MAJOR PROJECT REPORT

Bug Bounty Reconnaissance Assignment

Assigned Company: Revolut

Submitted by:

Name – Nidhi Kanwar

Roll Number - 301313124047

Submitted to:

Subject Name - Technical Training

College Name – Rungta Collage of Engineering and Technology

Academic Year: 2025–2026

Introduction

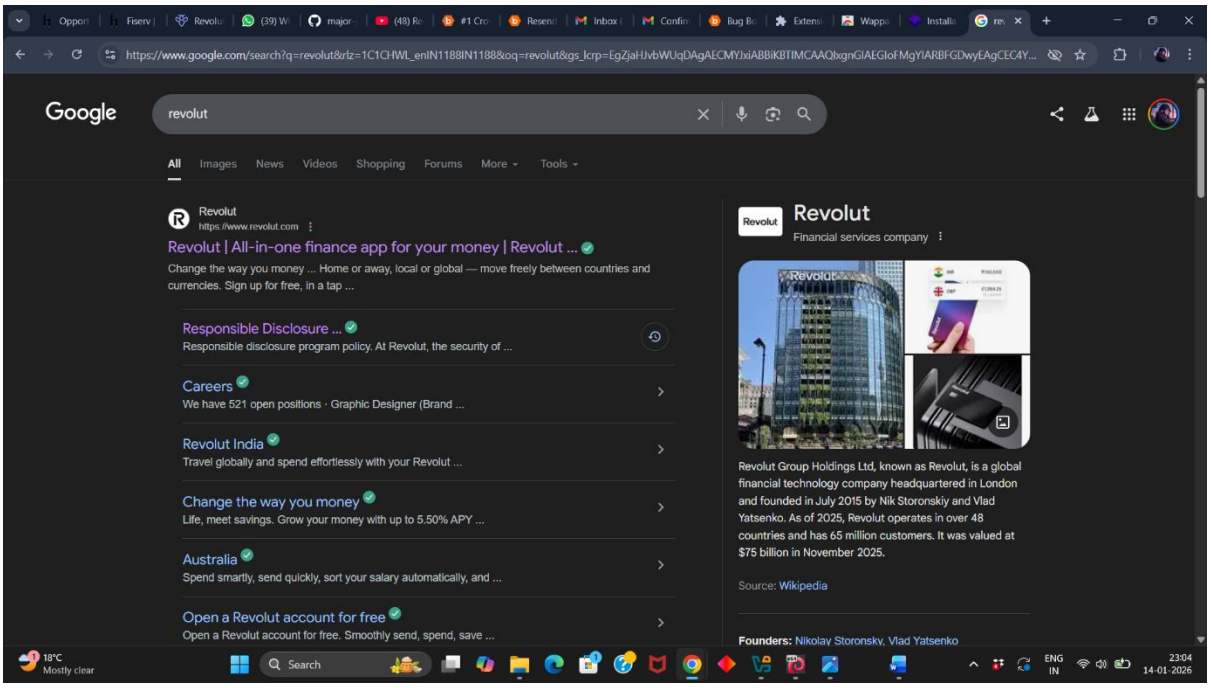
This project focuses on reconnaissance activities performed on the assigned company Revolut as part of a Bug Bounty Reconnaissance Assignment. The objective of this project is to understand how ethical hackers gather information about a target organization while strictly following legal and ethical guidelines. All activities were limited to passive reconnaissance, and no exploitation or unauthorized access was performed.

COMPANY OVERVIEW

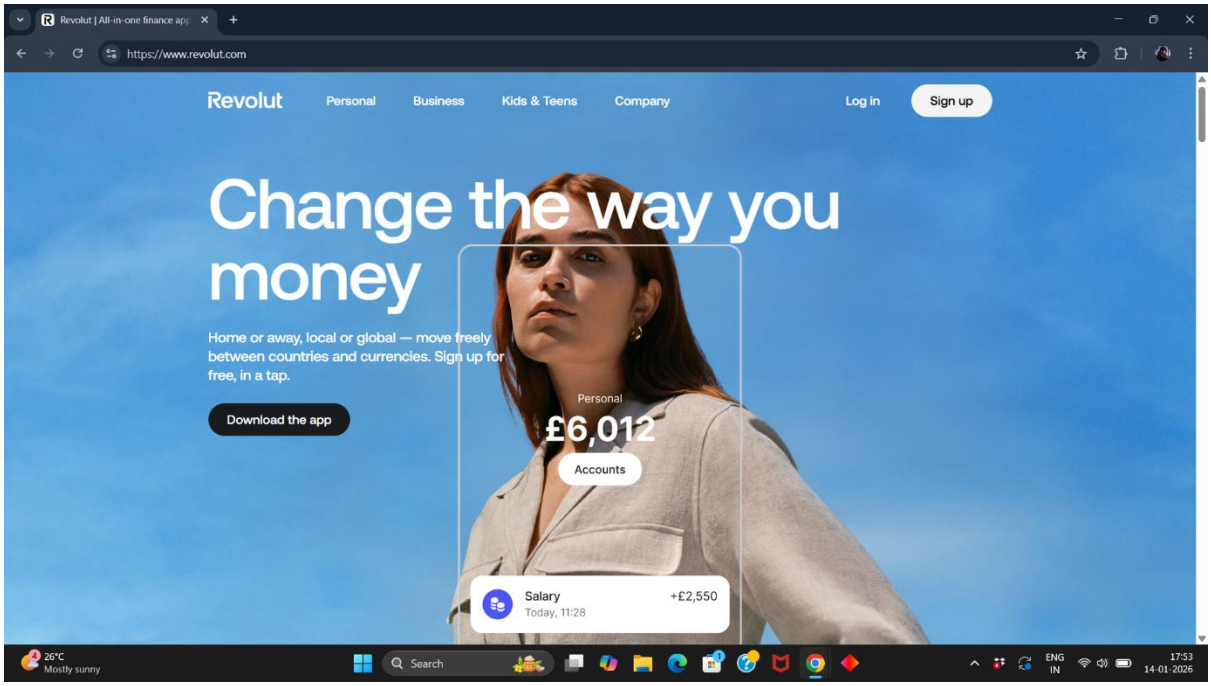
Revolut is a global financial technology company providing digital banking and payment services. It offers services such as international money transfers, cards, and mobile banking.

