Major-1 Project

SAMEERAN SURIN

ERP : 6605912

MAJOR PROJECT DOCUMENTATION

Bug Bounty Reconnaissance – Discover Financial Services

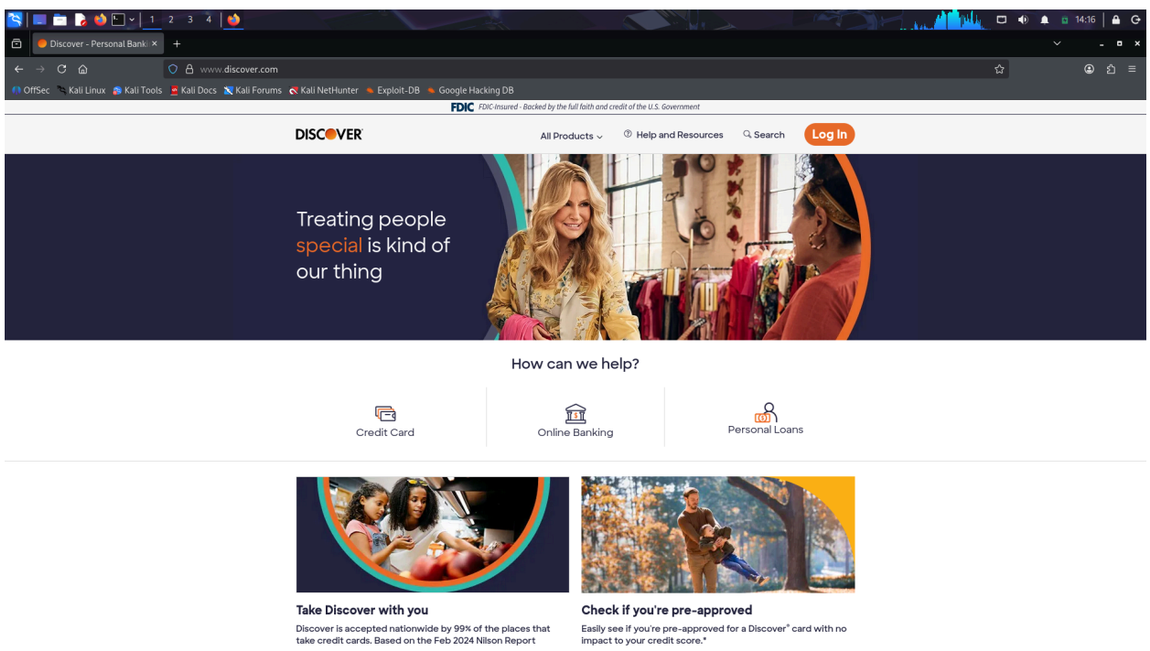
1. Main Domain Identification

Company Name: Discover Financial Services

Main Domain: `discover.com`

Method Used:

The official Discover website was identified using a Google search and verified through the homepage and contact pages.

