**Footprinting**

**Footprinting** is the process of gathering information about a target system or organization to understand its structure and identify potential vulnerabilities—like mapping out a building before planning an entry. By using 3rd party sources.

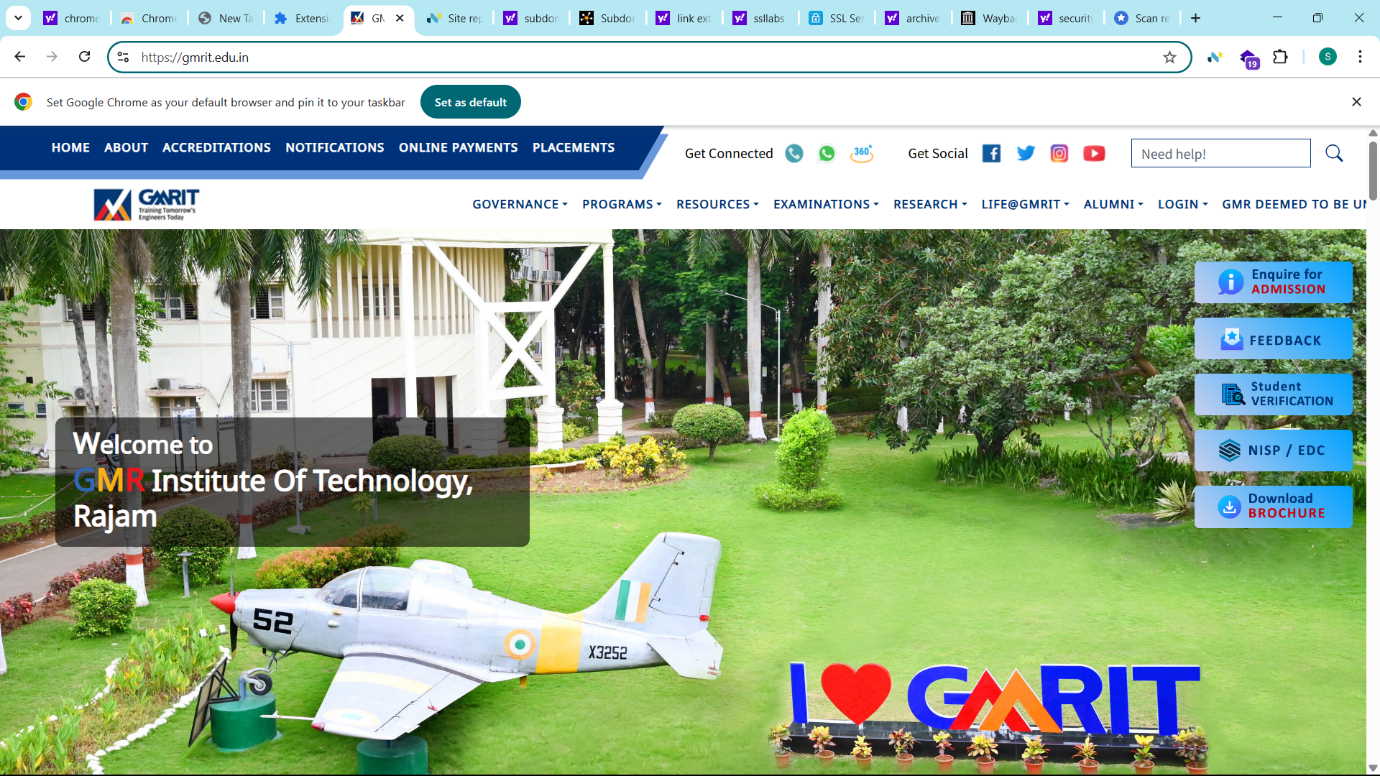
**Uses:-**

* Time saving
* Gather information about vulnerabilities
* Accurate attacks
* Efficiency of attacks

