Vulnerability Assessment Report: youtube.com

SECURITY SCORE: 81/100

OVERALL RISK LEVEL: MEDIUM

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: 142.250.207.174
+ Target Hostname: youtube.com
+ Target Port: 80
+ Start Time: 2026-02-13 16:20:16 (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-bwNgQqvKf9JGfwHKIC_2tw'
'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=S0-PaeOnHrazwcsPstG_0QQ&cad;=crash&error;=Page%20Crash&js
el;=1"
+ 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-hES7EHdUhq04L0yU4HgpRw' '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
+ /cfappman/index.cfm - Redirects (301) to https://youtube.com/cfappman/index.cfm ,
susceptible to ODBC/pipe-style exploit; see RFP9901
http://www.wiretrip.net/rfp/p/doc.asp/i2/d3.htm
+ /cfdocs/examples/cvbeans/beaninfo.cfm - Redirects (301) to
https://youtube.com/cfdocs/examples/cvbeans/beaninfo.cfm , susceptible to our ODBC
exploit; see RFP9901 http://www.wiretrip.net/rfp/p/doc.asp/i2/d3.htm
+ /cfdocs/examples/parks/detail.cfm - Redirects (301) to
https://youtube.com/cfdocs/examples/parks/detail.cfm , susceptible to our ODBC exploit;
see RFP9901 http://www.wiretrip.net/rfp/p/doc.asp/i2/d3.htm
+ /kboard/ - Redirects (301) to https://youtube.com/kboard/ , KBoard Forum 0.3.0 and
prior have a security problem in forum_edit_post.php, forum_post.php and
forum_reply.php
```

```
+ /lists/admin/ - Redirects (301) to https://youtube.com/lists/admin/ , PHPList pre
2.6.4 contains a number of vulnerabilities including remote administrative access,
harvesting user info and more. Default login to admin interface is admin/phplist
+ /ssdefs/ - Redirects (301) to https://youtube.com/ssdefs/ , Siteseed pre 1.4.2 has
'major' security problems.
+ /sshome/ - Redirects (301) to https://youtube.com/sshome/ , Siteseed pre 1.4.2 has
'major' security problems.
+ /tiki/ - Redirects (301) to https://youtube.com/tiki/ , Tiki 1.7.2 and previous
allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could
be admin/admin
+ /tiki/tiki-install.php - Redirects (301) to https://youtube.com/tiki/tiki-install.php
, Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'.
Default login/pass could be admin/admin
+ /scripts/samples/details.idc - Redirects (301) to
https://youtube.com/scripts/samples/details.idc , See RFP 9901; www.wiretrip.net
+ /includes/conexion.inc - Redirects (301) to https://youtube.com/includes/conexion.inc
, Database connection file found.
+ /.svn/entries - Redirects (301) to https://youtube.com/.svn/entries , Subversion
Entries file may contain directory listing information.
+ /.svn/wc.db - Redirects (301) to https://youtube.com/.svn/wc.db , Subversion SQLite
DB file may contain directory listing information.
+ /.git/index - Redirects (301) to https://youtube.com/.git/index , Git Index file may
contain directory listing information.
+ /.hg/dirstate - Redirects (301) to https://youtube.com/.hg/dirstate , Mercurial
DirState file may contain directory listing information.
+ 26 items checked: 0 error(s) and 11 item(s) reported on remote host
+ End Time: 2026-02-13 16:20:32 (GMT0) (16 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

3. Crawled Website Endpoints

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

4. Vulnerabilities Detected

- Cross-Site Scripting (XSS)
- Insecure Cookies
- Information Disclosure

5. Vulnerability Intelligence (CVE Mapping)

Legacy Vulnerability Intelligence
- ■■ NOTICE: Our engine identified 2 additional legacy vulnerabilities (pre-2016).

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.

Attack: Data Leaks / Reconnaissance
Mitigation: Restrict access to sensitive directories (like .git or /admin) and disable directory listing.