaboration across several teams and access to key systems:

- **Technical Team**: Developers and DevOps engineers for server-level configurations (e.g., `robots.txt`, security headers) and front-end code adjustments (e.g., structured data, performance optimizations).

- **Content/SEO Team**: For strategic guidance on structured data implementation and canonical tag review.
- **Access**: Administrative access to the web server configuration, Content Management System (CMS), Google Search Console, and Google Analytics 4.

Success Metrics + Measurement

1. **AI Crawler Access**: AI crawlers (e.g., GPTBot, Gemini) successfully access and crawl content, indicated by 200 HTTP status codes.
    - Measurement: Regular checks of server logs and `robots.txt` validation tools.
2. **Structured Data**: Key pages implement relevant JSON-LD structured data, enabling rich results.
    - Measurement: Google Search Console Rich Results report and schema validation tools.
3. **Performance**: Mobile PageSpeed score consistently above 70, with Largest Contentful Paint (LCP) below 2.5 seconds and Total Blocking Time (TBT) below 200ms.
    - Measurement: Google PageSpeed Insights and Google Search Console Core Web Vitals report.
4. **Security**: All critical security headers (Strict-Transport-Security, X-Frame-Options, Referrer-Policy) are present and correctly configured.
    - Measurement: Header inspection tools and security vulnerability scans.
5. **Canonical Tags**: All key pages have correctly implemented canonical tags.
    - Measurement: Google Search Console index coverage report.

1. DETECTED TECHNOLOGY STACK

Based on the available audit signals, no specific technology stack components such as a Content Management System (CMS), hosting provider, or Web Application Firewall/CDN could be definitively identified. While this means specific platform-level optimizations cannot be immediately prescribed, it also implies that many potential fixes would likely reside within the application layer itself.

Confirmed technical signals:

- A Content Management System (CMS) could not be confirmed from available signals.[1]
- The hosting provider could not be confirmed from available signals.[1]
- A Web Application Firewall (WAF) or Content Delivery Network (CDN) could not be

confirmed from available signals.[1]
- No specific server technologies or web frameworks were detected.[1]

Implementation implications:

- Given the absence of confirmed platform layers, most technical remediations, including performance optimizations, structured data implementation, and security header configurations, would likely need to be addressed directly within the application's codebase or server configuration.
- Any future platform changes or additions, such as a CDN or CMS, should be evaluated for their potential to streamline these types of fixes.

This assessment is based on signals from the audited sample of 15 pages and should be confirmed during the implementation phase.[2]

---

[1] Evidence: No CMS detected (JSON: stack_detection.cms.name=null), No hosting provider detected (JSON: stack_detection.hosting.provider=null), No WAF/CDN detected (JSON: stack_detection.waf_cdn.provider=null), No server layers detected (JSON: stack_detection.server_layers=[]), No frameworks detected (JSON: stack_detection.frameworks=[])

[2] Evidence: Sampled pages count (JSON: audit_scope.sampled_pages_count=15)

2. TECHNICAL SUMMARY

This section provides a rapid overview of the technical posture of the audited website, highlighting areas of stability and identifying key risks that require attention.

AI crawler access

A primary blocking signal was detected for several key AI crawlers, including GPTBot and Gemini, indicating that access for these agents is currently restricted. While Google-Extended and ClaudeBot appear to have access, the overall posture is partial, which could limit visibility and processing by advanced AI models.[1]

Canonical and page identity

The canonical signal layer was partially confirmed, with 80% of the audited pages correctly implementing canonical tags. However, 3 out of 15 pages were missing this crucial signal, which can lead to issues with page identity and indexation in search engines.[2]

Structured data

No structured data (schema.org markup) was detected across the entire audited sample. The absence of schema significantly hinders machine readability and the potential for rich results in search engine listings, impacting how content is understood and presented.[3]

Performance and user experience

The website's performance posture is significantly below optimal thresholds, particularly on mobile. The PageSpeed score for mobile is 40, and key metrics like Largest Contentful Paint (LCP) at 8.7 seconds and Total Blocking Time (TBT) at 520 milliseconds indicate a poor user experience and potential negative impact on search rankings.[4]

Security headers

Baseline security headers are largely missing, with `Strict-Transport-Security`, `X-Frame-Options`, and `Referrer-Policy` not detected. While `X-Content-Type-Options` is present, the overall absence of these headers signals a vulnerability to common web attacks and can impact user trust.[5]

Sitemap and discoverability

A sitemap.xml file was detected and is accessible, indicating a foundational element for discoverability is in place. The contents of the sitemap appear valid and do not contain suspicious URLs, supporting efficient crawling by search engines.[6]

Closing Summary:

1. **Stable Areas:**
    - A sitemap.xml file is present and valid, aiding search engine discoverability.
    - Basic Open Graph metadata is correctly implemented, supporting social sharing.[7]
2. **Areas of Risk:**
    - Significant portions of AI crawler access are blocked, limiting advanced AI processing.
    - Canonical tags are inconsistently applied, potentially causing indexation

issues.

