VULNSCAN.PRO

FULL ASSESSMENT

SECURITY ASSESSMENT REPORT

External Attack Surface Analysis

`example.com`

March 15, 2026 · 12 modules · 890s scan time · 8 findings

● **CRITICAL** | 1 Critical 2 High 4 Medium 1 Low

SUBDOMAINS	LIVE HOSTS	OPEN PORTS	SSL GRADE
16	6	6	B
discovered	responding	detected	needs work

01 Executive Summary

This report presents the results of a security assessment of **example.com**, conducted on March 15, 2026. The assessment utilized 12 scanning modules across 890 seconds of active testing.

A total of **8 findings** were identified: **1 critical**, **2 high**, **4 medium**, and **1 low** severity issues. The overall risk level is assessed as **CRITICAL**.

02 Attack Surface

LIVE HOSTS

URL	STATUS	TITLE	TECHNOLOGY
`https://example.com`	200	Example Domain	Cloudflare, Nginx
`https://www.example.com`	200	Example Domain	Cloudflare, Nginx
`https://api.example.com`	200	API Gateway	Express, Node.js
`https://admin.example.com`	403	Forbidden	Nginx
`https://staging.example.com`	200	Staging Environment	React, Next.js, Vercel
`https://blog.example.com`	200	Company Blog	WordPress, PHP, MySQL

OPEN PORTS

HOST	PORT	SERVICE	VERSION
`example.com`	80	http	nginx 1.24.0
`example.com`	443	https	nginx 1.24.0
`example.com`	22	ssh	OpenSSH 8.9p1
`example.com`	8080	http-proxy	—
`api.example.com`	443	https	Express
`api.example.com`	3000	http	Node.js

03 Vulnerability Findings

MEDIUM Missing HTTP Strict Transport Security (HSTS)

`https://example.com`

The server does not set the Strict-Transport-Security header. This allows attackers to perform protocol downgrade attacks and intercept traffic via man-in-the-middle.

REMEDIATION

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

Module: headers

MEDIUM Missing Content-Security-Policy Header

`https://example.com`

No Content-Security-Policy header is set, leaving the application vulnerable to XSS attacks and data injection.

REMEDIATION

Implement a strict CSP. Start with: Content-Security-Policy: default-src 'self'; script-src 'self'

Module: headers

LOW SPF Record Uses Softfail (~all)

`example.com`

The SPF record uses ~all (softfail) instead of -all (hardfail). Spoofed emails may still be delivered to inboxes.

REMEDIATION

Change the SPF record from ~all to -all after confirming all legitimate sending sources are included.

Module: dns

CRITICAL WordPress Core RCE — CVE-2024-12345

`https://blog.example.com`

WordPress version 6.2.1 is vulnerable to an unauthenticated Remote Code Execution via the REST API. An attacker can execute arbitrary PHP code on the server.

```
POST /wp-json/wp/v2/posts HTTP/1.1
Host: blog.example.com

{"content":"<?php system('id'); ?>","status":"publish"}

Response: uid=33(www-data) gid=33(www-data)
```

REMEDIATION

Immediately update WordPress to version 6.4+ and review all existing posts for injected content. Consider WAF rules to block exploit attempts.

CVSS: **9.8** CWE-94 OWASP: A03:2021 — Injection Module: nuclei

HIGH Staging Environment Publicly Accessible

`https://staging.example.com`

The staging environment is accessible from the public internet without authentication. It may contain test data, debug information, or unreleased features that could be exploited.

REMEDIATION

Restrict access to staging via IP whitelist, VPN, or HTTP Basic Auth. Never expose staging environments to the public internet.

Module: httpx

HIGH

API CORS Misconfiguration — Wildcard Origin

https://api.example.com

The API returns Access-Control-Allow-Origin: * with Access-Control-Allow-Credentials: true. This allows any website to make authenticated requests to the API on behalf of the user.

```
curl -H "Origin: https://evil.com" https://api.example.com/user

Access-Control-Allow-Origin: https://evil.com
Access-Control-Allow-Credentials: true
```

REMEDIATION

Configure CORS to only allow trusted origins. Never use wildcard (*) with credentials.

CVSS: **7.5** CWE-346 OWASP: A05:2021 — Security Misconfiguration Module: nuclei

MEDIUM

TLS 1.0 Protocol Still Enabled

example.com

The server still accepts TLS 1.0 connections, which has known vulnerabilities (BEAST, POODLE) and is deprecated by all major browsers.

REMEDIATION

Disable TLS 1.0 and 1.1 in your web server configuration. Only allow TLS 1.2 and 1.3.

CVSS: **5.3** CWE-326 Module: testssl

MEDIUM

Admin Panel Accessible (403 Forbidden)

https://admin.example.com

An admin panel was discovered at admin.example.com. While it returns 403, the server confirms its existence. Attackers may attempt bypass techniques or brute-force authentication.

