Recon

Target: tesla.com
Objective: Perform passive reconnaissance (OSINT) to identify publicly exposed assets, technologies, and services without active exploitation.

1. Scope & Rules

- **In-scope:** tesla.com and publicly accessible subdomains discovered via passive methods
- **Out-of-scope:** Active exploitation, credential attacks, DoS, or any intrusive testing
- **Methodology:** Passive OSINT only (WHOIS, search engines, tech fingerprinting, asset discovery)

2. Tools Used

- **Shodan** – Internet-exposed services and metadata
- **WHOIS (Sysinternals)** – Domain registration and DNS information
- **Subfinder** – Passive subdomain enumeration
- **Wappalyzer** – Technology stack identification
- **Google Docs** – Central documentation

3. Domain Information (WHOIS)

- **Domain:** tesla.com
- **Registrar:** MarkMonitor Inc.
- **Creation Date:** 1992-11-04
- **Expiry Date:** 2026-11-03
- **Domain Status:** clientDeleteProhibited, clientTransferProhibited, serverDeleteProhibited
- **Name Servers:**
    - A1–A28.AKAM.NET
    - EDNS69.ULTRADNS.(COM/NET/ORG/BIZ)

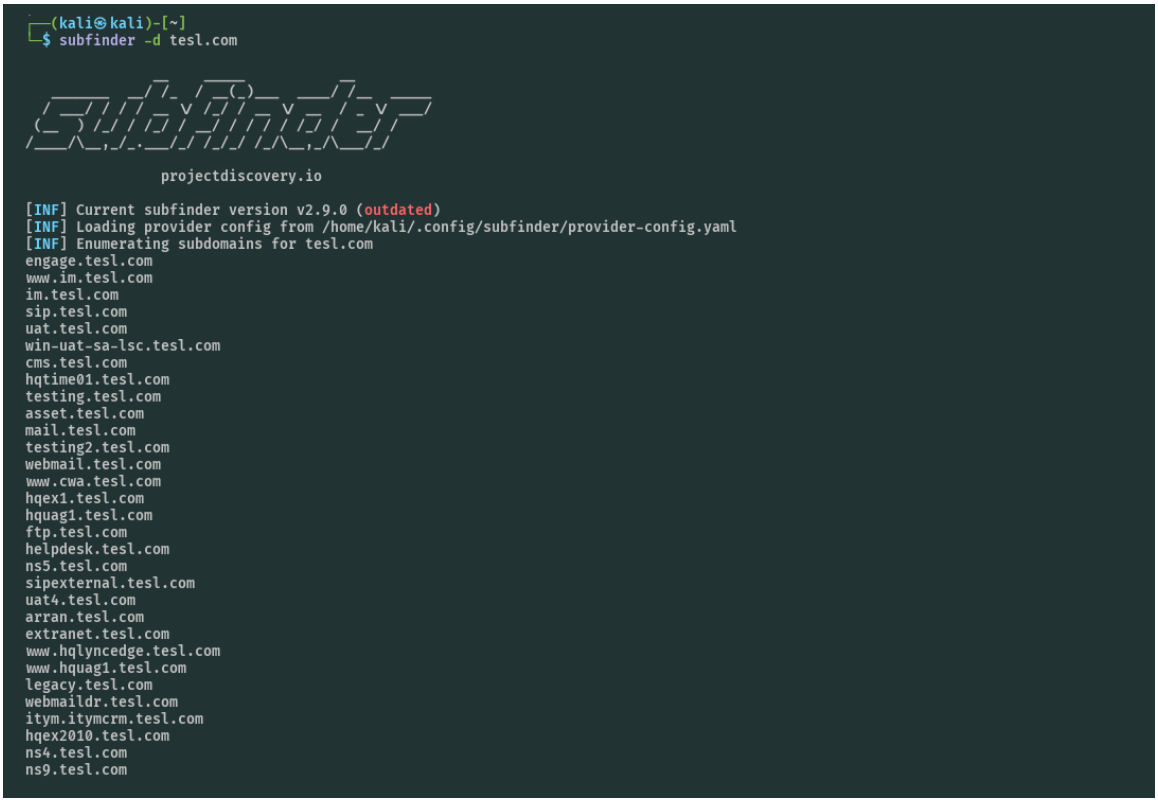
Observation: Tesla uses enterprise-grade DNS (Akamai + UltraDNS) with registry locks enabled, indicating mature security posture.

