Security Assessment Report

Web Security Assessment Report

By Netsectap Labs

Target Site: https://roadlesstrodden007-minda.github.io/news-aggregator/

Assessment Date: December 19, 2025

Assessor: Netsectap Labs

Client: External Assessment (GitHub Pages Site)

Report Version: 1.0

Status: [COMPLETE] Assessment Complete

Table of Contents

Executive Summary

Overall Security Rating

Current Score: 38/100 (Grade: F) **Classification**: Fail - Immediate action required **Production Status**: [WARNING] Multiple critical security headers missing

Key Findings

Strengths: - TLS 1.3 encryption enabled (latest protocol) - HSTS header present (1-year max-age) - Valid SSL certificate from Sectigo - HTTP/2 support enabled - Hosted on GitHub Pages with Fastly CDN

Critical Issues: - [WARNING] Missing Content Security Policy (CSP) - HIGH PRIORITY - [WARNING] Missing X-Frame-Options - HIGH PRIORITY (clickjacking risk) - [WARNING] Missing X-Content-Type-Options - MEDIUM PRIORITY - [WARNING] Missing Referrer-Policy - MEDIUM PRIORITY - [WARNING] Missing Permissions-Policy - MEDIUM PRIORITY - [WARNING] No Web Application Firewall (WAF) - GitHub Pages limitation - [WARNING] No DDoS protection beyond basic CDN - GitHub Pages limitation - [WARNING] No bot management - GitHub Pages limitation - [WARNING] Overly permissive CORS (access-control-allow-origin: *) - MEDIUM PRIORITY

Risk Assessment: **HIGH** The site is vulnerable to common web attacks including XSS, clickjacking, and MIME-sniffing attacks due to missing security headers. While GitHub Pages provides basic HTTPS and CDN, it lacks enterprise-grade protection layers.

Timeline & Investment

Metric	Value
Assessment Duration	15 minutes
Issues Found	9 (5 critical, 4 medium)
Critical Issues	5 security headers missing
Implementation Time	1-2 hours (add headers via meta tags or migrate)
Implementation Cost	$0 (meta tags) or $20-50/month (Cloudflare migration)

Score Breakdown

```
SSL/TLS Configuration:     15/20  (B+) - TLS 1.3 but RSA cert
Security Headers:           5/25  (F)  - Only 1/6 headers present
DDoS Protection:            8/15  (C+) - Fastly CDN only
Bot Management:             0/10  (F)  - None available
WAF (Firewall):             0/10  (F)  - None available
Privacy Controls:           2/10  (F)  - HSTS only, overly open CORS
Performance:                8/10  (B+) - HTTP/2, CDN caching
═══════════════════════════════════════════════════════
TOTAL:                     38/100 (F)
```

Path to Improvement

Option 1: Quick Fix (Meta Tags) - Score: ~58/100 (D) - Add security headers via HTML meta tags - Cost: $0 - Time: 1 hour - Limitation: Limited protection, meta tags less effective than HTTP headers

Option 2: CDN/Security Platform Migration - Score: ~85-95/100 (B to A+) - Migrate to a CDN/security platform with full HTTP header control - Enable security suite (WAF, DDoS protection, custom headers) - Platform options: Cloudflare, Akamai, AWS CloudFront, Fastly, Azure Front Door - Cost: $0-100/month (varies by provider and plan) - Time: 2-4 hours - Result: Enterprise-grade protection with vendor of your choice

Assessment Methodology

Testing Framework

This security assessment is based on industry-standard frameworks and best practices:

Primary Framework: OWASP Top 10 - Our assessment methodology aligns with the OWASP Top 10 Web Application Security Risks - Covers critical vulnerabilities including injection attacks, broken authentication, XSS, and security misconfigurations - Represents consensus among security experts on the most critical security risks

Additional Security Checks: Beyond OWASP Top 10, our assessment includes:

