Security Assessment — example.com

Generated by SepSecureAI · Scan duration: 47s · 184 checks executed · Sample report

Risk Score	Breach Probability	Compliance Score
72 / 100 MODERATE	**18%** ELEVATED	**84 / 100** GOOD

Executive summary

The scan of **example.com** identified 23 findings across HTTP security headers, TLS configuration, DNS hygiene, exposed metadata, and application-layer concerns. The site is generally well-configured but is missing several modern security headers (Content-Security-Policy, Permissions-Policy) and exposes server version banners that could aid an attacker in fingerprinting. Two medium-severity authentication weaknesses were detected in the login flow. No critical, internet-exposed vulnerabilities were observed.

Posture: **Moderate** · Grade: **B** · Estimated remediation: **1–2 sprints**

Severity breakdown

Severity	Count	Examples
Critical	0	—
High	3	Missing CSP, weak TLS cipher allowed, exposed .git/
Medium	8	No HSTS preload, verbose 500s, login no rate-limit
Low	9	Server header banner, missing Referrer-Policy, cookie SameSite
Info	3	Outdated jQuery, exposed sitemap, robots.txt comments

Compliance overview

Framework	Score	Status
OWASP Top 10 (2021)	82%	Pass
PCI DSS 4.0 (web surface)	78%	Partial
NIST CSF 2.0 (Protect)	85%	Pass

GDPR — cookie & headers	74%	Partial
ISO 27001 A.14 (web)	80%	Pass

Top findings (detailed)

Each finding includes a CVSS-aligned severity, business impact, attack scenario, and a concrete remediation step. Below is a sample of the highest-priority items.

HIGH **Missing Content-Security-Policy header** CVSS 7.4 · EPSS 0.12

Summary
The response does not include a Content-Security-Policy header. This control is the primary modern defense against cross-site scripting and data injection attacks.

Business impact
Successful XSS can hijack user sessions, steal credentials, or pivot to internal services. For e-commerce flows this directly threatens checkout integrity and PII.

Attack scenario
An attacker injects a script via an unescaped query parameter on /search and exfiltrates session cookies for authenticated users who follow a crafted link.

Remediation
Deploy a CSP starting in report-only mode: `default-src 'self'; script-src 'self' 'nonce-…'; object-src 'none'; base-uri 'self';` Monitor reports for two weeks, then enforce.

HIGH **Exposed .git/ directory on web root** CVSS 7.5 · EPSS 0.34

Summary
The directory `/.git/` is publicly readable and exposes repository metadata including commit history and source.

Business impact
Full source disclosure can leak hard-coded secrets (API keys, DB credentials), private business logic, and accelerate further attacks.

Attack scenario
An attacker mirrors the repo with `git-dumper`, recovers historical commits, and finds a committed AWS access key that grants S3 read access.

Remediation
Block `/.git` at the web server or CDN. Rotate every secret that has ever been committed and audit historical commits.

MEDIUM **Login endpoint missing rate limiting** CVSS 5.3 · EPSS 0.08

Summary
POST /login accepts unlimited authentication attempts from the same IP and account without throttling or CAPTCHA.

Business impact
Enables credential stuffing using leaked password dumps; account takeover at scale erodes user trust and triggers regulatory disclosure.

Attack scenario
An attacker replays a 10M-credential combo list at 50 req/s; with even a 0.1% hit rate that is 10,000 successful logins.

Remediation
Add per-account and per-IP rate limits (e.g. 5/min, 20/hour), require CAPTCHA after 3 failures, and integrate breached-password detection.

Remediation roadmap

Phase	Focus	Items	Effort	Risk reduction
Week 1	Quick wins	CSP report-only, block .git, server banners	1d	–22%
Week 2	Hardening	HSTS preload, Permissions-Policy, cookie flags	2d	–14%
Week 3–4	Auth	Rate-limit login, MFA, breached-password check	5d	–18%
Month 2	Pipeline	Pre-commit secret scanning, dependency SCA	1w	–9%

Methodology

SepSecureAI runs 180+ checks combining active probes (TLS, headers, DNS, common files, cookie attributes, common CMS fingerprints), passive intelligence (threat-feed correlation, EPSS scoring), and an AI curation pass (GPT-class models) that aggregates technical signals into prioritized, business-aligned findings.

Disclaimer