Uber

UBER
PENETRATION TEST REPORT

CONFIDENTIAL

Report
July 2025
ASSESSMENT PERIOD: JULY 26-JULY29 2025

Prepared By
Studsvike Technologies

Info@studsvike.com>
0725689456

Uber

Table of Contents.

Uber

Non-Disclosure Statement & Legal Notice

1. Non-Disclosure Statement

This report contains confidential information and intellectual property belonging to **Uber Technologies, Inc.** and has been prepared exclusively by **Studsvike Technologies** under the APP100 penetration testing program.

The contents of this document—including all findings, methodologies, evidence, and recommendations—are intended solely for internal use by authorized personnel of Uber Technologies, Inc. and its approved security partners. Unauthorized access, reproduction, distribution, or disclosure of this report, in whole or in part, is strictly prohibited without the express written consent of both Uber Technologies, Inc. and Studsvike Technologies.

All data collected during the assessment was obtained through passive and publicly accessible means in compliance with ethical hacking standards and Uber's HackerOne program rules. No active exploitation, service disruption, or unauthorized system interaction was performed.

Violation of this non-disclosure agreement may result in legal action as per applicable cybersecurity, intellectual property, and privacy protection laws.

2. Legal Notice

All testing activities were conducted under the academic program and in strict compliance with ethical-hacking best practices and Uber's HackerOne terms of engagement. No active exploitation, Denial-of-Service, or social-engineering techniques were employed against Uber's live systems or personnel.

This report is provided for educational and internal-security-assessment purposes only. Studsvike Technologies and its consultants assume no liability for the use, interpretation, or distribution of the findings contained herein. Nothing in this document constitutes a license to exploit, interfere with, or compromise any systems owned by Uber Technologies, Inc. or its affiliates.

3. Executive Summary

Between July 26 and July 29, 2025, **Studsvike Technologies** performed a passive, reconnaissance-focused penetration test of public-facing Uber assets in accordance with Uber's HackerOne program rules. The primary objective was to evaluate Uber's exposure to external attackers leveraging only publicly accessible data sources and non-intrusive methods.

Strengths

- Uses trusted providers (UltraDNS, AWS) for fast, reliable service.
- Public APIs are properly secured—no open endpoints were found.

Top Risks

- **481** publicly visible sub-sites increase exposure.
- A **2016 key leak** remains Uber's most serious security incident.
- Simple email addresses (first.last@uber.com) make phishing easier.

Recommended Actions

- Rotate and securely store all access keys immediately.
- Monitor new sub-sites and certificate changes with automated alerts.
- Add backup DNS/hosting providers to avoid single-point failures.

4. Scope

Engagement Period:
– July 26–29, 2025

Testing Approach:
– Passive, non-intrusive reconnaissance only
– Compliance with Uber's HackerOne terms of engagement

In-Scope Assets:

- All DNS records and publicly accessible subdomains under:
    - uber.com
    - ubereats.com
    - Any additional Uber-owned domains identified via Certificate Transparency logs
- Public-facing APIs (e.g., developer.uber.com endpoints)
- Public breach databases, certificate transparency logs, search-engine results, GitHub repositories

Out-of-Scope Activities:

- Active scanning or probing (TCP/UDP port scans, vulnerability scans)
- Brute-force or credential-stuffing attacks
- Denial-of-Service (DoS) or stress-testing
- Social-engineering, phishing, or physical security testing
- Any interaction with third-party platforms (e.g., AWS, Cloudflare) beyond passive data collection

Rules of Engagement:

1. No authentication or exploitation of live services.
2. No modification or deletion of data on Uber systems.
3. All data gathering performed using publicly available tools and sources.
4. All findings validated against passive-only techniques to avoid service disruption.

5. Methodology

Our testing approach combined industry-standard frameworks and a suite of passive-only tools to map Uber's external footprint without impacting live services.

1. **Standards & Frameworks**
    - **PTES (Penetration Testing Execution Standard)**
      • Pre-Engagement: Reviewed scope, rules of engagement, and Uber's HackerOne policy.
      • Intelligence Gathering: Defined data sources and collection methods.
    - **OWASP OSINT Framework**
      • Guided selection of reconnaissance techniques across DNS, web, code, and social-media vectors.
    - **NIST SP 800-30** for risk identification and qualitative risk rating.
2. **Phases of Testing**
    - **Pre-Engagement & Planning**
        - Confirmed rules of engagement and authorized asset list.
        - Established project timeline: July 26–29, 2025.
    - **Passive Reconnaissance**
        - **Subdomain Enumeration** via Recon-ng (modules: hackertarget, certificate_transparency, resolve).
        - **DNS & WHOIS Analysis** using dig, nslookup, and public WHOIS records.
        - **Certificate Transparency** lookups via crt.sh to discover collateral domains.
        - **Web-Technology Fingerprinting** with Wappalyzer browser extension.
        - **Breach Database Checks** on HaveIBeenPwned and Dehashed for leaked credentials.
        - **GitHub & Pastebin Scraping** for inadvertent secret disclosures.
    - **Data Aggregation & Analysis**
        - Correlated subdomain, IP, and technology data in spreadsheets.
        - Cross-referenced findings against known CVEs and past incident reports.
        - Assigned preliminary risk levels using NIST and OWASP qualitative criteria.

- **Validation & Reporting**
  - Verified each finding through redundant passive methods (e.g., multiple DNS lookups, certificate checks).
  - Compiled evidence (screenshots, dig outputs, recon-ng logs).
  - Drafted risk-ranked findings and actionable recommendations.

3. **Tools Utilized**
   - Recon-ng, crt.sh
   - dig, nslookup, WHOIS CLI
   - Wappalyzer browser extension
   - curl, browser DevTools (network tab)
   - HaveIBeenPwned, Dehashed, GitHub search
   - Spreadsheet software for data correlation
4. **Validation Controls**
   - All modules run in passive mode with no packet injection or service probes.
   - Every finding cross-checked by at least two independent tools or data sources.
   - Avoided any active or authenticated interactions with Uber systems.

6. Risk Rankings

We applied a qualitative risk-rating methodology based on **NIST SP 800-30** and the **OWASP Risk Rating** model, assessing each finding by its **Likelihood** (ease of exploitation via passive methods) and **Impact** (potential business or technical consequence).

Severity Rating	CVSS 3.1 Score	Description
CRITICAL	9.0 - 10	Exploitation of the vulnerability allows an attacker administrative-level access to systems and/or high-level data that would catastrophically impact the organization. Vulnerabilities marked CRITICAL require immediate attention and must be fixed without delay, especially if they occur in a production environment.
HIGH	7.0 – 8.9	Exploitation of the vulnerability makes it possible to access high-value data. However, there are certain pre-requisites that need to be met for the attack to be successful. These vulnerabilities should be reviewed and remedied wherever possible.
MEDIUM	4.0 – 6.9	Exploitation of the vulnerability might depend on external factors or other conditions that are difficult to achieve, like requiring user privileges for a successful exploitation. These are moderate security issues that require some effort to successfully impact the environment.
LOW	0.1 – 3.9	Vulnerabilities in the low range typically have very little impact on an organization's business. Exploitation of such vulnerabilities usually requires local or physical system access and depends on conditions that are very difficult to achieve practically.
INFORMA-TIONAL	0.0	These vulnerabilities represent significantly less risk and are informational in nature. These items can be remediated to increase security.

