Vulnerability Assessment Report: youtube.com

SECURITY SCORE: 46/100

OVERALL RISK LEVEL: HIGH

1. Network Scan Results (Nmap)

Port	State	Service	Version	Evidence
80	OPEN	http		**http-title:** Did not follow redirect to https://youtube.com/... **fingerprint-strings:** GetRequest: HTTP/1.0 200 OK Date: Tue, 24...
443	OPEN	https		**ssl-cert:** Subject: commonName=*.google.com Subject Alternati... **http-title:** Did not follow redirect to https://www.youtube.com... **fingerprint-strings:** GetRequest: HTTP/1.0 200 OK Date: Tue, 24...

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 142.250.77.46
+ Target Hostname: youtube.com
+ Target Port: 80
+ Start Time: 2026-02-24 16:33:33 (GMT0)
---------------------------------------------------------------------------
+ Server: ESF
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ 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 'content-security-policy-report-only' found, with contents:
object-src 'none';base-uri 'self';script-src 'nonce-UXVlg5GB83a-Jm3CWrfKcA'
'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=6NKdaarxC7-Z4-EPm7rDsA0&cad;=crash&error;=Page%20Crash&js
el;=1&bver;=2383&dpf;=e0ZuMWzO0Wkpy2cVaHPN-F9WldAfOM50Tr3hBj1kDzQ"
+ 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-UZf-2r5eNfch1ByUN0RTmg' '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: 2026-02-24 16:33:47 (GMT0) (14 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

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

3. Crawled & Fuzzed Endpoints

- https://www.youtube.com/about/press/
- https://www.youtube.com/t/contact_us/
- https://www.youtube.com/about/copyright/
- https://www.youtube.com/t/privacy
- https://www.youtube.com/ads/
- https://www.youtube.com/opensearch?locale=en_GB
- https://www.youtube.com/about/
- https://www.youtube.com/s/desktop/2a7df5b3/img/favicon_144x144.png
- https://www.youtube.com/s/desktop/2a7df5b3/cssbin/www-onepick.css
- https://www.youtube.com/s/desktop/2a7df5b3/img/favicon_48x48.png
- https://www.youtube.com/s/_/ytmainappweb/_/ss/k=ytmainappweb.kevlar_base.CQgof1ALkHc.L.X.O/am=AAAAQIAAQAM/d=0/rs=AGKMywH56zj2trWAcf0gagH-Fsw9glDKvg
- https://www.youtube.com/s/desktop/2a7df5b3/cssbin/www-main-desktop-home-page-skeleton.css
- https://www.youtube.com/howyoutubeworks?utm_campaign=ytgen&utm;_source=ythp&utm;_medium=LeftNav&utm;_content=txt&u;=https%3A%2F%2Fwww.youtube.com%2Fhowyoutubeworks%3Futm_source%3Dythp%26utm_medium%3DLeftNav%26utm_campaign%3Dytgen
- https://www.youtube.com/new
- https://www.youtube.com/t/terms
- https://www.youtube.com/s/desktop/2a7df5b3/img/favicon_96x96.png
- https://www.youtube.com/s/desktop/2a7df5b3/cssbin/www-main-desktop-watch-page-skeleton.css
- https://m.youtube.com/
- https://www.youtube.com/s/desktop/2a7df5b3/img/favicon_32x32.png
- http://youtube.com
- https://www.youtube.com/creators/
- https://www.youtube.com/manifest.webmanifest
- https://www.youtube.com/s/desktop/2a7df5b3/img/favicon.ico
- https://www.youtube.com/
- https://www.youtube.com/about/policies/

4. Vulnerability Intelligence (CVE Mapping)

No relevant CVEs identified.

5. Attack Possibilities & Mitigation

[LOW] Attack: Missing Anti-Clickjacking Protection
Mitigation: Implement DENY or SAMEORIGIN X-Frame-Options.

[NOTE] Attack: Missing Content-Security-Policy (CSP)

Mitigation: Implement a strict CSP header.

[CRITICAL] Attack: Blind SQL Injection (HTML Form at /howyoutubeworks/)
Evidence: Payload forced server to sleep for 3.17 seconds.
Mitigation: Use prepared statements.