1. **Infrastructure Security**
   - CDN and edge protection configuration
   - DDoS mitigation capabilities
   - Load balancing and failover mechanisms
2. **Network Security**
   - DNS configuration and DNSSEC
   - SSL/TLS implementation and cipher strength
   - Certificate chain validation
3. **Web Security Headers**
   - Content Security Policy (CSP)
   - HTTP Strict Transport Security (HSTS)
   - X-Frame-Options, X-Content-Type-Options
   - Referrer Policy and Permissions Policy
4. **Bot & Automation Protection**
   - Bot detection and mitigation
   - Rate limiting and throttling
   - Challenge mechanisms (CAPTCHA, JavaScript challenges)
5. **Web Application Firewall (WAF)**
   - Rule coverage and effectiveness
   - False positive rate
   - Custom rule implementation
6. **Privacy & Compliance**
   - Cross-Origin Resource Sharing (CORS)
   - Cross-Origin policies (CORP, COEP, COOP)
   - Data protection mechanisms
7. **Performance & Availability**
   - HTTP/2 and HTTP/3 support
   - Caching strategies
   - Geographic distribution

Assessment Tools & Techniques

Reconnaissance: - DNS enumeration (dig, nslookup, whois) - SSL/TLS analysis (openssl, SSL Labs) - HTTP header inspection (curl, browser dev tools)

Security Testing: - Manual security header verification - Automated scanning tools - Configuration analysis - Protection layer testing

Validation:

1. Initial Assessment

1.1 Site Information

Platform Details: - Platform: GitHub Pages (Static Site Hosting) - Application: Cybersecurity News Dashboard (News Aggregator) - Hosting Provider: GitHub.com - CDN: Fastly - Web Server: GitHub.com infrastructure - SSL/TLS Provider: Sectigo (via GitHub Pages) - Protocol Support: HTTP/2

Infrastructure: - **IP Addresses**: 185.199.108.153, 185.199.109.153, 185.199.110.153, 185.199.111.153 (GitHub Pages) - **CDN Provider**: Fastly (x-served-by: cache-bur-kbur8200078-BUR) - **Cache Strategy**: max-age=600 (10 minutes) - **Server Header**: GitHub.com

Technology Stack:

```
┌──────────────────────────────────────┐
│  Content: Static HTML/JS/CSS         │
│  (Cybersecurity News Aggregator)     │
├──────────────────────────────────────┤
│  Hosting: GitHub Pages               │
├──────────────────────────────────────┤
│  CDN: Fastly                         │
├──────────────────────────────────────┤
│  SSL/TLS: Sectigo (*.github.io)      │
│  Algorithm: RSA                      │
└──────────────────────────────────────┘
```

GitHub Pages Limitations: - No custom HTTP header control - No WAF or advanced DDoS protection - No bot management capabilities - Limited to static content - Shared wildcard SSL certificate (*.github.io)

1.2 Security Score Breakdown

Category	Score	Grade	Notes
SSL/TLS Configuration	15/20	B+	TLS 1.3 enabled, RSA cert (not ECC)
Security Headers	5/25	F	Only HSTS present, missing 5 critical headers
DDoS Protection	8/15	C+	Fastly CDN provides basic protection
Bot Management	0/10	F	No bot protection available
WAF (Firewall)	0/10	F	No WAF available on GitHub Pages
			HSTS only,

Privacy Controls	2/10	F	overly permissive CORS
Performance	8/10	B+	HTTP/2, Fastly CDN, good caching
TOTAL	**38/100**	**F**	Critical security gaps present

---

2. Security Headers Analysis

2.1 Current Headers - 1/6 PRESENT

Verification Command:

```
        curl -sI https://roadlesstrodden007-minda.github.io/news-aggregator/
| grep -iE "x-frame|x-content|strict-
transport|referrer|permissions|content-security"
```

Results:

Header Name	Status	Current Value	Impact
Content-Security-Policy	[WARNING] Missing	None	HIGH - Site vulnerable to XSS attacks
X-Frame-Options	[WARNING] Missing	None	HIGH - Site vulnerable to clickjacking
X-Content-Type-Options	[WARNING] Missing	None	MEDIUM - MIME-sniffing attacks possible
Strict-Transport-Security	[YES] Present	max-age=31556952	HIGH - HTTPS enforced for 1 year
Referrer-Policy	[WARNING] Missing	None	MEDIUM - Referrer information leakage
Permissions-Policy	[WARNING] Missing	None	MEDIUM - No browser feature restrictions

Additional Concerns: - **access-control-allow-origin:** * - Allows any domain to make cross-origin requests (potential security risk)

Assessment: CRITICAL - Only 1 of 6 essential security headers implemented. Site is vulnerable to multiple attack vectors.

---

3. SSL/TLS Configuration Analysis

3.1 Certificate Details

Verification Command:

```
        openssl s_client -connect roadlesstrodden007-minda.github.io:443 -
servername roadlesstrodden007-minda.github.io </dev/null 2>/dev/null
| openssl x509 -noout -text
```

Certificate Information:

```
Issuer:         Sectigo Limited
Subject:        CN = *.github.io
Type:           Wildcard certificate (covers all *.github.io
subdomains)
Algorithm:      RSA (not ECC - less efficient than modern ECC)
Valid From:     March 7, 2025 00:00:00 GMT
Valid To:       March 7, 2026 23:59:59 GMT
Validity:       1 year (standard for Sectigo)
```

Key Security Features: - Wildcard coverage for all GitHub Pages sites - Trusted root: Sectigo Limited - Auto-managed by GitHub (users cannot customize)

Limitations: - RSA algorithm (older, less efficient than ECC) - Shared certificate across all GitHub Pages users - No control over certificate configuration

3.2 Protocol & Cipher Analysis

TLS Configuration: - Protocol: **TLS 1.3** (Latest, most secure) [YES] - Cipher: **TLS_AES_128_GCM_SHA256** (128-bit encryption - adequate) - HTTP/2: [YES] Enabled - Perfect Forward Secrecy: [YES] Yes - Certificate Transparency: [YES] Yes

Assessment: GOOD - Modern TLS 1.3 protocol with adequate cipher. RSA certificate is the main limitation.

---

4. Protection Layers Analysis

4.1 Current Protection Stack

Layer 1: DDoS Protection [WARNING] LIMITED - Provider: Fastly CDN (basic protection) - Type: Network layer only - Capacity: Shared across GitHub Pages - Status: Basic protection, no advanced mitigation - **Gap**: No application-layer DDoS protection

Layer 2: Web Application Firewall (WAF) [WARNING] NONE - Provider: None (GitHub Pages limitation) - Status: No WAF available - **Gap**: No protection against SQL injection, XSS, or OWASP Top 10 attacks

Layer 3: Bot Management [WARNING] NONE - Provider: None - Status: No bot detection or mitigation - **Gap**: Site vulnerable to scraping, automated attacks, credential stuffing

Layer 4: SSL/TLS Encryption [YES] ACTIVE - TLS 1.3 encryption - HSTS enabled (1 year) - Automatic HTTPS redirect via GitHub Pages - Status: Good encryption layer

Layer 5: Security Headers [WARNING] CRITICAL GAPS - Only HSTS present - Missing: CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy - **Gap**: Site vulnerable to XSS, clickjacking, MIME-sniffing

Layer 6: CDN & Caching [YES] BASIC - Fastly CDN (GitHub Pages default) - Moderate caching (10 minutes) - Status: Basic CDN benefits, not optimized

---

5. Recommendations

5.1 CRITICAL: Add Security Headers

Priority: HIGH - Implement Immediately

Option A: Meta Tags (Quick Fix - Limited Effectiveness)

Add to <head> section of HTML:

```
        <!-- Security Headers via Meta Tags -->
        <meta http-equiv="Content-Security-Policy" content="default-src
'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-
inline'; img-src 'self' data: https:;">
        <meta http-equiv="X-Frame-Options" content="SAMEORIGIN">
        <meta http-equiv="X-Content-Type-Options" content="nosniff">
        <meta name="referrer" content="strict-origin-when-cross-origin">
```