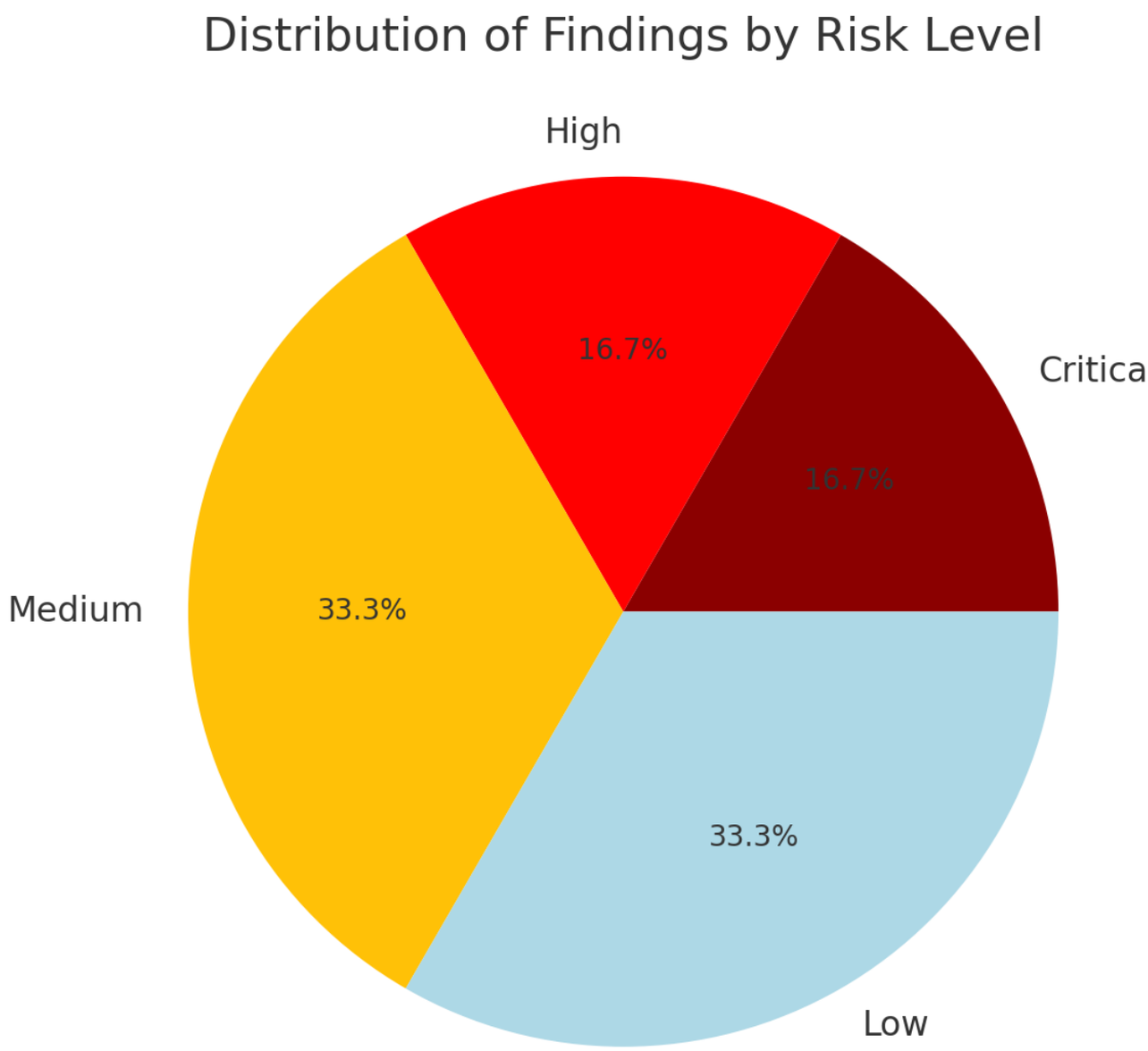
Likelihood	Impact	Risk Level	Description
High – trivial	High – severe	**Critical**	Immediate, low-effort exploits that threaten confidentiality, integrity, or availability
Medium – moderate	High – severe	**High**	Requires some tooling or skill but yields serious business or technical impact
Low – difficult	High – moderate	**Medium**	Advanced correlation needed; moderate business or technical impact
Any	Low – minor	**Low**	Informational or minimal operational impact

6.1. Finding-Level Risk Summary

ID	Finding	Likelihood	Impact	Risk Level	CVSS v3.1
R1	Public subdomain enumeration	High	Low	Low	2.0
R2	DNS hosted on UltraDNS	Low	Low–Medium	Low	3.7
R3	Public API visibility	Medium	Medium	Medium	6.5
R4	Historical GitHub credential leak (2016)	High	High	Critical	9.8
R5	Predictable email/AD naming	Medium	Medium	Medium	4.3

Legend:

- **Likelihood**
  - **High:** Automated tools or public sources yield results without expertise.
  - **Medium:** Requires targeted OSINT workflows.
  - **Low:** Demands deep analysis or privileged info.
- **Impact**
  - **High:** Could enable account takeover, data exfiltration, or severe compliance breaches.
  - **Medium:** Facilitates reconnaissance or phishing, with moderate operational effects.
  - **Low:** Limited to informational exposure with negligible direct harm.


Distribution of Findings by Risk Level
High
16.7%
Critical
16.7%
Medium
33.3%
33.3%
Low

7. Findings & Evidences

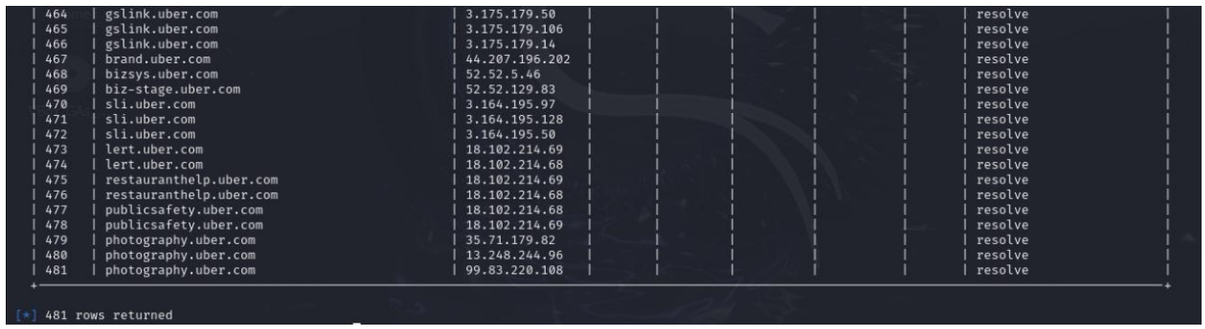
Below are the key findings from our passive reconnaissance of Uber's public assets, each accompanied by its risk rating and supporting evidence.