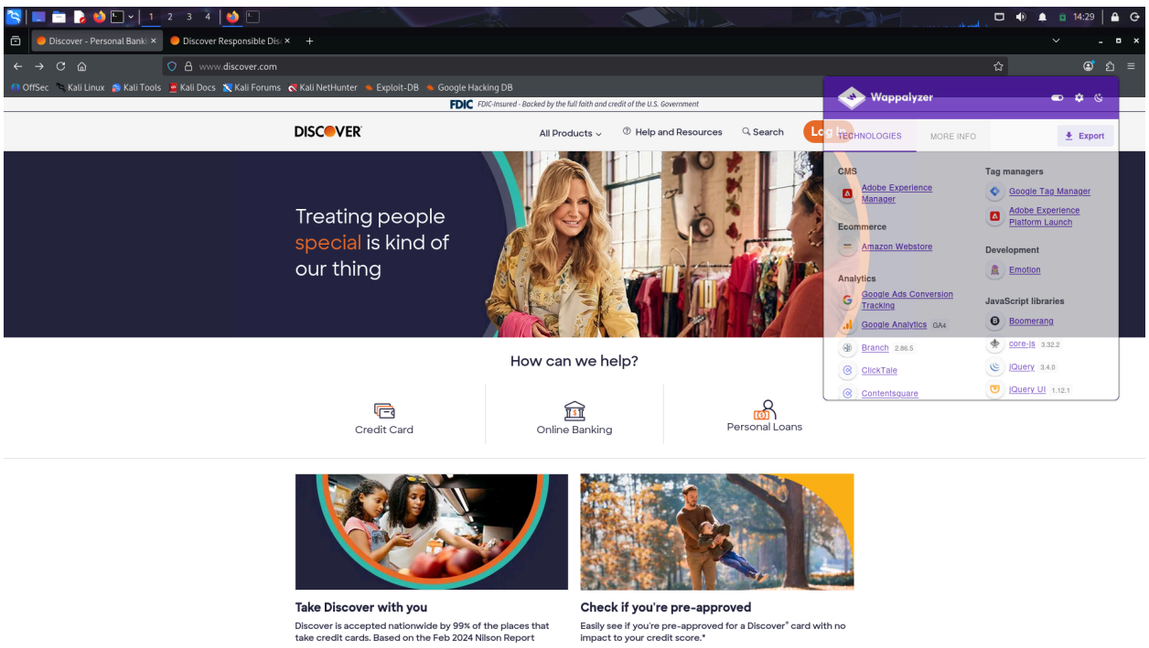


2. Bug Bounty / Vulnerability Disclosure Page

Discover maintains an official **Vulnerability Disclosure / Bug Bounty Program**, typically hosted on **HackerOne**.

Search Keywords Used:

> Discover bug bounty
> Discover vulnerability disclosure



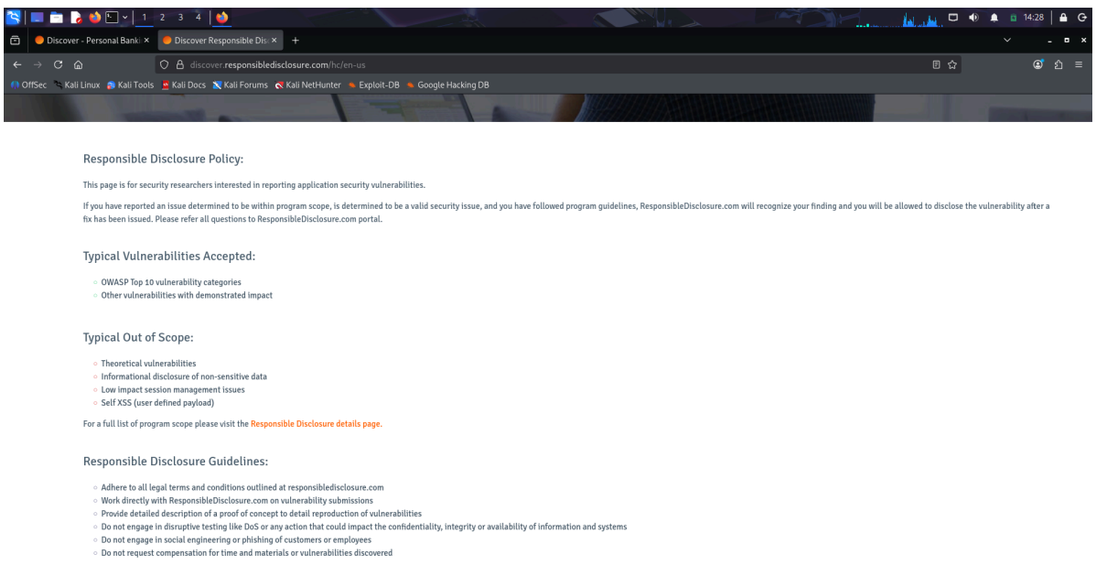
3. Bug Bounty Scope (In-Scope & Out-of-Scope)

In-Scope Assets (as defined by Discover):

- discover.com
- Discover-owned subdomains
- Discover web applications and services

Out-of-Scope Assets:

- Third-party services
- Customer-controlled accounts
- Social media platforms



4. Ping Test (ICMP Reachability)

Objective:

