

Vulnerability Assessment Report: google.com

SECURITY SCORE: 96/100

OVERALL RISK LEVEL: LOW

1. Network Scan Results (Nmap)

Port	Service	Version	State
------	---------	---------	-------

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 17:19:36 (GMT0)
-----
+ Server: gws
+ Uncommon header 'reporting-endpoints' found, with contents: default="//www.google.com
/httpservice/retry/jserror?ei=qTqbaeCwCvDu4-EP47CiiAY&cad;=crash&error;=Page%20Crash&js
el;=l&bver;=2383&dpf;=YjdYKBv9cOq1bBIPyIHbMyvAxxJmLAKU6BKdtYMiN2E"
+ Uncommon header 'content-security-policy-report-only' found, with contents:
object-src 'none';base-uri 'self';script-src 'nonce-RlNXN3bkPlJiw3Q4VUKcfg'
'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
+ 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-vltdMgzwh6F8zQ19d4Ux1w' 'strict-dynamic'
'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri
https://csp.withgoogle.com/csp/gws/other
+ 0 items checked: 0 error(s) and 11 item(s) reported on remote host
+ End Time: 2026-02-22 17:19:51 (GMT0) (15 seconds)
-----
+ 1 host(s) tested

[stderr]
+ ERROR: Host maximum execution time of 60 seconds reached
```

3. Crawled Website Endpoints

- https://www.google.com/setprefs?sig=0_kpAuBcLfPqOXzS_0e67FL4SehA0%3D&hl;=gu&source;=homepage&sa;=X&ved;=0ahUKEwiL3rLmze2SAxVcgFYBHZQPKmMQ2ZgBCDc

- https://www.google.com/advanced_search?hl=en-IN&fg;=1
- https://www.google.com/setprefs?sig=0_kpAuBcLfPqOXzS_0e67FL4SehA0%3D&hl;=ml&source;=homepage&sa;=X&ved;=0ahUKEwiL3rLmze2SAxVcgFYBHZQPKmMQ2ZgBCDk
- [FORM] <https://www.google.com/search>
- https://www.google.com/setprefs?sig=0_kpAuBcLfPqOXzS_0e67FL4SehA0%3D&hl;=hi&source;=homepage&sa;=X&ved;=0ahUKEwiL3rLmze2SAxVcgFYBHZQPKmMQ2ZgBCDI
- 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/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/setprefs?sig=0_kpAuBcLfPqOXzS_0e67FL4SehA0%3D&hl;=bn&source;=homepage&sa;=X&ved;=0ahUKEwiL3rLmze2SAxVcgFYBHZQPKmMQ2ZgBCDM
- https://www.google.com/setprefs?sig=0_kpAuBcLfPqOXzS_0e67FL4SehA0%3D&hl;=pa&source;=homepage&sa;=X&ved;=0ahUKEwiL3rLmze2SAxVcgFYBHZQPKmMQ2ZgBCDo
- https://www.google.com/setprefs?sig=0_kpAuBcLfPqOXzS_0e67FL4SehA0%3D&hl;=mr&source;=homepage&sa;=X&ved;=0ahUKEwiL3rLmze2SAxVcgFYBHZQPKmMQ2ZgBCDU
- https://www.google.com/setprefs?sig=0_kpAuBcLfPqOXzS_0e67FL4SehA0%3D&hl;=kn&source;=homepage&sa;=X&ved;=0ahUKEwiL3rLmze2SAxVcgFYBHZQPKmMQ2ZgBCDg
- <https://www.google.com/imghp?hl=en&ogbl;>
- <https://www.google.com/preferences?hl=en-IN&fg;=1>
- https://www.google.com/setprefs?sig=0_kpAuBcLfPqOXzS_0e67FL4SehA0%3D&hl;=ta&source;=homepage&sa;=X&ved;=0ahUKEwiL3rLmze2SAxVcgFYBHZQPKmMQ2ZgBCDY
- https://www.google.com/search?sca_esv=3587ac9b8d8afde8&q;=T20+World+Cup&oi;=ddle&noiga;=1&ct;=483672621&hl;=en-GB&si;=AL3DRZHMwLjWhgnaPB3UTu10R6S5qNLXiQiKMeezfKyB1FMsRkVCQTvj6Kt1pgtnbJG1xINL7DjtnWYziEw3WeiH-twRdmdfDLPKecAiskQ2DjTTiw__U_g%3D&sa;=X&ved;=0ahUKEwiL3rLmze2SAxVcgFYBHZQPKmMQPQgE
- https://www.google.com/setprefs?sig=0_kpAuBcLfPqOXzS_0e67FL4SehA0%3D&hl;=te&source;=homepage&sa;=X&ved;=0ahUKEwiL3rLmze2SAxVcgFYBHZQPKmMQ2ZgBCDQ

4. Vulnerability Intelligence (CVE Mapping)

No relevant CVEs identified.

5. Attack Possibilities & Mitigation

[LOW] Attack: Client-side Script Injection

Mitigation: Sanitize all user inputs and use output encoding.

[LOW] Attack: Session Hijacking / Cookie Theft

Mitigation: Set HttpOnly and Secure flags on all sensitive cookies.