Major Project

Bug Bounty Reconnaissance Assignment :

(Shivam Sahu)

Target Company : X (twitter)

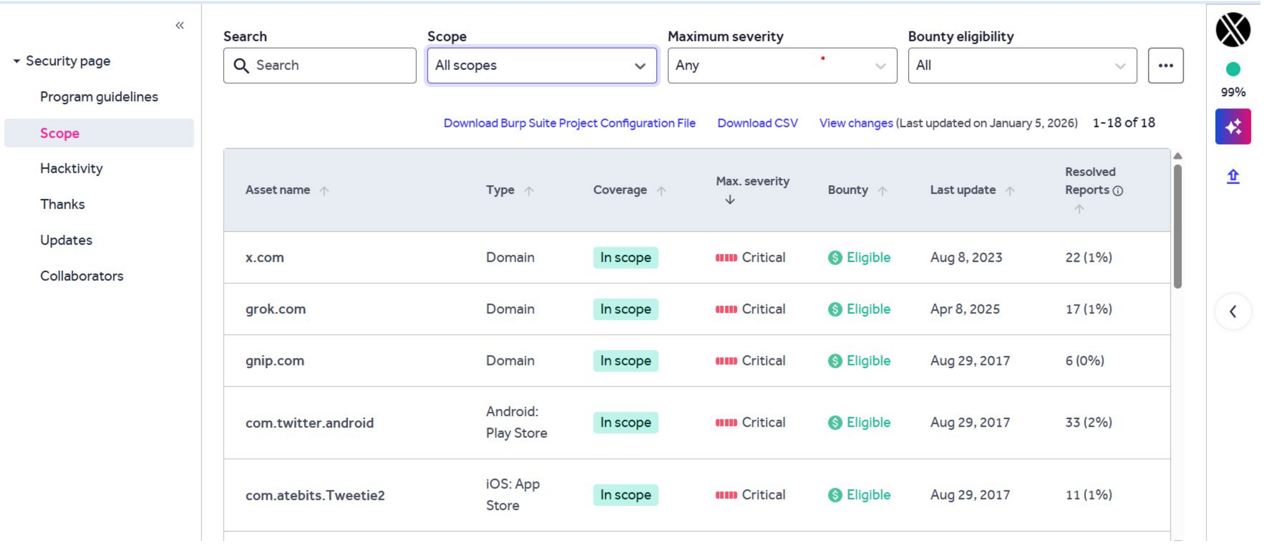
➢ Identify the Company’s Main Domain :

The official main domain of **X (formerly Twitter)** is **x.com .**

The old domain twitter.com is still active but now redirects to x.com .

➢ Locate the Bug Bounty / Vulnerability Disclosure Program :

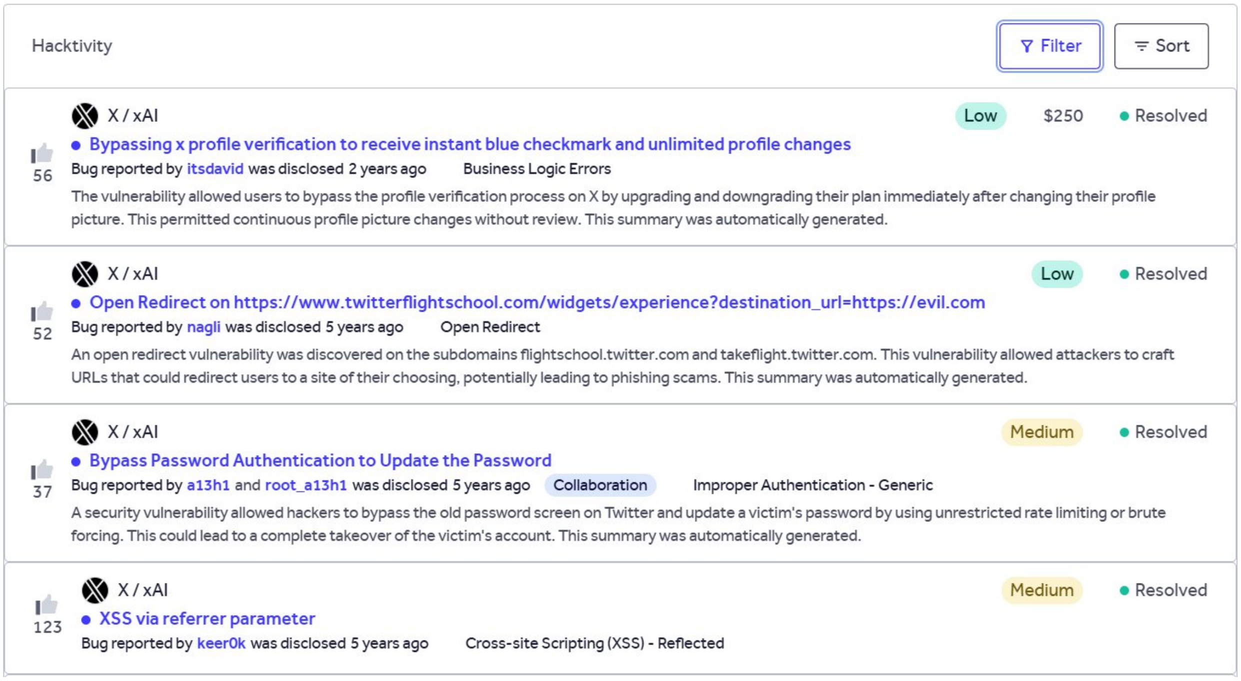
Link of the page : https://hackerone.com/x



