

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

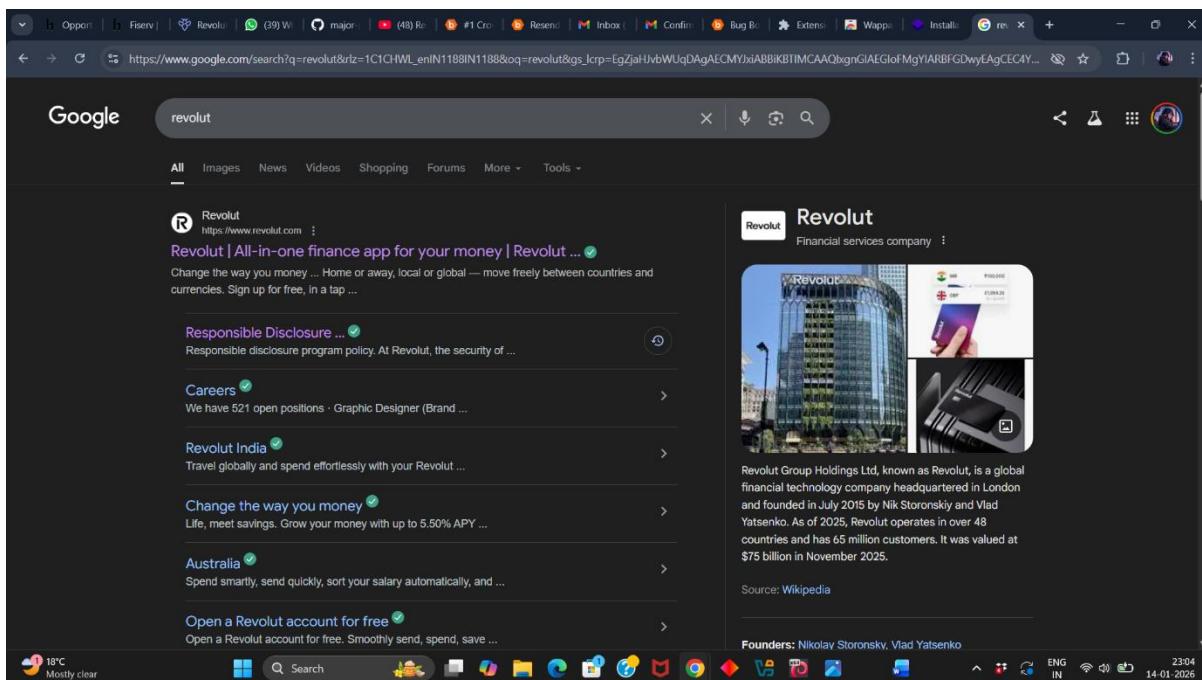
This project focuses on reconnaissance activities performed on the assigned company Revolut as part of a Bug Bounty Reconnaissance Assignment. The objective of this project is to understand how ethical hackers gather information about a target organization while strictly following legal and ethical guidelines.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

COMPANY OVERVIEW

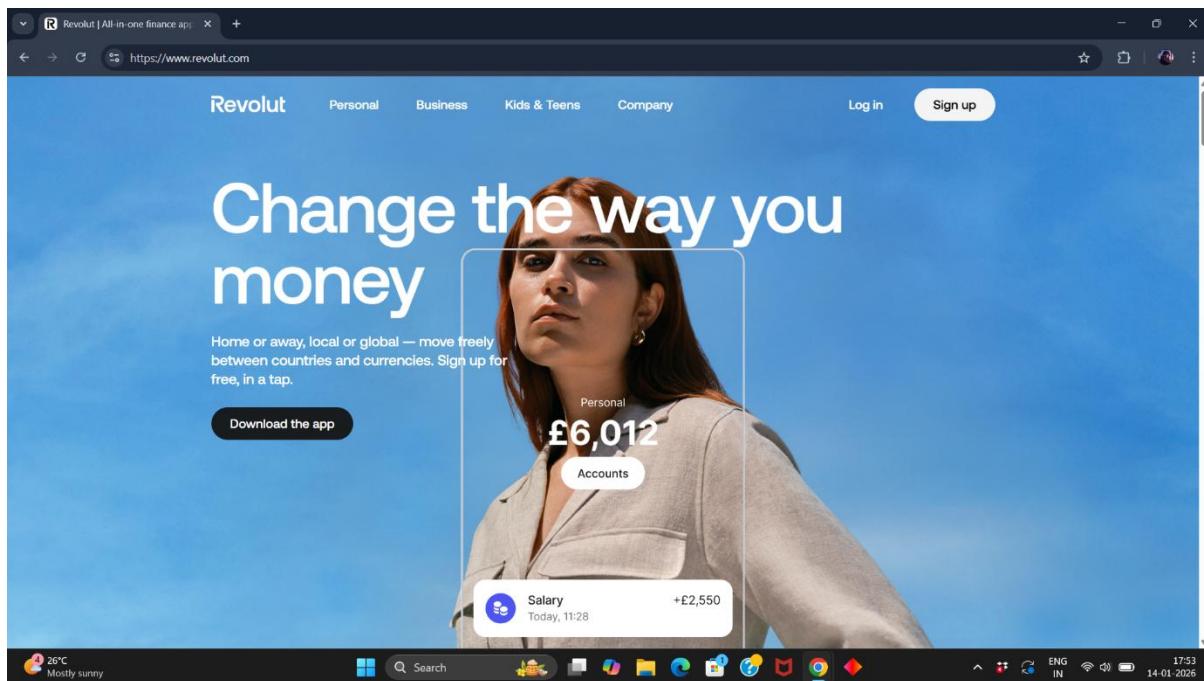
Revolut is a global financial technology company providing digital banking and payment services. It offers services such as international money transfers, cards, and mobile banking.

