Security Scan Report: example.com Website

Information Security Specialist

2026-01-17

Executive Summary

This report presents the results of a comprehensive security scan of the **example.com** website (IP: 188.114.96.12), conducted on January 13, 2026, using the Nikto 2.1.5 tool. The scan identified **3 potential security issues** that require administrator attention.

> **Overall Security Assessment**: MEDIUM RISK LEVEL
>
> The identified issues do not pose critical threats but require remediation to improve overall security posture.

.

Scan Details

Technical Parameters

Parameter	Value
Target Host	example.com
IP Address	188.114.96.12
Port	443 (HTTPS)
HTTP Server	Cloudflare
Scanning Tool	Nikto 2.1.5
Scan Date	January 13, 2026
Start Time	05:24:40
End Time	05:31:11
Total Duration	6 minutes 31 seconds (391 sec)

Scan Statistics

- **Items Checked**: 6,544
- **Errors Found**: 0
- **Issues Identified**: 3

Command Line Parameters

```
nikto -h https://example.com -ssl -o https_scan.html -F html
```

.

Identified Vulnerabilities and Issues

1. Missing X-Frame-Options Header

Risk Level: 🟡 Medium

Issue Description: The anti-clickjacking X-Frame-Options header is not present, leaving the site vulnerable to clickjacking attacks.

Technical Information:

- **URI**: /
- **HTTP Method**: GET
- **OSVDB ID**: OSVDB-0
- **Test Links**: https://example.com:443/

Potential Impact:

- Possibility of clickjacking attacks
- Site embedding in iframes on malicious resources
- User deception through hidden interface elements

2. Uncommon cf-ray Header

Risk Level: 🟢 Low (Informational)

Issue Description: Uncommon header 'cf-ray' found, with contents: 9bd22024ba62be6c-ZRH

Technical Information:

- **URI**: /
- **HTTP Method**: GET
- **Header Value**: 9ty22024ba62bc6c-ZRH
- **OSVDB ID**: OSVDB-0
- **Test Links**: https://example.com:443/

Comment: This header is standard for Cloudflare services and is used for request tracing. It does not pose a security threat.

3. SSL Certificate Mismatch

Risk Level: 🟡 Medium

Issue Description: Hostname 'example.com' does not match certificate's CN 'cdnjs.cloudflare.com'

Technical Information:

- **URI**: /
- **HTTP Method**: GET
- **Expected CN**: example.com
- **Actual CN**: cdnjs.cloudflare.com
- **OSVDB ID**: OSVDB-0

- **Test Links**: https://example.com:443/

Potential Impact:

- Browser warnings about insecure connections
- Reduced user trust
- Possible SEO and indexing issues

.

Remediation Recommendations

Priority Actions

1. **Configure X-Frame-Options Header**
   - Add header X-Frame-Options: DENY or X-Frame-Options: SAMEORIGIN
   - Alternative: use CSP header with frame-ancestors directive
2. **Fix SSL Certificate**
   - Obtain correct SSL certificate for example.com domain
   - Update Cloudflare configuration to use proper certificate
   - Verify DNS and proxy settings

Additional Security Measures

- **Implement Content Security Policy (CSP)**
  - Configure comprehensive content security policy
  - Protection against XSS attacks and other vectors
- **Add Additional Security Headers**:
  - X-Content-Type-Options: nosniff
  - X-XSS-Protection: 1; mode=block
  - Strict-Transport-Security: max-age=31536000
- **Regular Security Scanning**
  - Conduct monthly security assessments
  - Monitor for new vulnerabilities

.

Action Plan

Immediate Actions (1-3 days)

- ☐ Configure X-Frame-Options header in web server configuration
- ☐ Contact Cloudflare technical support regarding SSL certificate issue

Short-term Actions (1-2 weeks)

- ☐ Obtain and install correct SSL certificate
- ☐ Implement additional security headers
- ☐ Conduct follow-up scan to verify fixes

Long-term Actions (1 month)

- ☐ Develop regular security scanning policy
- ☐ Implement security monitoring system
- ☐ Train team on web security best practices

Conclusion

The security scan of example.com website identified **3 issues of medium and low criticality**. Despite the absence of critical vulnerabilities, it is recommended to address the identified issues to improve overall security posture.

Special attention should be paid to configuring the correct SSL certificate and implementing security headers. These measures will significantly enhance site security and user trust.

The next scan is recommended in 2 weeks after implementing fixes to confirm their effectiveness.

Appendix: Technical Information

Nikto Scan Details

Software: Nikto 2.1.5
Hosts Tested: 1
Total Execution Time: 391 seconds

Statistics by Category

Category	Count
Items Checked	6,544
Scan Errors	0
Issues Identified	3
Critical Vulnerabilities	0
Medium Risk	2
Low Risk	1