VULNSCAN.PRO

QUICK SCAN

SECURITY ASSESSMENT REPORT

External Attack Surface Analysis

example.com

March 15, 2026 · 10 modules · 285s scan time · 3 findings

MEDIUM | 0 Critical 0 High 2 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 10 scanning modules across 285 seconds of active testing.

A total of **3 findings** were identified: **0 critical**, **0 high**, **2 medium**, and **1 low** severity issues. The overall risk level is assessed as **MEDIUM**.

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

VulnScan.Pro — example.com Page 2 of 7 March 15, 2026

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

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	–

VulnScan.Pro — example.com Page 4 of 7 March 15, 2026

06 AI Security Analysis

Expert Security Assessment

Classification: CONFIDENTIAL

Executive Risk Rating: MEDIUM

The scan identified **0 critical**, **0 high**, **2 medium**, and **1 low** severity vulnerabilities across example.com.

Attack Chains Identified

Chain 1: Exposed Services → Lateral Movement
1 exposed service(s) → Brute-force or exploit known CVEs → Internal access
Impact: Direct network-level access to backend infrastructure.

Business Impact Assessment

- Email spoofing risk: domain can be impersonated for phishing campaigns
- 2 missing security headers leave users vulnerable to XSS, clickjacking, and MITM

Top Findings

1. MEDIUM: Missing HTTP Strict Transport Security (HSTS) — The server does not set the Strict-Transport-Security header. This allows attackers to perform protocol downgrade attacks and intercept traffic via...
2. MEDIUM: Missing Content-Security-Policy Header — No Content-Security-Policy header is set, leaving the application vulnerable to XSS attacks and data injection.

Priority Remediation Matrix

No critical or high findings require immediate action.

Attack Surface Summary

16 subdomains discovered, 6 live hosts responding, 6 open ports detected.

VulnScan.Pro — example.com Page 5 of 7 March 15, 2026

07 Compliance Dashboard

NON-COMPLIANT

PCI DSS 4.0

3 violation(s)

- ✗ Req 6.5.7: Cross-site scripting (XSS) risk — missing CSP
- ✗ Req 6.5.10: Missing security headers weaken client protections
- ✗ Req 5.4.1: Anti-phishing controls insufficient (missing SPF/DMARC)

NON-COMPLIANT

GDPR

3 violation(s)

- ✗ Art. 32: Missing HSTS/security headers — data in transit not adequately protected
- ✗ Art. 25: No CSP header — privacy by design violation
- ✗ Art. 32: Missing email authentication enables domain spoofing for social engineering

NON-COMPLIANT

ISO 27001

3 violation(s)

- ✗ A.14.1.2 — Securing application services: missing HTTP security headers
- ✗ A.13.1.1 — Network controls: DNS security misconfiguration
- ✗ A.13.1.3 — Segregation in networks: excessive exposed services

VulnScan.Pro — example.com Page 6 of 7 March 15, 2026

07 Methodology

This assessment was performed using VulnScan Pro's automated scanning pipeline, consisting of 10 specialized security modules.

MODULE	STATUS	DURATION
subfinder	✓ OK	23.2s
certTransparency	✓ OK	17.7s
httpx	✓ OK	54.6s
nmap	✓ OK	43.3s
testssl	✓ OK	19.2s
headers	✓ OK	51.0s
dns	✓ OK	36.6s
wafw00f	✓ OK	27.1s
whatweb	✓ OK	6.0s
nuclei	✓ OK	38.7s

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.

VulnScan.Pro — example.com Page 7 of 7 March 15, 2026