1. Identify the company's Main Domain

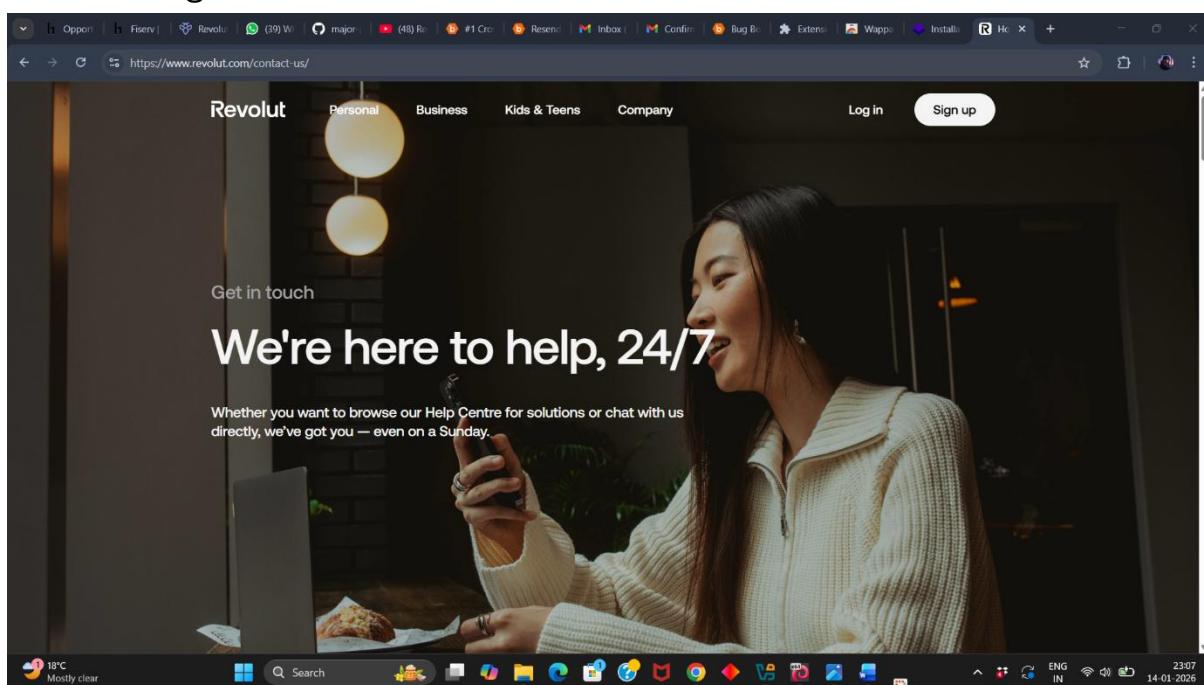
- ◆ Google Search



◆ 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

At Revolut, the security of our users' data is our priority. The purpose of this page (the "Responsible Disclosure Program") is to provide you with all the information you need if you have discovered or believe to have discovered a potential vulnerability in any of our services.