Limitations: - Meta tags are less secure than HTTP headers - Not supported by all browsers for all headers - CSP via meta tag has limited functionality

Estimated Score After: ~55/100 (D)

Option B: CDN/Security Platform (Strongly Recommended)

Available Platforms: - **Cloudflare** - Free tier available, easy setup, comprehensive features - **Akamai** - Enterprise-grade, global network, premium pricing - **AWS CloudFront + WAF** - Integrates with AWS ecosystem, pay-as-you-go - **Fastly** - Developer-friendly, real-time configuration, modern architecture - **Azure Front Door** - Microsoft ecosystem integration, enterprise features - **Sucuri** - Security-focused, WordPress optimization

General Implementation Steps: 1. **Sign up** for chosen platform 2. **Add domain** and configure DNS 3. **Configure Security Headers** (method varies by platform) 4. **Enable WAF** and protection features 5. **Test and optimize** configuration

Benefits (common across platforms): - Full HTTP header control - Enterprise-grade WAF - DDoS protection - Bot management - Analytics and monitoring

Estimated Score After: ~85-95/100 (B to A+, depending on configuration) **Cost**: $0-100/month (varies significantly by provider, traffic volume, and features)

5.2 Address CORS Configuration

Issue: `access-control-allow-origin: *` allows any domain to access resources

Recommendation: - Review if wildcard CORS is necessary - If API endpoints exist, restrict to specific domains - Implementation depends on how the news aggregator fetches data

5.3 Migration Path (If Custom Domain Exists)

If using custom domain (not *.github.io):

1. **Immediate**: Add meta tags to HTML
2. **Short-term** (1-2 weeks): Evaluate and select CDN/security platform (Cloudflare, Akamai, AWS, etc.)
3. **Mid-term** (1 month): Complete platform migration and configuration
4. **Long-term**: Consider more robust hosting with full server control if needed

---

6. Implementation Plan

6.1 Quick Win: Meta Tags (1 Hour)

Step 1: Edit HTML File

Locate the main `index.html` file in your repository and add to `<head>`:

```
        <head>
            <meta charset="UTF-8">
            <meta name="viewport" content="width=device-width, initial-
scale=1.0">
            <title>Cybersecurity News Dashboard</title>

            <!-- SECURITY HEADERS -->
            <meta http-equiv="Content-Security-Policy"
                  content="default-src 'self'; script-src 'self' 'unsafe-
inline' https://cdn.jsdelivr.net; style-src 'self' 'unsafe-inline';
img-src 'self' data: https:; font-src 'self' data:;">
            <meta http-equiv="X-Frame-Options" content="SAMEORIGIN">
            <meta http-equiv="X-Content-Type-Options" content="nosniff">
            <meta name="referrer" content="strict-origin-when-cross-origin">
            <!-- END SECURITY HEADERS -->

            <!-- Rest of your head content -->
        </head>
```

Step 2: Commit and Push

```
        git add index.html
        git commit -m "Add security headers via meta tags"
        git push origin main
```

Step 3: Verify (Wait 1-2 minutes for GitHub Pages to rebuild)

```
        curl -s https://roadlesstrodden007-minda.github.io/news-aggregator/
| grep -i "content-security-policy"
```

6.2 CDN/Security Platform Migration (2-4 Hours)

Platform Selection Criteria: - Budget constraints ($0 - $100+/month) - Existing infrastructure (AWS, Azure, Google Cloud) - Required features (WAF, bot protection, analytics) - Technical expertise level - Traffic volume and geographic distribution

General Migration Steps (Platform-Agnostic):

Step 1: Research and Select Platform - Compare: Cloudflare, Akamai, AWS CloudFront, Fastly, Azure Front Door, Sucuri - Evaluate pricing, features, and ease of use - Consider free tier options for testing

