# VULNERABILITY SCAN REPORT

## EXECUTIVE SUMMARY

**Target:** http://wcesd2tx.us/
**Scan Date:** 2025-08-27 03:58:47
**Risk Level:** HIGH
**Total Vulnerabilities Found:** 60
**Subdomains Found:** 1
**Exposed Directories:** 158
**Email Addresses:** 13
**WordPress Paths:** 53

## ■ CRITICAL VULNERABILITIES

### *Open Redirect Vulnerabilities (30 found):*

• Open Redirect: http://wcesd2tx.us?next=https://evil.com... -> https://wcesd2tx.us/?next=https://evil.com
• Open Redirect: http://wcesd2tx.us?continue=//evil.com... -> https://wcesd2tx.us/?continue=/evil.com
• Open Redirect: http://wcesd2tx.us?continue=javascript:alert('re... -> https://wcesd2tx.us/?continue=javascript:alert('redirect')
• Open Redirect: http://wcesd2tx.us?target=//evil.com... -> https://wcesd2tx.us/?target=/evil.com
• Open Redirect: http://wcesd2tx.us?link=javascript:alert('re... -> https://wcesd2tx.us/?link=javascript:alert('redirect')
... and 25 more

### *Local/Remote File Inclusion (30 found):*

• LFI/RFI: http://wcesd2tx.us?document=../../../etc/passwd... - test
• LFI/RFI: http://wcesd2tx.us?page=../../../etc/passwd... - test
• LFI/RFI: http://wcesd2tx.us?filename=../../../../etc/pass... - test
• LFI/RFI: http://wcesd2tx.us?pg=../../../../etc/pass... - test
• LFI/RFI: http://wcesd2tx.us?pg=../../../etc/passwd... - test
... and 25 more

## ■ INFORMATION DISCLOSURE

### *Email Addresses Found (13):*

• aaron.bonner@wcesd2tx.us
• alex.lopez@wcesd2tx.us

- careers@wcesd2tx.us
- chris.thuneman@wcesd2tx.us
- courses@wcesd2tx.us
- david.nieto@wcesd2tx.us
- eben@eyebytes.com
- filler@godaddy.com
- lonnie.bodiford@wcesd2tx.us
- publicrelations1@NETORGFT9620617.onmicrosoft.com
- records@wcesd2tx.us
- rudy.cantu@wcesd2tx.us
- sherry.heatherly@wcesd2tx.us

## ■■ INFRASTRUCTURE ANALYSIS

### *Subdomains (1):*

- www.wcesd2tx.us (301)

### *WordPress Installation (53 paths found):*

This appears to be a WordPress-based website with extensive admin functionality exposed.

- wp-admin/link-manager.php (301)
- wp-admin/network.php (301)
- wp-admin/options-head.php (301)
- wp-admin/options-media.php (301)
- wp-admin/site-health.php (301)
- wp-admin/tools.php (301)
- wp-admin/user-edit.php (301)
- wp-includes (301)
- wp-json/wp/v2/users (301)
- wp-login.php (301)

... and 43 more WordPress paths

### *Exposed Directories (158):*

The following directories and files are accessible:

**Admin/Control Panels:**

- admin (301)
- admin-area (301)
- admin-login (301)
- admin-panel (301)
- admin/account.php (301)

**Configuration Files:**

- .env (301)
- .env.development (301)
- .env.local (301)
- .env.production (301)
- backup (301)

**WordPress Files:**

- wp-admin (301)
- wp-config.php (301)
- wp-config.php.bak (301)
- wp-config.php.old (301)
- wp-config.php.swo (301)

## ■ SECURITY RECOMMENDATIONS

### *CRITICAL - Fix Open Redirect Vulnerabilities*

**Description:** Implement proper input validation and URL whitelisting for all redirect parameters.
**Impact:** Attackers can redirect users to malicious sites and steal credentials.

### *CRITICAL - Fix File Inclusion Vulnerabilities*

**Description:** Implement strict file path validation and disable dangerous PHP functions.
**Impact:** Attackers can read sensitive files and potentially execute code.

### *HIGH - Secure WordPress Installation*

**Description:** Implement proper access controls, use strong passwords, and keep WordPress updated.
**Impact:** Exposed WordPress admin areas can lead to site compromise.

### *MEDIUM - Protect Email Addresses*

**Description:** Use email obfuscation techniques and avoid exposing staff emails publicly.
**Impact:** Exposed emails can be used for phishing attacks and spam.

### *MEDIUM - Reduce Attack Surface*

**Description:** Remove or properly secure unnecessary directories and files.
**Impact:** Large attack surface increases the likelihood of successful exploitation.

### *HIGH - Implement Web Application Firewall (WAF)*

**Description:** Deploy a WAF to block common attack patterns and provide additional security layers.
**Impact:** WAF can prevent many automated attacks and provide real-time protection.

### *HIGH - Regular Security Audits*

**Description:** Conduct regular penetration testing and vulnerability assessments.
**Impact:** Proactive security testing helps identify and fix issues before exploitation.

### *MEDIUM - Security Headers*

**Description:** Implement security headers like CSP, HSTS, X-Frame-Options, etc.
**Impact:** Security headers provide defense-in-depth against various attacks.

## ■ TECHNICAL DETAILS

### *Scan Configuration:*

- Target URL: http://wcesd2tx.us/
- Domain: wcesd2tx.us
- Scan Timestamp: 2025-08-27 03:58:47
- Attack Modules: 15
- Subdomain Tests: 53
- Directory Tests: 163
- WordPress Tests: 75
- SQL Injection Tests: 27
- XSS Tests: 15
- LFI/RFI Tests: 25

### *Detailed Findings Summary:*

| Category | Count | Risk Level |
|---|---|---|
| Open Redirect | 30 | CRITICAL |
| LFI/RFI | 30 | CRITICAL |
| SQL Injection | 0 | NONE |
| XSS | 0 | NONE |
| Admin Access | 0 | NONE |
| WordPress Paths | 53 | MEDIUM |
| Exposed Directories | 158 | MEDIUM |
| Email Addresses | 13 | MEDIUM |
| Subdomains | 1 | NONE |

## ■ IMMEDIATE NEXT STEPS

1. **IMMEDIATE ACTION REQUIRED**: Fix open redirect vulnerabilities

2. **IMMEDIATE ACTION REQUIRED**: Fix file inclusion vulnerabilities

3. **HIGH PRIORITY**: Secure WordPress admin areas

4. **HIGH PRIORITY**: Implement input validation on all parameters

5. **MEDIUM PRIORITY**: Remove or secure exposed directories

6. **MEDIUM PRIORITY**: Implement security headers

7. **ONGOING**: Schedule regular security assessments

8. **ONGOING**: Monitor for new vulnerabilities