We are committed to ensuring our security is top tier and really appreciate the help of our community to achieve this. To make sure that any disclosures are made responsibly please ensure you follow the terms below:

- All submissions should be made through the Intigriti platform, you will need to register on the platform by using the link at the bottom of this page.
- Please make sure that any disclosures are made as soon as possible. Not only will this help in resolving security issues in a timely fashion but help ensure that you are the first to get any reward (if applicable).
- All rewards will be in the form of Intigriti reputation points and managed by Intigriti in accordance with their terms and conditions. More information can be found here - <https://kb.intigriti.com/en/articles/3379630-leaderboard-reputation-and-streak>.
- Public disclosures of any vulnerabilities (e.g. through social media or the press) can put our community at risk so please make sure you keep this confidential. All disclosures should be made in accordance with this Responsible Disclosure Program so that we can focus on resolving any issues as soon as possible. We reserve our right to take legal action or withhold rewards if this is not followed.
- If you do discover a vulnerability and come into possession of personal data about Revolut customers or employees you must ensure this is deleted as soon as you have made the disclosure through the form below. Personal data is any information that can

- ◆ Intigriti Page

Rules of engagement

@intigriti.me	User agent
Not applicable	Not applicable
Automated tooling	Request header
max. 2 requests /sec	Not applicable

By participating in this program, you agree to:

- Respect the [Community Code of Conduct](#)
- Respect the Intigriti [Terms and Conditions](#)
- Respect the scope of the program
- Never use or target accounts you don't have explicit permission to do so with
- Not discuss or disclose vulnerability information without prior written consent

Safe harbour for researchers is applied

Last 90 day response times

Avg. Time First Response	< 5 days
Avg. Time to Triage	< 1 week
Avg. Time to Decide	

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

◆ In Scope

The screenshot shows the INTEGRITI platform interface for the Revolut VDP bug bounty program. On the left, there's a sidebar with sections for 'In scope' and 'Out of scope'. The 'In scope' section contains an 'Introduction' and a 'Feedback' section. The 'Introduction' section includes a note about reports falling within the scope being transferred for reward. The 'Feedback' section has a link to a program feedback form. On the right, there's a timeline of activity logs:

- 12/2 u_vk created a submission
- 11/24 Revolut closed a submission
- 11/24 Revolut closed a submission
- 11/23 erimv created a submission

◆ Out scope

The screenshot shows the 'Out of scope' section of the INTEGRITI platform for the Revolut VDP bug bounty program. It lists several categories of issues that are not considered valid vulnerabilities:

- General**
 - In case that a reported vulnerability was already known to the company from their own tests, it will be flagged as a duplicate.
 - Theoretical security issues with no realistic exploit scenario(s) or attack surfaces.
 - Issues based upon social engineering or physical access to a victim's device.
 - Attacks requiring person-in-the-middle or compromised user accounts.
 - DoS/DDoS attacks.
 - Reports that state that software is out of date/vulnerable without a proof-of-concept.
 - Cloud credentials / keys without proving exploitability.
 - API key leakage used for insensitive activities/actions.
 - Verbose messages / files / directory listings without disclosing any sensitive information.
 - Anything related to email spoofing, SPF, DMARC or DKIM.
- Web Applications and APIs**
 - API key disclosure without proven business impact.
 - Pre-Auth Account takeover / OAuth squatting.
 - Self-XSS that cannot be used to exploit other users.
 - CORS misconfiguration on non-sensitive endpoints.
 - Missing cookie flags (`HttpOnly`, `Secure`, `SameSite`, etc.).
 - Misconfigurations in cloud services like AWS Lambda, CloudFront, S3, etc.

Opportunity Discover | Fiserv | Vulnerability | Revolut VDP - Bug Bu... | (41) WhatsApp | major-project/tanma | How Do I Contact Re... | (47) Recon to Master | +

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 URLs leaked because a malicious app has permission to view URLs opened

Opportunity Discover | Fiserv | Vulnerability | Revolut VDP - Bug Bu... | (41) WhatsApp | major-project/tanma | How Do I Contact Re... | (47) Recon to Master | +

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 URLs leaked because a malicious app has permission to view URLs 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

The screenshot shows the Intigriti platform interface. At the top, there are tabs for Opportunities, Fiserv, Requests, major..., (48) Resolved, #1 Cro..., Resend, Inbox, Confirm, Bug Bounty, Extens..., Wappo, Install..., How Do..., and a plus sign. The URL is https://app.intigriti.com/programs/revolut/revolutvdp/detail.

