

Major-1 Project

MAJOR PROJECT DOCUMENTATION

Bug Bounty Reconnaissance – Netflix

Student Name: Muskan Kumari

ERP : 6606646

Project Type: Major Project (Cybersecurity)

Domain: Bug Bounty Reconnaissance

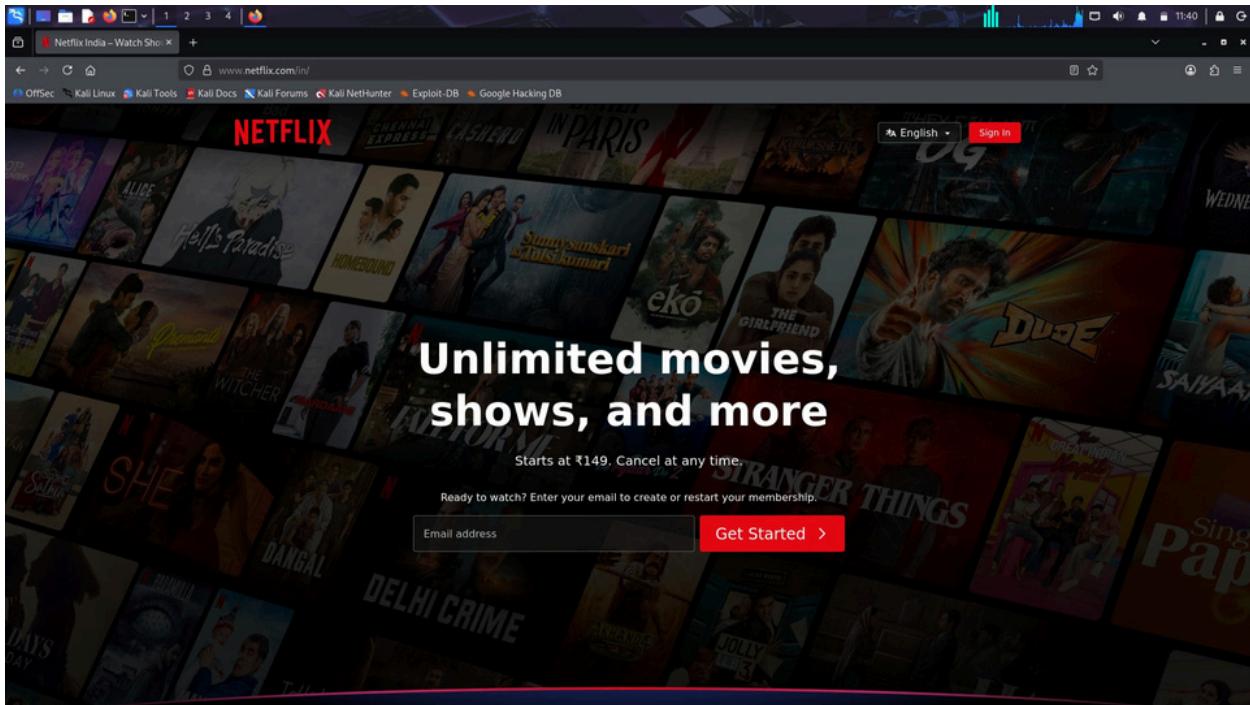
1. Main Domain Identification

Company Name: Netflix

Main Domain: netflix.com

Method Used:

The official Netflix website was identified using a Google search and verified through Netflix's homepage, legal pages, and contact information.



2. Bug Bounty / Vulnerability Disclosure Page

Netflix maintains an official Vulnerability Disclosure / Bug Bounty Program hosted on **HackerOne**.

Search Keywords Used:

- Netflix bug bounty
- Netflix vulnerability disclosure

A screenshot of a web browser showing the Netflix Bug Bounty Program page on HackerOne. The page includes sections for "Program highlights", "Rewards", and "Safe harbor". It highlights that the program is a "Gold Standard" and has a response efficiency of 98%. The "Rewards" section shows a range from \$100-\$600 for low-severity bugs.