4. Subdomain Enumeration (Subfinder)

Passive enumeration identified multiple subdomains related to business functions, testing, and infrastructure.

Sample Findings: - www.tesla.com - engage.tesla.com - mail.tesla.com - webmail.tesla.com - testing.tesla.com - legacy.tesla.com - extranet.tesla.com - ns*.tesla.com

Observation: Presence of testing and legacy subdomains increases attack surface if not properly hardened.

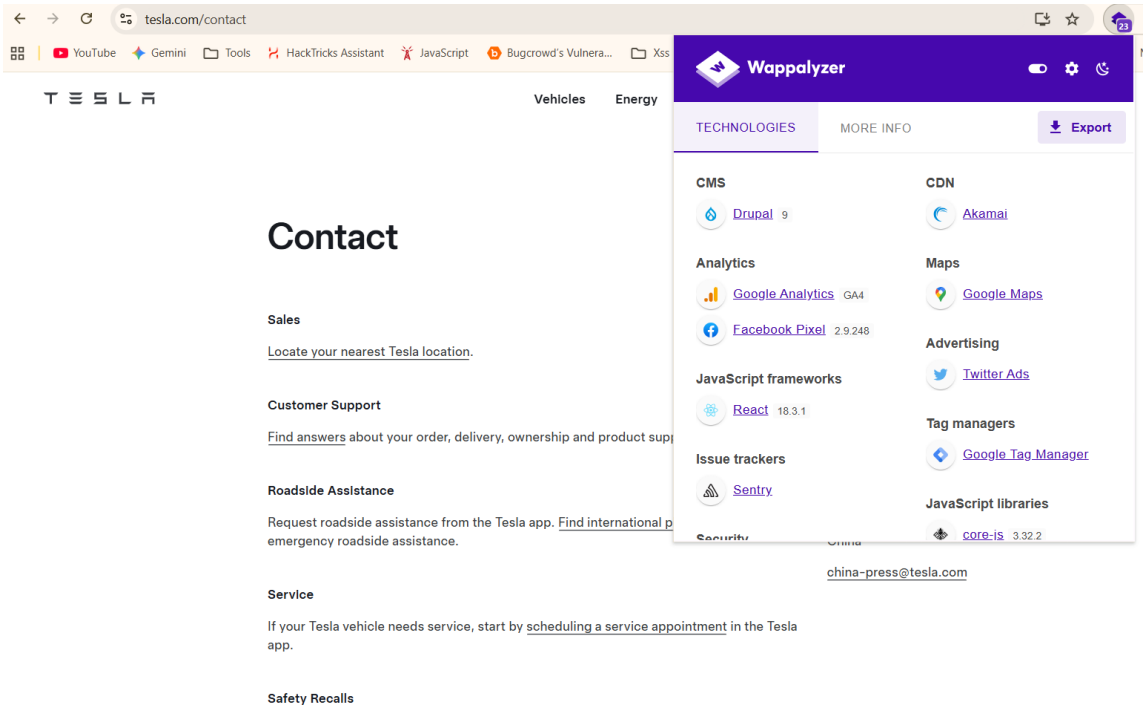


5. Technology Stack Identification (Wappalyzer)

Analysis of https://tesla.com/contact revealed the following stack:

- **CMS:** Drupal 9
- **CDN:** Akamai
- **Frontend:** React 18.3.1
- **Analytics:** Google Analytics (GA4), Facebook Pixel
- **Tag Management:** Google Tag Manager
- **Monitoring:** Sentry
- **Maps:** Google Maps

Observation: Modern frontend with third-party integrations. Analytics and tag managers are common entry points for misconfigurations.