The main content area displays the following information:

- max. 2 requests /sec** (highlighted in red)
- Not applicable**
- By participating in this program, you agree to:**
 - Respect the [Community Code of Conduct](#)
 - Respect the Intigriti [Terms and Conditions](#)
 - Respect the scope of the program
 - Never use or target accounts you don't have explicit permission to do so with
 - Not discuss or disclose vulnerability information without prior written consent
- Safe harbour for researchers is applied**

Revolut considers ethical hacking activities conducted consistent with the Researcher Guidelines, the Program description and restrictions (the Terms) to constitute "authorized" conduct under criminal law. Revolut will not pursue civil action or initiate a complaint for accidental, good faith violations, nor will they file a complaint for circumventing technological measures used by us to protect the scope as part of your ethical hacking activities.

If legal action is initiated by a third party against you and you have complied with the Terms, Revolut will take steps to make it known that your actions were conducted in compliance and with our approval.
- View changes**
- Last 90 day response times**

Avg. Time First Response	Avg. Time to Triage
< 5 days	< 1 week
- Avg. Time to Decide**

Avg. Time to Decide
< 5 days
- Activity**

Date	Action
1/12	Revolut accepted a submission
1/8	toborrm9 created a submission
12/31	Revolut closed a submission
12/30	grimar created a submission
12/4	Revolut closed a submission

4. Ping the Main Domain

RECONNAISSANCE STEPS (MOST IMPORTANT PART)

Command used: ping revolute.com

```
Session Actions Edit View Help
[root@kali]-[~]
# ping revolut.com
PING revolut.com (172.66.0.231) 56(84) bytes of data.
64 bytes from 172.66.0.231: icmp_seq=1 ttl=255 time=61.0 ms
64 bytes from 172.66.0.231: icmp_seq=2 ttl=255 time=58.1 ms
64 bytes from 172.66.0.231: icmp_seq=3 ttl=255 time=44.5 ms
64 bytes from 172.66.0.231: icmp_seq=4 ttl=255 time=51.1 ms
64 bytes from 172.66.0.231: icmp_seq=5 ttl=255 time=42.4 ms
64 bytes from 172.66.0.231: icmp_seq=6 ttl=255 time=49.9 ms
64 bytes from 172.66.0.231: icmp_seq=7 ttl=255 time=58.9 ms
64 bytes from 172.66.0.231: icmp_seq=8 ttl=255 time=47.7 ms
64 bytes from 172.66.0.231: icmp_seq=9 ttl=255 time=56.1 ms
64 bytes from 172.66.0.231: icmp_seq=10 ttl=255 time=43.8 ms
^C
--- revolut.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9022ms
rtt min/avg/max/mdev = 42.358/51.352/60.982/6.462 ms
```

◆ IP Address – 172.66.0.231

5. Technology Stack Identification

Tool Used: Wappalyzer

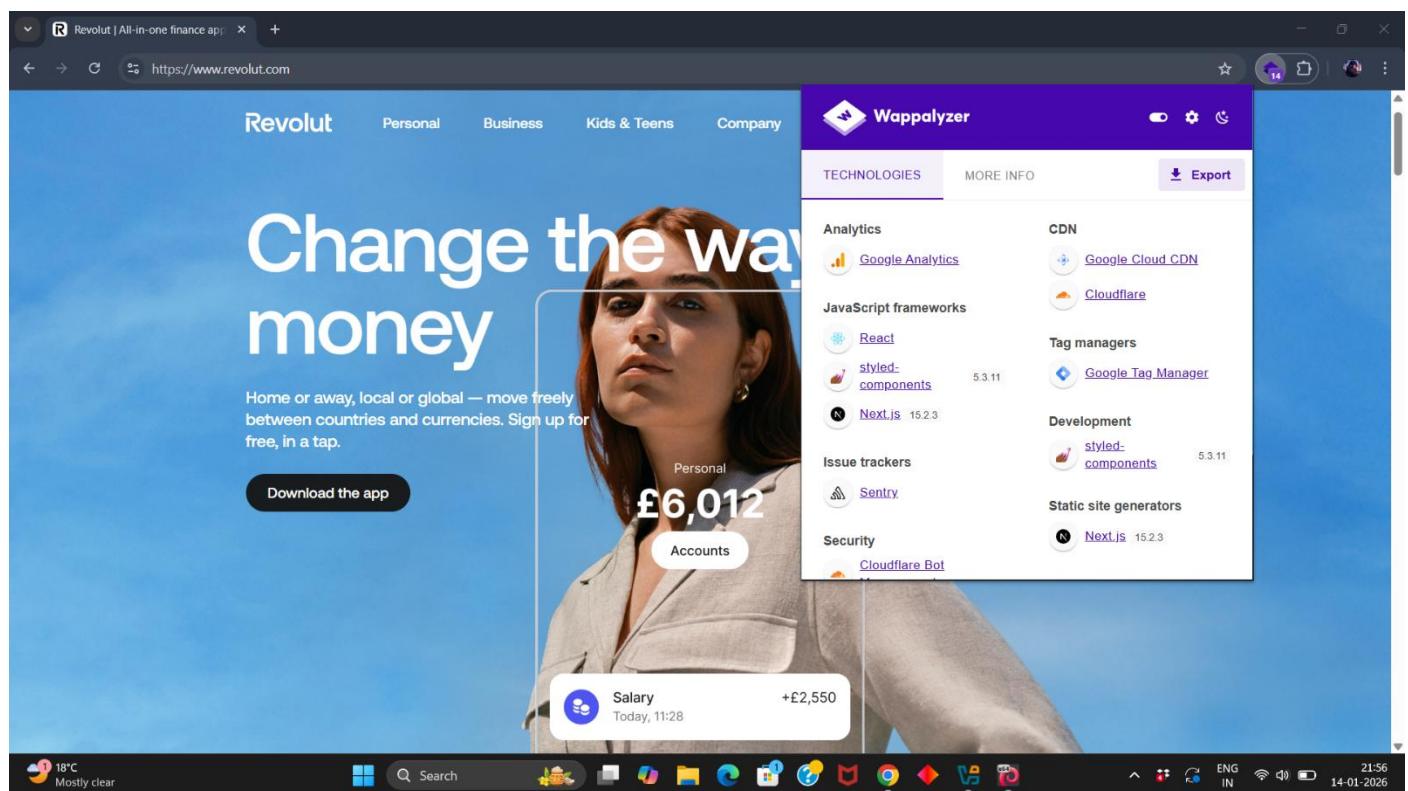
Observation: The main domain uses modern web technologies.