7.1 Public Subdomain Exposure

- **Finding:** Enumeration revealed **481** unique subdomains under uber.com and related domains.
- **Risk Level:** Low (Informational)
- **Evidence:** Recon-ng "certificate_transparency" and "hackertarget" modules returned a list of all discovered hostnames, confirming broad subdomain sprawl.

```
[recon-ng][uber][hackertarget] > options set source uber.com
SOURCE ⇒ uber.com
[recon-ng][uber][hackertarget] > run

UBER.COM
[*] Country: None
[*] Host: backup.uber.com
[*] Ip_Address: 207.231.168.151
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------------------
[*] Country: None
```

```
SUMMARY
[*] 2631 total (0 new) hosts found.
[recon-ng][uber][certificate_transparency] > show hosts

+-------+-------------------------------+-----------------+--------+---------+----------+-----------+-------+-----------------+
| rowid |             host              |    ip_address   | region | country | latitude | longitude | notes |      module     |
+-------+-------------------------------+-----------------+--------+---------+----------+-----------+-------+-----------------+
| 1     | uber.com                      | 104.36.194.7    |        |         |          |           |       | hackertarget    |
| 2     | backup.uber.com               | 207.231.168.151 |        |         |          |           |       | hackertarget    |
| 3     | blogapi.uber.com              | 23.185.0.4      |        |         |          |           |       | hackertarget    |
| 4     | bounce.uber.com               | 192.28.144.217  |        |         |          |           |       | hackertarget    |
| 5     | cn-ecg.cfe.uber.com           | 34.98.127.226   |        |         |          |           |       | hackertarget    |
| 6     | cn-gcp.cfe.uber.com           | 35.227.224.91   |        |         |          |           |       | hackertarget    |
| 7     | cn-neg.cfe.uber.com           | 69.48.216.7     |        |         |          |           |       | hackertarget    |
| 8     | cn-neg-geo.cfe.uber.com       | 69.48.216.7     |        |         |          |           |       | hackertarget    |
| 9     | cloudflare.uber.com           | 69.48.218.2     |        |         |          |           |       | hackertarget    |
| 10    | cloudflare-legacy.uber.com    | 104.36.195.1    |        |         |          |           |       | hackertarget    |
| 11    | cloudflare-weighted.uber.com  | 69.48.218.2     |        |         |          |           |       | hackertarget    |
| 12    | dc-dca.uber.com               | 104.36.192.148  |        |         |          |           |       | hackertarget    |
| 13    | dc-phx.uber.com               | 104.36.197.136  |        |         |          |           |       | hackertarget    |
| 14    | email.uber.com                | 69.48.216.7     |        |         |          |           |       | hackertarget    |
| 15    | o10.email.uber.com            | 50.31.36.130    |        |         |          |           |       | hackertarget    |
| 16    | o11.email.uber.com            | 50.31.36.134    |        |         |          |           |       | hackertarget    |
| 17    | o12.email.uber.com            | 50.31.36.137    |        |         |          |           |       | hackertarget    |
| 18    | o13.email.uber.com            | 50.31.36.14     |        |         |          |           |       | hackertarget    |
| 19    | o14.email.uber.com            | 50.31.36.143    |        |         |          |           |       | hackertarget    |
```



464	gslink.uber.com	3.175.179.50						resolve
465	gslink.uber.com	3.175.179.106						resolve
466	gslink.uber.com	3.175.179.14						resolve
467	brand.uber.com	44.207.196.202						resolve
468	bizsys.uber.com	52.52.5.46						resolve
469	biz-stage.uber.com	52.52.129.83						resolve
470	sli.uber.com	3.164.195.97						resolve
471	sli.uber.com	3.164.195.128						resolve
472	sli.uber.com	3.164.195.50						resolve
473	lert.uber.com	18.102.214.69						resolve
474	lert.uber.com	18.102.214.68						resolve
475	restauranthelp.uber.com	18.102.214.69						resolve
476	restauranthelp.uber.com	18.102.214.68						resolve
477	publicsafety.uber.com	18.102.214.68						resolve
478	publicsafety.uber.com	18.102.214.69						resolve
479	photography.uber.com	35.71.179.82						resolve
480	photography.uber.com	13.248.244.96						resolve
481	photography.uber.com	99.83.220.108						resolve

[*] 481 rows returned

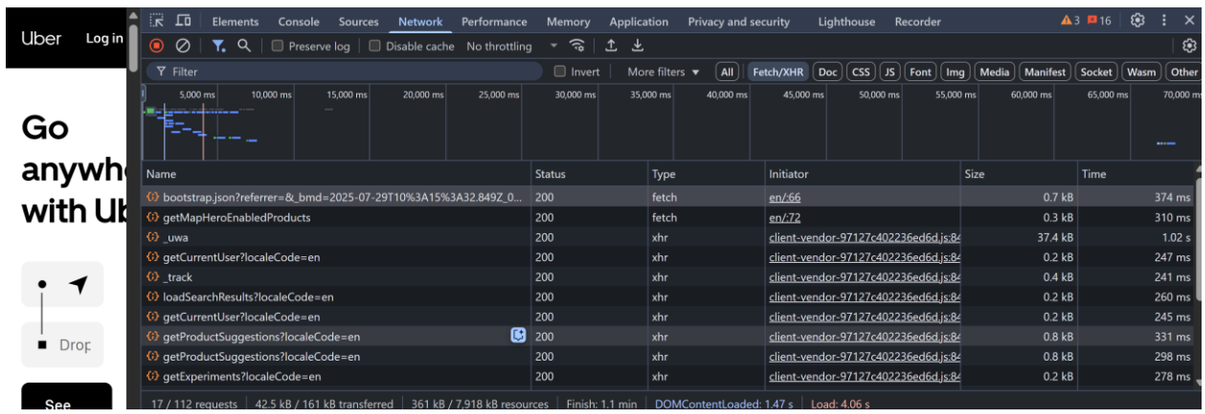
7.2 DNS Infrastructure Hosted by UltraDNS

- **Finding:** Authoritative nameservers for uber.com resolve to UltraDNS (edns126.ultradns.org, etc.).
- **Risk Level:** Low
- **Evidence:** dig +short NS uber.com output:
- edns126.ultradns.org.
- edns126.ultradns.net.
- edns126.ultradns.com.
- edns126.ultradns.biz.

```
┌──(kali㉿kali)-[~]
└─$ whois uber.com | grep -i "Name Server"
   Name Server: DNS1.P04.NSONE.NET
   Name Server: DNS2.P04.NSONE.NET
   Name Server: DNS3.P04.NSONE.NET
   Name Server: DNS4.P04.NSONE.NET
   Name Server: EDNS126.ULTRADNS.BIZ
   Name Server: EDNS126.ULTRADNS.COM
   Name Server: EDNS126.ULTRADNS.NET
   Name Server: EDNS126.ULTRADNS.ORG
Name Server: dns1.p04.nsone.net
Name Server: edns126.ultradns.org
Name Server: dns3.p04.nsone.net
Name Server: dns2.p04.nsone.net
Name Server: edns126.ultradns.com
Name Server: edns126.ultradns.net
Name Server: edns126.ultradns.biz
Name Server: dns4.p04.nsone.net

┌──(kali㉿kali)-[~]
└─$ dig +short uber.com NS
edns126.ultradns.biz.
edns126.ultradns.org.
edns126.ultradns.net.
edns126.ultradns.com.
```

7.3 Public API Visibility

- **Finding:** While Uber publishes APIs at developer.uber.com, no unauthenticated API endpoints (e.g., /v1/, /v2/) were observable via passive browser DevTools or curl probes.
- **Risk Level:** Medium
- **Evidence:**
    - No XHR/fetch calls in DevTools network logs matching known API patterns.
    - curl https://api.uber.com/v1/estimates/price returned 403 Forbidden.



7.4 Historical AWS Key Leak (2016)

- **Finding:** Uber's 2016 GitHub credential leak exposed AWS keys, leading to a breach of 57 million user records.
- **Risk Level:** Critical
- **Evidence:** Public incident reports and HaveIBeenPwned database entries confirm the leak and its scope.