- Structured data is entirely absent, hindering machine readability and rich result potential.
- Website performance is critically low, impacting user experience and search ranking.
- Key security headers are missing, exposing the site to security vulnerabilities.

---

[1] Evidence: GPTBot blocked (JSON: crawler_access.gptbot.allowed=false), Gemini blocked (JSON: crawler_access.gemini.allowed=false), Google-Extended allowed (JSON: crawler_access.google_extended_allowed=true), ClaudeBot allowed (JSON: crawler_access.claudebot.allowed=true), AI access summary (JSON: crawler_access.ai_access_summary=partial)

[2] Evidence: Canonical status partial (JSON: content_signals.canonical.status=partial), Canonical coverage ratio (JSON: content_signals.canonical.coverage_ratio=0.8), Pages missing canonical (JSON: content_signals.canonical.pages_missing=3), Pages checked for canonical (JSON: content_signals.canonical.pages_checked=15)

[3] Evidence: Schema status fail (JSON: content_signals.schema.status=fail), Schema coverage ratio (JSON: content_signals.schema.coverage_ratio=0)

[4] Evidence: Performance status fail (JSON: performance_signals.status=fail), Mobile PageSpeed score (JSON: performance_signals.pagespeed_score_mobile=40), Largest Contentful Paint (JSON: performance_signals.lcp_seconds=8.7), Total Blocking Time (JSON: performance_signals.tbt_ms=520)

[5] Evidence: Security status fail (JSON: security_signals.status=fail), Missing security headers (JSON: security_signals.missing_headers=["Strict-Transport-Security","X-Frame-Options","Referrer-Policy"]), X-Content-Type-Options present (JSON: security_signals.x_content_type_options=true)

[6] Evidence: Sitemap detected (JSON: content_signals.sitemap.detected=true), Sitemap valid (JSON: content_signals.sitemap.valid=true), Sitemap suspicious URLs (JSON: content_signals.sitemap.urls_suspicious=false), Sitemap status (JSON: content_signals.sitemap.status=pass)

[7] Evidence: Open Graph status (JSON: content_signals.open_graph.status=pass)

3. CRITICAL ISSUES (Priority 1 — Implement Within 7 Days)

1) AI crawler accessibility issue

Issue ID: P1_AI_ACCESS_001

Severity: P1

Scope: Finding on a sample of 15 audited pages.

Reason: AI crawler returned non-success HTTP status.

Recommendation: Review `robots.txt` rules and ensure AI crawlers (`GPTBot`, `OAI-SearchBot`, `Google-Extended`, `Gemini-Deep-Research`, `ClaudeBot`, `Claude-SearchBot`, `PerplexityBot`) are not unintentionally blocked. If blocking is intentional, document the decision.

Evidence:

- GPTBot: blocked, Gemini: blocked

Retest Commands:

- `curl -A "GPTBot" -I [redacted]/`
- `curl -A "Google-Extended" -I [redacted]/`

4. HIGH PRIORITY ISSUES (Priority 2 — Implement Within 30 Days)

1) Structured data missing

Issue ID: P2_SCHEMA_001

Severity: P2

Scope: Finding on a sample of 15 audited pages.

Reason: No schema detected in the audited sample.

Recommendation: Implement JSON-LD structured data (`@type: WebSite`, `Organization` or `Product`) in the page `<head>`. Validate with Google Rich Results Test.

Evidence:

- Schema coverage: 0% — status: fail

Retest Commands:

- `curl -s [redacted]/ | python3 -c "import sys,json,re; html=sys.stdin.read();`

`blocks=re.findall(r'<script[^>]+type=[\'\"]application/ld\+json[\'\"][^>]>(.?)</script>', html, re.S); print(json.dumps(blocks, indent=2))"`

- `curl -A "GPTBot" -sI [redacted]/`

2) Performance thresholds failed

Issue ID: P2_PERFORMANCE_001

Severity: P2

Scope: Finding on a sample of 15 audited pages.

Reason: Performance thresholds failed for one or more key metrics.

Recommendation: Improve LCP: preload hero image (`<link rel="preload">`), lazy-load off-screen images. Reduce TBT: move non-critical JS to `defer`/`async`. Fix CLS: set explicit dimensions on images.