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 Range 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)

```
(root㉿kali)-[~]
# dig revolut.com

; <>> DiG 9.20.11-4+b1-Debian <>> revolut.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 29504
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;revolut.com.           IN      A
;
;; ANSWER SECTION:
revolut.com.          69      IN      A      172.66.0.231
revolut.com.          69      IN      A      162.159.140.233
;
;; Query time: 308 msec
;; SERVER: 10.253.28.152#53(10.253.28.152) (UDP)
;; WHEN: Wed Jan 14 11:29:49 EST 2026
;; MSG SIZE  rcvd: 72
```

Command used: whois 172.66.0.231

```
root@kali:[~]
# whois 172.66.0.231

#
# 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.
#

NetRange:      172.64.0.0 - 172.71.255.255
CIDR:         172.64.0.0/13
NetName:       CLOUDFLARENET
NetHandle:     NET-172-64-0-0-1
Parent:        NET172 (NET-172-0-0-0-0)
NetType:       Direct Allocation
OriginAS:
Organization:  Cloudflare, Inc. (CLOUD14)
RegDate:      2015-02-25
Updated:       2024-09-04
Comment:      All Cloudflare abuse reporting can be done via https://www.cloudflare.com/abuse
Comment:      Geofeed: https://api.cloudflare.com/local-ip-ranges.csv
Ref:          https://rdap.arin.net/registry/ip/172.64.0.0
```

