**Name of Student :Bethi Roshni Intern ID:425**

**Tool Name: NerdyData and PublicWWW**

**Description:-**

NerdyData is a web-based source code search engine that allows users to search for HTML, JavaScript, CSS, tags, and embedded elements across millions of websites. It is primarily used to identify technologies, scripts, tracking codes, and digital assets embedded within web pages. It also provides domain enrichment, revealing company information and tech stacks. The platform is suitable for marketers, cybersecurity analysts, and OSINT professionals.

PublicWWW is a powerful code pattern and fingerprint search engine that indexes the public source code of websites. It allows users to search using plain text or regular expressions (regex) to identify patterns such as analytics tags, affiliate links, JavaScript libraries, and other embedded resources. Unlike NerdyData, PublicWWW focuses on exact code matching and provides keyword frequency analysis without offering enrichment or dynamic content support..

**What Are These Tools About?**

They are designed for digital footprinting, OSINT, marketing research, tech stack analysis, and cyber investigations. These tools index the visible and sometimes hidden source code to help users identify specific web elements or technologies.

**Key Characteristics / Features:**

**NerdyData.com**

1. ✅ Searches website source code (HTML, JavaScript, CSS)
2. ✅ Supports JavaScript-rendered content
3. ✅ Allows keyword or tag-based search (e.g., gtag, optimizely)
4. ✅ Detects analytics/tracking IDs (e.g., Google Analytics, FB Pixel)
5. ❌ No support for regex search
6. ✅ Offers domain enrichment (company name, tech stack, size, etc.)
7. ✅ Exports results in CSV/JSON formats
8. ✅ Includes a Chrome extension for live scanning
9. ✅ Search by meta tags, inline scripts, and embedded code
10. ✅ Simple, modern dashboard interface

**PublicWWW.com**

1. ✅ Searches full static source code of indexed web pages
2. ❌ Does not support JavaScript-rendered content
3. ✅ Allows search by keyword, tag, or pattern (e.g., Google Analytics)
4. ✅ Detects analytics, tracking tags, ad codes
5. ✅ Powerful regex-based search support
6. ❌ No domain enrichment (only URL lists)
7. ✅ Allows CSV export (paid plans)
8. ❌ No browser extension available
9. ✅ Searches meta tags, comments, inline code
10. ⚠️ UI is basic and functional

**Types / Modules Available**:

**NerdyData**

* Code Search
* Chrome Extension
* Bulk Domain Lookup
* Domain Enrichment

**PublicWWW**

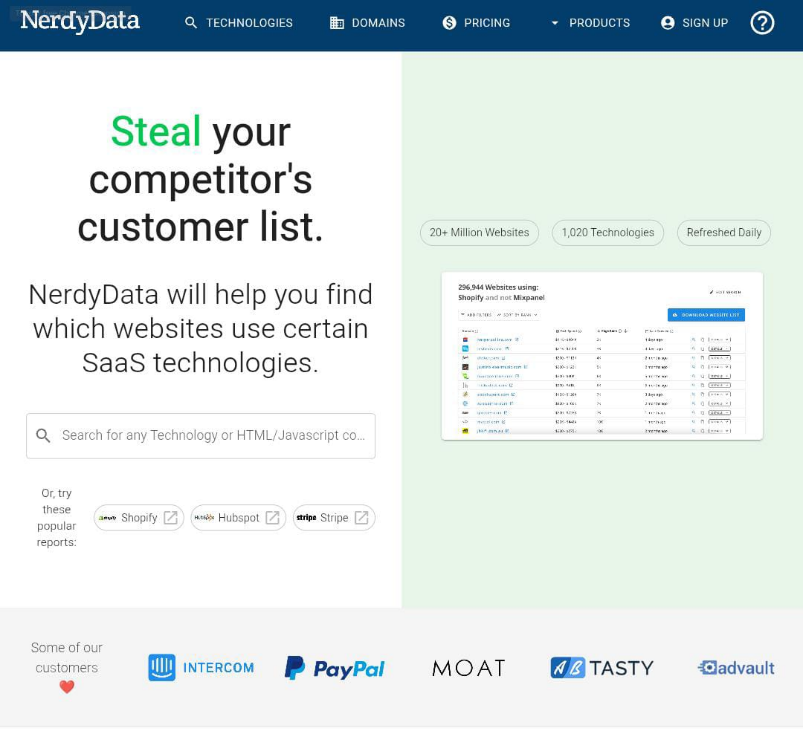
* Source Code Search
* Regex/Pattern Search
* Web Technology Lookup
* Analytics/Tracking Search