Search: Search
Scope: All scopes
Maximum severity: Any
Bounty eligibility: All

Download Burp Suite Project Configuration File   Download CSV   View changes (Last updated on January 5, 2026)   1-18 of 18

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
x.com	Domain	In scope	Critical	Eligible	Aug 8, 2023	22 (1%)
grok.com	Domain	In scope	Critical	Eligible	Apr 8, 2025	17 (1%)
gnip.com	Domain	In scope	Critical	Eligible	Aug 29, 2017	6 (0%)
com.twitter.android	Android: Play Store	In scope	Critical	Eligible	Aug 29, 2017	33 (2%)
com.atebits.Tweetie2	iOS: App Store	In scope	Critical	Eligible	Aug 29, 2017	11 (1%)



Hacktivity

56 X / xAI Low $250 ● Resolved

● Bypassing x profile verification to receive instant blue checkmark and unlimited profile changes

Bug reported by itsdavid was disclosed 2 years ago Business Logic Errors

The vulnerability allowed users to bypass the profile verification process on X by upgrading and downgrading their plan immediately after changing their profile picture. This permitted continuous profile picture changes without review. This summary was automatically generated.

52 X / xAI Low ● Resolved

● Open Redirect on https://www.twitterflightschool.com/widgets/experience?destination_url=https://evil.com

Bug reported by nagli was disclosed 5 years ago Open Redirect

An open redirect vulnerability was discovered on the subdomains flightschool.twitter.com and takeflight.twitter.com. This vulnerability allowed attackers to craft URLs that could redirect users to a site of their choosing, potentially leading to phishing scams. This summary was automatically generated.

37 X / xAI Medium ● Resolved

● Bypass Password Authentication to Update the Password

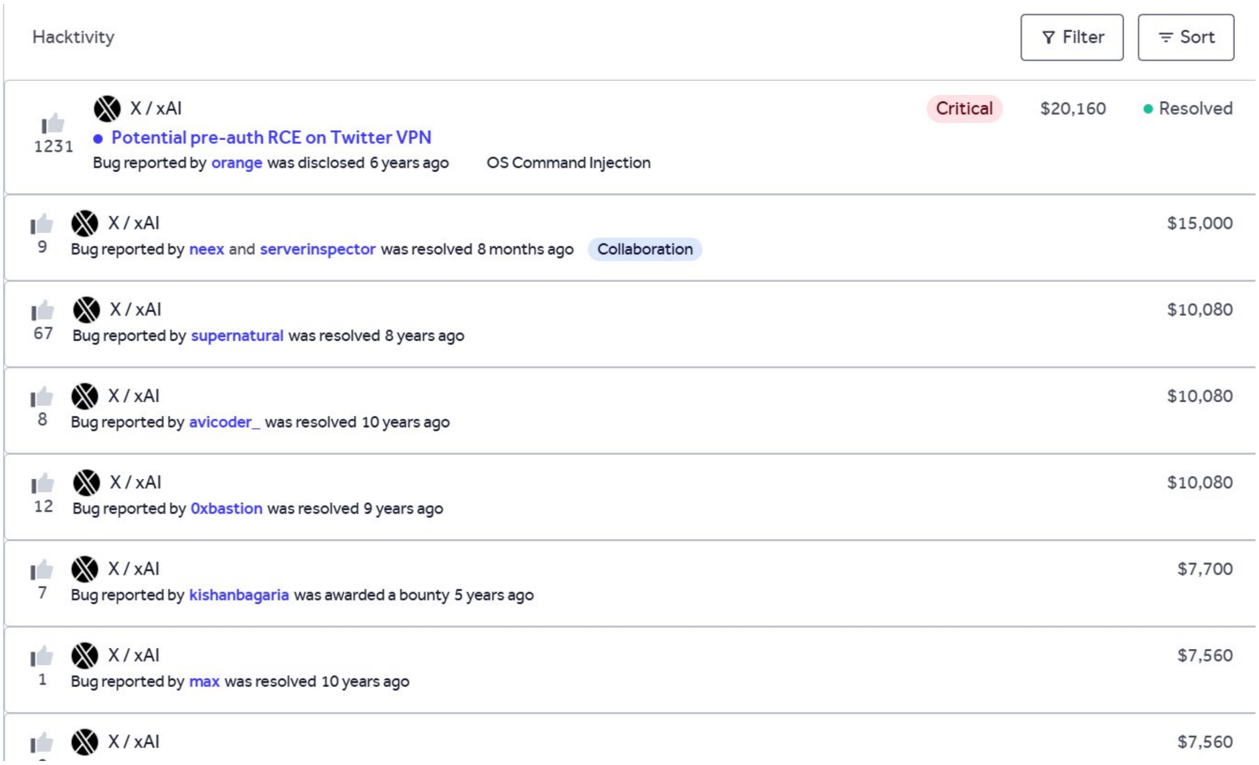
Bug reported by a13h1 and root_a13h1 was disclosed 5 years ago Collaboration Improper Authentication - Generic

