

# Major-1 Project

SAMEERAN SURIN

ERP : 6605912

## MAJOR PROJECT DOCUMENTATION

### Bug Bounty Reconnaissance – Discover Financial Services

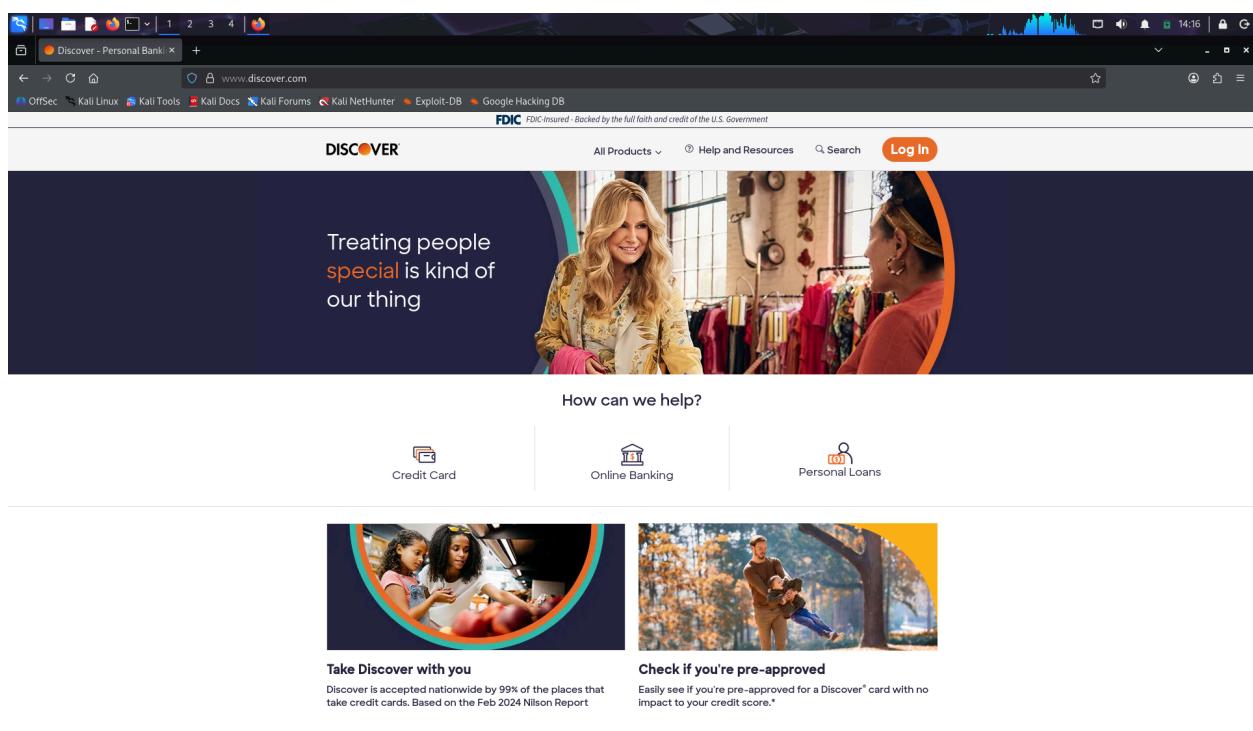
#### 1. Main Domain Identification

**Company Name:** Discover Financial Services

**Main Domain:** [discover.com](http://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

Discover - Personal Banking | Discover Responsible Disclosure | www.discover.com

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

**DISCOVER**

Treating people **special** is kind of our thing

How can we help?

Credit Card Online Banking Personal Loans

**Take Discover with you**  
Discover is accepted nationwide by 99% of the places that take credit cards. Based on the Feb 2024 Nilson Report

**Check if you're pre-approved**  
Easily see if you're pre-approved for a Discover® card with no impact to your credit score.\*

### 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

Responsible Disclosure Policy:

This page is for security researchers interested in reporting application security vulnerabilities.

If you have reported an issue determined to be within program scope, is determined to be a valid security issue, and you have followed program guidelines, ResponsibleDisclosure.com will recognize your finding and you will be allowed to disclose the vulnerability after a fix has been issued. Please refer all questions to ResponsibleDisclosure.com portal.