1. Identify the company's Main Domain

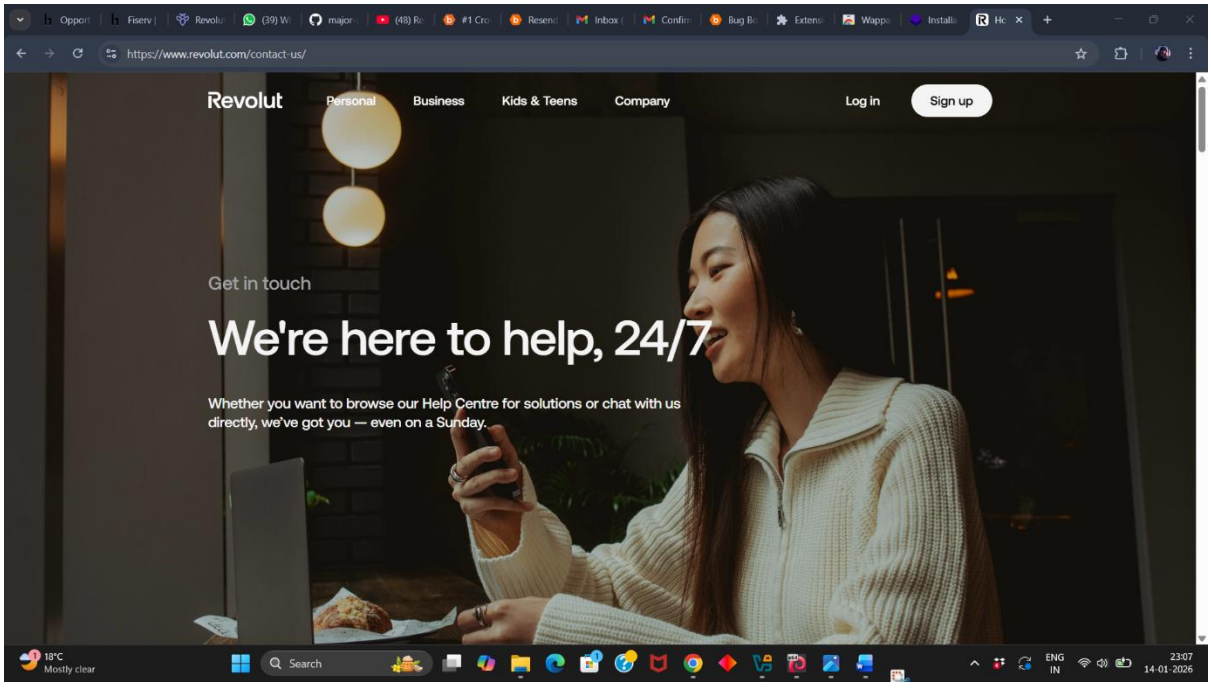
- Google Search



- Domain page of Revolut

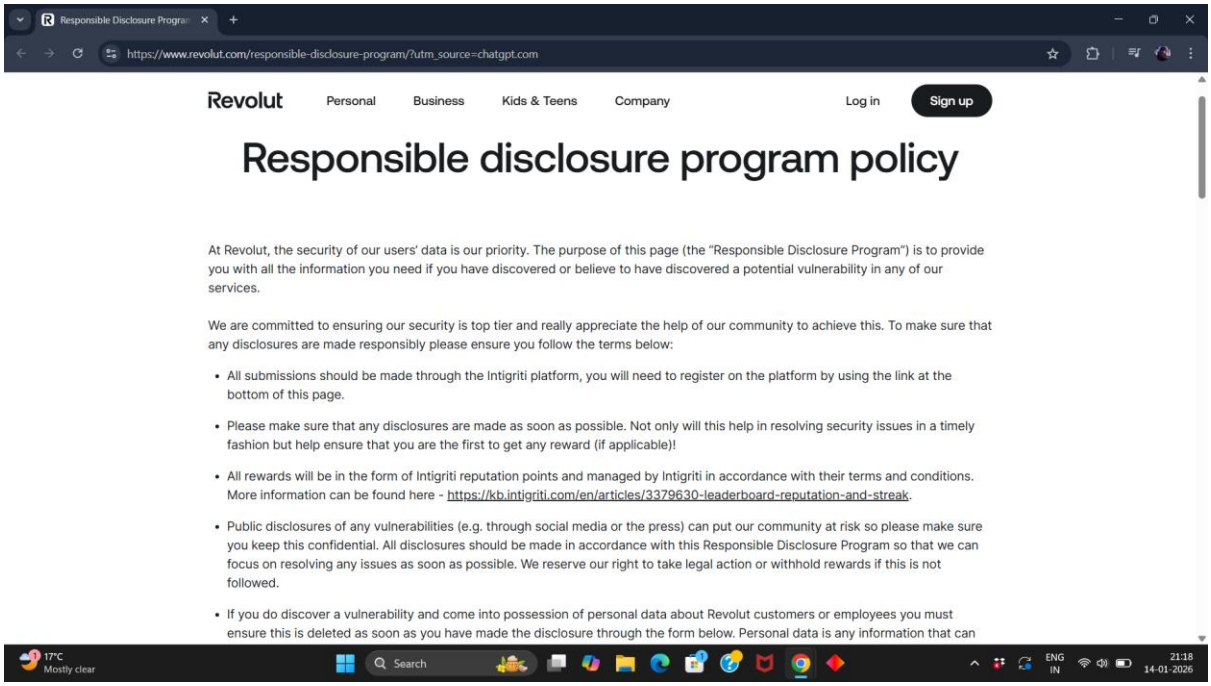


- Contact Page

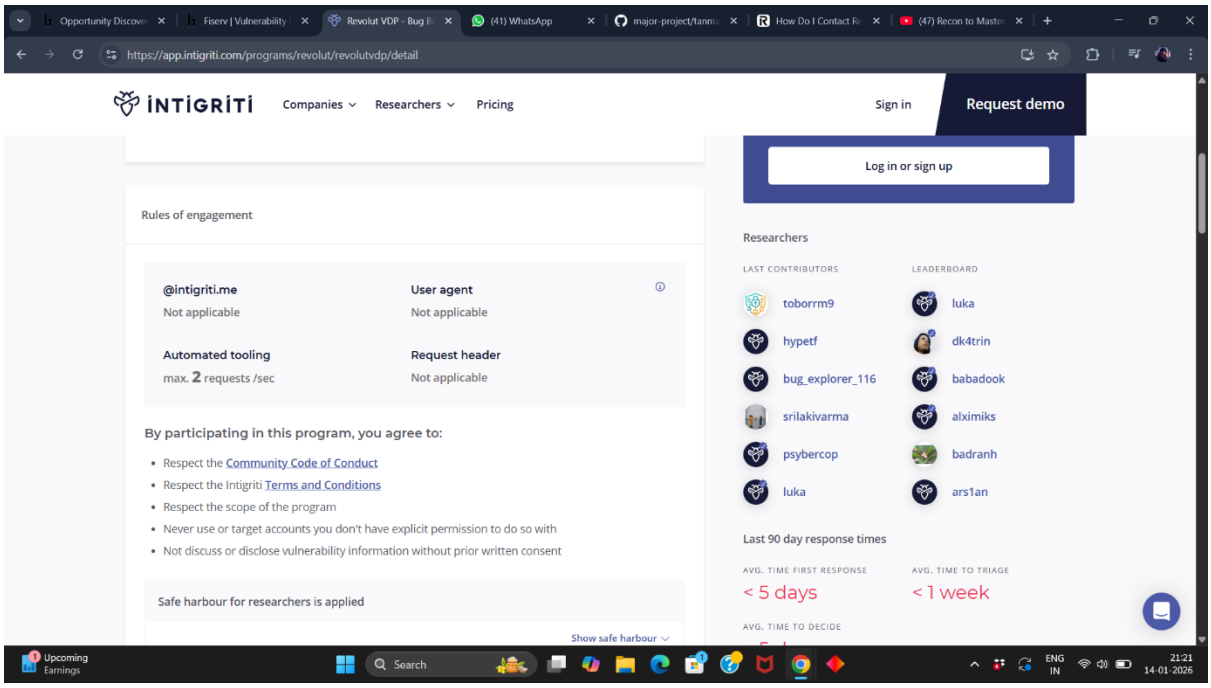


2. Locate the Bug Bounty / VDP program

- The official bug bounty / vulnerability disclosure program for Revolut is hosted on the Intigriti platform.
  The program name is Revolut VDP and can be accessed at:
  https://app.intigriti.com/programs/revolut/revolutvdp/detail
  Revolut's own responsible disclosure policy on the official website states that security vulnerabilities must be submitted via the Intigriti platform.
- Responsible Disclosure Program