REMEDIATION

Return 404 instead of 403 to avoid confirming the existence of admin interfaces. Better: remove from public DNS entirely.

Module: ffuf

04 SSL/TLS Configuration

example.com **B**

Protocols: TLSv1.2, TLSv1.3

Issuer: Let's Encrypt Authority X3

Valid until: Jun 15 23:59:59 2026 GMT

⚠ TLSv1.0 still enabled — should be disabled

⚠ HSTS header not set — susceptible to protocol downgrade

05 Security Headers

https://example.com **Score: 45/100**

HEADER	STATUS	VALUE
Strict-Transport-Security	✗ Missing	–

HEADER	STATUS	VALUE
Content-Security-Policy	✗ Missing	—
X-Frame-Options	✓ Present	`SAMEORIGIN`
X-Content-Type-Options	✓ Present	`nosniff`
X-XSS-Protection	✓ Present	`1; mode=block`
Permissions-Policy	✗ Missing	—
Referrer-Policy	✗ Missing	—
Cross-Origin-Opener-Policy	✗ Missing	—

06 AI Security Analysis

Risk Assessment

The external attack surface of example.com presents **significant security concerns** that require immediate attention.

Critical Findings

The WordPress installation at blog.example.com is running a critically vulnerable version (6.2.1) with a known RCE exploit. This is the highest priority remediation item — an attacker could compromise the server within minutes using publicly available exploit code.

Attack Chains

Chain 1: Blog Compromise → Lateral Movement

1. Exploit WordPress RCE on blog.example.com
2. Access internal network from compromised server
3. Pivot to API servers or database

Chain 2: CORS + Staging → Data Theft

1. Exploit CORS misconfiguration on api.example.com
2. Craft phishing page that makes authenticated API requests
3. Exfiltrate user data from victim's session

Recommendations (Priority Order)

1. **IMMEDIATE** — Patch WordPress to latest version
2. **IMMEDIATE** — Restrict staging.example.com access
3. **URGENT** — Fix CORS configuration on API
4. **SOON** — Implement HSTS and CSP headers
5. **PLANNED** — Disable TLS 1.0, harden SPF/DMARC

07 Compliance Dashboard

NON-COMPLIANT

OWASP Top 10

2 violation(s)

- ✗ A03:2021 — Injection
- ✗ A05:2021 — Security Misconfiguration

NON-COMPLIANT

PCI DSS 4.0

5 violation(s)

- ✗ Req 2.2.4: TLS 1.0/1.1 enabled (must use TLS 1.2+)
- ✗ Req 6.5.7: Cross-site scripting (XSS) risk — missing CSP
- ✗ Req 6.5.10: Missing security headers weaken client protections
- ✗ Req 4.1: Unencrypted credentials exposed in configuration files
- ✗ Req 5.4.1: Anti-phishing controls insufficient (missing SPF/DMARC)

NON-COMPLIANT

GDPR

4 violation(s)

- ✗ Art. 32: Missing HSTS/security headers — data in transit not adequately protected
- ✗ Art. 25: No CSP header — privacy by design violation
- ✗ Art. 5(1)(f): Configuration files with credentials publicly accessible
- ✗ Art. 32: Missing email authentication enables domain spoofing for social engineering

NON-COMPLIANT

ISO 27001

5 violation(s)

- ✗ A.12.6.1 — Technical vulnerability management: critical/high findings unresolved
- ✗ A.14.1.2 — Securing application services: missing HTTP security headers
- ✗ A.13.1.1 — Network controls: DNS security misconfiguration
- ✗ A.9.4.1 — Information access restriction: sensitive files publicly accessible
- ✗ A.13.1.3 — Segregation in networks: excessive exposed services

07 Methodology

This assessment was performed using VulnScan Pro's automated scanning pipeline, consisting of 12 specialized security modules.

MODULE	STATUS	DURATION
subfinder	✓ OK	31.7s
certTransparency	✓ OK	2.1s
httpx	✓ OK	50.5s
nmap	✓ OK	14.8s
testssl	✓ OK	12.5s
headers	✓ OK	23.8s
dns	✓ OK	30.7s
wafw00f	✓ OK	52.1s
whatweb	✓ OK	39.4s
nuclei	✓ OK	3.3s
nikto	✓ OK	58.0s
ffuf	✓ OK	38.9s

08 Disclaimer

This report is provided for informational purposes only. The findings represent the state of the target at the time of scanning and may not reflect the current security posture. VulnScan Pro is not responsible for any actions taken based on these findings. This report should be treated as confidential and shared only with authorized personnel. The automated scan results should be verified by a qualified security professional before taking remediation actions.