

Vulnerability Assessment Report: google.com

SECURITY SCORE: 96/100

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 14:46:41 (GMT0)
-----
+ Server: gws
+ Uncommon header 'reporting-endpoints' found, with contents: default="//www.google.com
/httpservice/retry/jserror?ei=0habac_7K-fflsQPwvmYyQ4&cad;=crash&error;=Page%20Crash&js
el;=l&bver;=2383&dpf;=IS-KImmhlG9ecEFH57lE8r0IrIWV7F1SRRCw4xf8B40"
+ Uncommon header 'content-security-policy-report-only' found, with contents:
object-src 'none';base-uri 'self';script-src 'nonce-m-UiiynRn3f9AClPfMVB3Q'
'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri
https://csp.withgoogle.com/csp/gws/other-hp
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ 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-cOyc3Dt8L83l4REWfGUSwA' '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 14:47:01 (GMT0) (20 seconds)
-----
+ 1 host(s) tested

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

3. Crawled Website Endpoints

- https://www.google.com/setprefs?sig=0_eN9FZw4wy84yK6p5rgdR-I5JwRA%3D&hl;=pa&source;=hoogle&sa;=X&ved;=0ahUKEwjy5bzRq-2SAxW-h1YBHXdRLEUQ2ZgBCDo
- https://www.google.com/setprefs?sig=0_eN9FZw4wy84yK6p5rgdR-I5JwRA%3D&hl;=mr&source;=hoogle&sa;=X&ved;=0ahUKEwjy5bzRq-2SAxW-h1YBHXdRLEUQ2ZgBCDU
- https://www.google.com/setprefs?sig=0_eN9FZw4wy84yK6p5rgdR-I5JwRA%3D&hl;=gu&source;=hoogle&sa;=X&ved;=0ahUKEwjy5bzRq-2SAxW-h1YBHXdRLEUQ2ZgBCDc
- https://www.google.com/setprefs?sig=0_eN9FZw4wy84yK6p5rgdR-I5JwRA%3D&hl;=kn&source;=hoogle&sa;=X&ved;=0ahUKEwjy5bzRq-2SAxW-h1YBHXdRLEUQ2ZgBCDg
- <https://www.google.com/preferences?hl=en-IN&fg;=1>
- https://www.google.com/setprefs?sig=0_eN9FZw4wy84yK6p5rgdR-I5JwRA%3D&hl;=ta&source;=hoogle&sa;=X&ved;=0ahUKEwjy5bzRq-2SAxW-h1YBHXdRLEUQ2ZgBCDY
- https://www.google.com/setprefs?sig=0_eN9FZw4wy84yK6p5rgdR-I5JwRA%3D&hl;=te&source;=hoogle&sa;=X&ved;=0ahUKEwjy5bzRq-2SAxW-h1YBHXdRLEUQ2ZgBCDQ
- <https://www.google.com/imghp?hl=en&ogbl;=1>
- https://www.google.com/services/?subid=ww-ww-et-g-awa-a-g_hpbfoot1_1!o2&utm;_source=google.com&utm;_medium=referral&utm;_campaign=google_hpbfooter&fg;=1
- https://www.google.com/advanced_search?hl=en-IN&fg;=1
- https://www.google.com/setprefs?sig=0_eN9FZw4wy84yK6p5rgdR-I5JwRA%3D&hl;=bn&source;=hoogle&sa;=X&ved;=0ahUKEwjy5bzRq-2SAxW-h1YBHXdRLEUQ2ZgBCDM
- https://www.google.com/intl/en_in/ads/?subid=ww-ww-et-g-awa-a-g_hpafoot1_1!o2&utm;_source=google.com&utm;_medium=referral&utm;_campaign=google_hpafooter&fg;=1
- https://www.google.com/setprefs?sig=0_eN9FZw4wy84yK6p5rgdR-I5JwRA%3D&hl;=hi&source;=hoogle&sa;=X&ved;=0ahUKEwjy5bzRq-2SAxW-h1YBHXdRLEUQ2ZgBCDI
- https://www.google.com/setprefs?sig=0_eN9FZw4wy84yK6p5rgdR-I5JwRA%3D&hl;=ml&source;=hoogle&sa;=X&ved;=0ahUKEwjy5bzRq-2SAxW-h1YBHXdRLEUQ2ZgBCDk
- https://www.google.com/search?sca_esv=eb31b015fd5c8452&q;=what%E2%80%99s+the+most+difficult+ground+for+india+to+play+on+in+the+super+8%E2%80%99s%3F+which+Indian+players+will+do+the+best+on+the+pitch%3F&udm;=50&oi;=ddle&noiga;=1&aep;=84&sa;=X&ved;=0ahUKEwjy5bzRq-2SAxW-h1YBHXdRLEUQPQgE
- [FORM] <https://www.google.com/search>

4. Vulnerability Intelligence (CVE Mapping)

Note: Findings categorized by severity.

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.