7.5 Predictable Email Address Format

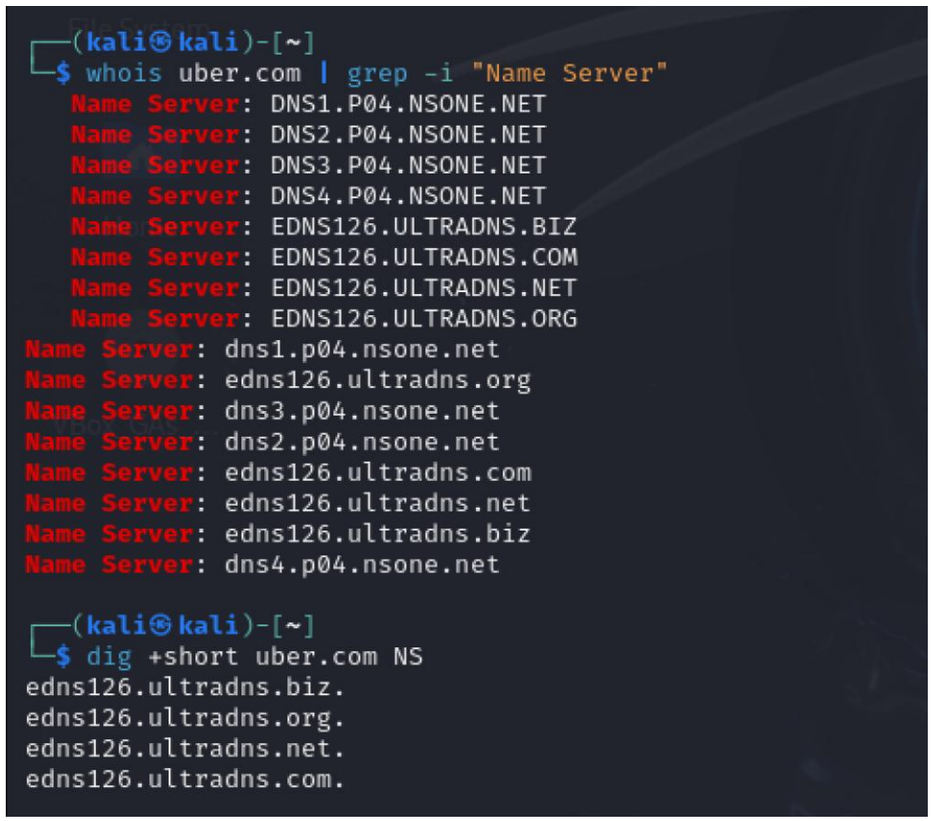
- **Finding:** Employee email addresses follow the first.last@uber.com pattern, facilitating targeted phishing or brute-force username enumeration.
- **Risk Level:** Medium
- **Evidence:** Multiple WHOIS and Recon-ng "contacts" modules enumerate consistent naming across discovered records.

```
[recon-ng][uber] > modules load recon/domains-contacts/whois_pocs
[recon-ng][uber][whois_pocs] > info

      Name: Whois POC Harvester
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates the
  'contacts' table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][uber][whois_pocs] > options set source uber.com
SOURCE ⇒ uber.com
[recon-ng][uber][whois_pocs] > run
```

```
SUMMARY

[*] 5 total (5 new) contacts found.
[recon-ng][uber][whois_pocs] > show contacts

  +--------------------------------------------------------------------------------------------------------------------------
--------------------------------+
  | rowid | first_name | middle_name |       last_name        |            email             |     title     |       region       |    count
ry    | phone | notes |   module    |
  +--------------------------------------------------------------------------------------------------------------------------
--------------------------------+
  | 1     | Brian      |             | Tam                    | bt@uber.com                  | Whois contact | San Francisco, CA | United S
tates |       |       | whois_pocs |
  | 2     |            |             | Uber Network Engineering | gni-notifications@uber.com | Whois contact | San Francisco, CA | United S
tates |       |       | whois_pocs |
  | 3     |            |             | Uber Network Engineering | corpnet-eng@uber.com       | Whois contact | San Francisco, CA | United S
tates |       |       | whois_pocs |
  | 4     |            |             | Network Engineering    | neteng+arin@uber.com         | Whois contact | Pittsburgh, PA    | United S
tates |       |       | whois_pocs |
  | 5     | Gabriel    |             | Ramos                  | Ramos@Uber.com               | Whois contact | San Francisco, CA | United S
tates |       |       | whois_pocs |
  +--------------------------------------------------------------------------------------------------------------------------
```

7.6 Cloud Hosting & Third-Party Dependencies

- **Finding:** Uber's DNS is provided by UltraDNS and web assets are fronted by Cloudflare and AWS, introducing critical external dependencies.
- **Risk Level:** High
- **Evidence:**
    - whois uber.com shows UltraDNS as the nameserver operator.
    - HTTP response headers include server: cloudflare, via: 1.1 varnish.



8. Recommendations

Based on our findings, we advise Uber to prioritize the following actions to remediate critical and high-risk issues, strengthen overall resilience, and reduce the external attack surface.

8.1 Immediate Remediation (Critical & High Risk)

Finding	Recommendation	Owner	Timeline
Historical AWS Key Leak (2016)	Rotate all AWS keys; audit IAM policies; implement robust secrets management (e.g., vaulting)	Cloud Security Team	Within 7 days
Exposed Public APIs (403 vs. 404)	Apply rate limiting; enforce authentication on all endpoints; return consistent error codes	API Engineering	Within 14 days
Third-Party DNS & CDN Dependencies	Establish multi-vendor DNS failover; review Cloudflare ACLs; monitor dependency health	Infrastructure Team	Within 14 days

8.2 Mid-Term Improvements (Medium Risk)

Finding	Recommendation	Owner	Timeline
Public Subdomain Sprawl	Implement automated subdomain monitoring (e.g., Amass, ChaosDB); deprecate unused records	Threat Intelligence Team	30–45 days
Predictable Email Address Format	Enforce aliasing or randomized local-part policy for high-privilege accounts	Identity Management	30–60 days
Public API Visibility (Passive)	Publish API usage guidelines; provide honeypot endpoints to detect unauthorized probing	Developer Relations	45–60 days

8.3 Long-Term Initiatives (Low Risk)

Finding	Recommendation	Owner	Timeline
Subdomain Enumeration (Informational)	Schedule quarterly external pen tests; integrate DNS findings into SIEM alerts	Red Team / SOC	90+ days
Infrastructure Fingerprinting (Wappalyzer)	Harden server headers; suppress version disclosure; adopt WAF rules to block known exploits	DevOps / Security Ops	90+ days

Notes on Implementation:

- **Secrets Management:** Adopt a centralized vault (e.g., HashiCorp Vault, AWS Secrets Manager) for all API keys and certificates.
- **Monitoring & Alerting:** Feed subdomain and DNS-related alerts into existing SIEM for real-time anomaly detection.
- **Dependency Resilience:** Test vendor failover plans quarterly to validate multi-DNS and multi-CDN configurations.

With these recommendations enacted, Uber will significantly reduce high-impact risks and maintain a proactive security posture against both opportunistic and targeted reconnaissance.