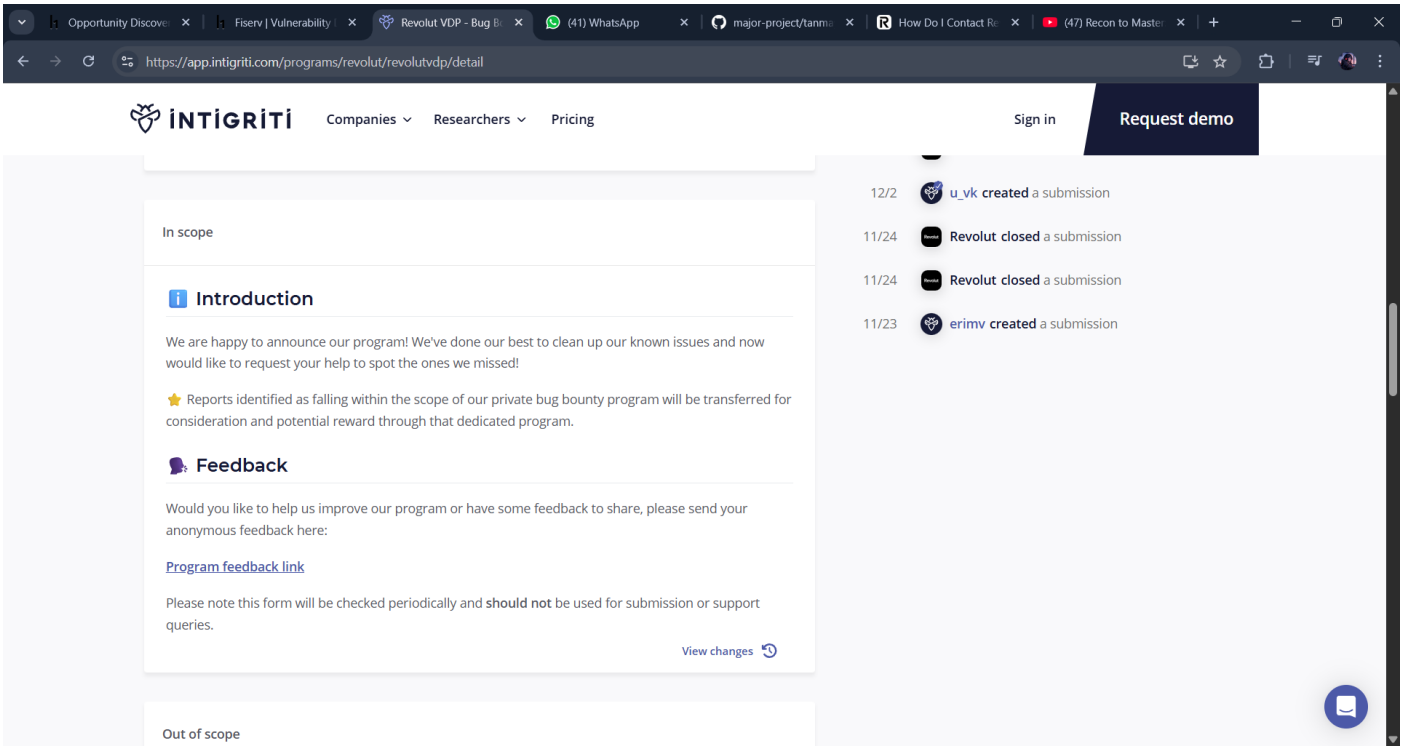


- Intigriti Page

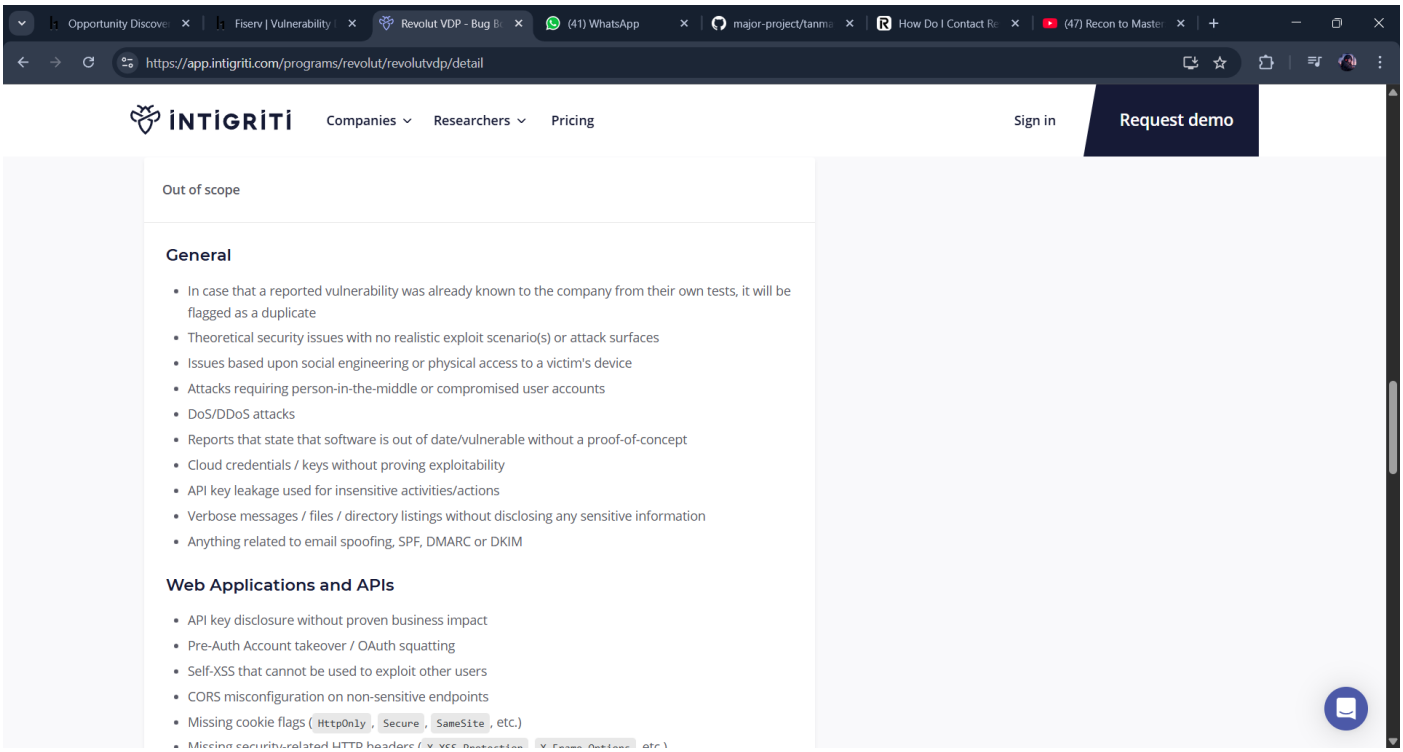


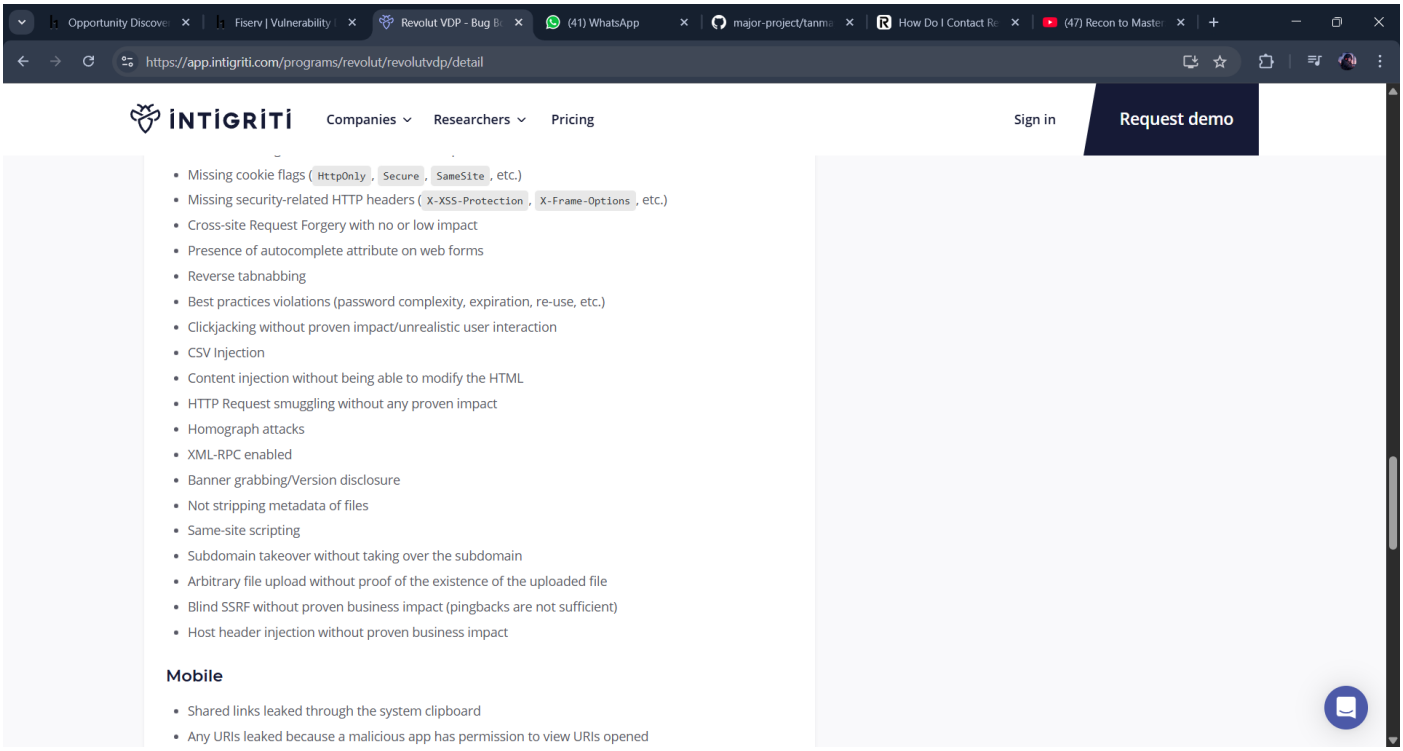
3. Identify Bug Bounty scope (in-scope & Out of scope)

