

# 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 14:26:57 (GMT0)
-----
+ Server: gws
+ 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-8kw9tMB_iA6NlyTd_o7vZw'
'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
/httplibservice/retry/jserror?ei=MhKbacbrOv3c1sQP3tzQmAg&cad;=crash&error;=Page%20Crash&js
el;=l&bver;=2383&dpf;=dYus08USER90trigtVY3BdAVTYHlj6h5HEeeQor005w"
+ 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-MDaENTdN6q4cfb7WjXH3Jw' '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 14:27:18 (GMT0) (21 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\\_6cZn8w8XcWkbHy4Nia5gVKGogms%3D&hl=en&source=home&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQ2ZgBCDU](https://www.google.com/setprefs?sig=0_6cZn8w8XcWkbHy4Nia5gVKGogms%3D&hl=en&source=home&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQ2ZgBCDU)
- [https://www.google.com/setprefs?sig=0\\_6cZn8w8XcWkbHy4Nia5gVKGogms%3D&hl=en&source=home&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQ2ZgBCDM](https://www.google.com/setprefs?sig=0_6cZn8w8XcWkbHy4Nia5gVKGogms%3D&hl=en&source=home&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQ2ZgBCDM)
- [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/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/preferences?hl=en-IN&fg=1>
- <https://www.google.com/imghp?hl=en&ogbl>
- [https://www.google.com/search?sca\\_esv=9a738b84887eeca&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=dde&noiga=1&aep=84&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQPQgE](https://www.google.com/search?sca_esv=9a738b84887eeca&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=dde&noiga=1&aep=84&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQPQgE)
- [https://www.google.com/setprefs?sig=0\\_6cZn8w8XcWkbHy4Nia5gVKGogms%3D&hl=en&source=home&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQ2ZgBCDY](https://www.google.com/setprefs?sig=0_6cZn8w8XcWkbHy4Nia5gVKGogms%3D&hl=en&source=home&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQ2ZgBCDY)
- [https://www.google.com/setprefs?sig=0\\_6cZn8w8XcWkbHy4Nia5gVKGogms%3D&hl=en&source=home&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQ2ZgBCDo](https://www.google.com/setprefs?sig=0_6cZn8w8XcWkbHy4Nia5gVKGogms%3D&hl=en&source=home&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQ2ZgBCDo)
- [https://www.google.com/advanced\\_search?hl=en-IN&fg=1](https://www.google.com/advanced_search?hl=en-IN&fg=1)
- [https://www.google.com/setprefs?sig=0\\_6cZn8w8XcWkbHy4Nia5gVKGogms%3D&hl=en&source=home&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQ2ZgBCDc](https://www.google.com/setprefs?sig=0_6cZn8w8XcWkbHy4Nia5gVKGogms%3D&hl=en&source=home&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQ2ZgBCDc)
- [FORM] <https://www.google.com/search>
- [https://www.google.com/setprefs?sig=0\\_6cZn8w8XcWkbHy4Nia5gVKGogms%3D&hl=en&source=home&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQ2ZgBCDg](https://www.google.com/setprefs?sig=0_6cZn8w8XcWkbHy4Nia5gVKGogms%3D&hl=en&source=home&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQ2ZgBCDg)
- [https://www.google.com/setprefs?sig=0\\_6cZn8w8XcWkbHy4Nia5gVKGogms%3D&hl=en&source=home&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQ2ZgBCDI](https://www.google.com/setprefs?sig=0_6cZn8w8XcWkbHy4Nia5gVKGogms%3D&hl=en&source=home&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQ2ZgBCDI)
- [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/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\\_6cZn8w8XcWkbHy4Nia5gVKGogms%3D&hl=en&source=home&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQ2ZgBCDQ](https://www.google.com/setprefs?sig=0_6cZn8w8XcWkbHy4Nia5gVKGogms%3D&hl=en&source=home&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQ2ZgBCDQ)
- [https://www.google.com/setprefs?sig=0\\_6cZn8w8XcWkbHy4Nia5gVKGogms%3D&hl=en&source=home&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQ2ZgBCDk](https://www.google.com/setprefs?sig=0_6cZn8w8XcWkbHy4Nia5gVKGogms%3D&hl=en&source=home&sa=X&ved=0ahUKEwjgq72dp-2SAxWes1YBHcL0CbMQ2ZgBCDk)

## 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.