9. Steps to produce

1. Getting sub domain and IP addresses

Tool: Recon-ng.
Command:

recon-ng> modules load recon/domains-hosts/hackertarget

recon-ng> modules load recon/domains-hosts/certificate_transparency

recon-ng> modules load recon/hosts-hosts/resolve

recon-ng> set SOURCE uber.com

recon-ng> run

Set SOURCE: uber.com.
Run.

```
[recon-ng][uber] > modules load recon/domains-hosts/hackertarget
[recon-ng][uber][hackertarget] > info

      Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
   Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  uber.com       yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][uber][hackertarget] > options set source uber.com
SOURCE => uber.com
[recon-ng][uber][hackertarget] > run

--------
UBER.COM
--------
[*] Country: None
[*] Host: backup.uber.com
[*] Ip_Address: 207.231.168.151
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

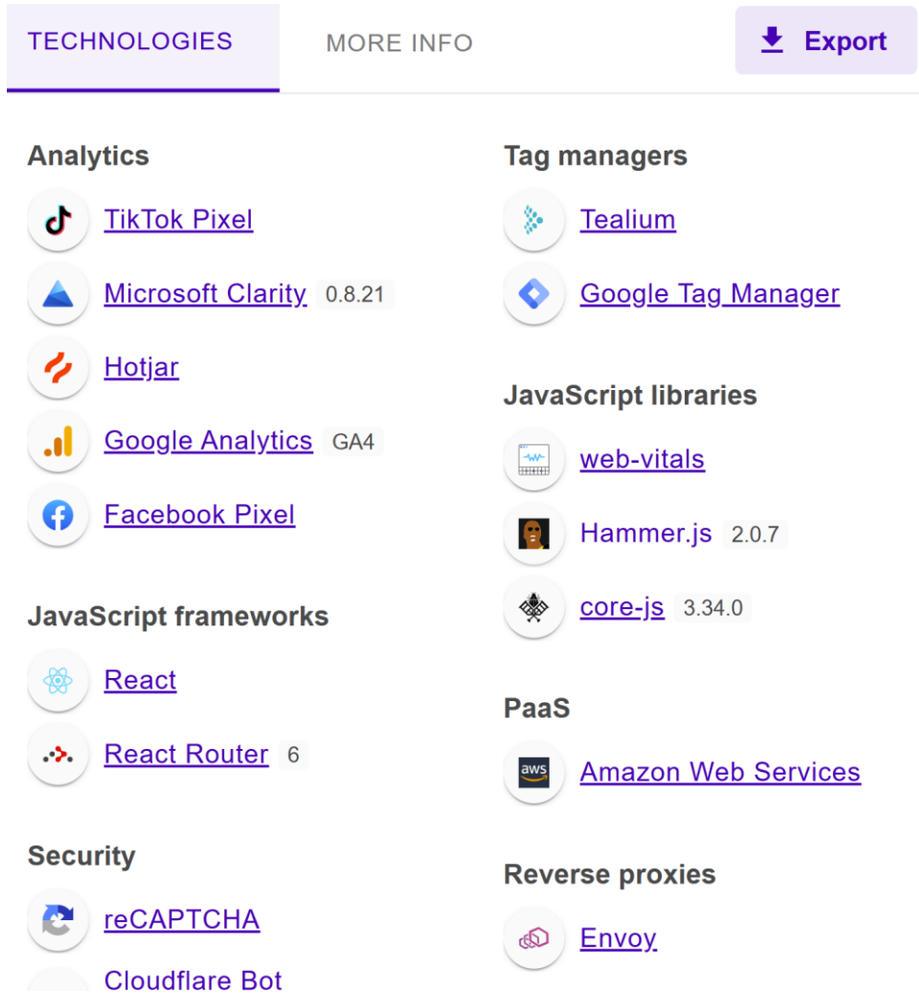
```
[recon-ng][uber][certificate_transparency] > options set source uber.com
SOURCE => uber.com
[recon-ng][uber][certificate_transparency] > run

--------
UBER.COM
--------
[*] Country: None
[*] Host: p.uber.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------------
[*] Country: None
[*] Host: qr.uber.com
```

2. Getting web stack for uber.

Tool: Wappalyzer

Run it as an extension in the browser

Load webpage and click on the extension.



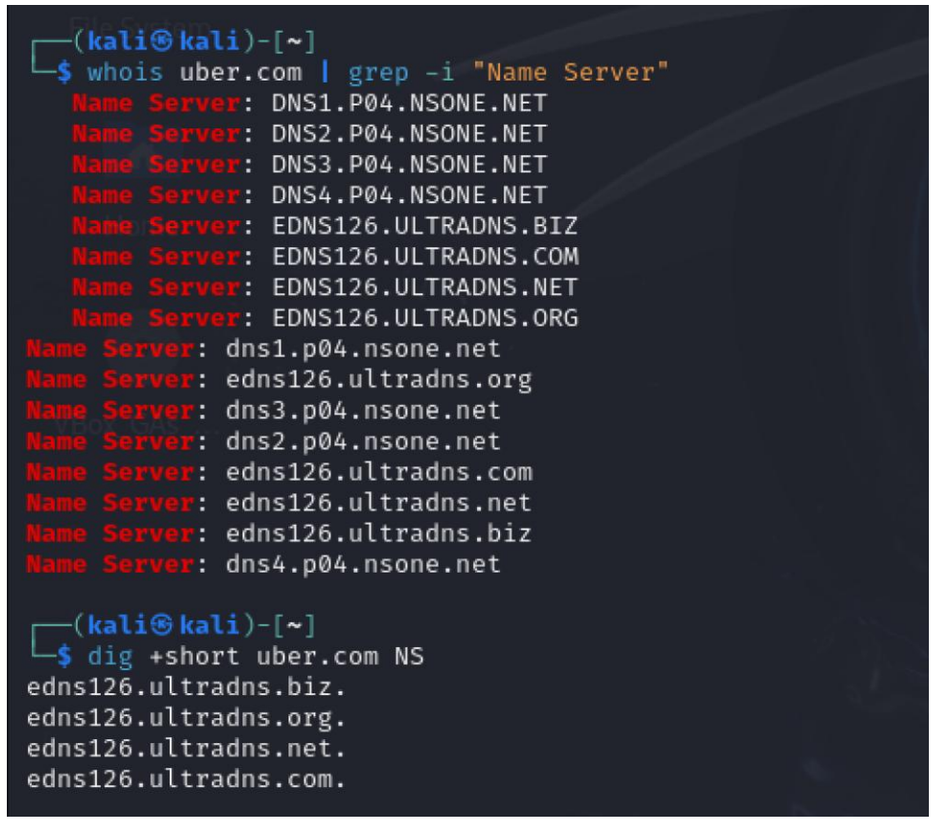
Category	Technology Used	Notes
Analytics	Microsoft Clarity 0.8.21, Hotjar, Google Analytics (GA4), Facebook Pixel	Behavioral tracking and performance monitoring
Security	reCAPTCHA, Cloudflare Bot Management, HSTS	Bot mitigation, session hardening, and HTTPS enforcement
CDN	Cloudflare, Amazon S3	Content caching and file distribution
Advertising	Microsoft Advertising, LinkedIn Ads	Targeted ads and user tracking
Tag Managers	Tealium, Google Tag Manager	Centralized tag and script management
PaaS / Cloud	Amazon Web Services (AWS)	Cloud infrastructure for compute, DNS, storage, etc.
Reverse Proxy	Envoy	Handles service routing and ingress
Authentication	Google Sign-In	OAuth-based federated login
Customer Data Platform	Tealium	Manages customer identities and segmentation

3. Checking for DNS Infrastructure Lookup

Tool: whois, dig

Command: whois uber.com | grep -I “Name Server”

Dig +short uber.com NS



4. Cheking who hosts uber servers

Tool: whois,dig

Get the uber ip address using dig +short uber.com

Use whois 10.4.36.194.7

```
┌──(kali㉿kali)-[~]
└─$ whois 104.36.194.7

#
# 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 1997-2025, American Registry for Internet Numbers, Ltd.
#


NetRange:       104.36.192.0 - 104.36.199.255
CIDR:           104.36.192.0/21
NetName:        UTPRODUCTION
NetHandle:      NET-104-36-192-0-1
Parent:         NET104 (NET-104-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS26673
Organization:   Uber Technologies, Inc (UT-33)
RegDate:        2014-06-06
Updated:        2021-12-14
Ref:            https://rdap.arin.net/registry/ip/104.36.192.0