Typical Vulnerabilities Accepted:

- OWASP Top 10 vulnerability categories
- Other vulnerabilities with demonstrated impact

Typical Out of Scope:

- Theoretical vulnerabilities
- Informational disclosure of non-sensitive data
- Low impact session management issues
- Self XSS (user defined payload)

For a full list of program scope please visit the [Responsible Disclosure details page](#).

Responsible Disclosure Guidelines:

- Adhere to all legal terms and conditions outlined at responsibledisclosure.com
- Work directly with Responsible Disclosure on vulnerability submissions
- Provide detailed description of a proof of concept to detail reproduction of vulnerabilities
- Do not engage in disruptive testing like DoS or any action that could impact the confidentiality, integrity or availability of information and systems
- Do not engage in social engineering or phishing of customers or employees
- Do not request compensation for time and materials or vulnerabilities discovered

#### **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.

```
[kali㉿kali)-~] ping discover.com
PING discover.com (23.8.242.145) 56(84) bytes of data.
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=1 ttl=128 time=79.7 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=2 ttl=128 time=82.5 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=3 ttl=128 time=82.5 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=4 ttl=128 time=83.1 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=5 ttl=128 time=83.6 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=6 ttl=128 time=83.1 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=7 ttl=128 time=77.5 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=8 ttl=128 time=81.7 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=9 ttl=128 time=83.2 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=10 ttl=128 time=80.9 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=11 ttl=128 time=80.7 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=12 ttl=128 time=80.9 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=13 ttl=128 time=80.7 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=14 ttl=128 time=80.7 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=15 ttl=128 time=91.0 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=16 ttl=128 time=80.7 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=17 ttl=128 time=82.1 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=18 ttl=128 time=80.7 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=19 ttl=128 time=80.3 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=20 ttl=128 time=80.3 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=21 ttl=128 time=80.5 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=22 ttl=128 time=81.1 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=23 ttl=128 time=80.4 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=24 ttl=128 time=165 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=25 ttl=128 time=85.9 ms
64 bytes from a23-8-242-145.deploy.static.akamaitechnologies.com (23.8.242.145): icmp_seq=26 ttl=128 time=84.2 ms
```
discover.com ping statistics
26 packets transmitted, 26 received, 0% packet loss, time 25051ms
rtt min/avg/max/mdev = 77.408/91.329/165.440/20.780 ms

[kali㉿kali)-~] Self XSS (user defined payload)

For a full list of program scope please visit the Responsible Disclosure details page.
```

## **5. Technology Stack Identification (Main Domain)**

## Tool Used:

## Wappalyzer (Browser Extension)

## **Technologies Identified May Include:**

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

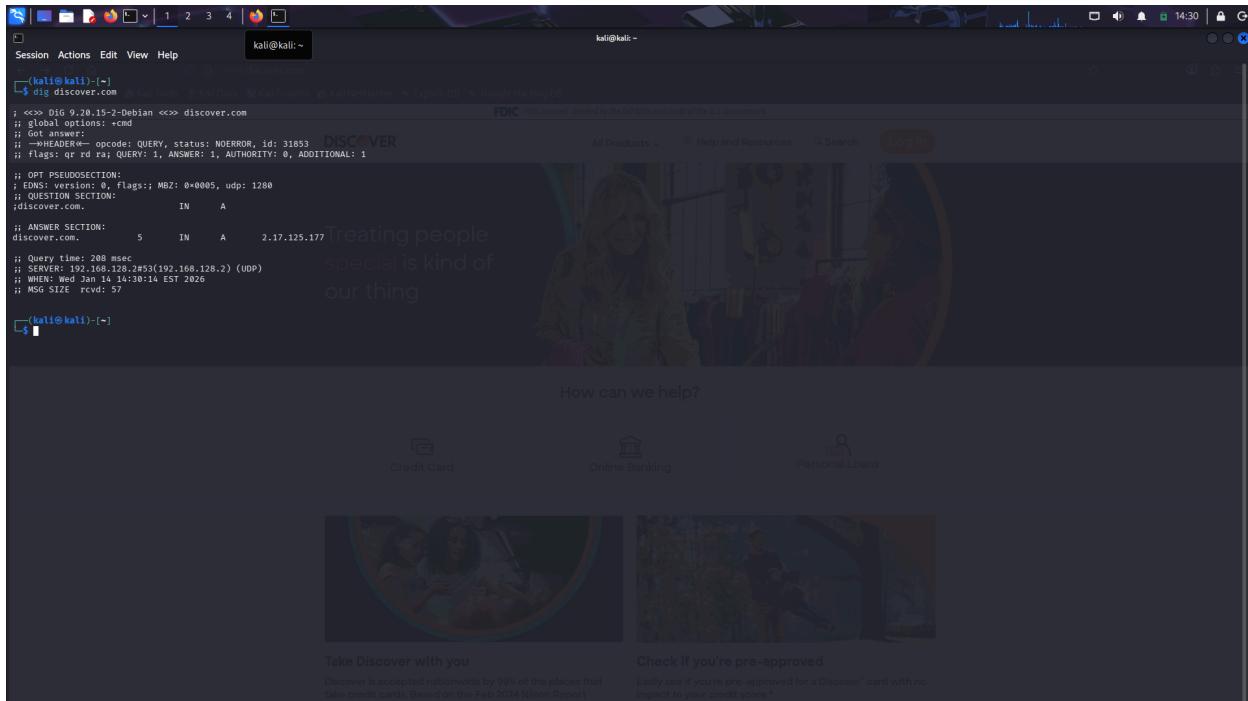
## 6. ASN Number and IP Range Identification

## **Objective:**

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

## **Commands Used:**