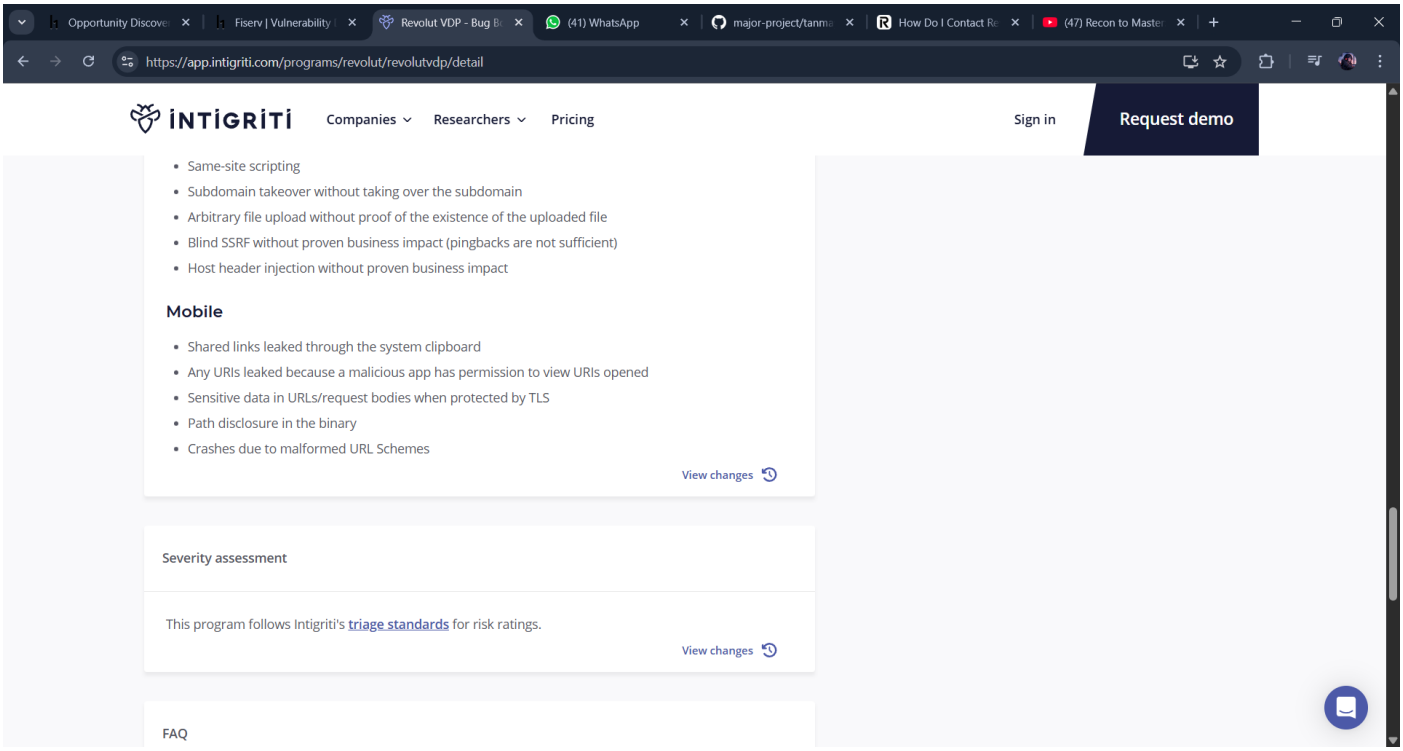
- In Scope



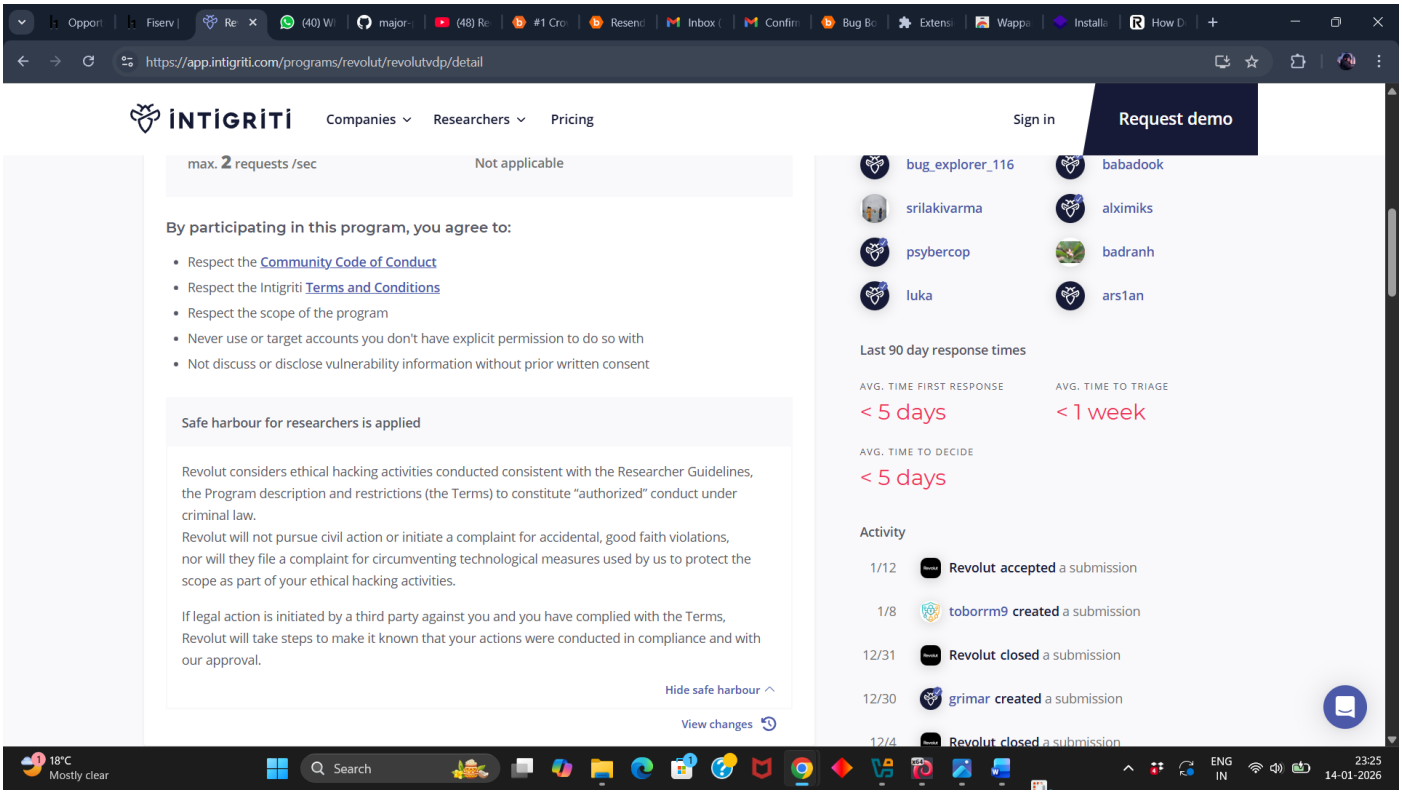
- Out scope




https://app.intigriti.com/programs/revolut/revolutvdp/detail
INTIGRITI
Companies
Researchers
Pricing
Sign in
Request demo
Missing cookie flags (HttpOnly , Secure , SameSite , etc.)
Missing security-related HTTP headers (X-XSS-Protection , X-Frame-Options , etc.)
Cross-site Request Forgery with no or low impact
Presence of autocomplete attribute on web forms
Reverse tabnabbing
Best practices violations (password complexity, expiration, re-use, etc.)
Clickjacking without proven impact/unrealistic user interaction
CSV Injection
Content injection without being able to modify the HTML
HTTP Request smuggling without any proven impact
Homograph attacks
XML-RPC enabled
Banner grabbing/Version disclosure
Not stripping metadata of files
Same-site scripting
Subdomain takeover without taking over the subdomain
Arbitrary file upload without proof of the existence of the uploaded file
Blind SSRF without proven business impact (pingbacks are not sufficient)
Host header injection without proven business impact
Mobile
Shared links leaked through the system clipboard
Any URIs leaked because a malicious app has permission to view URIs opened