OrgName:        Uber Technologies, Inc
OrgId:          UT-33
Address:        1725 Third Street
City:           San Francisco
StateProv:      CA
PostalCode:     94158
Country:        US
RegDate:        2014-01-28
```

5. Checking for Mail exchange records MX

Tool: Dig

Type dig +short uber.com MX

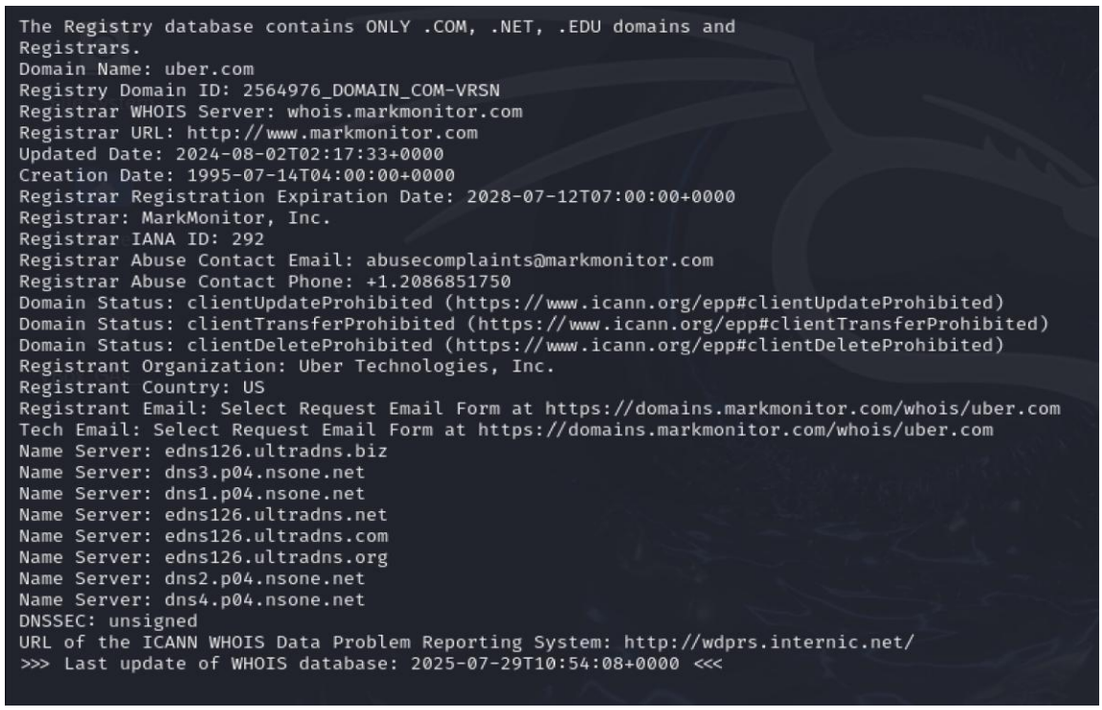
```
┌──(kali㉿kali)-[~]
└─$ dig +short uber.com MX
10 alt3.aspmx.l.google.com.
10 alt4.aspmx.l.google.com.
5 alt1.aspmx.l.google.com.
5 alt2.aspmx.l.google.com.
2 aspmx.l.google.com.
```

Priority	Mail server	Provider
10	alt3.aspmx.l.google.com	Google workspace
10	alt4.aspmx.l.google.com	Google workspace
5	alt1.aspmx.l.google.com	Google workspace
5	alt2.aspmx.l.google.com	Google workspace
2	aspmx.l.google.com	Google workspace

6. Cheking the contact directory

Tool:whois

Type whois uber.com

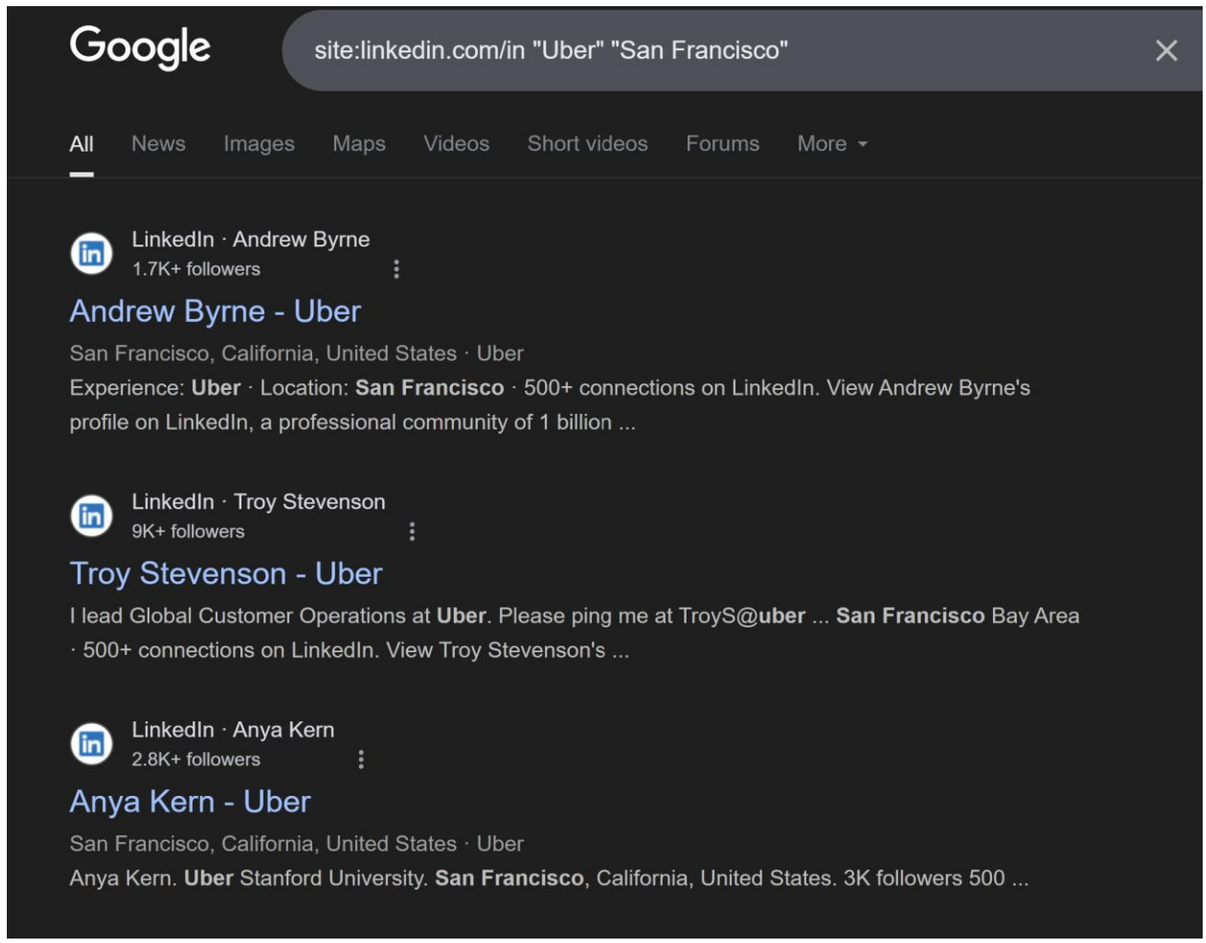


7. Web reconnaissance

In Identifying the people who work at uber.

Use google dorking where the following search string was used

Site:linkedin.com/in”Uber”San Francisco”



Name	Title	Source
Wei Sun	Software engineer	LinkedIn
Troy Stevenson	Global customer operations	LinkedIn
Anya Khan	Designer	LinkedIn
Mike Akamine	Product Manager	LinkedIn
Guy Peterson	Operations	LinkedIn
Kiran Reddy	IAM Engineer	LinkedIn
Wali Ansary	Security Operations	LinkedIn
Janani Narayanan	Security consultant	LinkedIn
Julia Paige	Senior Director	LinkedIn
Sam Gilbert	Tech sales	LinkedIn

8. Checking type of corporation

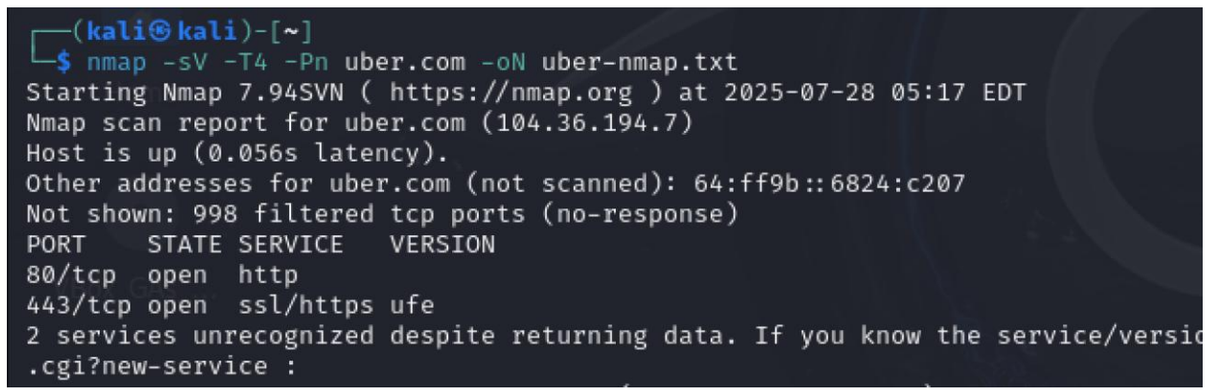
Tool:Openssl

Command: openssl s_client -connect uber.com:443 -showcerts

9. Service discovery on Uber domain

Tool: nmap

Command: nmap -sV -T4 -Pn uber.com



Port	State	Service
80	open	http
443	open	https

10. Naming convention of employees' email addresses:

Tool: Recon-ng, Github

Use recon-ng

Load module recon/domains-contacts/whois_pocs

Run the module

Then show contacts