We believe that responsible security research and disclosure help us continually improve how we keep our members, partners, and employees secure. Please report potential security vulnerabilities to us via our [HackerOne bug bounty program](#).

If you are a Netflix member and have questions concerning fraud or malware, please see the following support pages:

- Account fraud or unauthorized charges: [Unrecognized or unauthorized charges from Netflix](#)
- Potential malware or computer viruses: [I'm getting ads or pop-ups while watching Netflix on my computer.](#)

If you are a customer seeking information on your account, billing, or site content, please reach out to [customer support via phone or live chat](#).

Security Researcher Hall of Fame

Netflix would like to thank the following researchers for participating in our responsible disclosure program.

Participating security researchers

For a full and up-to-date list of contributing security researchers, please see the [HackerOne Netflix Hall of Fame page](#).

Was this article helpful? [Yes](#) [No](#)

[Need more help?](#) [Contact Us](#)

3. Bug Bounty Scope (In-Scope & Out-of-Scope)

In-Scope Assets (as defined by Netflix):

- netflix.com
- Netflix-owned subdomains
- Netflix web applications and services

Out-of-Scope Assets:

- Third-party hosted services
- Social media platforms
- Customer-controlled environments

Asset Name	Type	Coverage	Max. Severity	Bounty	Last update
www.netflix.com	Domain	In scope	Critical	Eligible	Jan 11, 2024

Asset Name	Type	Coverage	Max. Severity	Bounty	Last update
Third-party websites or systems hosted by non-Netflix entities	Other	Out of scope	None	Ineligible	Jan 12, 2024
Set-top-boxes, smart TVs, streaming sticks	Other	Out of scope	None	Ineligible	Jan 12, 2024

4. Ping Test (ICMP Reachability)

Objective:

To check whether the Netflix main domain responds to ICMP requests.

Command Used:

```
ping netflix.com
```

Observation:

ICMP responses may be blocked or rate-limited as part of Netflix's security infrastructure.

```
(kali㉿kali)-[~]
  $ ping netflix.com
PING netflix.com (52.214.181.141) 56(84) bytes of data.
"C
--- netflix.com ping statistics ---
155 packets transmitted, 0 received, 100% packet loss, time 157832ms

(kali㉿kali)-[~]
```

5. Technology Stack Identification (Main Domain)

Tool Used:

Wappalyzer (Browser Extension)

Technologies Identified May Include:

- Web server
- CDN (Netflix Open Connect / Cloud-based CDN)
- JavaScript frameworks
- Analytics and security tools

📸 Screenshot:

➡ Wappalyzer results for <https://www.netflix.com>

6. ASN Number and IP Range Identification

Objective:

To identify the ASN and network ownership related to Netflix's infrastructure.

Commands Used:

```
dig netflix.com
whois <IP_ADDRESS>
```

Information Collected:

- ASN Number
- Organization / ISP
- Netblocks

```

OrgName: Amazon Technologies Inc.
OrgId: AT-88-Z
Address: 410 Terry Ave N.
City: Seattle
StateProv: WA
PostalCode: 98109
Country: US
RegDate: 2011-12-08
Updated: 2024-01-24
Comment: All abuse reports MUST include:
Comment: + dest IP (your IP)
Comment: + dest port
Comment: + timestamp/datetime and timezone of activity
Comment: + Intensity/frequency (short log extracts)
Comment: + Your contact details (phone and email) Without these we will be unable to identify the correct owner of the IP address at that point in time.
Ref: https://rdap.arin.net/registry/entity/AT-88-Z

OrgAbuseHandle: AEAB-ARIN
OrgAbuseName: AWS RPKI Abuse
OrgAbusePhone: +1-206-555-0000
OrgAbuseEmail: trustandsafety@amazon.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/AEAB-ARIN

OrgRoutingHandle: ARNP-ARIN
OrgRoutingName: AWS RPKI Management POC
OrgRoutingPhone: +1-206-555-0000
OrgRoutingEmail: aws-rpki-routing-poc@amazon.com
OrgRoutingRef: https://rdap.arin.net/registry/entity/ARNP-ARIN

OrgRoutingHandle: IPROU3-ARIN
OrgRoutingName: IP Routing
OrgRoutingPhone: +1-206-555-0000
OrgRoutingEmail: aws-routing-poc@amazon.com
OrgRoutingRef: https://rdap.arin.net/registry/entity/IPROU3-ARIN

OrgNOCHandle: AN01-ARIN
OrgNOCName: Amazon AWS Network Operations
OrgNOCPhone: +1-206-555-0000
OrgNOCEmail: amzn-noc-contact@amazon.com
OrgNOCREf: https://rdap.arin.net/registry/entity/AN01-ARIN

OrgTechHandle: AN024-ARIN
OrgTechName: Amazon AWS Network Operations
OrgTechPhone: +1-206-555-0000
OrgTechEmail: amzn-noc-contact@amazon.com
OrgTechRef: https://rdap.arin.net/registry/entity/AN024-ARIN

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#