https://app.intigriti.com/programs/revolut/revolutvdp/detail
INTIGRITI
Companies
Researchers
Pricing
Sign in
Request demo
Same-site scripting
Subdomain takeover without taking over the subdomain
Arbitrary file upload without proof of the existence of the uploaded file
Blind SSRF without proven business impact (pingbacks are not sufficient)
Host header injection without proven business impact
Mobile
Shared links leaked through the system clipboard
Any URIs leaked because a malicious app has permission to view URIs opened
Sensitive data in URLs/request bodies when protected by TLS
Path disclosure in the binary
Crashes due to malformed URL Schemes
View changes
Severity assessment
This program follows Intigriti's triage standards for risk ratings.
View changes
FAQ

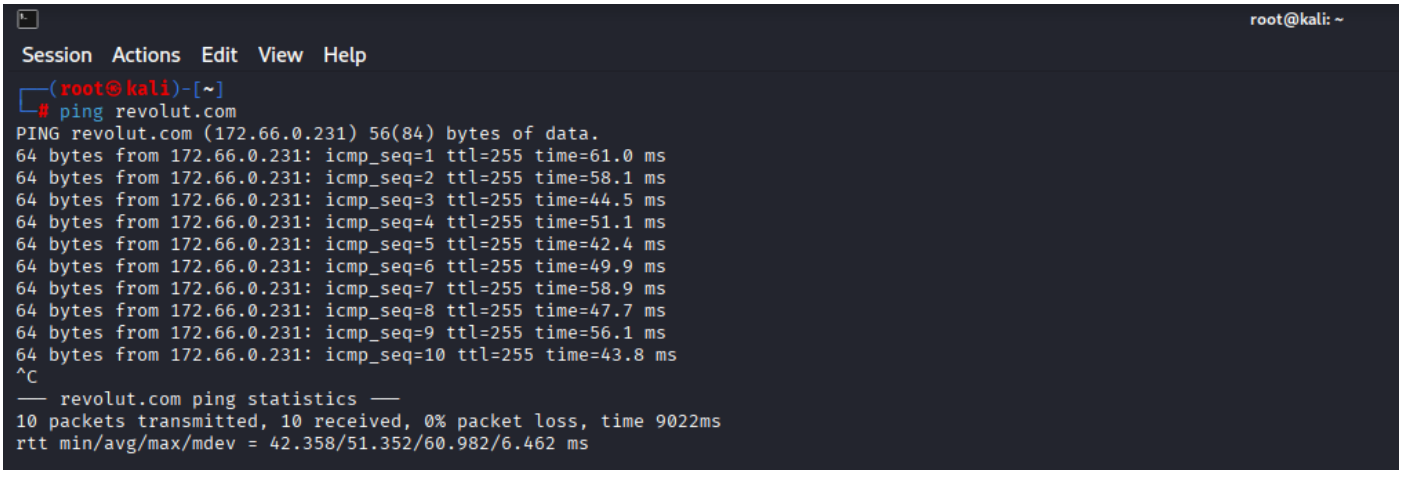
SCOPE IDENTIFICATION



4. Ping the Main Domain

RECONNAISSANCE STEPS (MOST IMPORTANT PART)

Command used: ping revolute.com



- IP Address – 172.66.0.231

5. Technology Stack Identification

Tool Used: Wappalyzer

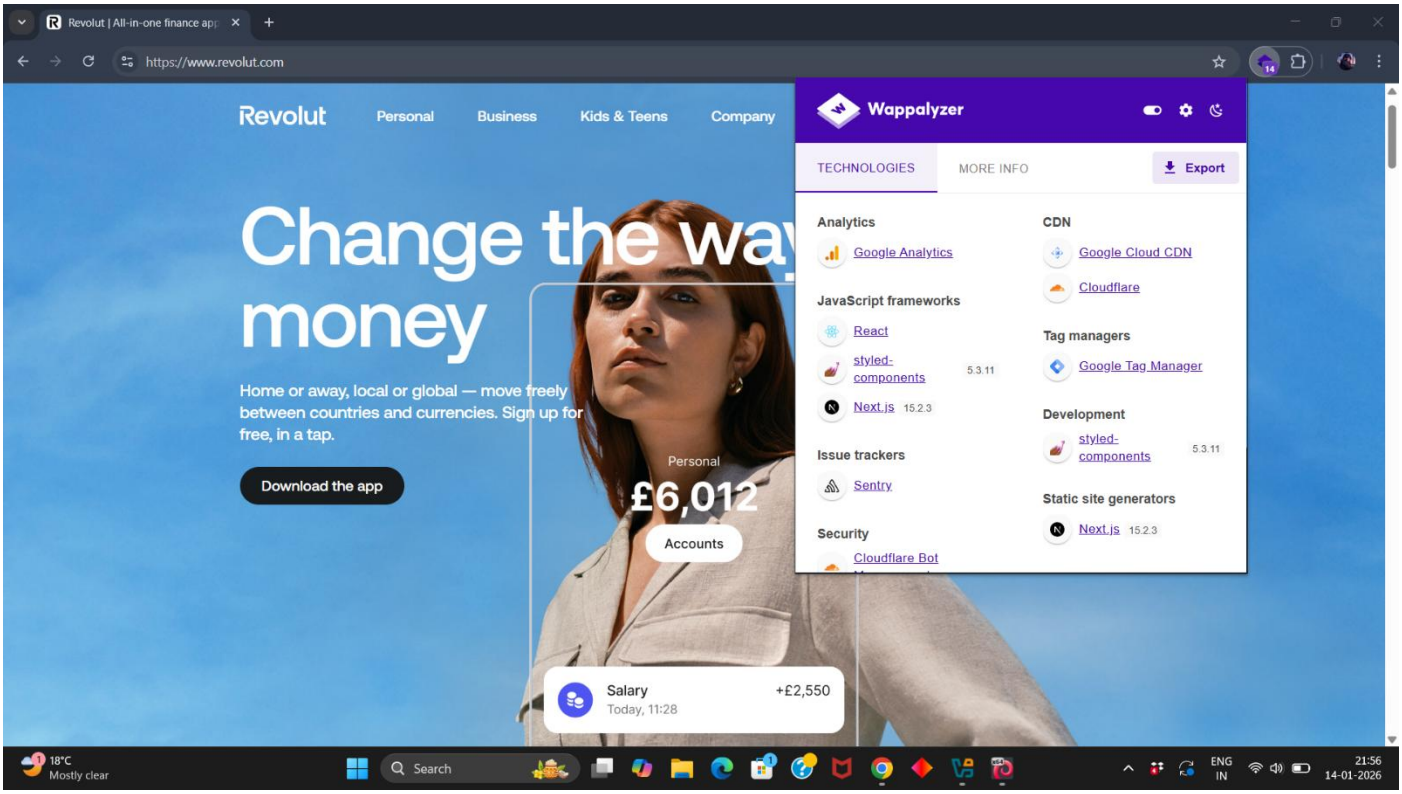
Observation: The main domain uses modern web technologies.

Purpose of Using Wappalyzer

- **Wappalyzer** is used to **identify the technology stack** of a website.

