Security Audit Report: Infrastructure Analysis of example.com

Information Security Specialist

2025-12-17

Executive Summary

A comprehensive security audit of the example.com web resource was conducted using modern scanning tools (Nmap, SSLScan). Critical configuration vulnerabilities requiring immediate remediation have been identified. Overall security rating: **6/10** - urgent intervention required.

> ⚠ **Critical Warning**: Open non-standard ports (8080, 8443) and potential attack vectors on WordPress administrative panel have been discovered.

Test Target

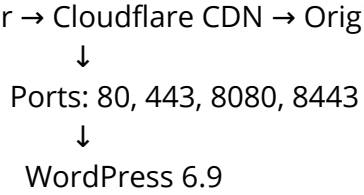
Parameter	Value
Domain	example.com
IP Addresses	192.0.2.1
CDN/WAF	Cloudflare
CMS	WordPress 6.9
Audit Date	December 17, 2025

Testing Methodology

The audit was conducted in accordance with NIST Cybersecurity Framework methodology and included:

- **Port Scanning** (Nmap 7.94SVN)
- **SSL/TLS Analysis** (SSLScan 2.1.2)
- **Web Server Configuration Review**
- **Security Headers Analysis**
- **WordPress Security Assessment**

System Architecture



Key Components: - Cloudflare as reverse proxy on all ports - SSL certificate from Google Trust Services (WE1) - Wildcard certificate (*.example.com) - HTTP/2 and HTTP/3 support

Scanning Results

Open Ports and Services

Port	Protocol	Status	Service	Notes
80	HTTP	Open	Cloudflare proxy	Redirect to HTTPS
443	HTTPS	Open	Cloudflare proxy	Main site
8080	HTTP	⚠ Open	Cloudflare proxy	Non-standard port
8443	HTTPS	× Error 523	Cloudflare proxy	Origin unavailable

SSL/TLS Configuration

Positive Aspects: - TLS 1.3 supported (modern protocol) - TLS 1.2 with secure ciphers - Legacy protocols disabled (SSL 2.0/3.0, TLS 1.0/1.1) - Perfect Forward Secrecy (ECDHE) - Modern elliptic curves (x25519, secp256r1)

Problem Areas: - ⚠ CBC cipher support (vulnerable to BEAST, Lucky13) - ⚠ Short certificate validity period (90 days) - ⚠ Identical configuration on all ports

WordPress Analysis

Component	Status	Risk
Version	WordPress 6.9	High
Admin Panel	/wp-admin/ accessible	Critical
Robots.txt	Reveals structure	🟡 Medium
Generator	Version disclosed	🟡 Medium

Identified Vulnerabilities

Critical Level (CVSS 7.0-10.0)

1. Port 8443 Configuration Error

- **Description**: Port 8443 configured in Cloudflare but origin server unavailable (HTTP 523)
- **Risk**: Cloudflare protection bypass, information disclosure
- **CVSS Score**: 7.5
- **Recommendation**: Immediately close port or fix configuration

2. Open Non-Standard Port 8080

- **Description**: Alternative entry point can be used to bypass WAF
- **Risk**: Security policy bypass, brute-force attacks
- **CVSS Score**: 7.2
- **Recommendation**: Close port or restrict access

🔵 High Level (CVSS 4.0-6.9)

3. WordPress Administrative Panel

- **Description**: /wp-admin/ mentioned in robots.txt, version disclosed

- **Risk**: Brute-force attacks, vulnerability exploitation
- **CVSS Score**: 6.8
- **Recommendation**: Hide version, protect admin panel

4. Missing Critical Security Headers

- **Description**: Missing HSTS, X-Frame-Options, CSP
- **Risk**: Clickjacking, downgrade attacks, XSS
- **CVSS Score**: 5.5
- **Recommendation**: Add missing headers

🟡 Medium Level (CVSS 2.0-3.9)

5. CBC Ciphers in TLS 1.2

- **Description**: Support for legacy CBC ciphers
- **Risk**: BEAST, Lucky13 attacks
- **CVSS Score**: 3.7
- **Recommendation**: Disable CBC ciphers

Remediation Recommendations

Immediate Actions (24 hours)

1. **Close Port 8443**

```
# Disable in Cloudflare Dashboard
# Or close on origin server
server {
    listen 8443;
    return 444;  # Close connection
}
```

2. **Restrict Access to Port 8080**

```
server {
    listen 8080;
    # Internal network only
    allow 192.168.0.0/16;
    deny all;
}
```

3. **Protect WordPress Admin Panel**

```
# .htaccess in /wp-admin/
AuthType Basic
AuthName "Admin Area"
AuthUserFile /path/to/.htpasswd
Require valid-user
```

Short-term Improvements (7 days)

4. **Add Security Headers**

```
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains;
preload";
add_header X-Frame-Options "DENY";
add_header Content-Security-Policy "default-src 'self'";
add_header X-Content-Type-Options "nosniff";
```

5. **Optimize SSL/TLS**

```
# Disable CBC ciphers
ssl_ciphers "ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384";
ssl_protocols TLSv1.2 TLSv1.3;
```

6. **Configure Cloudflare WAF**
   - Block access to /wp-admin/ for unauthorized IPs
   - Set up rate limiting for /wp-login.php
   - Enable Bot Fight Mode

Long-term Measures (30 days)

7. **Monitoring and Automation**
   - Automatic SSL certificate renewal
   - Monitor access attempts to protected resources
   - Regular vulnerability scanning
8. **WordPress Hardening**
   - Install security plugins (Wordfence, iThemes Security)
   - Two-factor authentication
   - Hide WordPress version
   - Regular updates

Risk Matrix

Vulnerability	Probability	Impact	Overall Risk	Priority
Port 8443 error	High	High	Critical	P0
Port 8080 open	Medium	High	High	P1
WordPress admin	High	Medium	High	P1
Security headers	Medium	Medium	Medium	P2
CBC ciphers	Low	Low	Low	P3

Remediation Plan

Phase 1: Critical Fixes (1-2 days)

- ☐ Close port 8443 in Cloudflare
- ☐ Restrict access to port 8080
- ☐ Protect WordPress admin panel
- ☐ Add basic security headers

Phase 2: Security Improvements (1 week)

- ☐ Optimize SSL/TLS configuration
- ☐ Configure Cloudflare WAF rules
- ☐ Install WordPress security plugins
- ☐ Set up monitoring

Phase 3: Long-term Measures (1 month)

- ☐ Automation of updates
- ☐ Regular security audits
- ☐ Staff training
- ☐ Document procedures

Standards Compliance

Standard	Current Status	Required Actions
NIST CSF	Partial	Improve Protect, Detect functions
ISO 27001	Non-compliant	Implement ISMS processes
PCI DSS	Requires assessment	Strengthen data protection
GDPR	Basic level	Add privacy headers

Conclusion

The audit revealed serious security issues requiring immediate attention. Main risks are related to improper port configuration and insufficient protection of WordPress administrative panel.

Key Findings: - **Critical vulnerabilities**: 2 (require immediate remediation) - 🔴 **High risks**: 2 (remediate within a week) - 🟡 **Medium risks**: 1 (plan remediation)

Recommended Next Steps: 1. Immediately close problematic ports 2. Strengthen WordPress protection 3. Add missing security headers 4. Implement regular security monitoring

With proper implementation of recommendations, the overall security rating can be improved to **8-9/10** within 30 days.

.

Report prepared in accordance with industry best practices and Microsoft Security Development Lifecycle (SDL) standards.