```

7. Subdomain Enumeration

Objective:

To discover publicly accessible Netflix subdomains.

Tool Used: amass

Command:

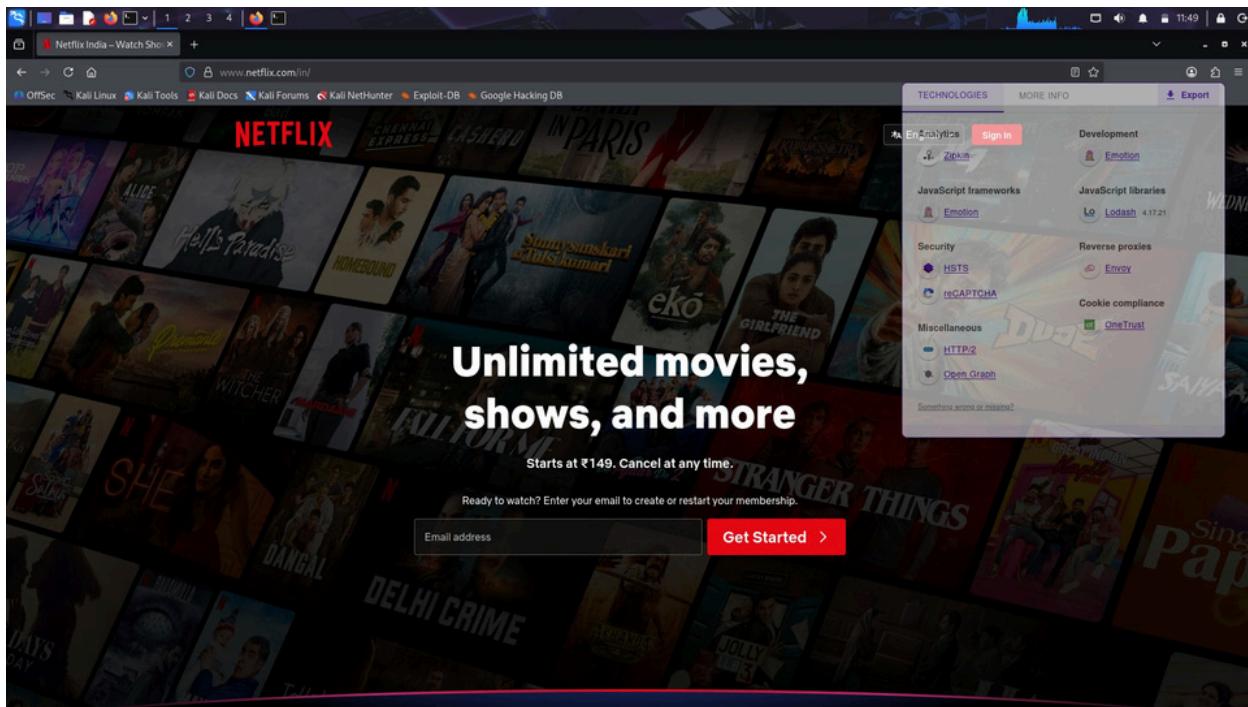
```
amass enum -passive -d netflix.com
```

8. Technology Stack on Subdomains

Selected Subdomains:

- help.netflix.com
- jobs.netflix.com
- media.netflix.com
- partner.netflix.com
- www.netflix.com

Each subdomain was analyzed using Wappalyzer to compare technology stacks.



