

Vulnerability Assessment Report: google.com

SECURITY SCORE: 93/100

OVERALL RISK LEVEL: LOW

*Score capped at 97 due to professional residual uncertainty (Black-box surface scan limitation).

*Score modified due to CMS Ecosystem Risk (Unknown plugin/theme vulnerabilities).

1. Network Scan Results (Nmap)

Port	Service	Version	Evidence
80	http		fingerprint-strings: GetRequest: HTTP/1.0 200 OK Date: Tue, 24... http-title: Did not follow redirect to http://www.google.com/...
443	https		http-title: Did not follow redirect to https://www.google.com/... ssl-cert: Subject: commonName=*.google.com Subject Alternati... fingerprint-strings: GetRequest: HTTP/1.0 200 OK Date: Tue, 24...

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
-----
+ Target IP: 142.250.206.142
+ Target Hostname: google.com
+ Target Port: 80
+ Start Time: 2026-02-24 14:50:10 (GMT0)
-----
+ Server: gws
+ Uncommon header 'content-security-policy-report-only' found, with contents:
object-src 'none';base-uri 'self';script-src 'nonce-9T4dTRFhdJKvXcr_p6RM7Q'
'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http://report-uri
https://csp.withgoogle.com/csp/gws/other-hp
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ Uncommon header 'reporting-endpoints' found, with contents: default="//www.google.com
/httpservice/retry/jserror?ei=pLqdacmAB9DQ2roPt9yE2Qo&cad;=crash&error;=Page%20Crash&js
el;=1&bver;=2383&dpf;=7q1Kg0nIXtdGodxsyzW6mC9x17aF3949Ehhs6I_osVM"
+ Root page / redirects to: http://www.google.com/
+ Uncommon header 'referrer-policy' found, with contents: no-referrer
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'gws' to 'sffe' which may suggest a WAF, load balancer
or proxy is in place
+ Uncommon header 'cross-origin-resource-policy' found, with contents: cross-origin
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Cookie __Secure-STRP created without the httponly flag
+ Cookie AEC created without the httponly flag
+ Cookie NID created without the httponly flag
+ Uncommon header 'content-security-policy' found, with contents: object-src
'none';base-uri 'self';script-src 'nonce-vxYSeBhRBkoySJ00lJqKsw'
'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http://report-uri
```

```

https://csp.withgoogle.com/csp/gws/other
+ 26 items checked: 0 error(s) and 11 item(s) reported on remote host
+ End Time: 2026-02-24 14:50:25 (GMT0) (15 seconds)
-----
+ 1 host(s) tested

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

```

3. Crawled & Fuzzed Endpoints

- http://www.google.com/setprefs?sig=0__Yzr2LGJG3IIUJgWZm_-eFpL3TY%3D&hl;=ml&source;=hom
 - epage&sa;=X&ved;=0ahUKEwis9rCRsPKSAxW0s1YBHUXnFboQ2ZgBCA0
- https://www.google.com/imghp?hl=en&tab;=wi
- http://www.google.com/intl/en/ads/
- http://www.google.com/setprefs?sig=0__Yzr2LGJG3IIUJgWZm_-eFpL3TY%3D&hl;=gu&source;=hom
 - epage&sa;=X&ved;=0ahUKEwis9rCRsPKSAxW0s1YBHUXnFboQ2ZgBCAs
- http://www.google.com/setprefs?sig=0__Yzr2LGJG3IIUJgWZm_-eFpL3TY%3D&hl;=kn&source;=hom
 - epage&sa;=X&ved;=0ahUKEwis9rCRsPKSAxW0s1YBHUXnFboQ2ZgBCAw
- http://www.google.com/setprefs?sig=0__Yzr2LGJG3IIUJgWZm_-eFpL3TY%3D&hl;=mr&source;=hom
 - mepage&sa;=X&ved;=0ahUKEwis9rCRsPKSAxW0s1YBHUXnFboQ2ZgBCAk
- http://www.google.com/advanced_search?hl=en-IN&authuser;=0
- http://www.google.com/setprefs?sig=0__Yzr2LGJG3IIUJgWZm_-eFpL3TY%3D&hl;=ta&source;=hom
 - epage&sa;=X&ved;=0ahUKEwis9rCRsPKSAxW0s1YBHUXnFboQ2ZgBCAo
- http://google.com
- https://play.google.com/?hl=en&tab;=w8
- https://drive.google.com/?tab=wo
- http://www.google.com/preferences?hl=en
- http://www.google.com/intl/en/about.html
- http://www.google.com/setprefs?sig=0__Yzr2LGJG3IIUJgWZm_-eFpL3TY%3D&hl;=pa&source;=hom
 - epage&sa;=X&ved;=0ahUKEwis9rCRsPKSAxW0s1YBHUXnFboQ2ZgBCA4
- https://accounts.google.com/ServiceLogin?hl=en&passive;=true&continue;=http://www.google.com/&ec;=GAZAAQ
- http://www.google.com/intl/en/policies/terms/
- http://www.google.com/intl/en/policies/privacy/
- http://www.google.com/setprefs?sig=0__Yzr2LGJG3IIUJgWZm_-eFpL3TY%3D&hl;=te&source;=hom
 - epage&sa;=X&ved;=0ahUKEwis9rCRsPKSAxW0s1YBHUXnFboQ2ZgBCAg
- http://www.google.com/setprefdomain?prefdom=IN&prev;=http://www.google.co.in/&sig;=K_PXDwlM
 - H3kmX59Kh-vAm24-yXBmE%3D
- https://news.google.com/?tab=wn
- http://www.google.com/setprefs?sig=0__Yzr2LGJG3IIUJgWZm_-eFpL3TY%3D&hl;=bn&source;=hom
 - epage&sa;=X&ved;=0ahUKEwis9rCRsPKSAxW0s1YBHUXnFboQ2ZgBCAc
- https://mail.google.com/mail/?tab=wm
- http://www.google.com/setprefs?sig=0__Yzr2LGJG3IIUJgWZm_-eFpL3TY%3D&hl;=hi&source;=hom
 - epage&sa;=X&ved;=0ahUKEwis9rCRsPKSAxW0s1YBHUXnFboQ2ZgBCAY

4. Vulnerability Intelligence (CVE Mapping)

No relevant CVEs identified.

5. Attack Possibilities & Mitigation

[NOTE] Attack: Missing Content-Security-Policy (CSP)

Mitigation: Implement a strict CSP header.

[NOTE] Attack: CMS Architecture Detected: WordPress (Residual Risk)

Evidence: Found structural indicators for WordPress in source code.

Mitigation: Maintain strict patching routines for WordPress core, plugins, and themes. Obfuscate version numbers.