Vulnerability Assessment Report: youtube.com

SECURITY SCORE: 96/100

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: 172.217.174.78
+ Target Hostname: youtube.com
+ Target Port: 80
+ Start Time: 2026-02-22 16:17:32 (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=JyybadHXI6LWseMPzPS68Qk&cad;=crash&error;=Page%20Crash&js
el;=1&bver;=2383&dpf;=YjdYKBv9cOq1bBIPyIHbMyvAxxJmLAKU6BKdtYMiN2E"
+ Uncommon header 'content-security-policy-report-only' found, with contents:
object-src 'none';base-uri 'self';script-src 'nonce-OeHC0E2lcqy6cSWNBi5RPw'
'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-NfNfdWglb2GkC2rkX3n3Vw' '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: 2026-02-22 16:17:47 (GMT0) (15 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

[stderr]
+ ERROR: Host maximum execution time of 86400 seconds reached
```

3. Crawled Website Endpoints

- https://www.youtube.com/t/contact_us/
- https://www.youtube.com/about/press/
- 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/about/policies/
- https://www.youtube.com/t/privacy
- https://www.youtube.com/
- https://www.youtube.com/about/copyright/
- https://www.youtube.com/about/
- https://www.youtube.com/new
- https://www.youtube.com/t/terms
- https://www.youtube.com/creators/
- https://www.youtube.com/ads/

4. Vulnerability Intelligence (CVE Mapping)

No relevant CVEs identified.

5. Attack Possibilities & Mitigation

[LOW] Attack: Session Hijacking / Cookie Theft
Mitigation: Set HttpOnly and Secure flags on all sensitive cookies.

[LOW] Attack: Client-side Script Injection
Mitigation: Sanitize all user inputs and use output encoding.