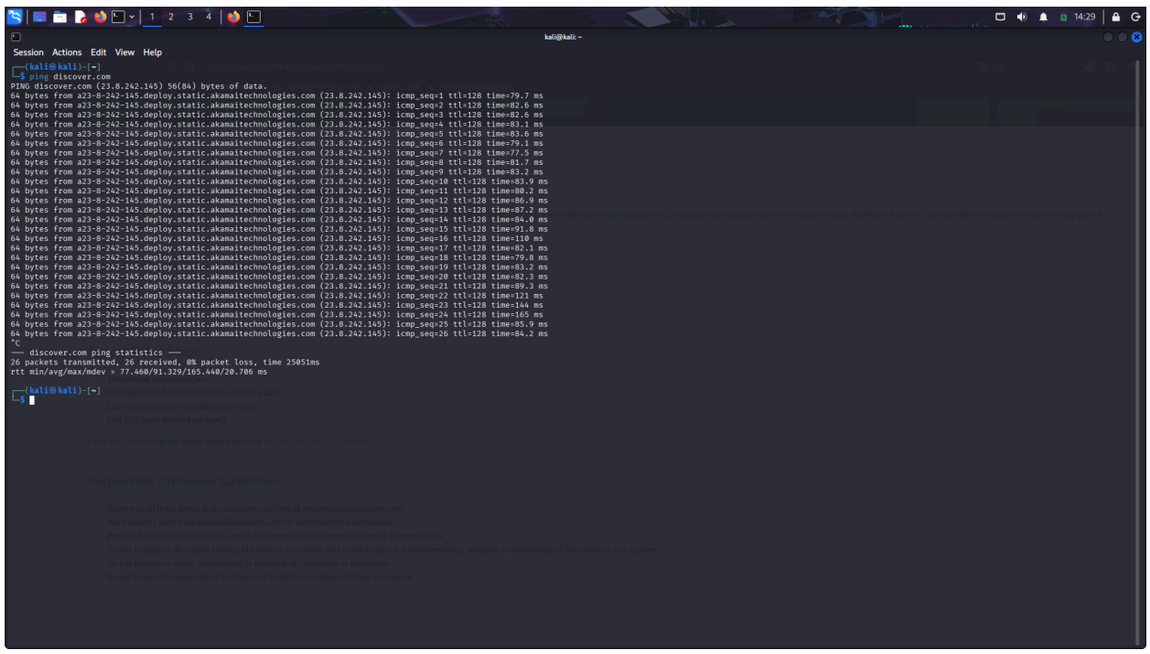
To check whether the Discover main domain responds to ICMP requests.

Command Used:

```
ping discover.com
```

Observation:

ICMP requests are usually blocked as part of Discover's security controls.



---

5. Technology Stack Identification (Main Domain)

Tool Used:

Wappalyzer (Browser Extension)

Technologies Identified May Include:

- Web server
- CDN
- JavaScript frameworks
- Analytics and security tools

---

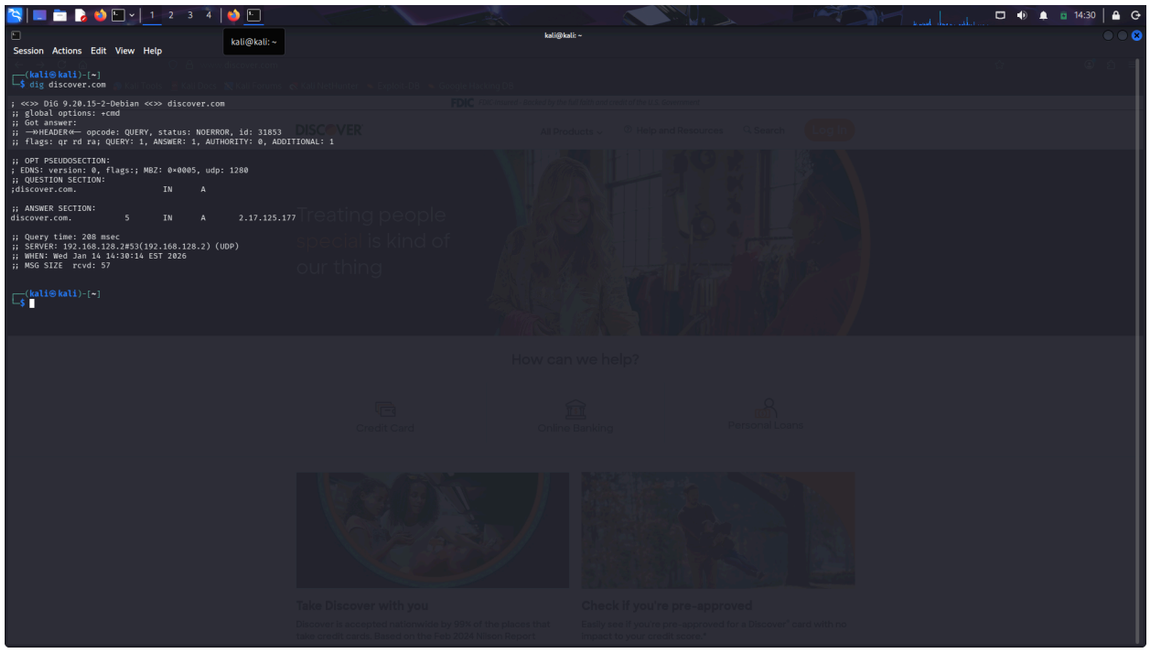
6. ASN Number and IP Range Identification

Objective:

To identify ASN and network ownership for Discover's infrastructure.

