

# Vulnerability Assessment Report: google.com

## 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: 142.251.220.46
+ Target Hostname: google.com
+ Target Port: 80
+ Start Time: 2026-01-29 03:34:32 (GMT0)
-----
+ Server: gws
+ Uncommon header 'content-security-policy-report-only' found, with contents:
object-src 'none';base-uri 'self';script-src 'nonce-uykS0_LicaptCcKnA5e3KA'
'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 '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-UmZYYyBp6R70RLpVjwWihA' '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 10 item(s) reported on remote host
+ End Time: 2026-01-29 03:34:52 (GMT0) (20 seconds)
-----
+ 1 host(s) tested
```