A security vulnerability allowed hackers to bypass the old password screen on Twitter and update a victim's password by using unrestricted rate limiting or brute forcing. This could lead to a complete takeover of the victim's account. This summary was automatically generated.

123 X / xAI Medium ● Resolved

● XSS via referrer parameter

Bug reported by keer0k was disclosed 5 years ago Cross-site Scripting (XSS) - Reflected



Hacktivity

1231 X / xAI Critical $20,160 ● Resolved

● Potential pre-auth RCE on Twitter VPN

Bug reported by orange was disclosed 6 years ago OS Command Injection

9 X / xAI $15,000

Bug reported by neex and serverinspector was resolved 8 months ago Collaboration

67 X / xAI $10,080

Bug reported by supernatural was resolved 8 years ago

8 X / xAI $10,080

Bug reported by avicoder_ was resolved 10 years ago

12 X / xAI $10,080

Bug reported by 0xbastion was resolved 9 years ago

7 X / xAI $7,700

Bug reported by kishanbagaria was awarded a bounty 5 years ago

1 X / xAI $7,560

Bug reported by max was resolved 10 years ago

X / xAI $7,560

List of vulnerabilities reported on Hackerone for X (twitter) by security Experts under Bug Bounty / Vulnerability Disclosure Program.

➢ Identify Bug Bounty Scope (In-Scope & Out-of Scope)

♦ In-scope :-

Based on the Rules of Engagement and Report Eligibility defined on X’s HackerOne program, the following are considered in scope:

- Security vulnerabilities affecting assets owned and operated by X
- Issues that demonstrate a clear and verifiable security impact on X’s websites or applications
- Vulnerabilities discovered using test accounts without violating user privacy
- Issues that do not negatively impact X users (e.g., no spam, no denial of service)
- Vulnerabilities that comply with X’s disclosure and reporting guidelines
- Reports submitted manually after proper verification

Note:
X does not provide a fixed list of in-scope assets. Scope is determined by eligibility rules and engagement guidelines published on the HackerOne program page.