**Basic steps of footprinting:-**

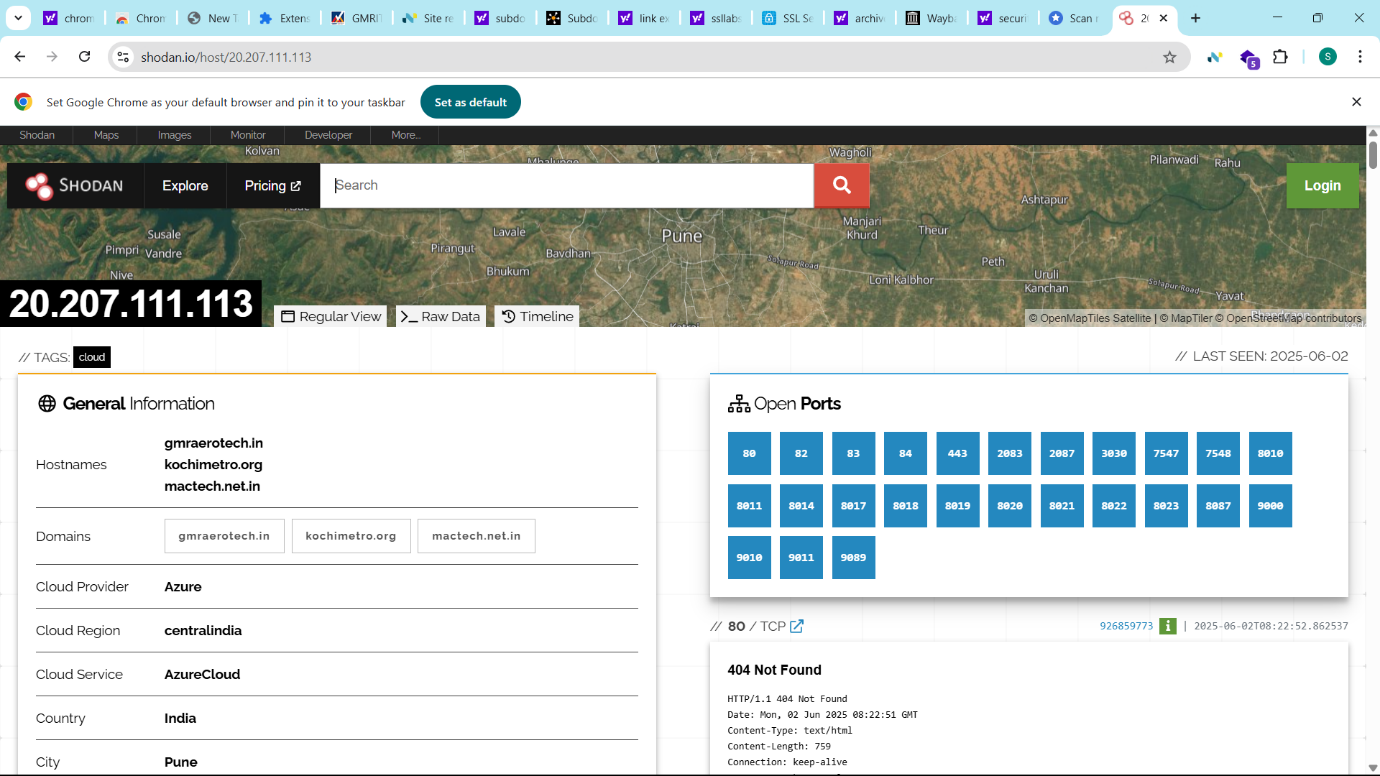
**1)Know your target:-**

**What:** Collect public information about a target from social networking sites.  
**Why:** To gain insights into personal or organizational details that can aid in social engineering or targeted attacks.  
**How:** Manually browse profiles or use OSINT tools to extract data from platforms like Facebook, LinkedIn, Twitter, Instagram, and Pinterest.