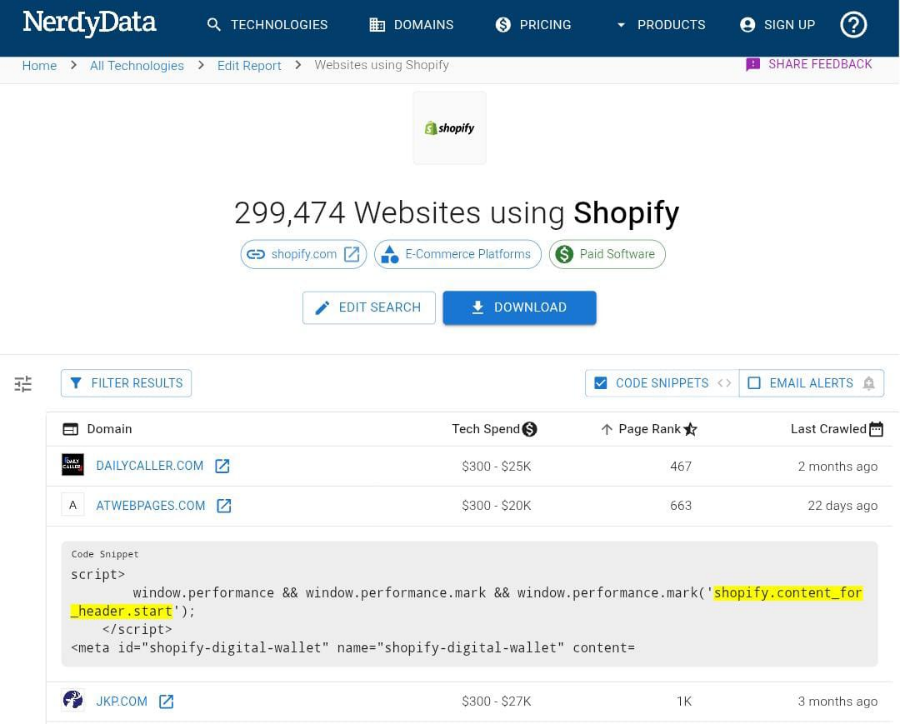
**How Will These Tools Help?**

* Identify websites using a specific CMS, JS library, or script
* Track competitor tags like “Google Analytics,” “Hotjar,” or “Pixel”
* Discover web app vulnerabilities by finding outdated code patterns
* Lead generation based on technology usage
* Help in threat intelligence and OSINT investigations

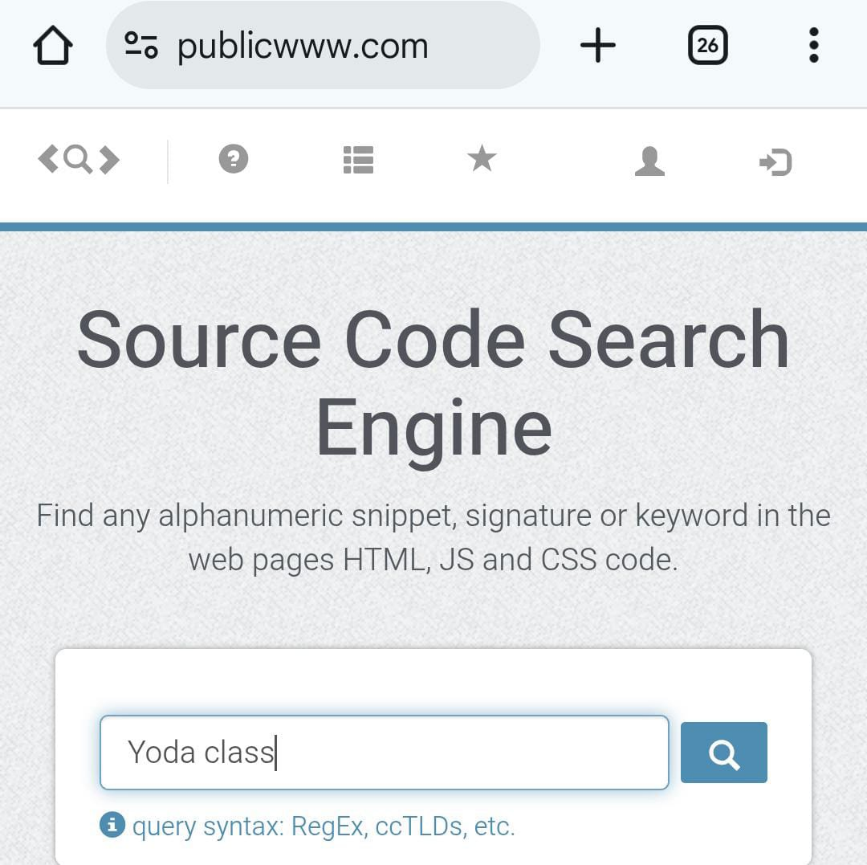
**Proof of Concept (PoC) Images (Insert as needed):**