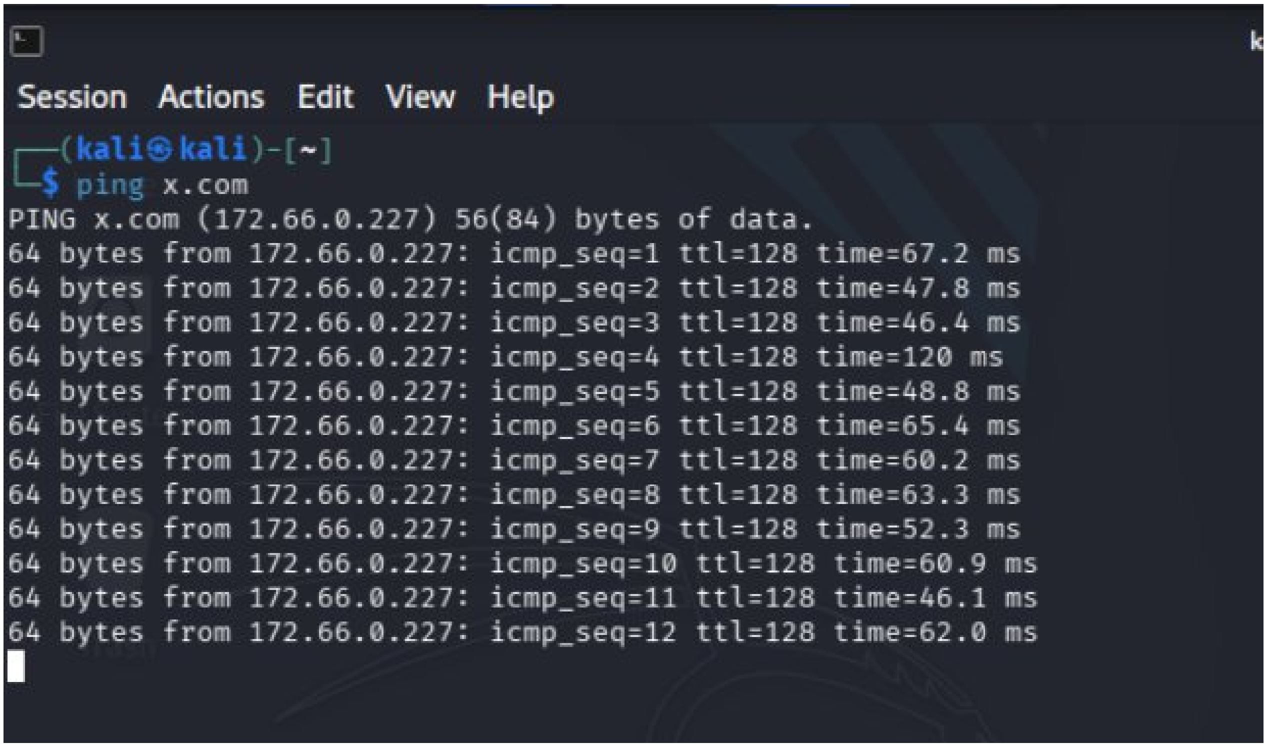
♦ Out-of-Scope / Ineligible Issues :-

The following issues are outside the scope of X’s vulnerability rewards program:

- Attacks requiring physical access to a user's device
- Physical attacks against X property or data centers

- Forms missing CSRF tokens without proven exploitability
- Logout CSRF
- Password and account recovery policy issues
- Invalid or missing SPF records
- Content spoofing or text injection
- Issues related to software or protocols not under X’s control
- Spam reports
- Bypass of URL malware detection
- Vulnerabilities affecting only outdated or unpatched browsers or platforms
- Social engineering of X staff or contractors
- Issues without clear security impact (e.g., clickjacking on static pages, missing headers)
- Denial of Service (DoS/DDoS) attacks
- Cache poisoning affecting service availability
- Broken hyperlinks without security impact
- Client-side feature unlocking on modified, rooted, or jailbroken devices
- Open redirects without significant security risk
- Manipulation of likes/follows/views due to caching behavior
- Homoglyph URL attacks without broader platform impact
- Rate-limit bypass reports on Grok or xAI APIs

➢ Ping the Main Domain :-



```
┌──(kali㉿kali)-[~]
└─$ ping x.com
PING x.com (172.66.0.227) 56(84) bytes of data.
64 bytes from 172.66.0.227: icmp_seq=1 ttl=128 time=67.2 ms
64 bytes from 172.66.0.227: icmp_seq=2 ttl=128 time=47.8 ms
64 bytes from 172.66.0.227: icmp_seq=3 ttl=128 time=46.4 ms
64 bytes from 172.66.0.227: icmp_seq=4 ttl=128 time=120 ms
64 bytes from 172.66.0.227: icmp_seq=5 ttl=128 time=48.8 ms
64 bytes from 172.66.0.227: icmp_seq=6 ttl=128 time=65.4 ms
64 bytes from 172.66.0.227: icmp_seq=7 ttl=128 time=60.2 ms
64 bytes from 172.66.0.227: icmp_seq=8 ttl=128 time=63.3 ms
64 bytes from 172.66.0.227: icmp_seq=9 ttl=128 time=52.3 ms
64 bytes from 172.66.0.227: icmp_seq=10 ttl=128 time=60.9 ms
64 bytes from 172.66.0.227: icmp_seq=11 ttl=128 time=46.1 ms
64 bytes from 172.66.0.227: icmp_seq=12 ttl=128 time=62.0 ms
```

Returned IP Address : 172.66.0.227

➢ Technology Stack Identification (Main Domain) :-

Tool used: Wappalyzer (Browser Extension)

Target: Main Domain homepage

Detected Technologies

Frontend / JavaScript Framework

- React – Used for building the user interface of the website.