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

7. Subdomain Enumeration

Tool Used: Amass

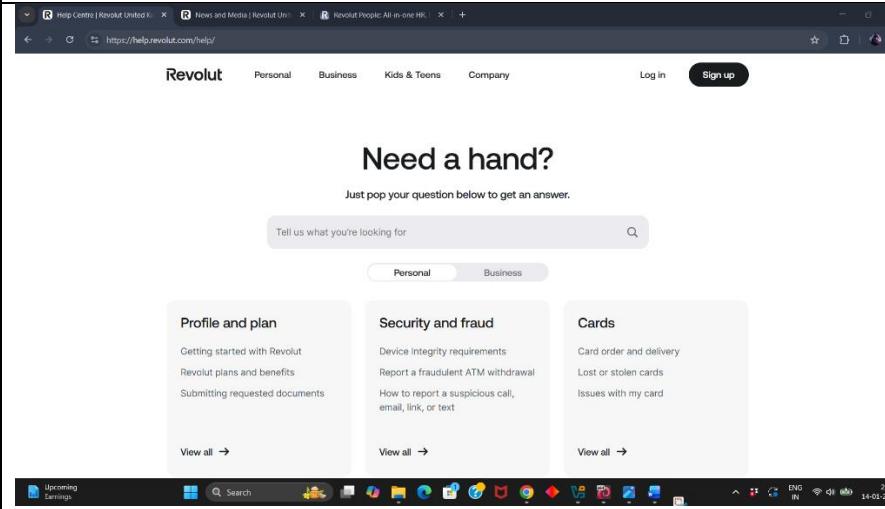
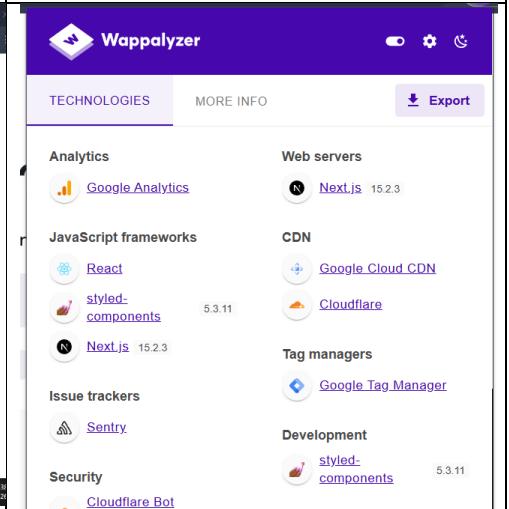
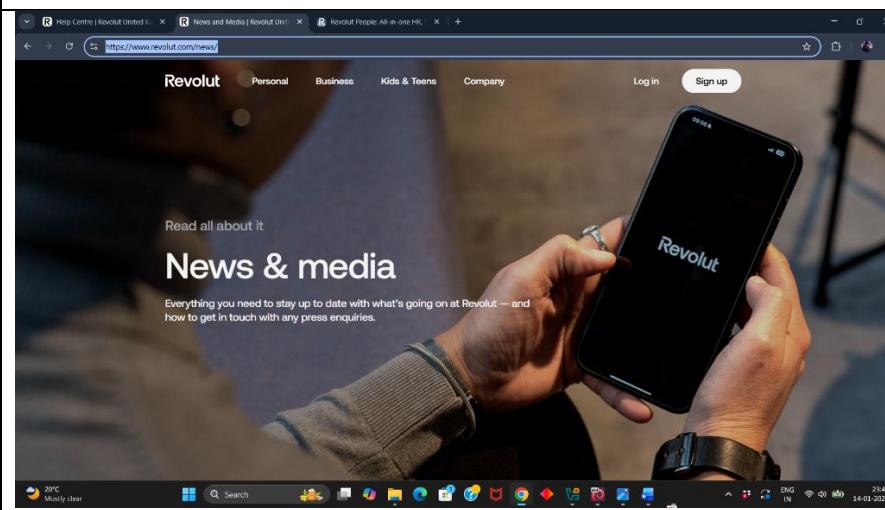
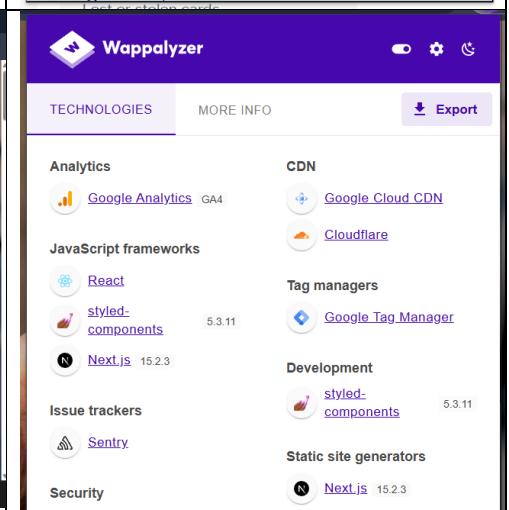
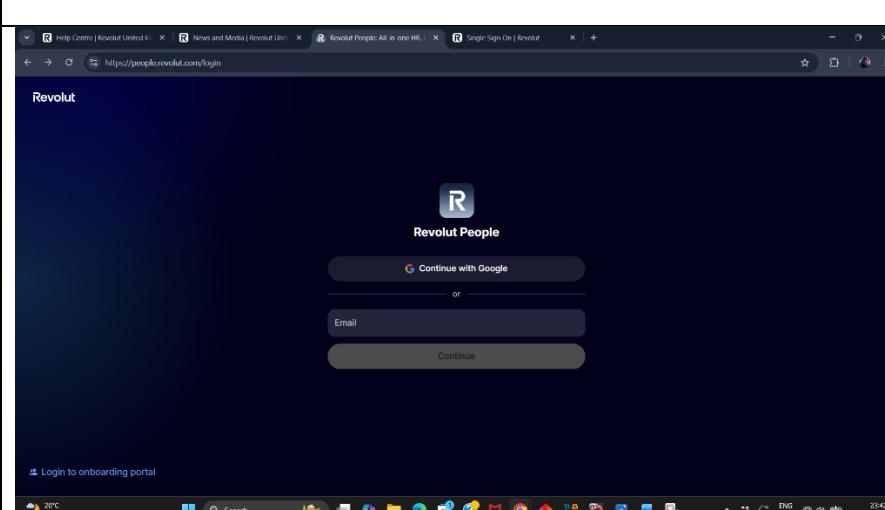
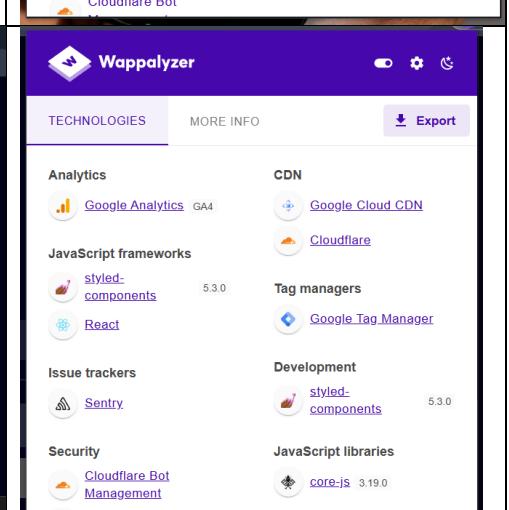
Command: `amass enum -d revolut.com`