```
[recon-ng][uber] > modules load recon/domains-contacts/whois_pocs
[recon-ng][uber][whois_pocs] > info

      Name: Whois POC Harvester
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates the
  'contacts' table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][uber][whois_pocs] > options set source uber.com
SOURCE ⇒ uber.com
[recon-ng][uber][whois_pocs] > run
```

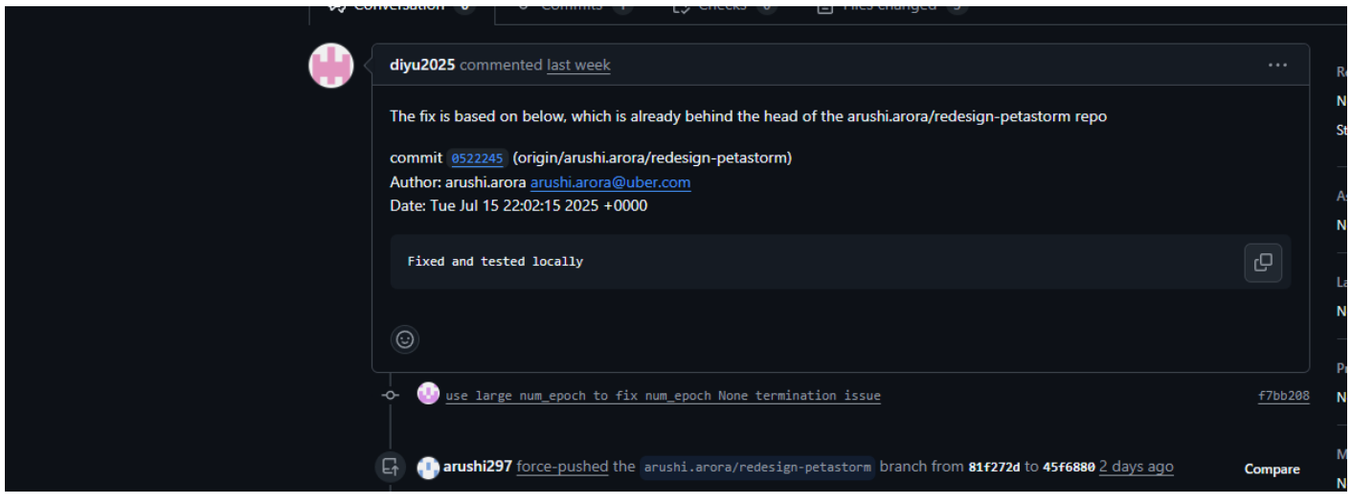
```
SUMMARY

[*] 5 total (5 new) contacts found.
[recon-ng][uber][whois_pocs] > show contacts

 | rowid | first_name | middle_name |        last_name         |           email            |     title     |       region      |   count
ry    | phone | notes |   module    |

