

# 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: 216.58.203.14
+ Target Hostname: google.com
+ Target Port: 80
+ Start Time: 2026-02-12 15:47:11 (GMT0)
-----
+ Server: gws
+ 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-4GWZuYHxevSWUQysLXIaOQ'
'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
/httpservice/retry/jserror?ei=AfaNaeOzLdLlseMPl7fpqQU&cad=crash&error=Page%20Crash&js
el=1"
+ 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 '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-gelJTF9A5Ur7Xj_ndUFYAQ' '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: 2026-02-12 15:47:27 (GMT0) (16 seconds)
-----
+ 1 host(s) tested
```

## 3. Crawled Website Endpoints

- https://www.google.com/setprefs?sig=0\_3BJNwCrTZov\_duDGK50eb1zJxKc%3D&hl=ml&source=homepage&sa=X&ved=0ahUKEwiAxI3AptSSAxW8n68BHUhXLa0Q2ZgBCDA
- 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\_3BJNwCrTZov\_duDGK50eb1zJxKc%3D&hl=gu&source=homepage&sa=X&ved=0ahUKEwiAxI3AptSSAxW8n68BHUhXLa0Q2ZgBCC4

- [FORM] <https://www.google.com/search>
- [https://www.google.com/setprefs?sig=0\\_3BJNwCrTZov\\_duDGK50eb1zJxKc%3D&hl;=bn&source;=homepage&sa;=X&ved;=0ahUKEwiAxI3AptSSAxW8n68BHUhXLa0Q2ZgBCCo](https://www.google.com/setprefs?sig=0_3BJNwCrTZov_duDGK50eb1zJxKc%3D&hl;=bn&source;=homepage&sa;=X&ved;=0ahUKEwiAxI3AptSSAxW8n68BHUhXLa0Q2ZgBCCo)
- [https://www.google.com/setprefs?sig=0\\_3BJNwCrTZov\\_duDGK50eb1zJxKc%3D&hl;=kn&source;=homepage&sa;=X&ved;=0ahUKEwiAxI3AptSSAxW8n68BHUhXLa0Q2ZgBCC8](https://www.google.com/setprefs?sig=0_3BJNwCrTZov_duDGK50eb1zJxKc%3D&hl;=kn&source;=homepage&sa;=X&ved;=0ahUKEwiAxI3AptSSAxW8n68BHUhXLa0Q2ZgBCC8)
- [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/preferences?hl=en-IN&fg;=1>
- [https://www.google.com/setprefs?sig=0\\_3BJNwCrTZov\\_duDGK50eb1zJxKc%3D&hl;=te&source;=homepage&sa;=X&ved;=0ahUKEwiAxI3AptSSAxW8n68BHUhXLa0Q2ZgBCCs](https://www.google.com/setprefs?sig=0_3BJNwCrTZov_duDGK50eb1zJxKc%3D&hl;=te&source;=homepage&sa;=X&ved;=0ahUKEwiAxI3AptSSAxW8n68BHUhXLa0Q2ZgBCCs)
- [https://www.google.com/setprefs?sig=0\\_3BJNwCrTZov\\_duDGK50eb1zJxKc%3D&hl;=mr&source;=homepage&sa;=X&ved;=0ahUKEwiAxI3AptSSAxW8n68BHUhXLa0Q2ZgBCCw](https://www.google.com/setprefs?sig=0_3BJNwCrTZov_duDGK50eb1zJxKc%3D&hl;=mr&source;=homepage&sa;=X&ved;=0ahUKEwiAxI3AptSSAxW8n68BHUhXLa0Q2ZgBCCw)
- [https://www.google.com/setprefs?sig=0\\_3BJNwCrTZov\\_duDGK50eb1zJxKc%3D&hl;=pa&source;=homepage&sa;=X&ved;=0ahUKEwiAxI3AptSSAxW8n68BHUhXLa0Q2ZgBCDE](https://www.google.com/setprefs?sig=0_3BJNwCrTZov_duDGK50eb1zJxKc%3D&hl;=pa&source;=homepage&sa;=X&ved;=0ahUKEwiAxI3AptSSAxW8n68BHUhXLa0Q2ZgBCDE)
- [https://www.google.com/search?sca\\_esv=2cf3e72a8cc0c0c9&q=icc+men%27s+t20+world+cup&oi=ddle&noiga;=1&ct=483694412&hl;=en-GB&sa;=X&ved;=0ahUKEwiAxI3AptSSAxW8n68BHUhXLa0QPQgE](https://www.google.com/search?sca_esv=2cf3e72a8cc0c0c9&q=icc+men%27s+t20+world+cup&oi=ddle&noiga;=1&ct=483694412&hl;=en-GB&sa;=X&ved;=0ahUKEwiAxI3AptSSAxW8n68BHUhXLa0QPQgE)
- [https://www.google.com/setprefs?sig=0\\_3BJNwCrTZov\\_duDGK50eb1zJxKc%3D&hl;=hi&source;=homepage&sa;=X&ved;=0ahUKEwiAxI3AptSSAxW8n68BHUhXLa0Q2ZgBCCk](https://www.google.com/setprefs?sig=0_3BJNwCrTZov_duDGK50eb1zJxKc%3D&hl;=hi&source;=homepage&sa;=X&ved;=0ahUKEwiAxI3AptSSAxW8n68BHUhXLa0Q2ZgBCCk)
- <https://www.google.com/imghp?hl=en&ogbl;>
- [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/setprefs?sig=0\\_3BJNwCrTZov\\_duDGK50eb1zJxKc%3D&hl;=ta&source;=homepage&sa;=X&ved;=0ahUKEwiAxI3AptSSAxW8n68BHUhXLa0Q2ZgBCC0](https://www.google.com/setprefs?sig=0_3BJNwCrTZov_duDGK50eb1zJxKc%3D&hl;=ta&source;=homepage&sa;=X&ved;=0ahUKEwiAxI3AptSSAxW8n68BHUhXLa0Q2ZgBCC0)

## 4. Vulnerabilities Detected

- Cross-Site Scripting (XSS)
- Insecure Cookies

## 5. Vulnerability Intelligence (CVE Mapping)

### Vulnerabilities in gws

- [MEDIUM 5.0] CVE-2000-0720: news.cgi in GWScripts News Publisher does not properly authenticate requests to add an author to the author index, which allows remote attackers to ad...
- [MEDIUM 5.0] CVE-2014-1962: Gwsync in SAP CRM 7.02 EHP 2 allows remote attackers to obtain sensitive information via unspecified vectors, related to an XML External Entity (XXE) ...

### Vulnerabilities in gws

- [MEDIUM 5.0] CVE-2000-0720: news.cgi in GWScripts News Publisher does not properly authenticate requests to add an author to the author index, which allows remote attackers to ad...
- [MEDIUM 5.0] CVE-2014-1962: Gwsync in SAP CRM 7.02 EHP 2 allows remote attackers to obtain sensitive information via unspecified vectors, related to an XML External Entity (XXE) ...

## 6. Attack Possibilities & Mitigation

**Attack:** Client-side Script Injection

**Mitigation:** Sanitize all user inputs and use output encoding.

**Attack:** Session Hijacking / Cookie Theft

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