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

---

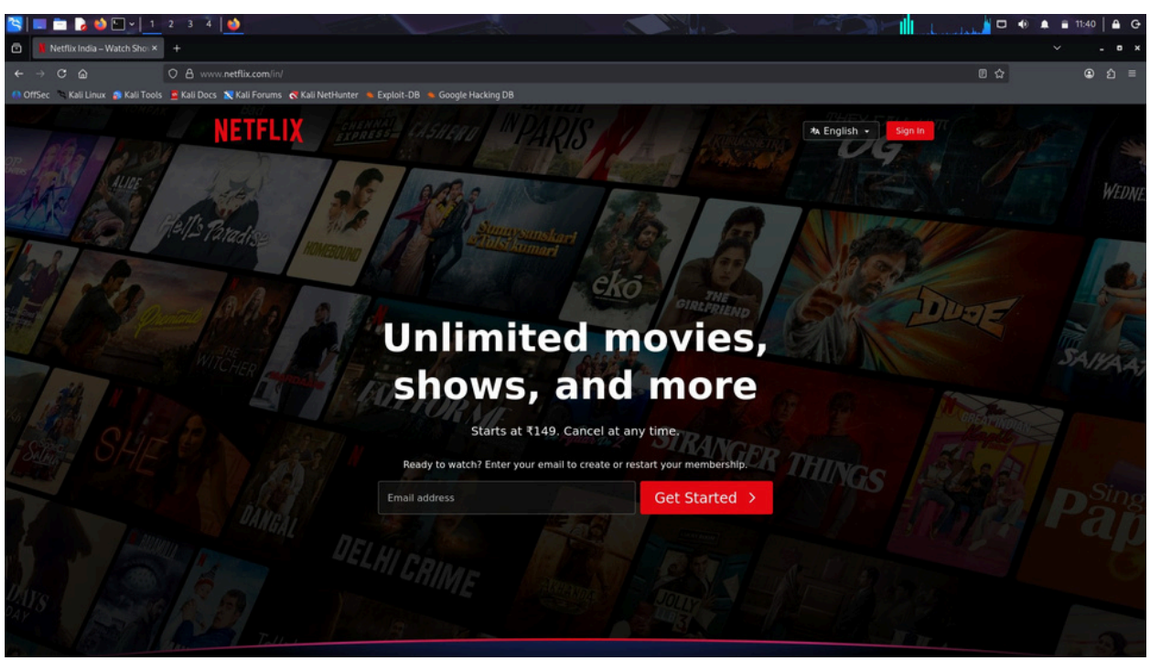
1. Main Domain Identification

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.