Commands Used:

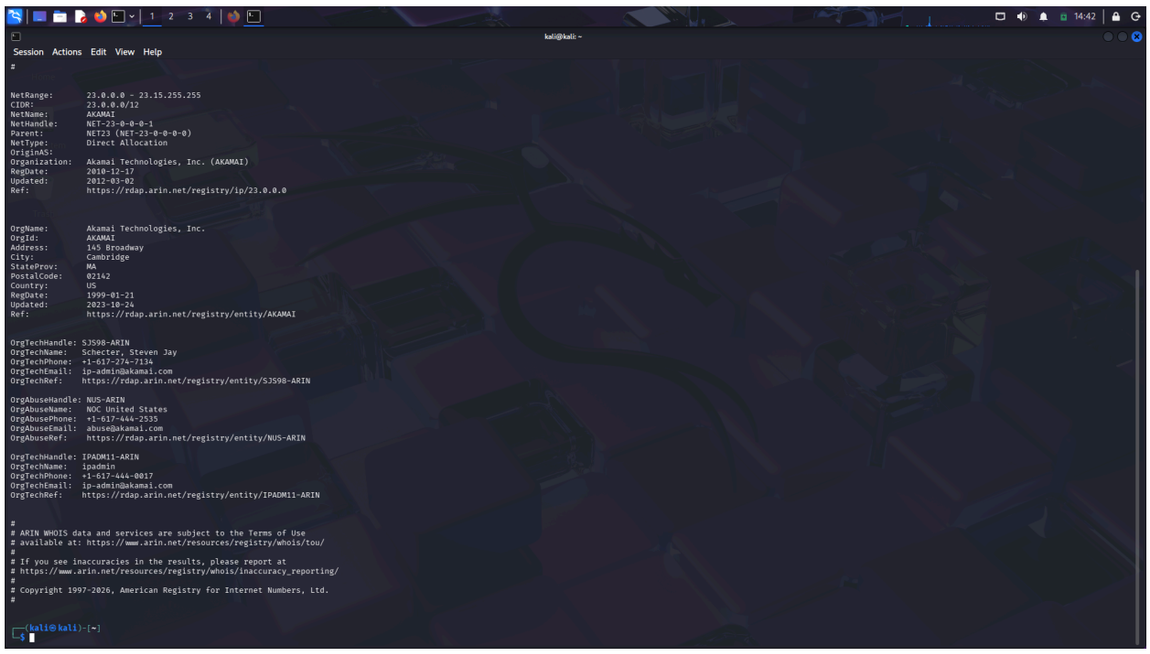
```
dig discover.com
```




```
whois <IP_ADDRESS>
```

Information Collected:

- ASN Number
- Organization / ISP
- Netblocks



---

7. Subdomain Enumeration

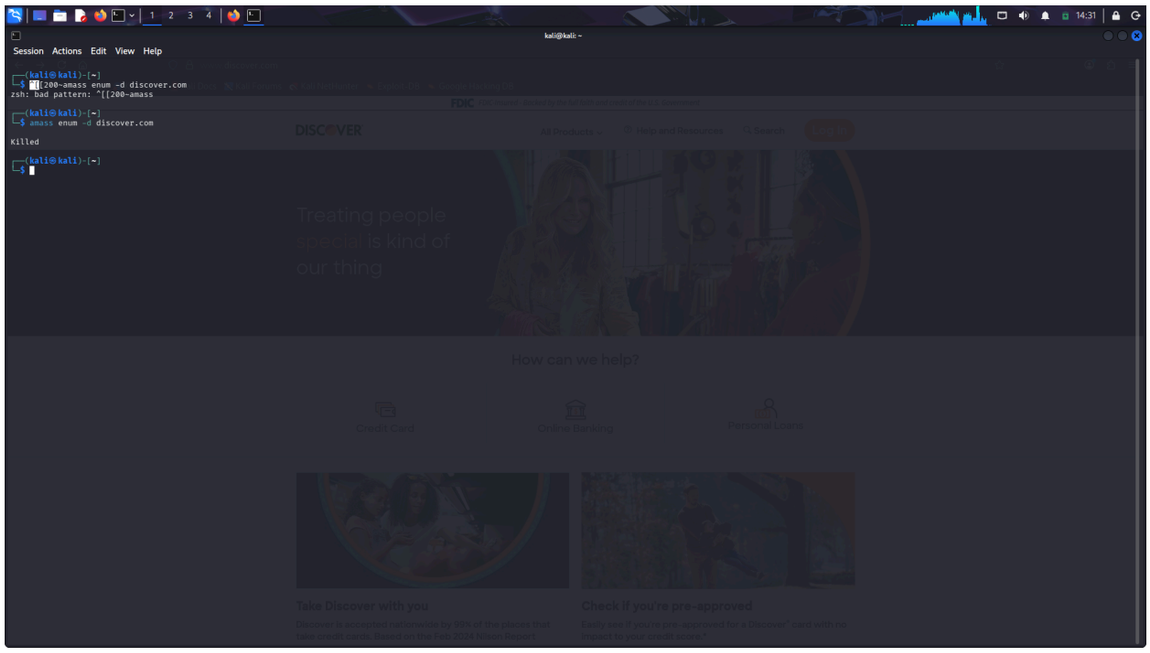
Objective:

To discover publicly accessible Discover subdomains.

Tool Used: `amass`

Command:

```
amass enum -d discover.com
```



---

8. Technology Stack on Subdomains

Selected Subdomains:

- `www.discover.com`
- `portal.discover.com`
- `jobs.discover.com`
- `apply.discover.com`
- `secure.discover.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)

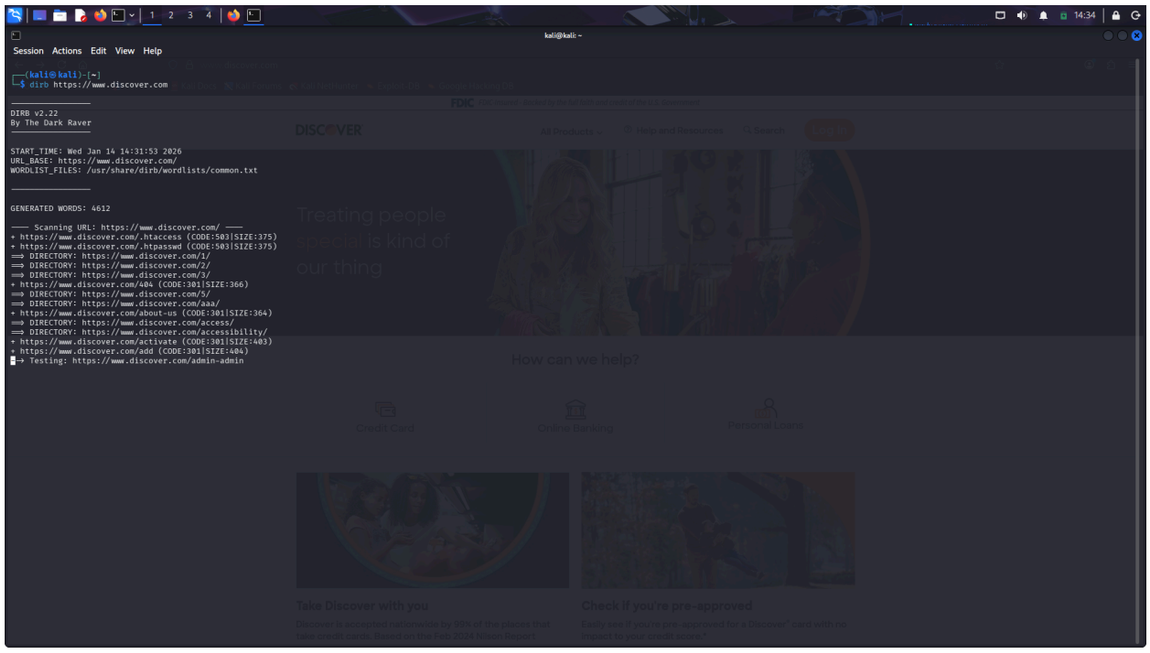
Tool Used: `dirb`

Command:

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

Observation:

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



---

10. Declaration

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

No exploitation, brute-force attacks, or unauthorized access was performed, in compliance with Discover’s bug bounty policy and academic guidelines.