Web Framework (Backend)

- Express – Node.js web framework used for server-side routing and APIs.

UI Framework

- Tailwind CSS

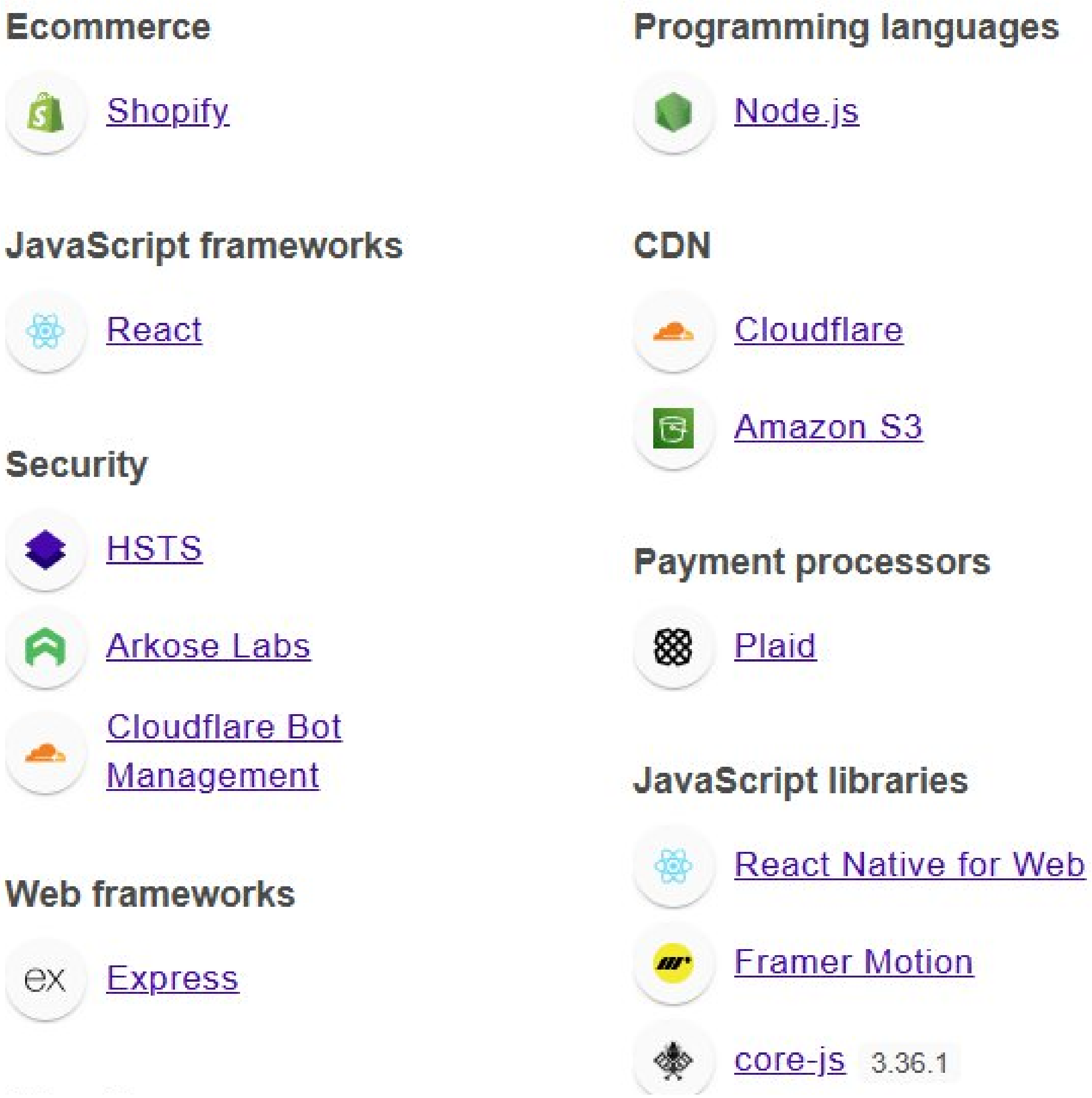
Programming language

- Node.js

Content Delivery & Hosting

- Cloudflare
- Amazon S3

Note: No analytics tools , CMS were detected on the main domain using Wappalyzer during passive reconnaissance.