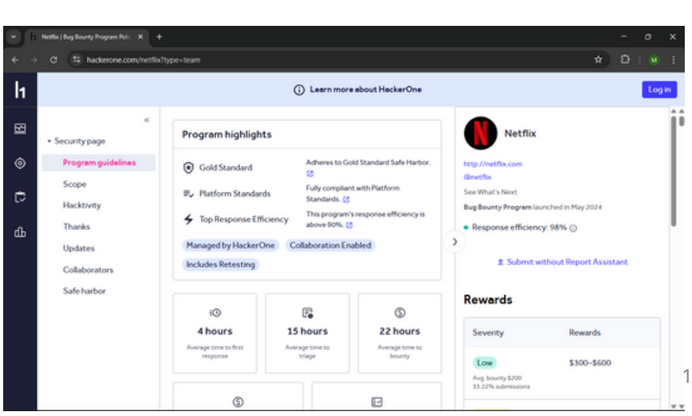
---

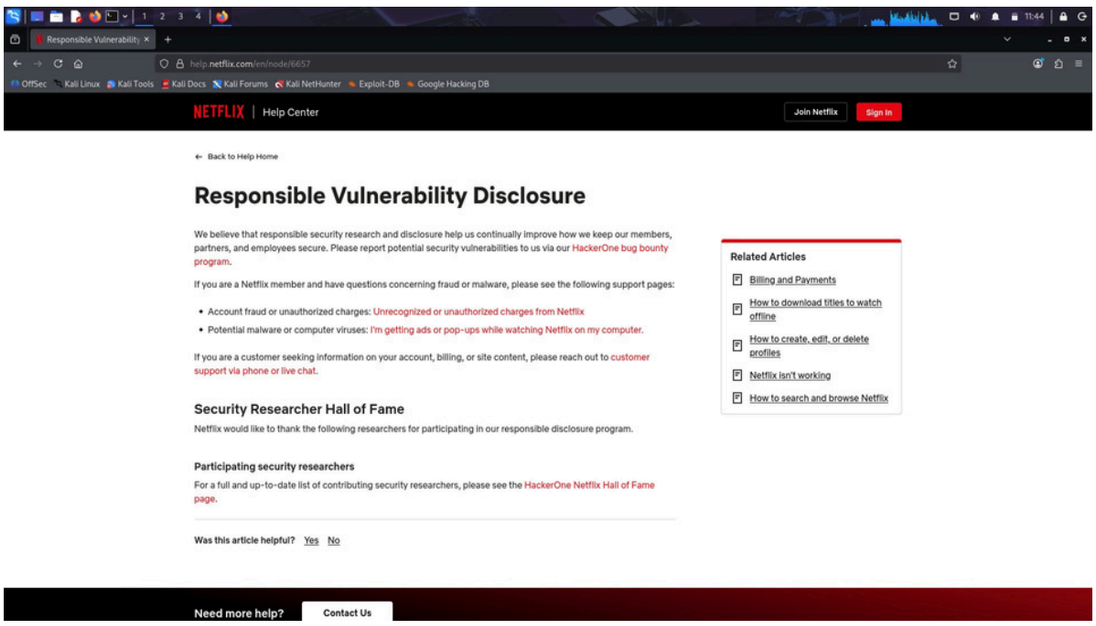
2. Bug Bounty / Vulnerability Disclosure Page

NetflixmaintainsanofficialVulnerabilityDisclosure / BugBountyProgram hosted on **HackerOne**.

Search Keywords Used:

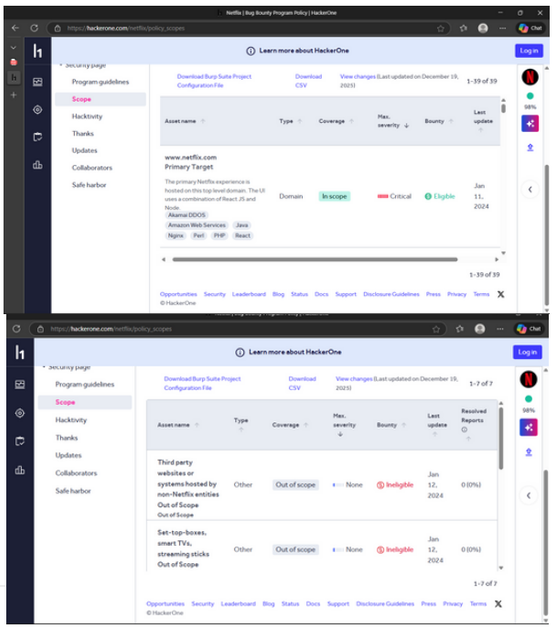
- Netflix bug bounty
- Netflix vulnerability disclosure





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

4. Ping Test (ICMP Reachability)

Objective:

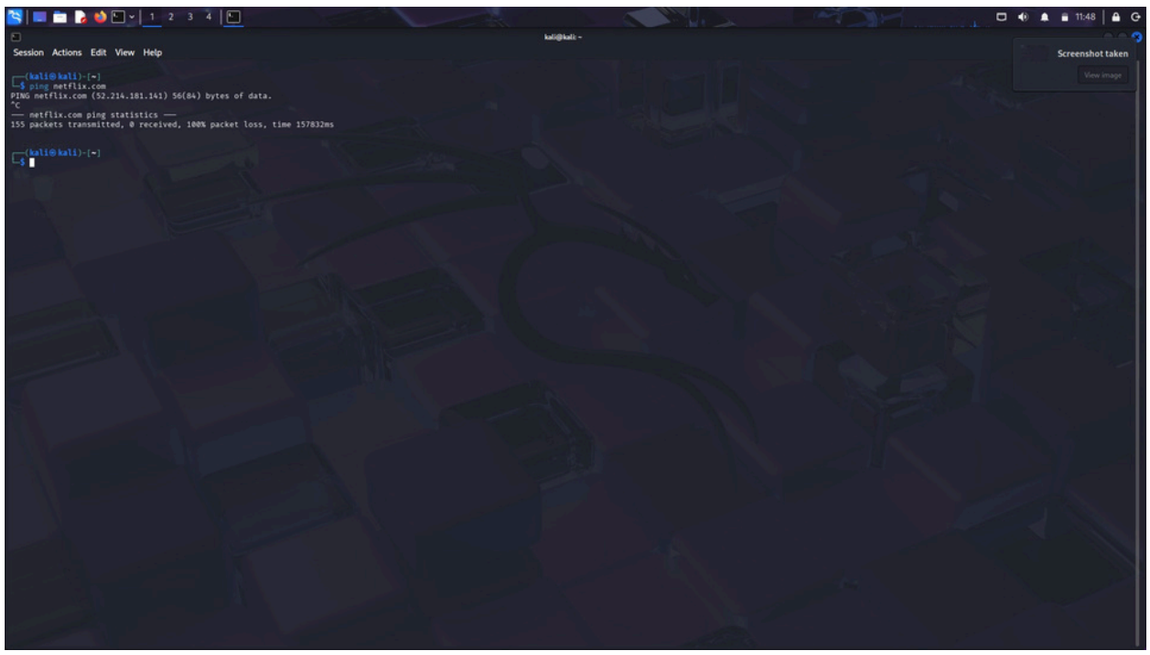
To check whether the Netflix main domain responds to ICMP requests.