```
dig discover.com
```

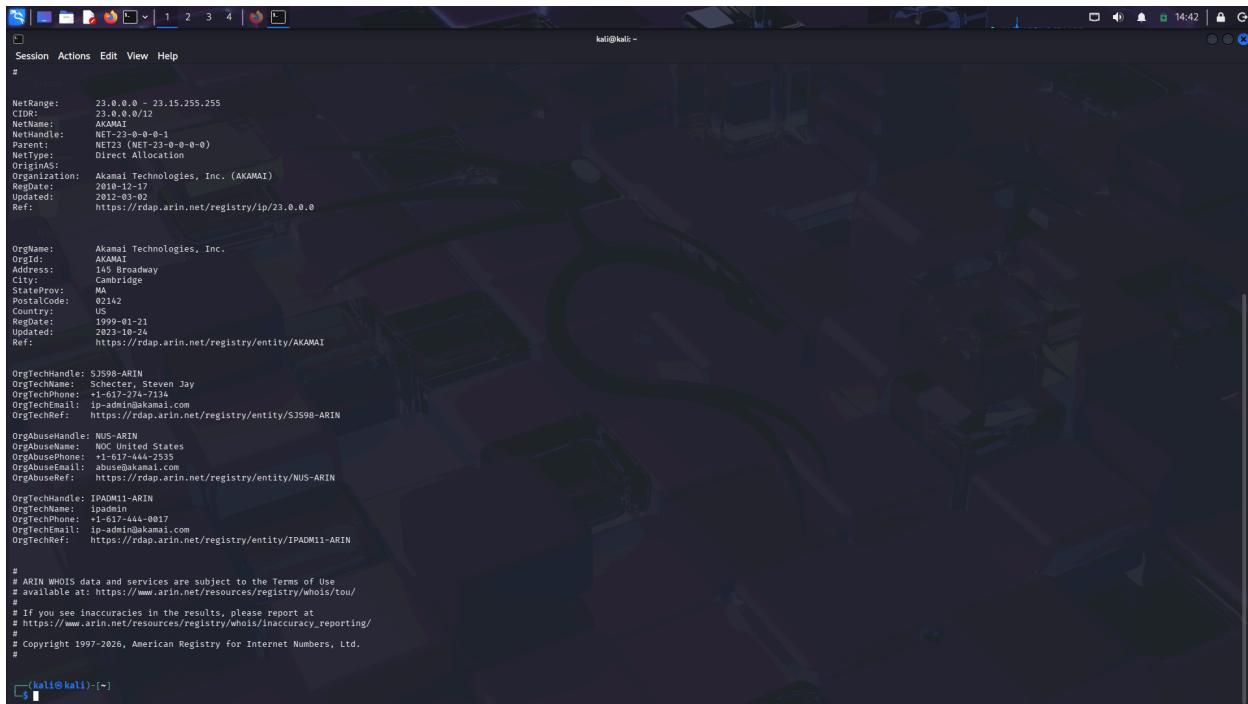


```
[kali㉿kali: ~] dig discover.com
; <>> SOA discover.com. 14300 1000 1000 1000 1000
;; global options: +cd
;; Got answer:
;; ->HEADER: opcode: QUERY, status: NOERROR, id: 31853
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: MBZ: 0x0005, udp: 1280
; QUESTION SECTION:
;idiscover.com. IN A
;; ANSWER SECTION:
discover.com. 5 IN A 2.17.125.177
;; Query time: 208 msec
;; SERVER: 192.168.128.2#53(192.168.128.2) (UDP)
;; WHEN: Wed Jan 14 14:30:14 EST 2026
;; MSG SIZE rcvd: 57
```

```
whois <IP_ADDRESS>
```

### Information Collected:

- ASN Number
- Organization / ISP
- Netblocks



```
[kali㉿kali: ~] whois 23.0.0.0
; <>> whois 23.0.0.0
NetRange: 23.0.0.0 - 23.15.255.255
CIDR: 23.0.0.0/12
NetName: AKAMAI
NetHandle: NET23-0-0-0-1
Parent: NET23 (NET-23-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: Akamai Technologies, Inc. (AKAMAI)
RegDate: 2010-12-17
Updated: 2012-03-02
Ref: https://rdap.arin.net/registry/ip/23.0.0.0

OrgName: Akamai Technologies, Inc.
OrgID: AKAMAI
Address: 145 Broadway
City: Cambridge
StateProv: MA
PostalCode: 02142
Country: US
RegDate: 1999-01-21
Updated: 2023-10-24
Ref: https://rdap.arin.net/registry/entity/AKAMAI

OrgTechName: S3598-ARIN
OrgTechName: Schacter, Steven Jay
OrgTechPhone: +1-617-274-7134
OrgTechEmail: ip-admin@akamai.com
OrgTechRef: https://rdap.arin.net/registry/entity/S3598-ARIN

OrgAbuseHandle: NUS-ARIN
OrgAbuseName: NOC United States
OrgAbusePhone: +1-617-444-2838
OrgAbuseEmail: abuse@akamai.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/NUS-ARIN