Evidence:

- LCP: 8.7s | CLS: 0.099 | TBT: 520ms | Failed: pagespeed_mobile, lcp, tbt

Retest Commands:

- `curl -o /dev/null -w "%{time_total}s  HTTP %{http_code}" -s [redacted]/`
- `curl "https://www.googleapis.com/pagespeedonline/v5/runPagespeed?url=[redacted]/&strategy=mobile" | python3 -c "import sys,json; d=json.load(sys.stdin); c=d['lighthouseResult']['categories']; print({k:round(v['score']*100) for k,v in c.items()})"`

3) Security headers missing

Issue ID: P2_SECURITY_HEADERS_001

Severity: P2

Scope: Finding on a sample of 15 audited pages.

Reason: Required security headers are missing.

Recommendation: Configure missing security headers at the web server level: `Strict-Transport-Security`, `X-Frame-Options`, `X-Content-Type-Options`, `Referrer-Policy`.

Evidence:

- Missing headers: Strict-Transport-Security, X-Frame-Options, Referrer-Policy

Retest Commands:

- `curl -sI [redacted]/ | grep -iE "strict-transport|x-frame|x-content-type|referrer-policy|content-security"`
- `curl -A "GPTBot" -sI [redacted]/ | grep -iE "strict-transport|x-frame|x-content-type|referrer-policy"`

6. IMPLEMENTATION TIMELINE

Time estimates for these tasks are not available. The following is a realistic sequential plan for addressing the identified issues, prioritizing critical items and foundational changes first.

1. **General Safety and Backup Procedures**
    - **Description:** Before any changes are implemented, ensure a full backup of the website, database, and server configurations is performed. Establish a clear rollback plan in case of unforeseen issues.
    - **Dependencies:** None.
    - **Parallel possible:** No.

1. **Address AI Crawler Accessibility Issue (P1_AI_ACCESS_001)**
    - **Description:** Review and adjust `robots.txt` rules to ensure that legitimate AI crawlers (e.g., GPTBot, Gemini, ClaudeBot) are not unintentionally blocked. Verify that the server returns a 200 HTTP status for these crawlers.
    - **Dependencies:** Completion of general safety and backup procedures.
    - **Parallel possible:** No.

1. **Implement Missing Security Headers (P2_SECURITY_HEADERS_001)**
    - **Description:** Configure the web server to include `Strict-Transport-Security`, `X-Frame-Options`, and `Referrer-Policy` headers. This is a server-level configuration change.
    - **Dependencies:** Completion of general safety and backup procedures.
    - **Parallel possible:** No.

1. **Implement Structured Data (P2_SCHEMA_001)**

- **Description:** Develop and implement JSON-LD structured data (e.g., `@type: WebSite`, `Organization`, or `Product`) within the `<head>` section of the website's pages.
- **Dependencies:** Completion of server-level configurations (tasks 2 and 3).
- **Parallel possible:** Yes, with task 5 if different teams/skill sets are involved.

1. **Improve Performance Thresholds (P2_PERFORMANCE_001)**
    - **Description:** Optimize page load performance by addressing issues related to Largest Contentful Paint (LCP), Total Blocking Time (TBT), and Cumulative Layout Shift (CLS). This may involve image optimization, lazy loading, preloading critical resources, and deferring non-critical JavaScript.
    - **Dependencies:** Completion of server-level configurations (tasks 2 and 3).
    - **Parallel possible:** Yes, with task 4 if different teams/skill sets are involved.

7. BUSINESS IMPACT SUMMARY

This section outlines the potential business impact of resolving the identified issues, based on the audit findings.

1. **Total resolved issues count**
    i. **Priority 1 (P1):**
        - P1_AI_ACCESS_001: AI crawler accessibility issue

    ii. **Priority 2 (P2):**
        - P2_SCHEMA_001: Structured data missing
        - P2_PERFORMANCE_001: Performance thresholds failed
        - P2_SECURITY_HEADERS_001: Security headers missing

    iii. **Priority 3 (P3):**
        - None identified

1. **Expected technical impact (qualitative)**
    - **AI crawler accessibility issue:** Resolving this issue will ensure that AI crawlers can properly access and process the website's content, which is crucial for content discovery and potential inclusion in AI-driven search

results and knowledge bases.[2]