Command Used:

```
ping netflix.com
```

Obser vation:

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



---

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:

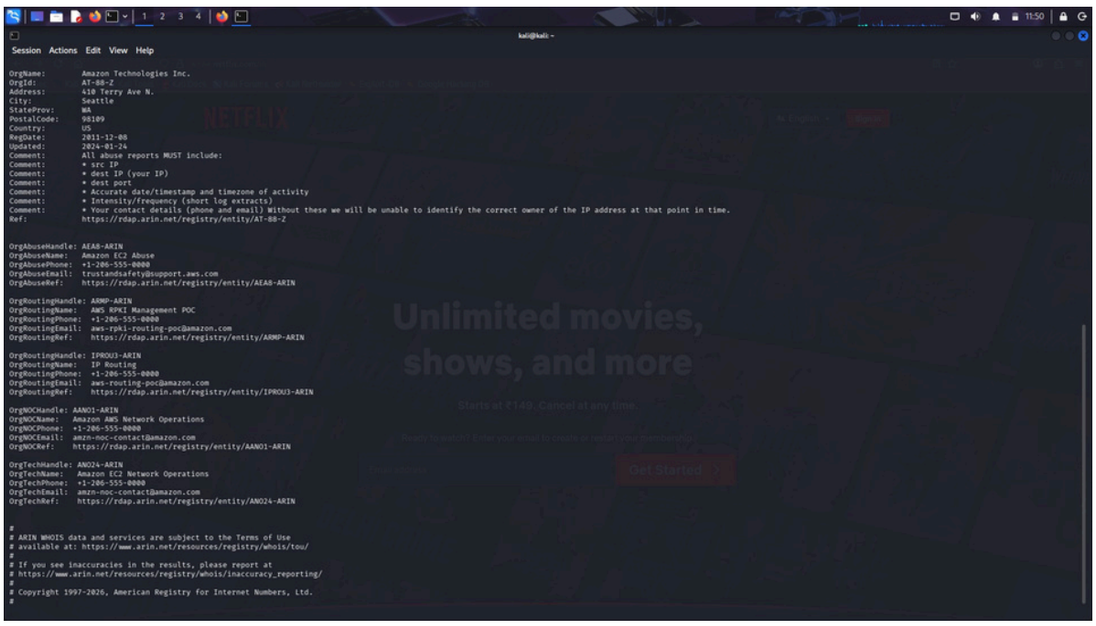
To identify the ASN and network ownership related to Netflix’s infrastructure.

Commands Used:

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

Information Collected:

- ASN Number
- Organization / ISP
- Netblocks



7. Subdomain Enumeration

Objective:

To discover publicly accessible Netflix subdomains.

Tool Used: amass

Command:

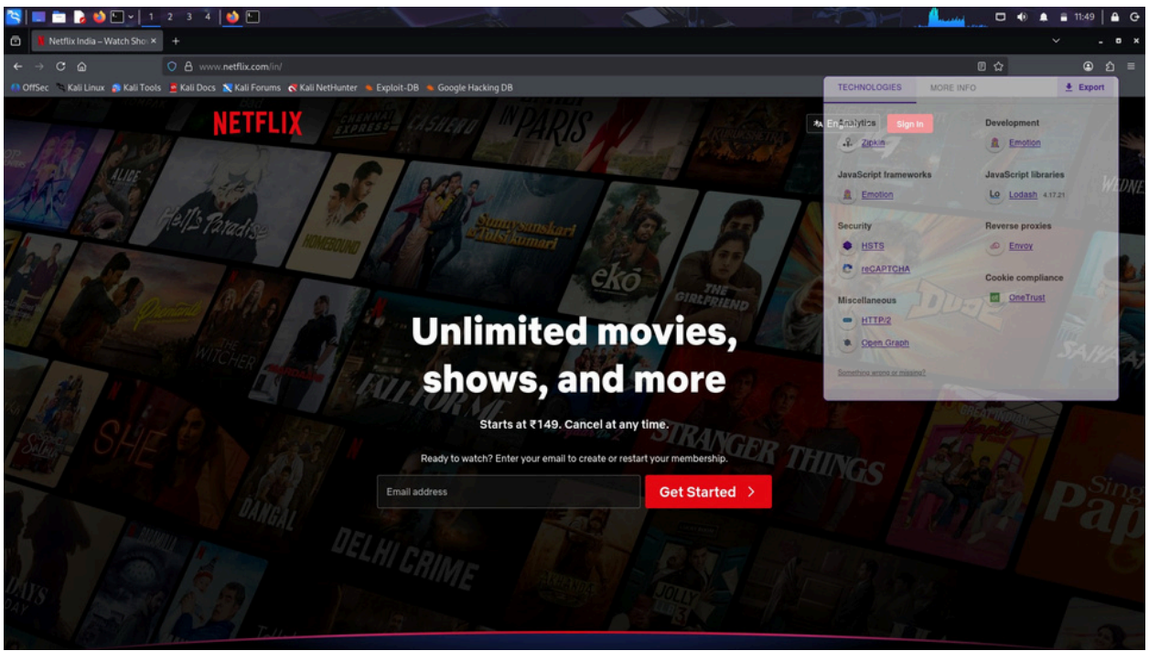
```
amass enum -passive -d netflix.com
```

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)

⚠Onlythe maindomainwasscanned(nosubdomains)

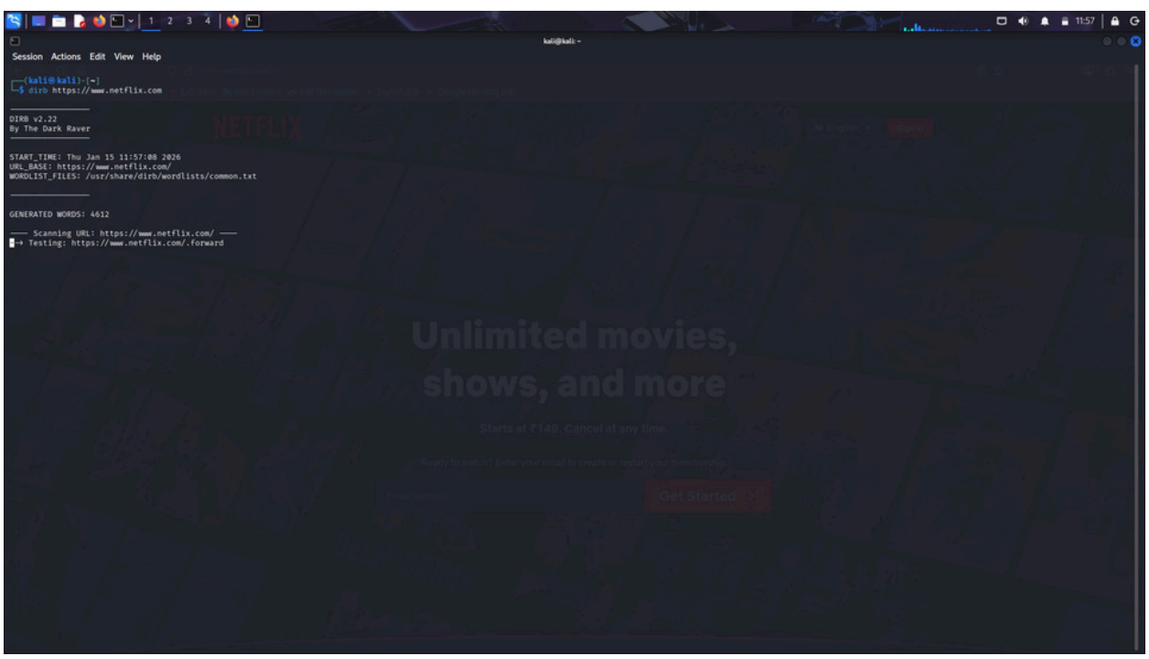
Tool Used: dirb

Command:

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

Obser vation:

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



10. Declaration

Iherebydeclarethatthis 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.