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

```
[root@kali:~]# amass enum -d revolut.com
revolut.com (FQDN) → mx_record → alt2.aspmx.l.google.com (FQDN)
revolut.com (FQDN) → mx_record → alt4.aspmx.l.google.com (FQDN)
revolut.com (FQDN) → mx_record → aspmx.l.google.com (FQDN)
revolut.com (FQDN) → mx_record → alt1.aspmx.l.google.com (FQDN)
revolut.com (FQDN) → mx_record → alt3.aspmx.l.google.com (FQDN)
revolut.com (FQDN) → ns_record → ns-cloud-d4.google domains.com (FQDN)
revolut.com (FQDN) → ns_record → ns-cloud-d1.google domains.com (FQDN)
revolut.com (FQDN) → ns_record → ns-cloud-d3.google domains.com (FQDN)
revolut.com (FQDN) → ns_record → ns-cloud-d2.google domains.com (FQDN)
alt2.aspmx.l.google.com (FQDN) → a_record → 172.217.78.26 (IPAddress)
alt2.aspmx.l.google.com (FQDN) → aaaa_record → 2607:f8b0:4023:1c05::1b (IPAddress)
alt4.aspmx.l.google.com (FQDN) → a_record → 192.178.218.26 (IPAddress)
alt4.aspmx.l.google.com (FQDN) → aaaa_record → 2607:f8b0:4023:2009::1b (IPAddress)
aspmx.l.google.com (FQDN) → a_record → 74.125.68.27 (IPAddress)
aspmx.l.google.com (FQDN) → aaaa_record → 2404:6800:4003:c03::1a (IPAddress)
alt1.aspmx.l.google.com (FQDN) → a_record → 172.253.130.26 (IPAddress)
alt1.aspmx.l.google.com (FQDN) → aaaa_record → 2607:f8b0:400e:c17::1a (IPAddress)
alt3.aspmx.l.google.com (FQDN) → a_record → 108.177.11.26 (IPAddress)
alt3.aspmx.l.google.com (FQDN) → aaaa_record → 2607:f8b0:4023:c06::1b (IPAddress)
drive.revolut.com (FQDN) → cname_record → ghs.googlehosted.com (FQDN)
www.revolut.com (FQDN) → cname_record → www.revolut.com.cdn.cloudflare.net (FQDN)
pl.revolut.com (FQDN) → a_record → 199.36.158.100 (IPAddress)
data-portal.revolut.com (FQDN) → a_record → 34.111.94.67 (IPAddress)
growth.revolut.com (FQDN) → cname_record → go.pardot.com (FQDN)
in-aqueduct.revolut.com (FQDN) → a_record → 34.107.151.113 (IPAddress)
bmrvpnclient.revolut.com (FQDN) → a_record → 92.82.180.114 (IPAddress)
trustcentre.revolut.com (FQDN) → cname_record → trustcentre.revolut.com.cdn.cloudflare.net (FQDN)
chat.revolut.com (FQDN) → cname_record → chat.revolut.com.cdn.cloudflare.net (FQDN)
news.revolut.com (FQDN) → cname_record → news.revolut.com.cdn.cloudflare.net (FQDN)
pos.revolut.com (FQDN) → cname_record → pos.revolut.com.cdn.cloudflare.net (FQDN)
pay.revolut.com (FQDN) → a_record → 34.149.61.165 (IPAddress)
enterpriseregistration.revolut.com (FQDN) → cname_record → enterpriseregistration.windows.net (FQDN)
ideal.revolut.com (FQDN) → a_record → 35.227.205.174 (IPAddress)
skywalker.revolut.com (FQDN) → a_record → 34.120.122.151 (IPAddress)
oba-br.revolut.com (FQDN) → cname_record → ingress.saas.oof.opus-software.com.br (FQDN)
invest.revolut.com (FQDN) → cname_record → invest.revolut.com.cdn.cloudflare.net (FQDN)
sso.revolut.com (FQDN) → cname_record → sso.revolut.com.cdn.cloudflare.net (FQDN)
community.revolut.com (FQDN) → cname_record → community.revolut.com.cdn.cloudflare.net (FQDN)
aqueduct.revolut.com (FQDN) → a_record → 34.36.148.157 (IPAddress)
api.revolut.com (FQDN) → a_record → 35.201.77.50 (IPAddress)
revolut.com (FQDN) → a_record → 162.159.140.233 (IPAddress)
revolut.com (FQDN) → a_record → 172.66.0.231 (IPAddress)
tails.revolut.com (FQDN) → a_record → 34.120.173.100 (IPAddress)
sandbox-merchant.revolut.com (FQDN) → cname_record → sandbox-merchant.revolut.com.cdn.cloudflare.net (FQDN)
help.revolut.com (FQDN) → cname_record → help.revolut.com.cdn.cloudflare.net (FQDN)
ametist.revolut.com (FQDN) → a_record → 34.111.147.97 (IPAddress)
forms.revolut.com (FQDN) → cname_record → forms.revolut.com.cdn.cloudflare.net (FQDN)
```

