VULNSCAN.PRO

ENTERPRISE AUDIT

SECURITY ASSESSMENT REPORT

External Attack Surface Analysis

example.com

March 15, 2026 · 13 modules · 1850s scan time · 12 findings

CRITICAL | 2 Critical 3 High 6 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 an comprehensive security assessment of **example.com**, conducted on March 15, 2026. The assessment utilized 13 scanning modules across 1850 seconds of active testing.

A total of **12 findings** were identified: **2 critical**, **3 high**, **6 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

VulnScan.Pro — example.com Page 2 of 9 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

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

HIGH

SSH Server Uses Weak Key Exchange Algorithm

`example.com:22`

The SSH server accepts diffie-hellman-group1-sha1 key exchange, which uses a 1024-bit prime vulnerable to state-level adversaries (Logjam attack).

```
nmap --script ssh2-enum-algos example.com
Kex algorithms: diffie-hellman-group1-sha1, diffie-hellman-group14-sha256
```

REMEDIATION

Disable weak key exchange algorithms. Only allow curve25519-sha256, diffie-hellman-group16-sha512, or stronger.

CVSS: **7.4** CWE-327 Module: nmap

CRITICAL **Environment File (.env) Publicly Accessible**

`https://staging.example.com/.env`

The .env file containing database credentials, API keys, and application secrets is publicly accessible on the staging server.

```
GET https://staging.example.com/.env

DB_HOST=rds-prod-01.amazonaws.com
DB_PASSWORD=Pr0d_S3cret!2024
STRIPE_SECRET_KEY=sk_live_...
JWT_SECRET=super_secret_jwt_key
```

REMEDIATION

IMMEDIATELY: 1) Block access to .env files in web server config. 2) Rotate ALL exposed credentials. 3) Audit access logs for unauthorized access.

CVSS: **9.8** CWE-538 OWASP: A05:2021 — Security Misconfiguration Module: ffuf

MEDIUM **DMARC Policy Set to None**

`example.com`

The DMARC policy is set to p=none, which means failed authentication results are reported but emails are still delivered. This allows email spoofing.

REMEDIATION

Gradually transition DMARC policy: p=none → p=quarantine → p=reject. Monitor reports during transition.

CWE-290 Module: dns

MEDIUM **WordPress XML-RPC Enabled**

`https://blog.example.com/xmlrpc.php`

XML-RPC is enabled on the WordPress installation. This can be abused for brute-force amplification attacks and DDoS.

```
POST /xmlrpc.php
<?xml version="1.0"?><methodCall><methodName>system.listMethods</methodName></methodCall>

Response: 200 OK with 80+ available methods
```

REMEDIATION

Disable XML-RPC via plugin or .htaccess: <Files xmlrpc.php> Require all denied </Files>

CVSS: **5.3** CWE-16 Module: nuclei

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	–
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 6 of 9 March 15, 2026

06 AI Security Analysis

Comprehensive Risk Assessment

The security posture of example.com requires **urgent remediation**. Two critical vulnerabilities and multiple high-severity issues create viable attack paths that could lead to full compromise.

Critical Risk: Credential Exposure

The exposed .env file on staging.example.com contains production database credentials and Stripe API keys. This is a **data breach in progress** — any attacker who accessed this file has the keys to production systems. Credential rotation must happen immediately, followed by forensic analysis of access logs.

Critical Risk: WordPress RCE

The WordPress installation is running a version with a known unauthenticated RCE. Public exploits exist. Exploitation is trivial and could happen within hours of discovery.

Attack Surface Analysis

- **16 subdomains** discovered, 6 responding to HTTP
- **6 open ports** across 2 hosts
- **SSH exposed** with weak key exchange algorithms
- **Admin panel** discoverable (403 response confirms existence)

Compliance Impact

- **PCI DSS**: 5 violations — TLS 1.0, exposed credentials, missing security headers
- **GDPR**: 3 violations — data protection gaps
- **SOC 2**: 3 violations — access control failures
- **ISO 27001**: 3 violations — security management gaps

Remediation Roadmap

Priority	Action	Timeline
P0	Rotate ALL credentials from exposed .env	Immediately
P0	Patch WordPress or take blog offline	Within 2 hours
P1	Restrict staging access (VPN/IP whitelist)	Within 24 hours
P1	Fix CORS on API	Within 24 hours
P2	Disable TLS 1.0, harden SSH	Within 7 days
P2	Implement HSTS + CSP	Within 7 days
P3	Harden email (SPF -all, DMARC reject)	Within 30 days

VulnScan.Pro — example.com Page 7 of 8 March 15, 2026

07 Compliance Dashboard

NON-COMPLIANT

PCI DSS 4.0

5 violation(s)

- ✗ Req 2.2.4: TLS 1.0 enabled (must use TLS 1.2+)
- ✗ Req 6.5.1: SQL injection not tested (automated only)
- ✗ Req 6.5.7: XSS not tested (automated only)
- ✗ Req 8.2.1: Missing MFA on admin panel
- ✗ Req 4.1: Unencrypted credentials in .env file

NON-COMPLIANT

GDPR

3 violation(s)

- ✗ Art. 32: Missing HSTS — data in transit not adequately protected
- ✗ Art. 25: No CSP header — privacy by design violation
- ✗ Art. 33: No incident response plan documented

NON-COMPLIANT

SOC 2 Type II

3 violation(s)

- ✗ CC6.1: Staging environment publicly accessible without auth
- ✗ CC6.6: Missing WAF on staging/blog subdomains
- ✗ CC7.2: No intrusion detection on exposed SSH

NON-COMPLIANT

ISO 27001

3 violation(s)

- ✗ A.12.6.1: WordPress not patched (known CVE)
- ✗ A.14.1.2: Exposed .env file with production secrets
- ✗ A.10.1.1: Weak SSH key exchange algorithm

VulnScan.Pro — example.com Page 8 of 8 March 15, 2026

07 Methodology

This assessment was performed using VulnScan Pro's automated scanning pipeline, consisting of 13 specialized security modules.

MODULE	STATUS	DURATION
subfinder	✓ OK	12.3s
certTransparency	✓ OK	17.0s
httpx	✓ OK	46.9s
nmap	✓ OK	7.2s
testssl	✓ OK	20.3s
headers	✓ OK	4.2s
dns	✓ OK	53.7s
wafw00f	✓ OK	11.9s
whatweb	✓ OK	37.1s
nuclei	✓ OK	34.6s
nikto	✓ OK	9.3s
zap	✓ OK	45.2s
ffuf	✓ OK	10.6s

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 9 of 9 March 15, 2026