In this project, it helps identify:

- Web server (e.g., Nginx)
- Frameworks (e.g., React)
- Programming language (e.g., JavaScript)
- CMS (if any)
- CDN
- Analytics tools



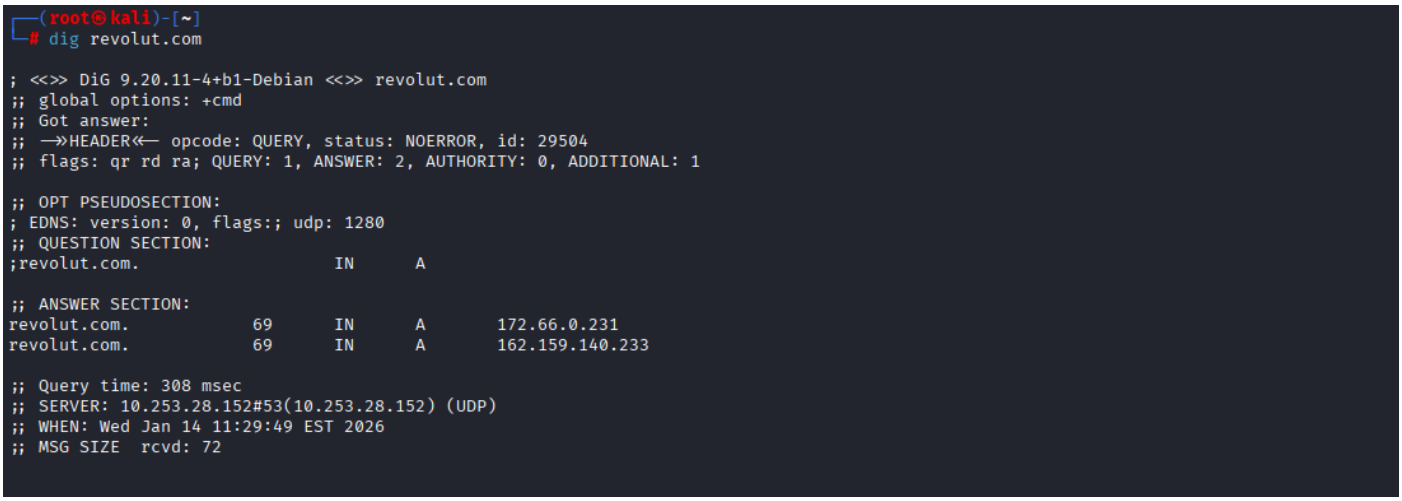
6. ASN number & Organization IP Rang Information

Command used: dig revolut.com

- Purpose of Using dig: The dig (Domain Information Groper) command is used to retrieve DNS information about a domain.

In this project, it is used to:

- Resolve the domain name to an IP address
- Identify DNS records
- Support further network reconnaissance steps (ASN lookup)



Command used: whois 172.66.0.231

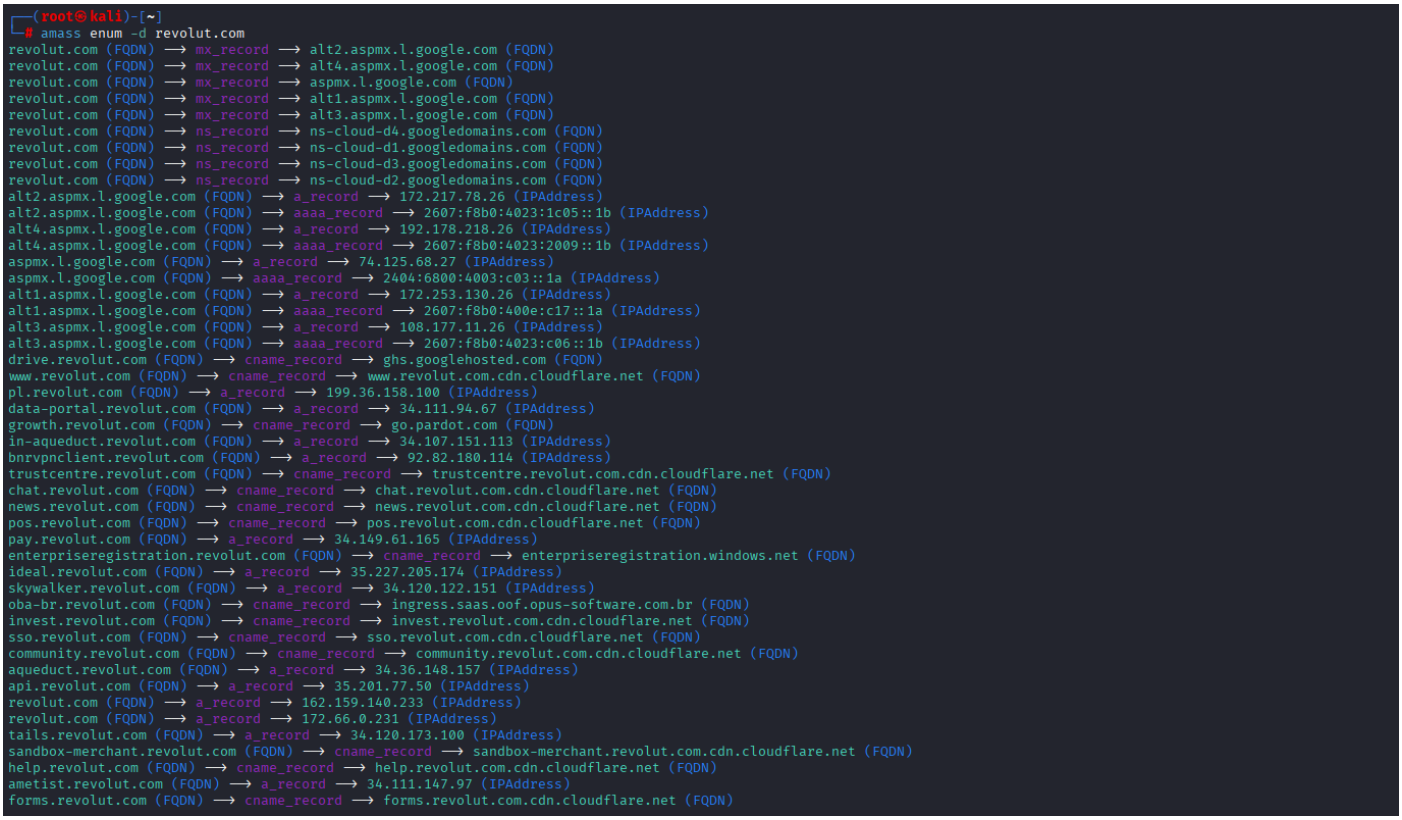
ASN and IP ownership details were identified to understand network infrastructure.