8. Technology Stack on Subdomains

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

Subdomain	Technology
	
	
	

You're on the United Kingdom website. Choose your country or region to see location-specific content.

India

Log in Sign up

Blog

All topics All years

Help Centre | Revolut United Kingdom | News and Media | Revolut United Kingdom | Revolut People: All in one HR | Blog | Revolut United Kingdom | Revolut Docs

20°C Mostly clear Search 23:44 14-01-2026

Revolut Guides APIs SDKs Resources More...

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

Sandbox

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

Miscellaneous

- Docusaurus 3.9.1
- Webpack
- RSS
- Open Graph

JavaScript frameworks

- React
- styled-components 5.3.11

Issue trackers

- Sentry

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

```
[root@kali] ~
# dirb https://www.revolut.com

_____
DIRB v2.22
By The Dark Raver
_____

START_TIME: Wed Jan 14 11:57:07 2026
URL_BASE: https://www.revolut.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
_____
GENERATED WORDS: 4612

_____
Scanning URL: https://www.revolut.com/
+ https://www.revolut.com/.bash_history (CODE:403|SIZE:4514)
+ https://www.revolut.com/.bashrc (CODE:403|SIZE:4514)
+ https://www.revolut.com/.cvs (CODE:403|SIZE:4514)
+ https://www.revolut.com/.history (CODE:403|SIZE:4514)
+ https://www.revolut.com/.htaccess (CODE:403|SIZE:4514)
+ https://www.revolut.com/.htpasswd (CODE:403|SIZE:4514)
+ https://www.revolut.com/.mysql_history (CODE:403|SIZE:4514)
+ https://www.revolut.com/.passwd (CODE:403|SIZE:4514)
+ https://www.revolut.com/.profile (CODE:403|SIZE:4514)
+ https://www.revolut.com/.ssh (CODE:403|SIZE:4514)
+ https://www.revolut.com/.svn (CODE:403|SIZE:4514)
+ https://www.revolut.com/.access_log (CODE:403|SIZE:4514)
+ https://www.revolut.com/api (CODE:308|SIZE:5)
+ https://www.revolut.com/apis (CODE:308|SIZE:6)
+ https://www.revolut.com/app (CODE:301|SIZE:162)
+ https://www.revolut.com/authorized_keys (CODE:403|SIZE:4514)
+ https://www.revolut.com/error_log (CODE:403|SIZE:4514)
+ https://www.revolut.com/get (CODE:301|SIZE:162)
```

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