Domain Security Assessment Report

May 05, 2025
Confidential

Tucson Unified School District

Member	Assessment Date	Domains Assessed
Tucson Unified School District	May 05, 2025	1/1

Executive Summary

This report presents the findings of a security assessment conducted for Tucson Unified School District on May 05, 2025. The assessment focused on domain security configurations, including DNS settings, HTTP security headers, and SSL/TLS implementations.

Critical	High	Medium	Low	Info
0	0	3	7	0
Issues requiring immediate attention	Significant security concerns	Moderate risk concerns	Minor security improvements	Informational findings

Key Findings

Our assessment identified a total of 10 issues across 1 domains. The findings are categorized by severity to help prioritize remediation efforts.

Severity	Count	Description	Recommended Action
Medium	3	Security issues that should be addressed	Address within 1 month
Low	7	Minor security concerns	Address during next maintenance cycle

Detailed Findings: TUSD1.org

⚠ **Issues found:** 10 issue(s) detected

Technical Information

DNS Configuration

Resolves to IP: Yes 104.18.43.227, 172.64.144.29

SPF Record: Yes

DMARC Record: Yes

DNSSEC Enabled: No

Web Server

HTTPS Supported: Yes

Web Server: cloudflare

HTTP Version: HTTP/1.1

Security Headers: 0 implemented

Security Findings

Missing HTTP Strict Transport Security (HSTS) Header

Medium

The HTTP Strict Transport Security (HSTS) header is not set

```
Evidence: Header not present in response
```

Recommendation: Add Strict-Transport-Security: max-age=31536000; includeSubDomains header

Missing Content Security Policy (CSP) Header

Medium

The Content Security Policy (CSP) header is not set

```
Evidence: Header not present in response
```

Recommendation: Add Content-Security-Policy: default-src 'self' header

Insecure Cookie

Medium

Cookie 'ASP.NET_SessionId' is set without the Secure flag

```
Evidence: Cookie ASP.NET_SessionId missing Secure flag
```

Recommendation: Set the Secure flag for all cookies

DNSSEC Not Enabled

Low

DNSSEC is not enabled for TUSD1.org. This can allow DNS poisoning attacks.

```
Evidence: No DNSKEY records found
```

Recommendation: Enable DNSSEC to add cryptographic authentication to DNS

Missing X-Content-Type-Options Header

Low

The X-Content-Type-Options header is not set

```
Evidence: Header not present in response
```

Recommendation: Add X-Content-Type-Options: nosniff header

Missing X-Frame-Options Header

Low

The X-Frame-Options header is not set

```
Evidence: Header not present in response
```

Recommendation: Add X-Frame-Options: SAMEORIGIN header

Missing X-XSS-Protection Header Low

The X-XSS-Protection header is not set

```
Evidence: Header not present in response
```

Recommendation: Add X-XSS-Protection: 1; mode=block header

Missing Referrer Policy Header Low

The Referrer Policy header is not set

```
Evidence: Header not present in response
```

Recommendation: Add Referrer-Policy: strict-origin-when-cross-origin header

Missing Permissions Policy Header Low

The Permissions Policy header is not set

```
Evidence: Header not present in response
```

Recommendation: Add Permissions-Policy: Present (with appropriate restrictions) header

Missing Feature Policy (deprecated) Header Low

The Feature Policy (deprecated) header is not set

```
Evidence: Header not present in response
```

Recommendation: Add Feature-Policy: Present (with appropriate restrictions) header

Remediation Recommendations

DNS Security Recommendations

- **Implement SPF Records:** Sender Policy Framework helps prevent email spoofing by specifying which servers are authorized to send email from your domain.
- **Configure DMARC:** Domain-based Message Authentication, Reporting, and Conformance provides additional protection against email spoofing and phishing.
- **Enable DNSSEC:** DNS Security Extensions add cryptographic signatures to DNS records to prevent DNS poisoning attacks.
- **Secure Name Servers:** Ensure name servers are properly configured and not vulnerable to zone transfer attacks or acting as open resolvers.

Web Security Recommendations

- **Implement HTTPS:** All websites should use HTTPS with a valid SSL/TLS certificate.
- **Security Headers:** Implement recommended security headers to protect against common web vulnerabilities:
  - Strict-Transport-Security (HSTS): Forces browsers to use HTTPS
  - Content-Security-Policy (CSP): Prevents cross-site scripting (XSS) attacks
  - X-Content-Type-Options: Prevents MIME type sniffing
  - X-Frame-Options: Protects against clickjacking attacks
  - Referrer-Policy: Controls what information is sent in the Referer header
- **Secure Cookies:** Set the Secure and HttpOnly flags on cookies containing sensitive information.
- **Hide Version Information:** Configure servers to hide software versions in HTTP headers to prevent targeted attacks.

SSL/TLS Recommendations

- **Use Modern Protocols:** Only support TLS 1.2 and TLS 1.3; disable older protocols (SSL 3.0, TLS 1.0, TLS 1.1).
- **Strong Cipher Suites:** Use only strong cipher suites with forward secrecy.
- **Certificate Maintenance:** Ensure certificates are valid, issued by trusted authorities, and renewed before expiration.

Methodology

This assessment was conducted using passive scanning techniques to analyze domain security configurations. The assessment focused on two main areas:

DNS Configuration Analysis

- Verification of domain resolution and DNS record configuration
- Analysis of SPF, DKIM, and DMARC email security records
- Checking for DNSSEC implementation
- Review of name server configurations

Header-Based Fingerprinting

- HTTP/HTTPS protocol support verification
- Web server technology identification
- Security header implementation check
- SSL/TLS configuration assessment
- Cookie security analysis

The assessment is designed to be non-intrusive and focuses only on publicly accessible information. No active vulnerability scanning or penetration testing was performed.

Brought to you by CyberPools

Security Assessment Report generated on May 05, 2025 for Tucson Unified School District. This report is confidential and intended for authorized use only.