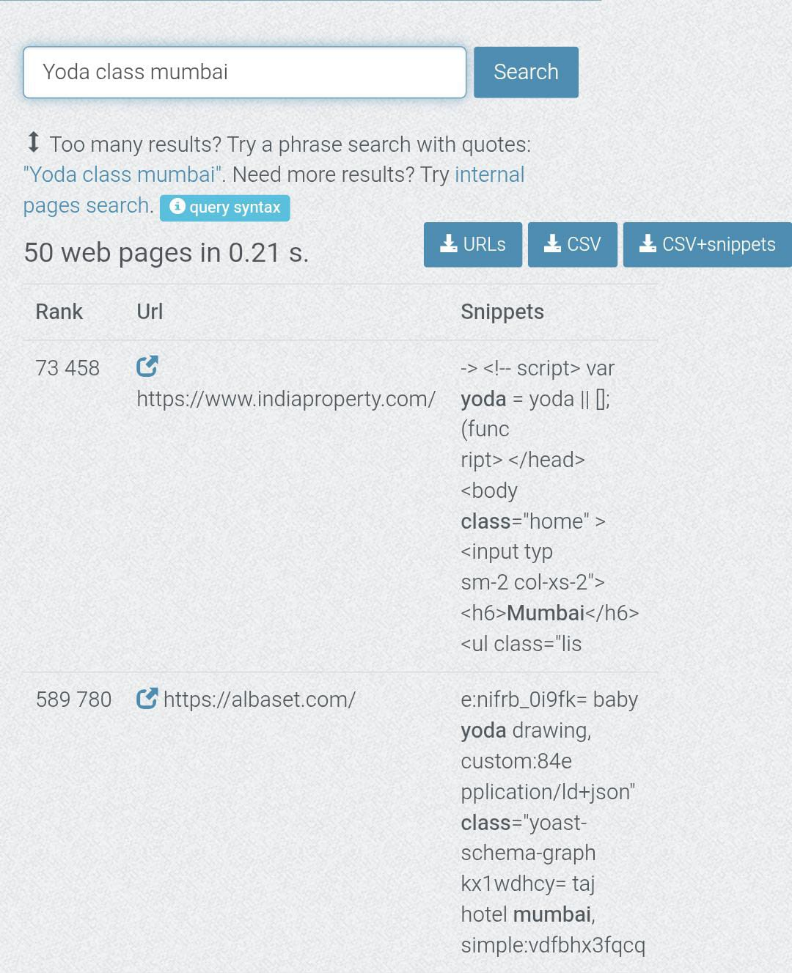
**NerbyData:**

****

****

**PublicWWW:**

****

****

**15-Liner Summary:**

1. Searches through web source code
2. Ideal for OSINT and cyber investigations
3. Detects analytics and JS libraries
4. Exportable reports in CSV
5. Supports mass domain analysis
6. UI for manual and CLI/API use (NerdyData)
7. PublicWWW supports Regex queries
8. NerdyData offers domain metadata
9. Great for competitive tech intel
10. Search by script ID or code pattern
11. High-speed, cloud-based
12. NerdyData supports dynamic rendering
13. PublicWWW offers clean keyword stats
14. Used by marketers, analysts, security experts
15. No installation required

**Time to Use / Best Case Scenarios:**

* Pre-marketing campaign competitor analysis
* Investigating phishing/malware distribution
* Identifying websites using outdated libraries
* Sourcing leads by tech stack
* Tracking specific advertising networks or cookies

**When to Use During Investigation**:

* OSINT investigations
* Digital footprint profiling
* Malware or tracker detection
* Finding cloned/phishing domains
* Identifying networks using same analytics ID

**Best Person to Use & Required Skills:**

* Best Users: Cybersecurity Analysts, Digital Marketers, OSINT Researchers

**Skills Needed:**

* Regex (for PublicWWW)
* Basic understanding of web source code
* Familiarity with JavaScript libraries and tags
* Ability to interpret metadata/enrichment

**Flaws / Suggestions to Improve:**

* NerdyData No real-time updates, lacks regex, limited free use
* PublicWWW No enrichment data, no browser plugin, UI outdated

**Good About the Tools:**

* Accurate source code matching
* Fast search and data exports
* Excellent for tech intelligence
* NerdyData is more user-friendly
* PublicWWW has powerful pattern matching