 | 1     | Brian      |             | Tam                      | bt@uber.com                | Whois contact | San Francisco, CA | United S
tates |       |       | whois_pocs  |
 | 2     |            |             | Uber Network Engineering | gni-notifications@uber.com | Whois contact | San Francisco, CA | United S
tates |       |       | whois_pocs  |
 | 3     |            |             | Uber Network Engineering | corpnet-eng@uber.com       | Whois contact | San Francisco, CA | United S
tates |       |       | whois_pocs  |
 | 4     |            |             | Network Engineering      | neteng+arin@uber.com       | Whois contact | Pittsburgh, PA    | United S
tates |       |       | whois_pocs  |
 | 5     | Gabriel    |             | Ramos                    | Ramos@Uber.com             | Whois contact | San Francisco, CA | United S
tates |       |       | whois_pocs  |
```

- Pattern identified: first.last@uber.com e.g. bt@uber.com
- corpnet-eng@ uber.com Ramos@Uber.com

11. AD naming convention

Based on Uber's email convention (first.last@uber.com), the likely AD naming convention is first.last or first initial + last name.

From github I found naming conventions like wjang@uber.com, ignas@uber.com and shangx@uber.com. Its likely the AD naming convention is first.last or first initial + last name.

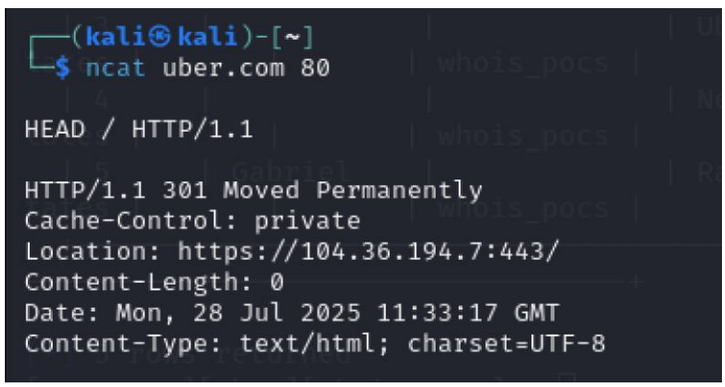


12. Banner Grabbing

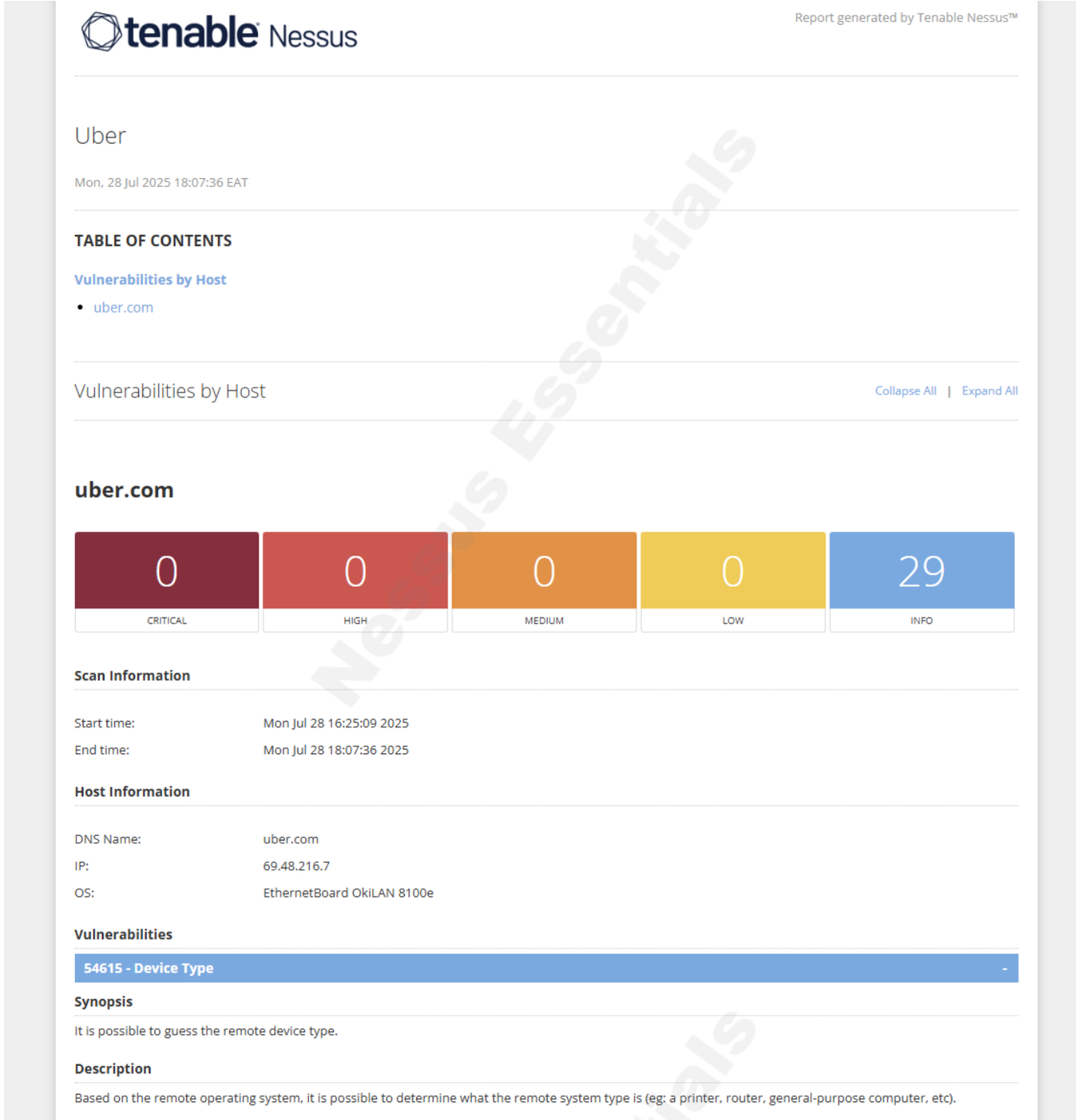
Tool:ncat

Command: ncat uber.com 80

Ncat -v -ssl uber.com 443 -w 3



13. Vulnerability scan



tenable Nessus

Report generated by Tenable Nessus™

Uber

Mon, 28 Jul 2025 18:07:36 EAT

TABLE OF CONTENTS

Vulnerabilities by Host

- uber.com

Vulnerabilities by Host

Collapse All | Expand All

uber.com

0	0	0	0	29
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Mon Jul 28 16:25:09 2025

End time: Mon Jul 28 18:07:36 2025

Host Information

DNS Name: uber.com

IP: 69.48.216.7

OS: EthernetBoard OkiLAN 8100e

Vulnerabilities

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

A vulnerability scan was done using nessus on the domain and informational flags were noted.

10. Conclusion

Uber's external attack surface exhibits both strengths and residual risks. On one hand, reliance on enterprise-grade DNS (UltraDNS) and CDN services (Cloudflare, AWS) delivers robust performance and DDoS resilience. Passive reconnaissance failed to uncover any unintended API endpoints or use of weak authentication schemes, demonstrating sound perimeter controls.

However, high-severity historical issues—most notably the 2016 AWS key exposure—continue to pose a critical threat to confidentiality and customer trust. Furthermore, extensive subdomain sprawl and predictable email/AD naming patterns amplify attackers' reconnaissance capabilities, while single-vendor dependencies introduce potential points of failure.

Key Takeaways

- **Resilient Infrastructure:** Third-party DNS/CDN platforms and self-managed IP blocks provide strong uptime guarantees.
- **Controlled API Exposure:** No unauthenticated API access observed, but documented endpoints should be continuously monitored.
- **Lingering Secrets Risk:** Legacy credential leaks underscore the need for rigorous secrets-management and regular key rotation.
- **Surface Visibility:** Nearly 500 public subdomains and standardized email formats enable efficient attacker mapping.

Next Steps

1. **Immediate Remediation:** Rotate legacy AWS/secret keys, enforce vaulting, and apply rate-limits/authentication on all APIs.
2. **Continuous Monitoring:** Integrate automated subdomain and certificate transparency alerts into the SIEM.
3. **Periodic Review:** Schedule quarterly external assessments and annual vendor resilience tests to validate DNS/CDN failover.

By executing these actions and maintaining an iterative testing cadence, Uber can minimize its exposure to both opportunistic and targeted reconnaissance, ensuring sustained protection of its valuable assets and reputation.

11. Contact Information

For any questions, clarifications, or follow-up discussions regarding this report, please reach out to:

Studsvike Technologies
Email: nicholas.oyaro@student.moringaschool.com
Phone: +254 720 075 564
Website: www.studsvike.com

Report Prepared By:
Nicholas Oyaro
Lead Security Consultant, Studsvike Technologies

12. Bibliography

- Recon-ng. (n.d.). GitHub repository https://github.com/lanmaster53/recon-ng
- crt.sh. (n.d.). Certificate search. https://crt.sh
- Wappalyzer. (n.d.). Web technology profiler. https://www.wappalyzer.com
- WHOIS. (n.d.). Domain lookup service. https://www.iana.org/whois
- Have I Been Pwned. (n.d.). Breach notification service. https://haveibeenpwned.com
- Uber HackerOne Program. (n.d.). https://hackerone.com/uber
- UltraDNS. (n.d.). Enterprise DNS services. https://www.ultradns.com
- Cloudflare. (n.d.). Content delivery and security. https://www.cloudflare.com
- Amazon Web Services. (n.d.). AWS documentation. https://docs.aws.amazon.com
- OWASP OSINT Framework. (n.d.). https://github.com/OWASP/OWASP-OSINT-Framework
- NIST. (2012). *Guide for Conducting Risk Assessments* (SP 800-30 Rev. 1). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf