Vulnerability Assessment Report: example.com

SECURITY SCORE: 98/100

OVERALL RISK LEVEL: LOW
Note: Target is protected by a WAF/CDN. Score adjusted for mitigated risks.

1. Network Scan Results (Nmap)

Port	Service	Version	Evidence
80	http		**http-title:** Example Domain...
443	http		**ssl-cert:** Subject: commonName=example.com Subject Alternativ... **http-title:** Example Domain...
8080	http		None
8443	http		**ssl-cert:** Subject: commonName=example.com Subject Alternativ... **http-title:** 400 The plain HTTP request was sent to HTTPS port...

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 104.18.26.120
+ Target Hostname: example.com
+ Target Port: 80
+ Start Time: 2026-02-24 02:21:22 (GMT0)
---------------------------------------------------------------------------
+ Server: cloudflare
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'cf-cache-status' found, with contents: HIT
+ Uncommon header 'cf-ray' found, with contents: 9d2b7d4218517eda-MAA
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'referrer-policy' found, with contents: same-origin
+ Uncommon header 'proxy-status' found, with contents:
Cloudflare-Proxy;error=http_request_error
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ 26 items checked: 0 error(s) and 6 item(s) reported on remote host
+ End Time: 2026-02-24 02:21:26 (GMT0) (4 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

[stderr]
+ ERROR: Host maximum execution time of 600 seconds reached
```

3. Crawled Website Endpoints

- example.com

4. Vulnerability Intelligence (CVE Mapping)

No relevant CVEs identified.

5. Attack Possibilities & Mitigation

[LOW] Attack: Missing Anti-Clickjacking Protection
Mitigation: The X-Frame-Options header is missing entirely. Implement DENY or SAMEORIGIN to prevent UI redressing.

[NOTE] Attack: Missing Content-Security-Policy (CSP)
Mitigation: Implement a strict CSP header to prevent unauthorized script execution and data exfiltration.