- **Structured data missing:** Implementing structured data will help search engines better understand the content and context of the website, potentially leading to enhanced visibility in search results and eligibility for rich snippets.[3]
- **Performance thresholds failed:** Addressing performance issues will result in faster page load times, a smoother user experience, and improved Core Web Vitals scores, which are important ranking factors for search engines.[4]
- **Security headers missing:** Configuring the missing security headers will enhance the website's overall security posture, protecting users from common web vulnerabilities such as cross-site scripting (XSS), clickjacking, and insecure data transmission.[5]

1. **Missing data for quantification**

To fully quantify the business impact of these changes, the following external data sources are required:

- **Google Analytics 4 (GA4):** To measure user engagement metrics (e.g., bounce rate, session duration, conversion rates) before and after implementation.
- **Google Search Console (GSC):** To track organic search performance (e.g., impressions, clicks, click-through rates, average position), Core Web Vitals performance, and crawl statistics.
- **Server Logs:** To analyze AI crawler access patterns, HTTP status codes returned to various user agents, and overall server response times.

1. **Closing statement**

Implementing these recommendations will significantly improve the website's technical foundation, enhancing its visibility to search engines and AI systems, improving user experience, and strengthening security. Regular monitoring and a robust governance framework will be essential to maintain these improvements and adapt to evolving web standards and user expectations.

---

[1] Evidence: No P3 issues found (JSON: issue_candidates.p3=[])

[2] Evidence: AI crawler returned non-success HTTP status (JSON: issue_candidates.p1[0].reason="AI crawler returned non-success HTTP status.")

[3] Evidence: No schema detected in the audited sample (JSON: issue_candidates.p2[0].reason="No schema detected in the audited sample.")

[4] Evidence: Performance thresholds failed for one or more key metrics (JSON: issue_candidates.p2[1].reason="Performance thresholds failed for one or more key metrics.")

[5] Evidence: Required security headers are missing (JSON: issue_candidates.p2[2].reason="Required security headers are missing.")

8. IMPLEMENTATION OPTIONS

The remediation for the identified issues can be effectively managed within two primary layers of your web infrastructure. This approach offers a practical and feasible path forward, avoiding the need for a complete architectural overhaul.

Application Layer Fixes:

This layer is crucial for establishing a machine-readable identity for your pages. Fixes here directly impact how search engines and other automated systems understand and categorize your content.

- Implement correct canonical tags to prevent duplicate content issues.
- Add structured data (schema.org markup) to enhance content visibility in search results.
- Ensure Open Graph (OG) tags are correctly configured for social media sharing.
- Optimize rendering performance by preloading critical resources and deferring non-essential scripts.

CDN/WAF Layer Fixes (e.g., Cloudflare):

The CDN/WAF layer is vital for maintaining technical hygiene and ensuring consistent delivery standards across your site.

- Configure missing security headers like `Strict-Transport-Security` and `X-Frame-Options` to improve site security.
- Implement response-level rules to enforce best practices for content delivery.
- Apply selected performance optimizations, such as caching policies and image optimization, at the edge.

We recommend splitting the remediation work into two parallel streams: an "Application Team Stream" and an "Infrastructure/Cloudflare Team Stream." This parallel approach will significantly reduce the overall implementation time by allowing specialized teams to address their

respective areas concurrently.

It is important to note that the specific deployment workflow was not confirmed as part of this audit. While this does not impede the direction of the remediation, it means that clear ownership for each task will need to be established and confirmed during the implementation phase.

In practical terms, most of the identified fixes are achievable without fundamental architectural changes; the key to successful remediation lies in assigning clear ownership between your application development team and your infrastructure or Cloudflare management team.

9. NEXT STEPS

Here are the immediate next steps, prioritized by severity:

- P1_AI_ACCESS_001**: Review `robots.txt` rules to ensure AI crawlers are not unintentionally blocked.**
- P2_SCHEMA_001**: Implement JSON-LD structured data in the page `<head>` for all relevant pages.**
- P2_PERFORMANCE_001**: Address core web vital issues by optimizing LCP, TBT, and CLS metrics.**
- P2_SECURITY_HEADERS_001**: Configure missing security headers at the web server or CDN level.**

10. APPENDIX

Evidence Summary

- Rendered sample size: 15
- Primary audited URL: [redacted]/
- AI crawler access: GPTBot blocked, Gemini blocked
- Canonical status: partial
- Schema status: fail
- Open Graph status: pass
- Sitemap status: pass
- Performance status: fail (pagespeed_mobile, lcp, tbt)
- Missing security headers: Strict-Transport-Security, X-Frame-Options, Referrer-Policy

Consolidated Re-test Commands

- `curl -A "GPTBot" -I [redacted]/`
- `curl -A "Google-Extended" -I [redacted]/`
- `curl -A "ClaudeBot" -I [redacted]/`