

# Vulnerability Assessment Report: youtube.com

SECURITY SCORE: 96/100

RISK ASSESSMENT: LOW

■■ INFO: Edge protection (WAF/CDN) detected. Results reflect externally visible attack surface.

## 1. Network Scan Results (Nmap)

Port	State	Service	Version	Evidence
80	OPEN	http		<b>http-title:</b> Did not follow redirect to https://youtube.com/... <b>fingerprint-strings:</b> GetRequest: HTTP/1.0 200 OK Date: Wed, 25...
443	OPEN	https		<b>ssl-cert:</b> Subject: commonName=*.google.com Subject Alternati... <b>http-title:</b> Did not follow redirect to https://www.youtube.com... <b>fingerprint-strings:</b> GetRequest: HTTP/1.0 200 OK Date: Wed, 25...

## 2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
-----
+ Target IP: 142.250.77.46
+ Target Hostname: youtube.com
+ Target Port: 80
+ Start Time: 2026-02-25 04:39:10 (GMT0)
-----
+ Server: ESF
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Root page / redirects to: https://youtube.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'ESF' 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 'reporting-endpoints' found, with contents: default="//www.google.com
/httpservice/retry/jserror?ei=93yeabiWJbSdhhbIP-Oe5wAE&cad;=crash&error;=Page%20Crash&js
el;=1&bver;=2384"
+ Uncommon header 'content-security-policy-report-only' found, with contents:
object-src 'none';base-uri 'self';script-src 'nonce-0fn6fEc3McciDad2nc5mNw'
'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri
https://csp.withgoogle.com/csp/gws/other-hp
+ 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-b5fGcRgh2QgrI-RkFks7gQ' 'strict-dynamic'
'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri
https://csp.withgoogle.com/csp/gws/other
+ Uncommon header 'referrer-policy' found, with contents: no-referrer
```

```
+ 26 items checked: 0 error(s) and 11 item(s) reported on remote host
+ End Time: 2026-02-25 04:39:22 (GMT0) (12 seconds)
-----
+ 1 host(s) tested

[stderr]
+ ERROR: Host maximum execution time of 600 seconds reached
```

### 3. Vulnerability Intelligence (CVE Mapping)

No relevant CVEs identified.

### 4. Attack Findings & Mitigation

**[NOTE] Missing Content-Security-Policy (CSP)**

*Evidence: See scan logs*

Mitigation: Implement a strict CSP header.