**Vulnerability Assessment Report for nullclass.com**

**Table of Contents**

1.1 Executive Summary ........................................................................................................   
1.2 Overview ...........................................................................................................................   
1.3 High-Level Test Outcomes .........................................................................................   
1.4 Overall Risk Rating ........................................................................................................   
1.5 Prioritized Recommendations ....................................................................................

2.1 Test Scope and Method ..............................................................................................   
2.2 Extent of Testing ............................................................................................................   
2.3 Test Scope Summary .................................................................................................

3.1 Internal Phase ................................................................................................................   
3.2 Phase Summary ..........................................................................................................   
3.3 Actions Taken ..............................................................................................................

4.1 External Phase ............................................................................................................   
4.2 Phase Summary .........................................................................................................   
4.3 Actions Taken .............................................................................................................

5.1 Conclusions ..................................................................................................................   
5.2 Most Likely Compromise Scenarios ........................................................................   
5.3 Implications..................................................................................................................

References ............................................................................................................................

**1. Executive Summary**

**1.1 Executive Summary**

This report presents the findings of a vulnerability assessment conducted on nullclass.com as of June 20, 2025. The scan focused on assessing public-facing security controls including SSL/TLS configuration, HTTP headers, cookie security, DNS, and email protection mechanisms.

**1.2 Overview**

* **Target Domain**: nullclass.com
* **Date of Assessment**: 20/06/2025
* **Assessment Type**: External (Black Box)
* **Tools Used**: SSL/TLS Analyzer, Header Security Analyzer, DNS Enumeration Tools

**1.3 High-Level Test Outcomes**

| **Category** | **Status / Finding** |
| --- | --- |
| SSL/TLS | ✅ Strong TLSv1.3 with AES 256 GCM |
| CSP | ❌ Not Implemented |
| X-Frame-Options | ❌ Missing |
| HSTS | ✅ Enabled |
| Cookie Security | ✅ Secure Cookies Used |
| Mixed Content | ✅ No Mixed Content Detected |
| Web Application Firewall | ✅ Cloudflare Detected |
| Security Headers Score | ⚠️ 25/100 – Several Headers Missing |
| Server Disclosure | ⚠️ Cloudflare Detected (Version Disclosure) |
| DNSSEC | ✅ Enabled |
| DMARC/DKIM | ✅ Found and Validated |

**1.4 Overall Risk Rating**

| **Risk Level** | **Description** |
| --- | --- |
| **Medium** | Several missing HTTP headers and CSP increase the risk of client-side attacks such as XSS and Clickjacking. |

**1.5 Prioritized Recommendations**

| **Priority** | **Recommendation** |
| --- | --- |
| High | Implement Content Security Policy (CSP) |
| High | Add X-Frame-Options header |
| Medium | Improve Security Headers Score (>80 recommended) |
| Medium | Hide server technology disclosure where possible |

**2. Assessment Details**

**2.1 Test Scope and Method**

The assessment focused on passive and active enumeration of the web domain, evaluating cryptographic strength, misconfigurations, and security headers.

**2.2 Extent of Testing**

* No credentialed or authenticated testing performed
* No application-level penetration testing
* Public infrastructure only

**2.3 Test Scope Summary**

| **Item** | **In Scope** |
| --- | --- |
| SSL/TLS Analysis | ✅ |
| HTTP Header Security | ✅ |
| DNS/DNSSEC Checks | ✅ |
| Email Spoofing Protection | ✅ |
| Application Source Code | ❌ Not Available |

**3. Internal Phase**

*No internal testing was conducted as this was an external black-box scan.*

**4. External Phase**

**4.1 Phase Summary**

External testing identified multiple areas of strength including TLS 1.3 support and DNSSEC. However, it also revealed gaps in HTTP response header configurations and lack of a CSP policy.

**4.2 Actions Taken**

| **Action** | **Result** |
| --- | --- |
| SSL/TLS Certificate Validity Check | ✅ Valid (Expires: 21 Aug 2025) |
| TLS Version and Cipher Analysis | ✅ TLS 1.3, Strong Cipher Suite |
| Header Security Inspection | ⚠️ Several Missing Headers |
| Cookie Security Check | ✅ All cookies are Secure |
| CSP Evaluation | ❌ Not Implemented |
| Frame Options Check | ❌ X-Frame-Options header missing |
| DNSSEC Validation | ✅ Enabled |
| WAF Detection | ✅ Cloudflare |
| DMARC/DKIM Verification | ✅ Properly configured |

**5. Conclusions & Recommendations**

**5.1 Conclusions**

The security posture of nullclass.com is generally good, especially with strong cryptographic configurations and DNS/email protections. However, the lack of essential security headers such as CSP and X-Frame-Options significantly exposes the site to client-side attacks.

**5.2 Most Likely Compromise Scenarios**

* **XSS via Unrestricted Script Sources**: Lack of a CSP allows third-party scripts to be loaded.
* **Clickjacking Attacks**: Absence of X-Frame-Options allows page embedding.

**5.3 Implications**

* Reputation damage from potential client-side attacks
* Increased risk of phishing or malware injection
* Legal non-compliance with standards like PCI DSS and GDPR