Vulnerability Assessment Report: google.com

SECURITY SCORE: 100/100

OVERALL RISK LEVEL: LOW

1. Network Scan Results (Nmap)

Port	Service	Version	State
80	http		open
443	https		open

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 216.58.203.46
+ Target Hostname: google.com
+ Target Port: 80
+ Start Time: 2026-02-22 14:41:25 (GMT0)
---------------------------------------------------------------------------
+ Server: gws
+ Uncommon header 'reporting-endpoints' found, with contents: default="//www.google.com
/httpservice/retry/jserror?ei=lhWbaYnhFbjT1sQPisuwqQ0&cad;=crash&error;=Page%20Crash&js
el;=1&bver;=2383&dpf;=IS-KImmh1g9ecEFH571E8r0IrIWV7F1SRRCw4xf8B40"
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ 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-w3OBTK-VlfhquWL13mvxOQ'
'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri
https://csp.withgoogle.com/csp/gws/other-hp
+ 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-syqNprGrQFVFK1qoVB89gg' '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: 2026-02-22 14:41:45 (GMT0) (20 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

[nikto stderr]
+ ERROR: Host maximum execution time of 180 seconds reached
```

3. Crawled Website Endpoints

- No endpoints found

4. Vulnerability Intelligence (CVE Mapping)

Legacy Vulnerability Intelligence
- ■■ NOTICE: Our engine identified 4 additional legacy vulnerabilities (pre-2016) associated with these services. These have been filtered to prioritize current threats.

5. Attack Possibilities & Mitigation

Attack: Session Hijacking / Cookie Theft
Mitigation: Set HttpOnly and Secure flags on all sensitive cookies.

Attack: Client-side Script Injection
Mitigation: Sanitize all user inputs and use output encoding.