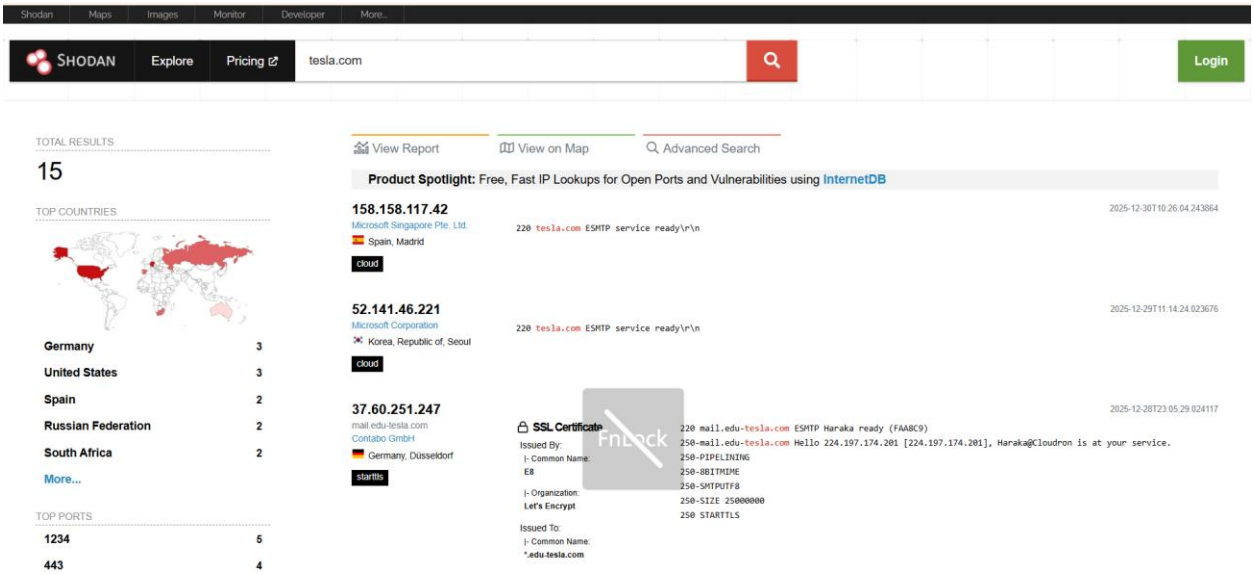


6. Exposed Services (Shodan)

Shodan search for Tesla-related assets returned a large dataset of indexed IPs and services.

General Observations: - Global distribution of assets - Cloud-hosted infrastructure - Use of enterprise CDNs and reverse proxies

> Note: No direct vulnerability exploitation was performed. Findings are observational only.



7. Asset Mapping Log (Slack-Friendly)

Timestamp (UTC)	Tool	Finding
2026-01-01 10:15:00	WHOIS	MarkMonitor registrar, Akamai + UltraDNS NS
2026-01-01 10:25:00	Subfinder	Subdomains: testing.tesla.com, legacy.tesla.com
2026-01-01 10:40:00	Wappalyzer	Drupal 9, React 18, Akamai CDN
2026-01-01 11:00:00	Shodan	Large global asset footprint detected

8. Reconnaissance Checklist

- ✓ Perform WHOIS lookup
- ✓ Identify DNS and registrar protections
- ✓ Enumerate subdomains (Subfinder)
- ✓ Identify technology stack (Wappalyzer)
- ✓ Review exposed services via Shodan
- ✓ Document findings in Google Docs

9. Recon Summary

Tesla.com demonstrates a mature security posture with enterprise DNS, CDN protection, and modern web technologies. Passive reconnaissance revealed a wide global asset footprint, multiple functional subdomains, and a Drupal-React stack. No immediate misconfigurations were observed during OSINT-only analysis.