Step 2: Platform Setup 1. Sign up for chosen platform 2. Add your domain/site 3. Update DNS records as instructed by provider 4. Wait for DNS propagation (5-60 minutes)

Step 3: Configure Security Headers - Configuration method varies by platform: - **Cloudflare**: Rules → Transform Rules → Modify Response Header - **AWS CloudFront**: Lambda@Edge or CloudFront Functions - **Akamai**: Property Manager → Response Headers - **Fastly**: VCL snippets or managed configurations - Configure all 6 security headers per platform documentation

Step 4: Enable Security Features 1. Enable WAF with managed rulesets 2. Configure bot protection/challenge mechanisms 3. Set SSL/TLS to strict mode 4. Enable DDoS protection (usually automatic) 5. Configure rate limiting as needed

Step 5: Test and Verify 1. Test site functionality 2. Verify security headers: https://securityheaders.com 3. Check SSL configuration: https://www.ssllabs.com/ssltest/ 4. Monitor for any issues

Expected Time: 2-4 hours (varies by platform complexity) **Expected Result**: Security score increases to ~85-95/100 (B to A+)

---

7. Cost Analysis

7.1 Current Investment

Item	Cost	Notes
GitHub Pages Hosting	$0/month	Free for public repositories
SSL Certificate	$0/year	Included with GitHub Pages
CDN (Fastly)	$0/month	Included with GitHub Pages
Total Current	**$0/month**	No costs currently

7.2 Recommended Investment Options

Option	One-	Monthly	Notes

	Time		Security Score	
Option 1: Meta Tags	$0	$0	55/100 (D)	Limited effectiveness, quick fix
Option 2A: CDN Free Tier	$0	$0	85/100 (B)	Cloudflare Free, AWS Free Tier (12 months)
Option 2B: CDN Entry Plan	$0	$20-50	90/100 (A)	Cloudflare Pro, Sucuri Basic, Fastly
Option 2C: CDN Business Plan	$0	$100-200	95/100 (A+)	Akamai, AWS Enterprise, Azure Premium

Platform Comparison: - **Cloudflare**: Free tier available, $20-200/month paid plans - **AWS CloudFront + WAF**: Pay-as-you-go, typically $50-150/month - **Fastly**: $50/month minimum, developer-friendly - **Akamai**: Enterprise pricing, $200+/month - **Azure Front Door**: $35/month + usage - **Sucuri**: $20-300/month, security-focused

Recommended: Start with **Option 1** (immediate), then evaluate **Option 2A/2B** providers within 30 days based on budget and requirements.

---

8. Conclusion

Overall Assessment: FAIL (F) - Immediate Action Required

The Cybersecurity News Dashboard currently has a **critical security gap** due to missing security headers. While the site benefits from TLS 1.3 encryption and basic CDN protection via GitHub Pages, it lacks essential protections against:

- Cross-Site Scripting (XSS) attacks
- Clickjacking attacks
- MIME-sniffing vulnerabilities
- Web application attacks (no WAF)
- Bot attacks and scraping

Security Score: 38/100 (F)

Risk Level: HIGH

Immediate Actions Required:

1. **TODAY**: Add security headers via HTML meta tags (1 hour effort)
2. **THIS WEEK**: Research and evaluate CDN/security platform options
3. **WITHIN 30 DAYS**: Migrate to a CDN/security platform with full HTTP header control

Expected Outcomes:

After Meta Tags: 55/100 (D) - Basic protection **After Platform Migration**: 85-95/100 (B to A+) - Enterprise-grade protection

Platform Selection Factors:

- Budget and traffic volume
- Existing cloud infrastructure (AWS, Azure, Google Cloud)
- Required features (WAF, bot protection, analytics)
- Technical expertise and support needs
- Geographic distribution requirements

Note: Given this is a **Cybersecurity News Dashboard**, the current security posture may negatively impact credibility. We strongly recommend implementing security best practices to align with the cybersecurity-focused content.