7. Subdomain Enumeration

Tool Used: Amass

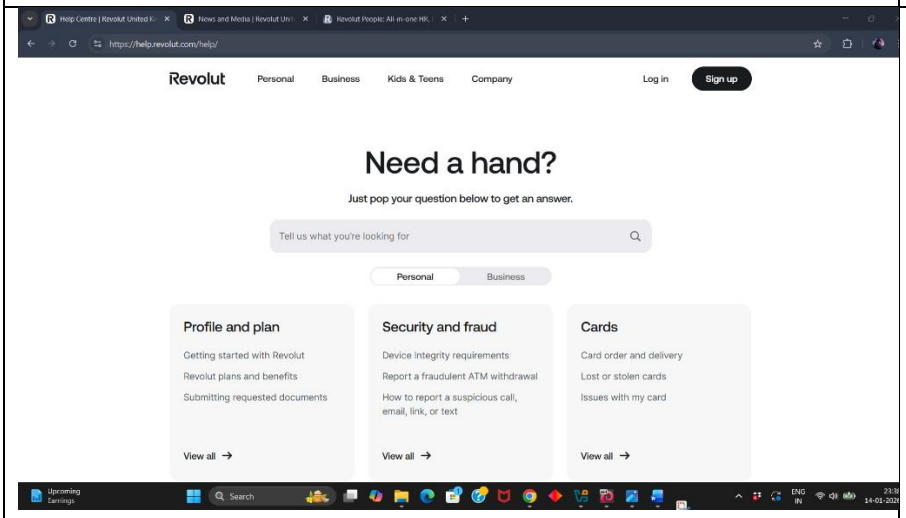
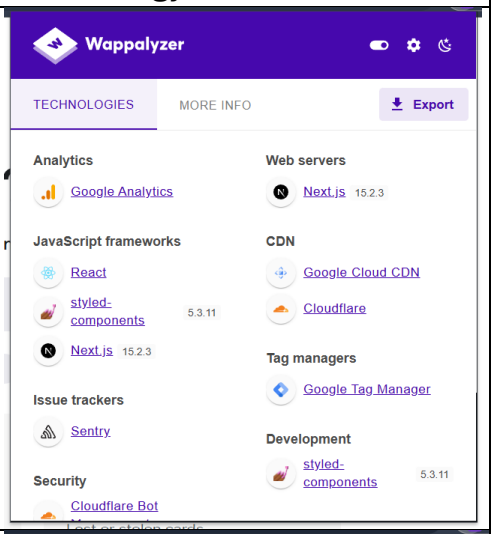
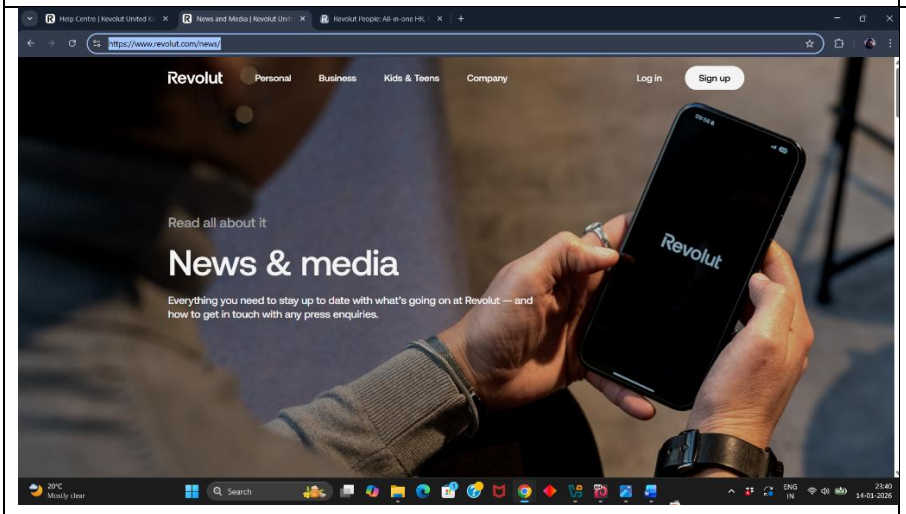
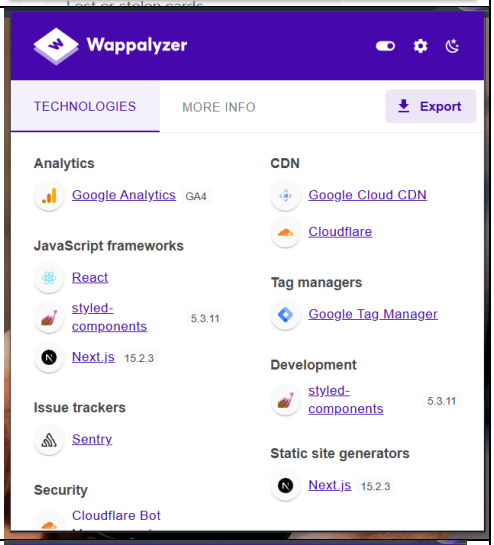
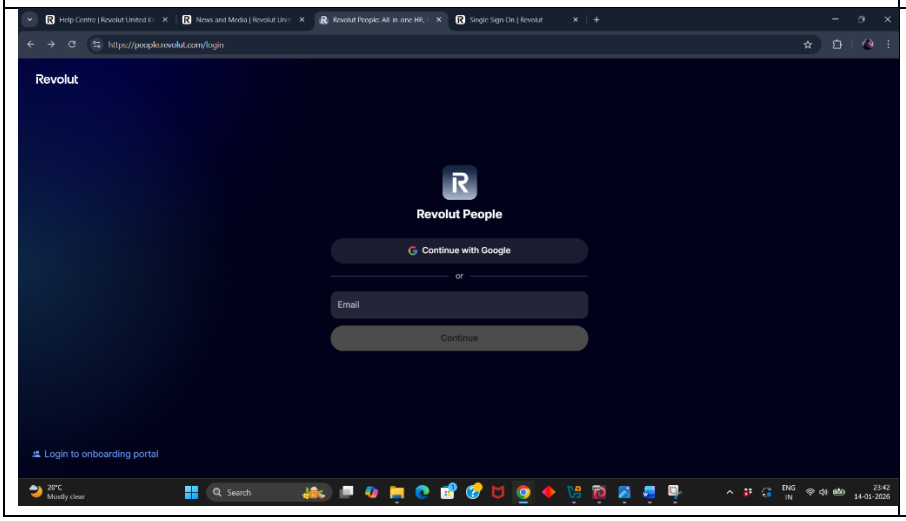
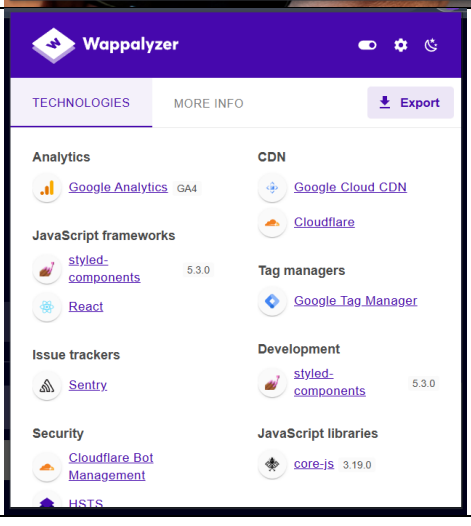
Command: amass enum -d revolut.com

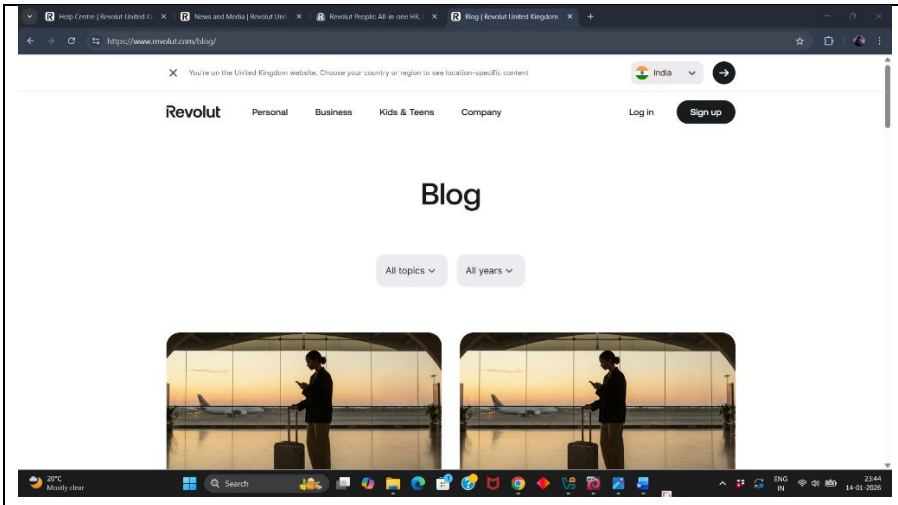
- Purpose of Using Amass: Amass is used to discover subdomains of the main domain.