9. Hidden Files & Directories (Main Domain Only)

⚠ Only the main domain was scanned (no subdomains)

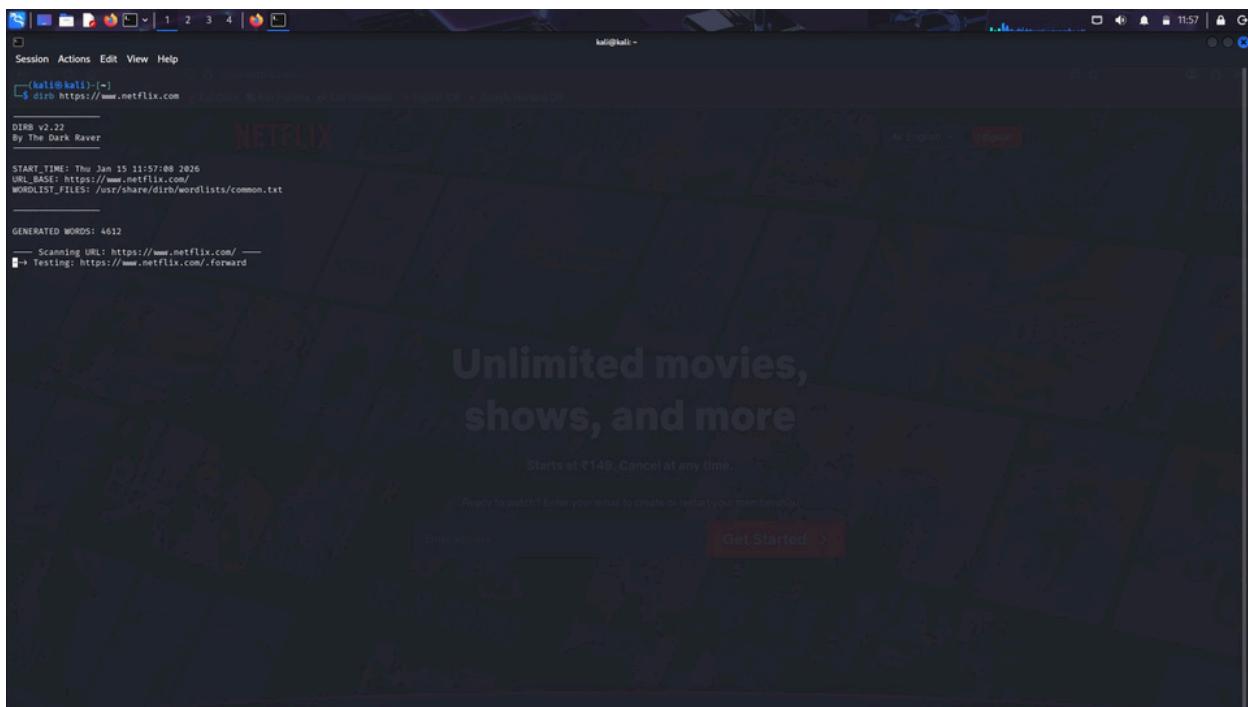
Tool Used: dirb

Command:

```
dirb https://www.netflix.com
```

Observation:

Minimal or no directory exposure was observed, indicating strong security practices.



10. Declaration

I hereby declare that this project was carried out strictly for **educational purposes** and involved **reconnaissance-only activities**.

No exploitation, vulnerability abuse, or unauthorized access was performed, in full compliance with Netflix's bug bounty policy and academic guidelines.

Project Outcome:

This project demonstrates a structured and ethical approach to bug bounty reconnaissance aligned with real-world security practices.