**🔄 Project Title: ConsentScope – Analyzing and Visualizing Web Tracker Behavior Based on User Consent**

🧠 Core Idea:

Build a Python-based system that:

Simulates both “Accept All” and “Reject All” actions on cookie banners.

Detects all third-party trackers and network requests triggered in each case.

Classifies trackers by function (ads, analytics, social, etc.).

Visualizes differences in data flows depending on user consent, highlighting violations or privacy leaks.

🎯 Objectives:

To detect and classify web trackers embedded in websites.

To analyze how user consent (accepting vs rejecting cookies) impacts data sharing.

To visualize and compare third-party data flows under different consent states.

To assess compliance with privacy policy declarations.

🛠️ Tech Stack:

Python: Core logic and automation.

Selenium + ChromeDriver: Interact with and click cookie banners.

BeautifulSoup / Requests / Scapy: Page structure and HTTP request capture.

NetworkX / Matplotlib / D3.js: Consent-based graph visualization.

GeoIP APIs / WHOIS: Identify tracker ownership/location.

NLP (Optional): Match trackers against privacy policy content.

📌 Methodology:

Step 1: Crawl and Load Web Pages

Input: A list of URLs to test.

Launch using headless Selenium in two modes:

Mode A: Accept all cookies.

Mode B: Reject all cookies.

Step 2: Capture Network Requests

Monitor all HTTP(S) requests made by the browser.

Record request headers, domains, payloads, and timestamps.

Step 3: Tracker Detection and Classification

Identify third-party domains by comparing to first-party.

Use regex, public lists (like EasyPrivacy), and WHOIS data to classify:

Ad trackers

Analytics tools

Fingerprinting scripts

Social media widgets

Step 4: Compare Consent Paths

Match domains and requests across "Accept" vs "Reject" sessions.

Highlight which trackers ignore user consent.

Step 5: Visualization

Create a network graph showing:

First-party and third-party connections

Request frequency and data volume

Paths triggered only under "Accept All"

Violations (trackers present even after rejecting)

Step 6 (Optional): Policy Check

Scrape the site’s privacy policy.

Use NLP to extract declared services.

Flag discrepancies between policy and actual behavior.

📈 Expected Deliverables:

A dashboard or CLI tool that outputs:

Tracker report for each site (JSON/CSV)

Consent-based data flow visualization

Compliance summary (color-coded)

A report of findings from real-world websites