Ecommerce

Shopify

JavaScript frameworks

React

Security

HSTS

Arkose Labs

Cloudflare Bot Management

Web frameworks

Express

Programming languages

Node.js

CDN

Cloudflare

Amazon S3

Payment processors

Plaid

JavaScript libraries

React Native for Web

Framer Motion

core-js 3.36.1

Miscellaneous

- Plaid
- PWA
- Open Graph

Web servers

- Express

Caching

- Varnish

PaaS

- Amazon Web Services

Reverse proxies

- Envoy

UI frameworks

- Tailwind CSS

Authentication

- Google Sign-in
- Apple Sign-in

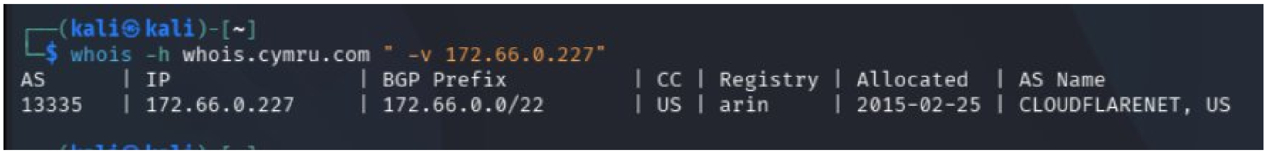
➢ ASN Number and Organization IP Ranges :-

ASN(Autonomous System Number): AS13335

Organization Name: Cloudflare,Inc.(CLOUDFLARENET)

IP Ranges (Netblocks) : 172.66.0.0/22

Commands used : whois -h whois.cymru.com " -v 172.66.0.27"



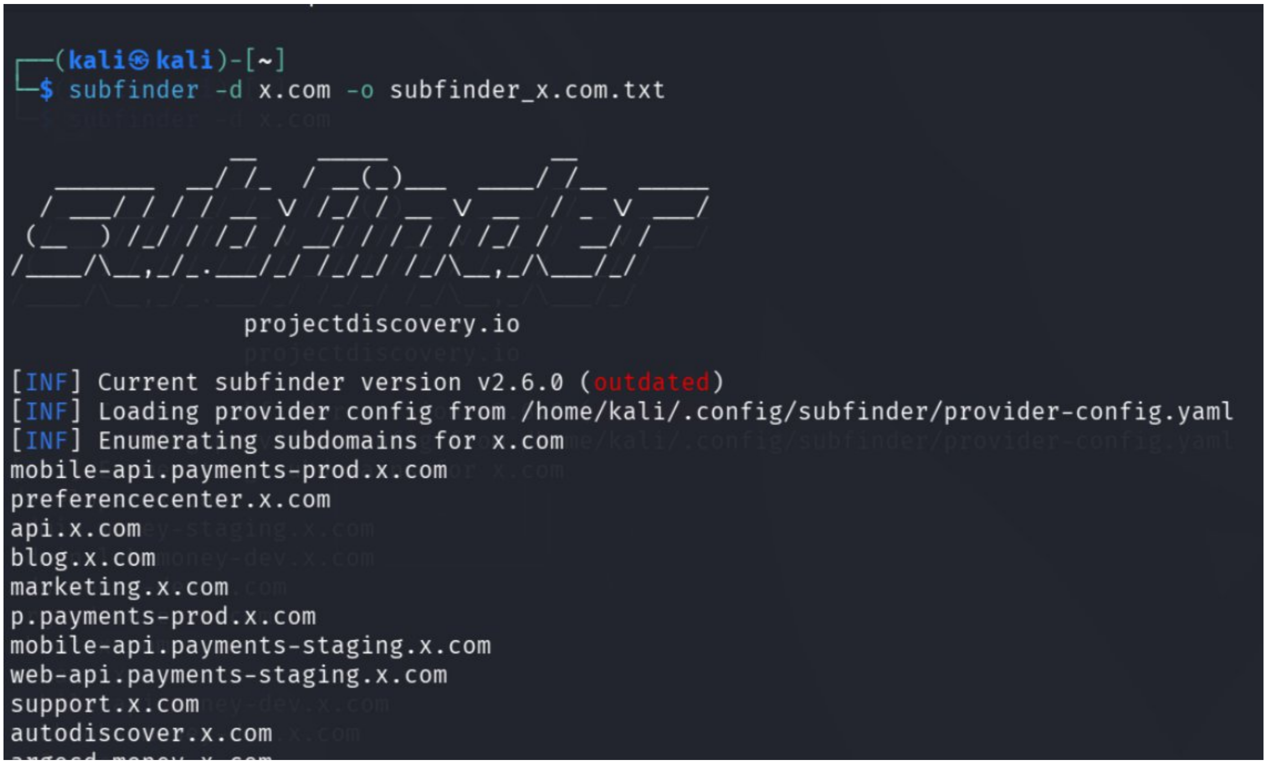
```
┌──(kali㉿kali)-[~]
└─$ whois -h whois.cymru.com " -v 172.66.0.227"
AS      | IP               | BGP Prefix          | CC | Registry | Allocated  | AS Name
13335   | 172.66.0.227     | 172.66.0.0/22       | US | arin     | 2015-02-25 | CLOUDFLARENET, US
```