OrgTechName: IPADM11-ARIN
OrgTechName: ipadmin
OrgTechPhone: +1-617-444-0017
OrgTechEmail: ip-admin@akamai.com
OrgTechRef: https://rdap.arin.net/registry/entity/IPADM11-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 1997-2026, American Registry for Internet Numbers, Ltd.
#
```

## 7. Subdomain Enumeration

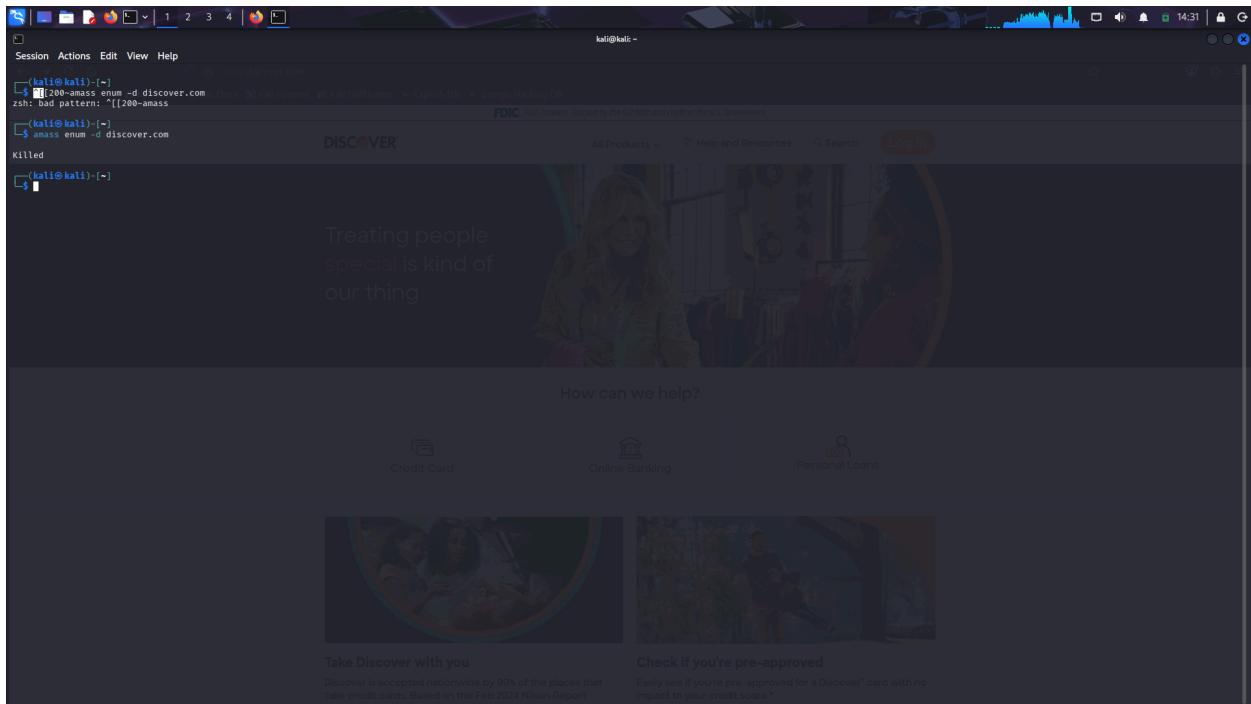
## Objective:

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)

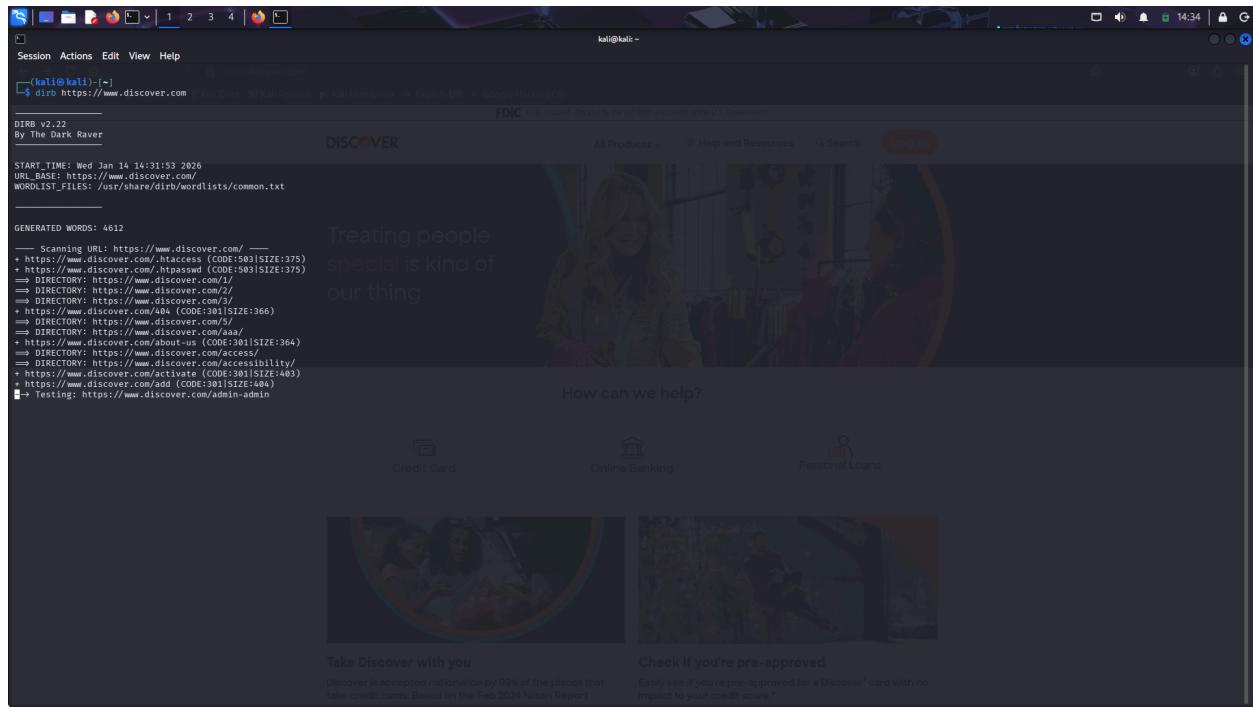
Tool Used: `dirb`

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.