Vulnerability Assessment Report: netflix.com

1. Network Scan Results (Nmap)

Port	Service	Version	State
80	http-proxy		open
443	http-proxy		open

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 54.246.79.9
+ Target Hostname: netflix.com
+ Target Port: 80
+ Start Time: 2026-02-12 12:42:21 (GMT0)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ Retrieved via header: 1.1 i-008f80f6423bb5d0f (eu-west-1)
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'x-netflix.proxy.execution-time' found, with contents: 3
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'x-xss-protection' found, with contents: 1; mode=block;
report=https://www.netflix.com/ichnaea/log/freeform/xssreport
+ Uncommon header 'x-originating-url' found, with contents: http://netflix.com/
+ Uncommon header 'x-netflix-cookieandmsl.profileguid.match' found, with contents: NA
+ Uncommon header 'x-netflix-headerandcookie.profileguid.match' found, with contents:
NA
+ Uncommon header 'x-netflix.nfstatus' found, with contents: 1_21
+ Uncommon header 'strict-transport-security' found, with contents: max-age=31536000;
includeSubDomains
+ Uncommon header 'x-netflix-headerandmsl.profileguid.match' found, with contents: NA
+ Cookie nfvdid created without the httponly flag
+ Root page / redirects to: https://netflix.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ lines
+ /crossdomain.xml contains 1 line which should be manually viewed for improper domains
or wildcards.
+ Uncommon header 'access-control-expose-headers' found, with contents: X-Netflix.Retry
.Server.Policy,X-Netflix.Response.Tag,X-Netflix.Geo.Info,X-Netflix.request.inbound.iden
tity.changed,Via,X-Netflix.Retry.Server.Policy.retryAfterSeconds,X-Netflix.Retry.Server
.Policy.maxRetries,X-Ftl-Error,X-Netflix.uiVersion,X-Netflix.Playapi.Backoff,X-Netflix-
TraceId,X-B3-TraceId
+ Uncommon header 'access-control-allow-credentials' found, with contents: true
+ Uncommon header 'access-control-allow-origin' found, with contents: *
+ Uncommon header 'accept-ch' found, with contents:
Sec-CH-UA-Model,Sec-CH-UA-Platform-Version
+ Uncommon header 'access-control-allow-headers' found, with contents: Authorization,Co
ntent-Type,Content-Encoding,Accept,X-Netflix.application.name,X-Netflix.application.ver
sion,X-Netflix.esn,X-Netflix.device.type,X-Netflix.certification.version,X-Netflix.requ
est.uuid,X-Netflix.originating.request.uuid,X-Netflix.user.id,X-Netflix.oauth.consumer.
key,X-Netflix.oauth.token,X-Netflix.ichnaea.request.type,X-Netflix.Request.Routing,X-NE
TFLIX-PREAPP-PARTNER-ID,X-NETFLIX-PREAPP-INTEGRITY-VALUE,X-Netflix.Request.Priority,X-N
etflix.Retry.Client.Policy,X-Netflix.Client.Request.Name,X-Netflix.Request.Retry.Policy
,X-Netflix.Request.Retry.Policy.Default,X-Netflix.request.client.user.guid,X-Netflix.Re
quest.NonJson.Headers,X-Netflix.esnPrefix,X-Netflix.browserName,X-Netflix.browserVersio
n,X-Netflix.osName,X-Netflix.osVersion,X-Netflix.uiVersion,X-Netflix.clientType,X-NETFL
IX-PERSONALIZATION-ID,X-NETFLIX-DET-TOKEN,x-netflix.context.locales,x-netflix.context.u
i-flavor,x-netflix.context.app-version,x-netflix.context.schema-variant,X-Netflix.osFul
lName,X-Netflix.playerThroughput,X-Netflix.playerThroughputNiqr,x-netflix.request.inbou
```

```
nd.identity.changed,X-Netflix.Request.toplevel.uuid,x-netflix.context.is-inapp-browser,
f9hi42t,6kw0ty,83fl5s0,j39egs,i1ht0d,d12e19,x-session,x-netflix.context.operation-name,
X-Netflix-CGL,x-netflix.context.ale.token,x-netflix.request.attempt,x-netflix.request.c
lient.context,X-Netflix.Request.Originating.Url,X-Netflix.Request.Id,x-netflix.request.
clcs.bucket,x-netflix.context.form-factor,x-netflix.request.growth.session.id,x-netflix
.context.hawkins-version,x-netflix.context.feature-capabilities,X-NETFLIX-DET-PARTNER-P
AI,X-NETFLIX-RESPONSE-OVERRIDDEN,X-NETFLIX-DET-DEPRECATION,X-Netflix.context.locales,X-
Netflix.context.ui-flavor,X-Netflix.context.ale.token,X-Netflix.context.app-version,X-N
etflix.context.schema-variant,X-Netflix.Request.Attempt,X-Netflix.Request.Client.Contex
t,B3
+ Uncommon header 'access-control-allow-methods' found, with contents: GET, HEAD, POST,
PUT, DELETE, TRACE, OPTIONS, SCRIPT
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS, SCRIPT
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save
files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files
on the web server.
+ /cfappman/index.cfm - Redirects (301) to https://netflix.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://netflix.com/cfdocs/examples/cvbeans/beaninfo.cfm , susceptible to our ODBC
exploit; see RFP9901 http://www.wiretrip.ne
```

3. Crawled Website Endpoints

- https://www.netflix.com/youraccount
- https://www.netflix.com/in/login
- https://www.netflix.com/in/
- https://www.netflix.com/watch
- https://www.netflix.com/in/browse/genre/839338

4. Vulnerabilities Detected

- Information Disclosure
- Insecure Cookies
- Cross-Site Scripting (XSS)
- Missing Security Headers

5. Vulnerability Intelligence (CVE Mapping)

Vulnerabilities in http-proxy

- [LOW 2.6] CVE-2012-2632: SEIL routers with firmware SEIL/x86 1.00 through 2.35, SEIL/X1 2.30 through 3.75, SEIL/X2 2.30 through 3.75, and SEIL/B1 2.30 through 3.75, when the h...
- [HIGH 7.5] CVE-2017-16014: Http-proxy is a proxying library. Because of the way errors are handled in versions before 0.7.0, an attacker that forces an error can crash the serve...
- [HIGH 7.5] CVE-2017-16075: http-proxy.js was a malicious module published with the intent to hijack environment variables. It has been unpublished by npm....
- [CRITICAL 9.8] CVE-2019-10196: A flaw was found in http-proxy-agent, prior to version 2.1.0. It was discovered http-proxy-agent passes an auth option to the Buffer constructor witho...
- [HIGH 7.5] CVE-2024-21536: Versions of the package http-proxy-middleware before 2.0.7, from 3.0.0 and before 3.0.3 are vulnerable to Denial of Service (DoS) due to an UnhandledP...

6. Attack Possibilities & Mitigation

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

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

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

Attack: Clickjacking / Cross-Site Scripting (XSS)
Mitigation: Implement X-Frame-Options and Content-Security-Policy headers.