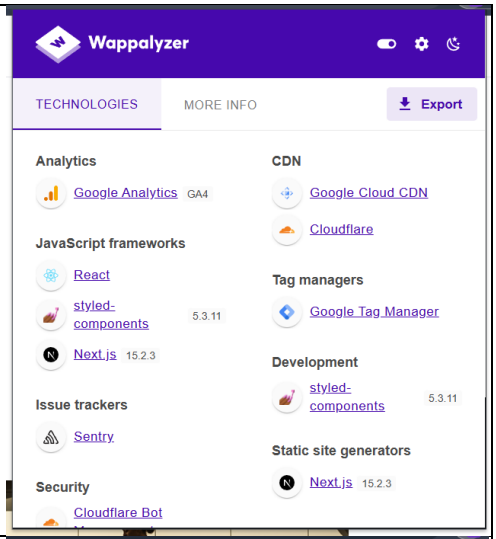


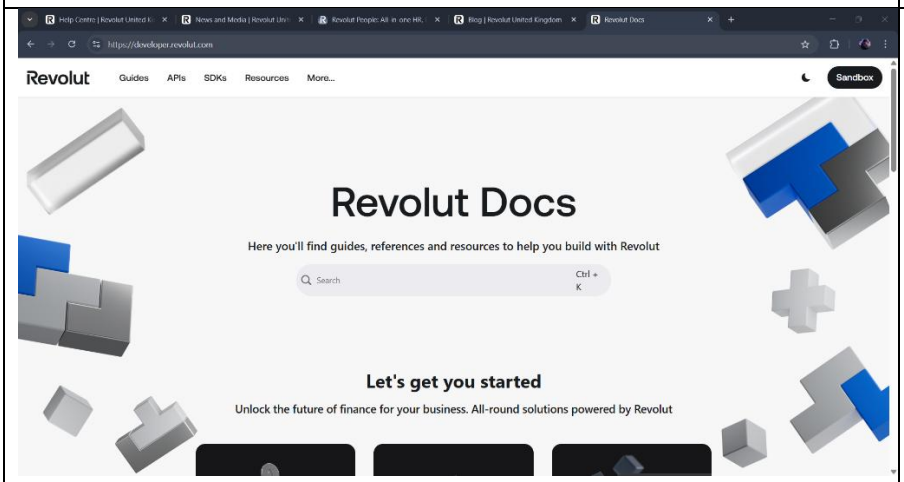
8. Technology Stack on Subdomains

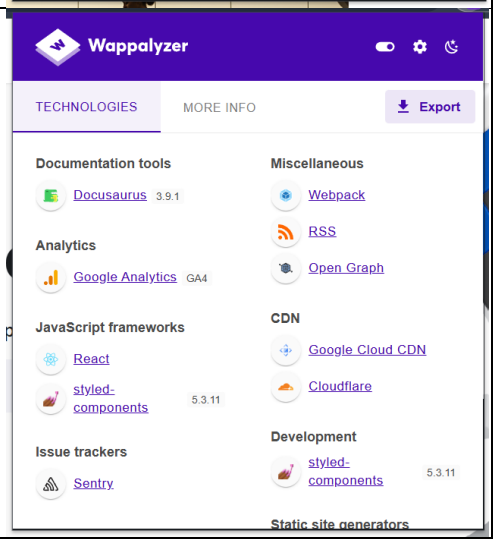
- Five selected subdomains were analysed, and the technology stack used on each subdomain was identified.

Subdomain	Technology
	
	
	


Revolut
Personal
Business
Kids & Teens
Company
Log in
Sign up
Blog
All topics
All years


Wappalyzer
TECHNOLOGIES
MORE INFO
Export
Analytics
Google Analytics GA4
JavaScript frameworks
React
styled-components 5.3.11
Next.js 15.2.3
Issue trackers
Sentry
Security
Cloudflare Bot
CDN
Google Cloud CDN
Cloudflare
Tag managers
Google Tag Manager
Development
styled-components 5.3.11
Static site generators
Next.js 15.2.3


Revolut
Guides
APIs
SDKs
Resources
More...
Sandbox
Revolut Docs
Here you'll find guides, references and resources to help you build with Revolut
Search
Ctrl + K
Let's get you started
Unlock the future of finance for your business. All-round solutions powered by Revolut

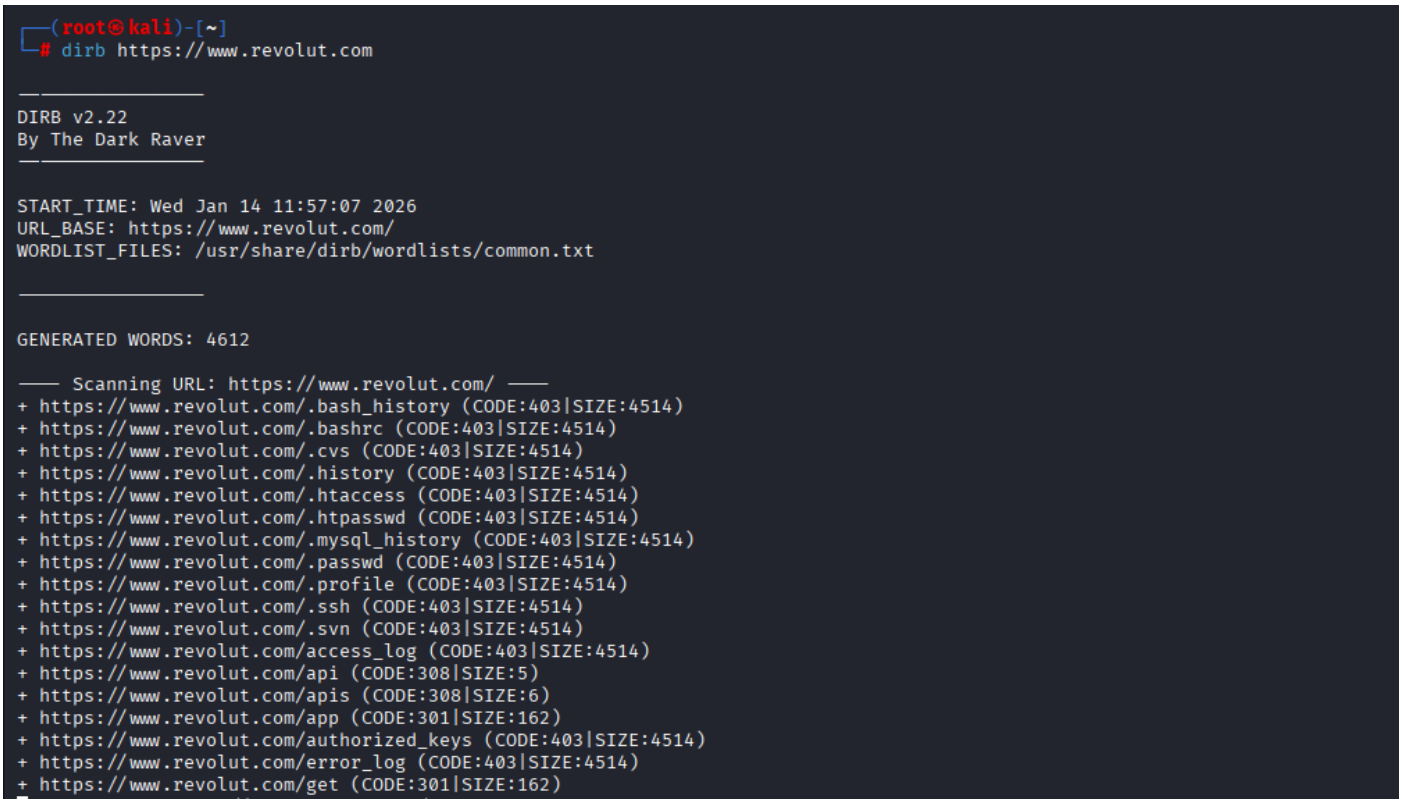

Wappalyzer
TECHNOLOGIES
MORE INFO
Export
Documentation tools
Docusaurus 3.9.1
Analytics
Google Analytics GA4
JavaScript frameworks
React
styled-components 5.3.11
Issue trackers
Sentry
Miscellaneous
Webpack
RSS
Open Graph
CDN
Google Cloud CDN
Cloudflare
Development
styled-components 5.3.11
Static site generators

9. Directory Enumeration

Tool Used: Dirb

Command: dirb https://revolut.com

- Purpose of Using DIRB : DIRB is used to identify hidden or non-obvious directories and files on the main domain of the company



Directory enumeration was limited to the main domain only.

CONCLUSION

This project demonstrated how reconnaissance techniques are used in bug bounty programs to gather information about a target organization. All activities were performed ethically and strictly within the defined scope of the Vulnerability Disclosure Program.

ETHICS & DISCLAIMER (VERY IMPORTANT)

This project was conducted strictly for educational purposes. No exploitation, attack, or unauthorized access was performed. All reconnaissance activities complied with the rules of the Vulnerability Disclosure Program.

REFERENCES

- ♦ Revolut official website
- ♦ Intigriti VDP page
- ♦ Kali Linux