Vulnerability Assessment Report: google.com

SECURITY SCORE: 91/100

OVERALL RISK LEVEL: LOW
■■ **HIGH-VALUE TARGET:** Application architecture indicates stateful authentication or sensitive data. Scoring strictness amplified.
**Score capped at 97 due to professional residual uncertainty.*

1. Network Scan Results (Nmap)

Port	State	Service	Version	Evidence
80	OPEN	http		**http-title:** Did not follow redirect to http://www.google.com/... **fingerprint-strings:** GetRequest: HTTP/1.0 200 OK Date: Wed, 25...
443	OPEN	https		**http-title:** Did not follow redirect to https://www.google.com/... **ssl-cert:** Subject: commonName=*.google.com Subject Alternati... **fingerprint-strings:** FourOhFourRequest: HTTP/1.0 404 Not Found ...

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 142.250.206.142
+ Target Hostname: google.com
+ Target Port: 80
+ Start Time: 2026-02-25 06:26:46 (GMT0)
---------------------------------------------------------------------------
+ Server: gws
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Uncommon header 'content-security-policy-report-only' found, with contents:
object-src 'none';base-uri 'self';script-src 'nonce-zYAXJyq_7VA2ikVV1mungw'
'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri
https://csp.withgoogle.com/csp/gws/other-hp
+ Uncommon header 'reporting-endpoints' found, with contents: default="//www.google.com
/httpservice/retry/jserror?ei=KpaeaewY59fWxA_Lt4moCg&cad;=crash&error;=Page%20Crash&jse
l;=1&bver;=2383&dpf;=vBDTAt0YznmttjV9wDXTu7kyET4MEb_yLBRFwcwuMXE"
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ 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 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'cross-origin-resource-policy' found, with contents: cross-origin
+ 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-qBVRRLHjHbZsv4OYsgCtKQ' '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: 2026-02-25 06:27:07 (GMT0) (21 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

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

3. Crawled & Fuzzed Endpoints

- http://www.google.com/intl/en/policies/privacy/
- https://www.google.com/imghp?hl=en&tab;=wi
- https://mail.google.com/mail/?tab=wm
- http://www.google.com/intl/en/policies/terms/
- http://www.google.com/setprefs?sig=0_noO8h6SUynTf1jODb1-84Jf1Dw8%3D&hl;=ml&source;=homepage&sa;=X&ved;=0ahUKEwjW6Oe_gfSSAxWzNTUKHcniJ3UQ2ZgBCA0
- http://www.google.com/setprefs?sig=0_noO8h6SUynTf1jODb1-84Jf1Dw8%3D&hl;=pa&source;=homepage&sa;=X&ved;=0ahUKEwjW6Oe_gfSSAxWzNTUKHcniJ3UQ2ZgBCA4
- http://maps.google.co.in/maps?hl=en&tab;=wl
- http://www.google.com/setprefdomain?prefdom=IN&prev;=http://www.google.co.in/&sig;=K_99sc9800cLTZP1hdoItMEwOJQnA%3D
- https://play.google.com/?hl=en&tab;=w8
- http://www.google.com/preferences?hl=en
- http://www.google.com/setprefs?sig=0_noO8h6SUynTf1jODb1-84Jf1Dw8%3D&hl;=te&source;=homepage&sa;=X&ved;=0ahUKEwjW6Oe_gfSSAxWzNTUKHcniJ3UQ2ZgBCAg
- http://www.google.com/advanced_search?hl=en-IN&authuser;=0
- http://www.google.com/setprefs?sig=0_noO8h6SUynTf1jODb1-84Jf1Dw8%3D&hl;=hi&source;=homepage&sa;=X&ved;=0ahUKEwjW6Oe_gfSSAxWzNTUKHcniJ3UQ2ZgBCAY
- http://www.google.com/setprefs?sig=0_noO8h6SUynTf1jODb1-84Jf1Dw8%3D&hl;=kn&source;=homepage&sa;=X&ved;=0ahUKEwjW6Oe_gfSSAxWzNTUKHcniJ3UQ2ZgBCAw
- http://www.google.com/intl/en/ads/
- https://news.google.com/?tab=wn
- http://www.google.co.in/services/
- https://www.youtube.com/?tab=w1
- http://www.google.com/intl/en/about.html
- http://www.google.com/setprefs?sig=0_noO8h6SUynTf1jODb1-84Jf1Dw8%3D&hl;=gu&source;=homepage&sa;=X&ved;=0ahUKEwjW6Oe_gfSSAxWzNTUKHcniJ3UQ2ZgBCAs
- https://www.google.co.in/intl/en/about/products?tab=wh
- http://www.google.com/setprefs?sig=0_noO8h6SUynTf1jODb1-84Jf1Dw8%3D&hl;=mr&source;=homepage&sa;=X&ved;=0ahUKEwjW6Oe_gfSSAxWzNTUKHcniJ3UQ2ZgBCAk
- http://www.google.com/setprefs?sig=0_noO8h6SUynTf1jODb1-84Jf1Dw8%3D&hl;=ta&source;=homepage&sa;=X&ved;=0ahUKEwjW6Oe_gfSSAxWzNTUKHcniJ3UQ2ZgBCAo
- https://accounts.google.com/ServiceLogin?hl=en&passive;=true&continue;=http://www.google.com/&ec;=GAZAAQ
- https://drive.google.com/?tab=wo
- http://google.com
- http://www.google.co.in/history/optout?hl=en
- http://www.google.com/setprefs?sig=0_noO8h6SUynTf1jODb1-84Jf1Dw8%3D&hl;=bn&source;=homepage&sa;=X&ved;=0ahUKEwjW6Oe_gfSSAxWzNTUKHcniJ3UQ2ZgBCAc

4. Vulnerability Intelligence (CVE Mapping)

No relevant CVEs identified.

5. Attack Possibilities & Mitigation

[LOW] Attack: Missing Anti-Clickjacking Protection
Mitigation: Implement DENY or SAMEORIGIN X-Frame-Options.

[NOTE] Attack: Missing Content-Security-Policy (CSP)
Mitigation: Implement a strict CSP header.