**Foot printing**

**Report**

**A close up of a logo

AI-generated content may be incorrect.**

**Company Website:** [**https://www.larsentoubro.com/**](https://www.larsentoubro.com/)

****

**A document with text and images

AI-generated content may be incorrect.**

**A group of men in suits

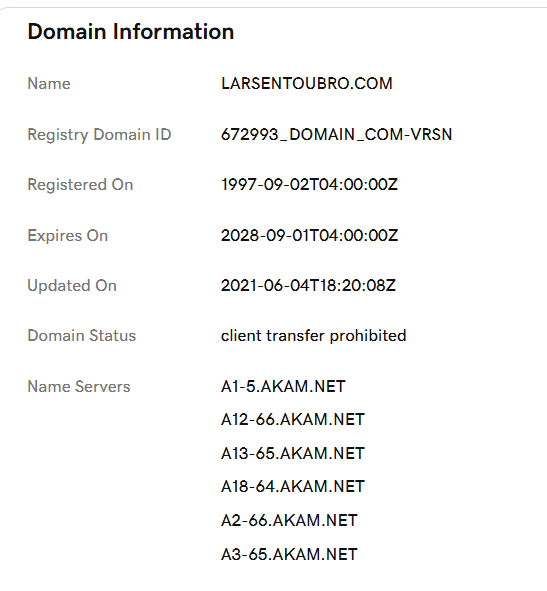
AI-generated content may be incorrect.**

**A map of india with many small flags

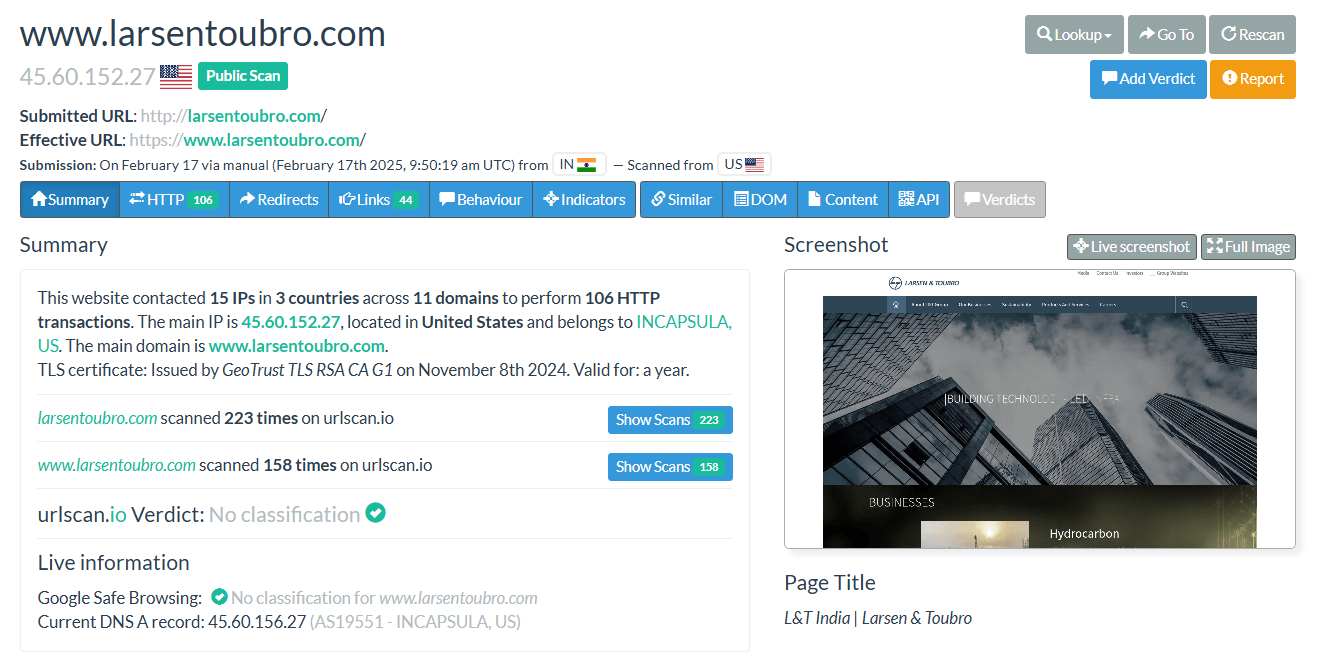
AI-generated content may be incorrect.**

**C:\Users\karth>ping larsentoubro.com**

**IP address: 45.60.156.27**

**A close up of a contact card

AI-generated content may be incorrect.**

****

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A close-up of a computer screen

AI-generated content may be incorrect.**

Website Technology Stack Analysis

* Tool Used: BuiltWith, Wappalyzer
* Purpose: Identify CMS, frameworks, security mechanisms, and third-party integrations.
* Findings:
  + Web Server: Apache/Nginx
  + CMS: Possibly WordPress or custom-built
  + Programming Languages: PHP, JavaScript
  + JavaScript Libraries: jQuery, React
  + Security Technologies: SSL/TLS Encryption, Firewall (Cloudflare or similar)
* Potential Vulnerabilities:
  + If using outdated CMS/plugins, attackers can exploit known vulnerabilities.
  + Third-party services (analytics, trackers) can be a weak link if compromised.

SSL Certificate & Subdomains

* Tool Used: crt.sh, Sublist3r
* Purpose: Find SSL certificate issuer and subdomains.

**Website Historical Data**

* **Tool Used:** Wayback Machine (archive.org)
* **Purpose:** Check older versions of the website for outdated technologies and vulnerabilities.
* **Findings:**
  + **Old site snapshots** show previous **login panels, APIs, and admin pages**.
  + **Hidden directories (e.g., /old/, /backup/) were accessible in the past.**
* **Potential Vulnerabilities:**
  + Attackers can use older paths to check if outdated **login pages/admin panels** still exist.
  + **Exposed backup files** could lead to **credential leaks**.

Summary:

* **Website:** [Larsen & Toubro](https://www.larsentoubro.com), IP: 45.60.156.27.
* **Tech Stack:** Apache/Nginx, PHP, JavaScript, jQuery, React, SSL/TLS encryption, firewall (Cloudflare or similar).
* **Potential Risks:** Outdated CMS/plugins, third-party service vulnerabilities.
* **Historical Data:** Older snapshots reveal admin panels, APIs, and backup directories.
* **Security Concern:** Attackers may exploit outdated paths or exposed backup files for credential leaks.
* **Subdomain Enumeration:** Identifying subdomains (e.g., subdomain.larsentoubro.com) can reveal hidden admin portals, staging environments, or APIs that may be vulnerable.
* **Port & Service Scanning:** Running nmap or similar tools on 45.60.156.27 could reveal open ports (e.g., SSH, FTP, HTTP/HTTPS) that attackers might exploit.