Observation :-

The identified IP range belongs to Cloudflare, Inc. and represents Cloudflare’s CDN infrastructure. The actual backend IP range of the target organization is hidden due to Cloudflare protection.

➢ Subdomain Enumeration :-

Command executed : subfinder –d x.com



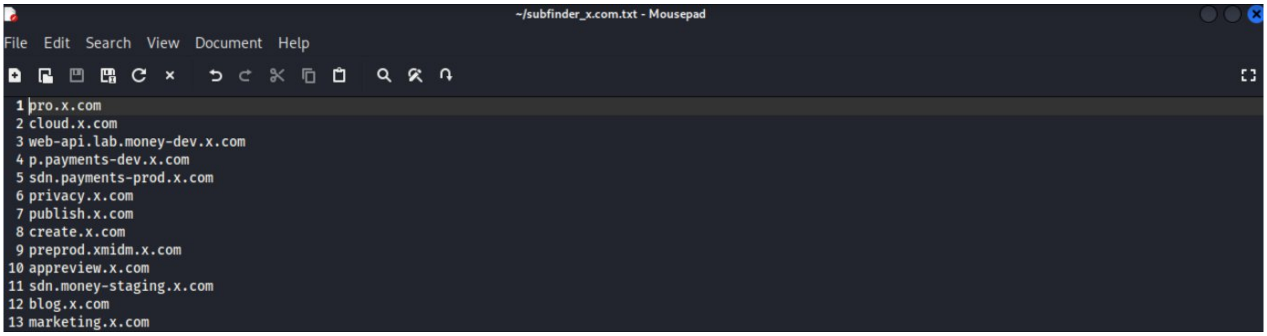
```
┌──(kali㉿kali)-[~]
└─$ subfinder -d x.com -o subfinder_x.com.txt

               __    _____           __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for x.com
mobile-api.payments-prod.x.com
preferencecenter.x.com
api.x.com
blog.x.com
marketing.x.com
p.payments-prod.x.com
mobile-api.payments-staging.x.com
web-api.payments-staging.x.com
support.x.com
autodiscover.x.com
```

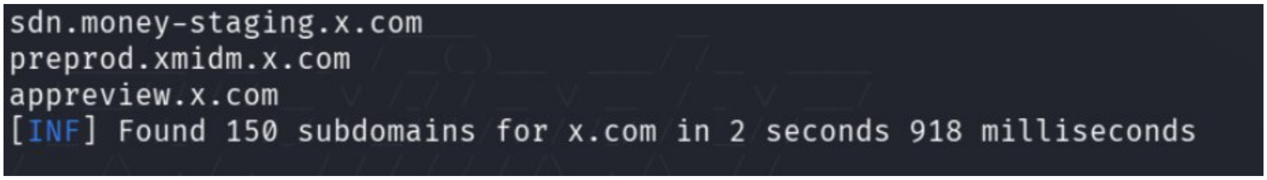
(Saved the output in a .txt file as subfinder_x.com.txt)



~/subfinder_x.com.txt - Mousepad
File Edit Search View Document Help

```
pro.x.com
cloud.x.com
web-api.lab.money-dev.x.com
p.payments-dev.x.com
sdn.payments-prod.x.com
privacy.x.com
publish.x.com
create.x.com
preprod.xmidm.x.com
appreview.x.com
sdn.money-staging.x.com
blog.x.com
marketing.x.com
```

Total number of subdomains found is 150.



```
sdn.money-staging.x.com
preprod.xmidm.x.com
appreview.x.com
[INF] Found 150 subdomains for x.com in 2 seconds 918 milliseconds
```

➢Technology Stack on Subdomains :-

Technologies	Programming Languages	CDN	Java Script Libaries	Security
blog.x.com	Java	Cloudflare	core-js	Cloudfl Bot Management ,HSTS, Arkose Labs
developer.x.com	Java	Cloudflare	LazySizes , core-js	Cloudfl Bot Management ,HSTS, Arkose Labs
career.x.com		Cloudflare	Framer Motion	Cloudfl Bot Management , HSTS
shop.x.com		Cloudflare	core-js	Cloudfl Bot Management , HSTS
help.x.com	Java	Cloudflare	Swiper, LazySizes , core-js	Cloudfl Bot Management ,HSTS, Arkose Labs

➢ Hidden Files & Directories on Main Domain:-

Tool Used :

Dirb v2.22

Command Executed :

dirb –d https://x.com/ –o dirb_x.com.txt

Wordlist Used :

/usr/share/dirb/wordlists/common.txt

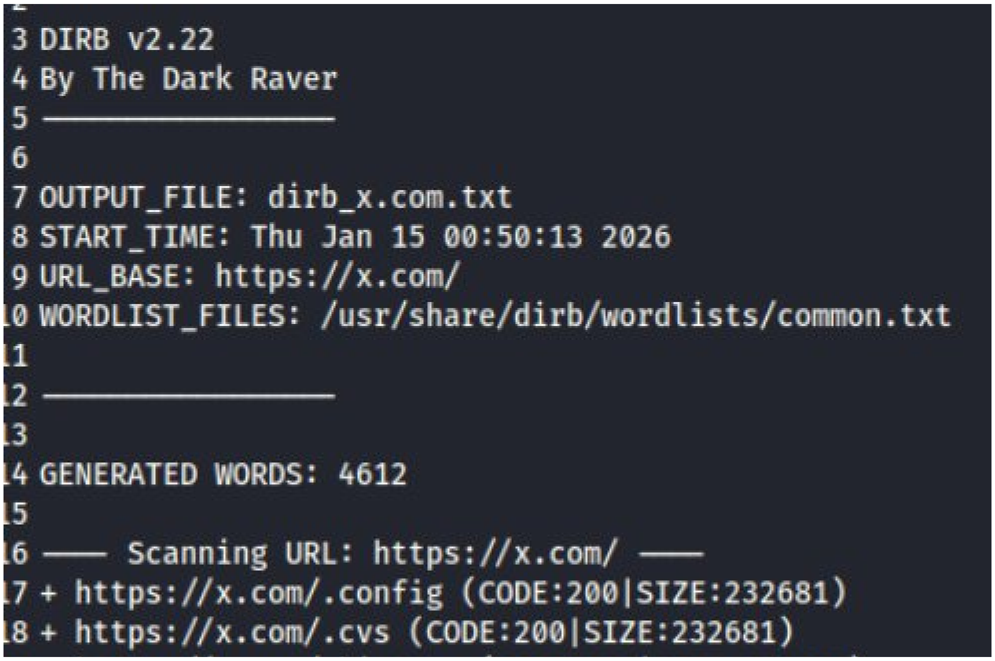
(Output saved to dirb_x.com.txt file)

Scan Summary :

Total Words tested: 4612

Target: Main Domain only (https://x.com/)

Reconnaissance only (No exploitation)



```
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: dirb_x.com.txt
START_TIME: Thu Jan 15 00:50:13 2026
URL_BASE: https://x.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://x.com/ ----
+ https://x.com/.config (CODE:200|SIZE:232681)
+ https://x.com/.cvs (CODE:200|SIZE:232681)
```

Observations:

During the scan, the server responded with HTTP 200 status codes for a large number of paths, including numeric, dot-prefixed, and random strings. Most responses had identical content sizes, indicating dynamic routing behavior rather than the presence of actual directories or files.

Example patterns observed:

- Numeric paths (/100, /403, /2004)
- Dot-prefixed paths (/.cvs, /.mysql_history)
- Random strings (/abc, /2g)

This behavior suggests that the application returns a default page for non-existent paths.

Valid Public Endpoints Identified

Some known public paths were observed, such as:

- /about (301 redirect)
- /accessibility
- /accounts
- /accountsettings

These endpoints are publicly accessible and expected for a production web application.

Conclusion :

No sensitive hidden directories or files were identified on the main domain. The scan was intentionally stopped to avoid unnecessary noise and false positives. This behavior indicates strong routing controls and protection mechanisms on the target application.