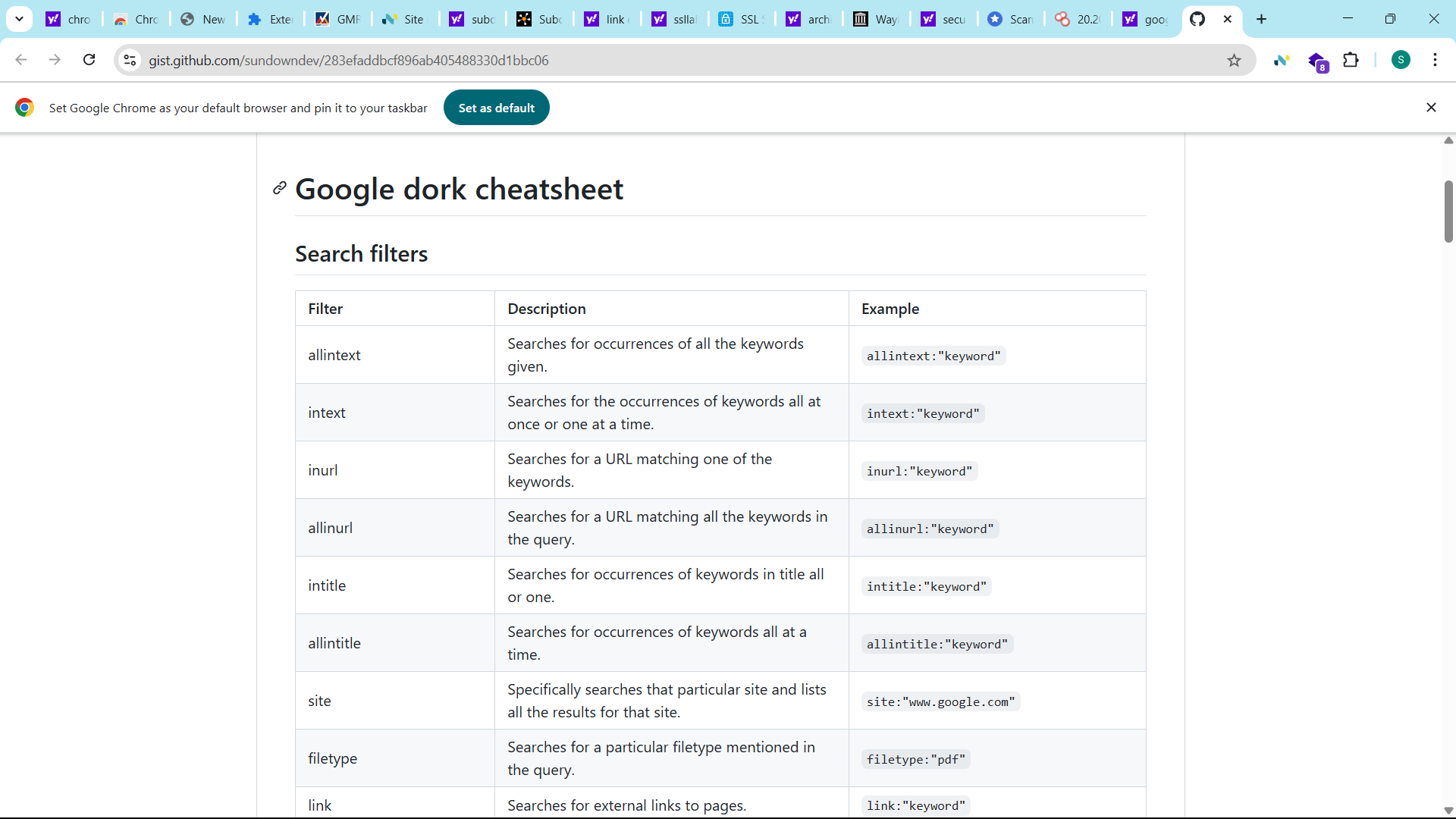
**2)Use Hacking Search Engines:-**

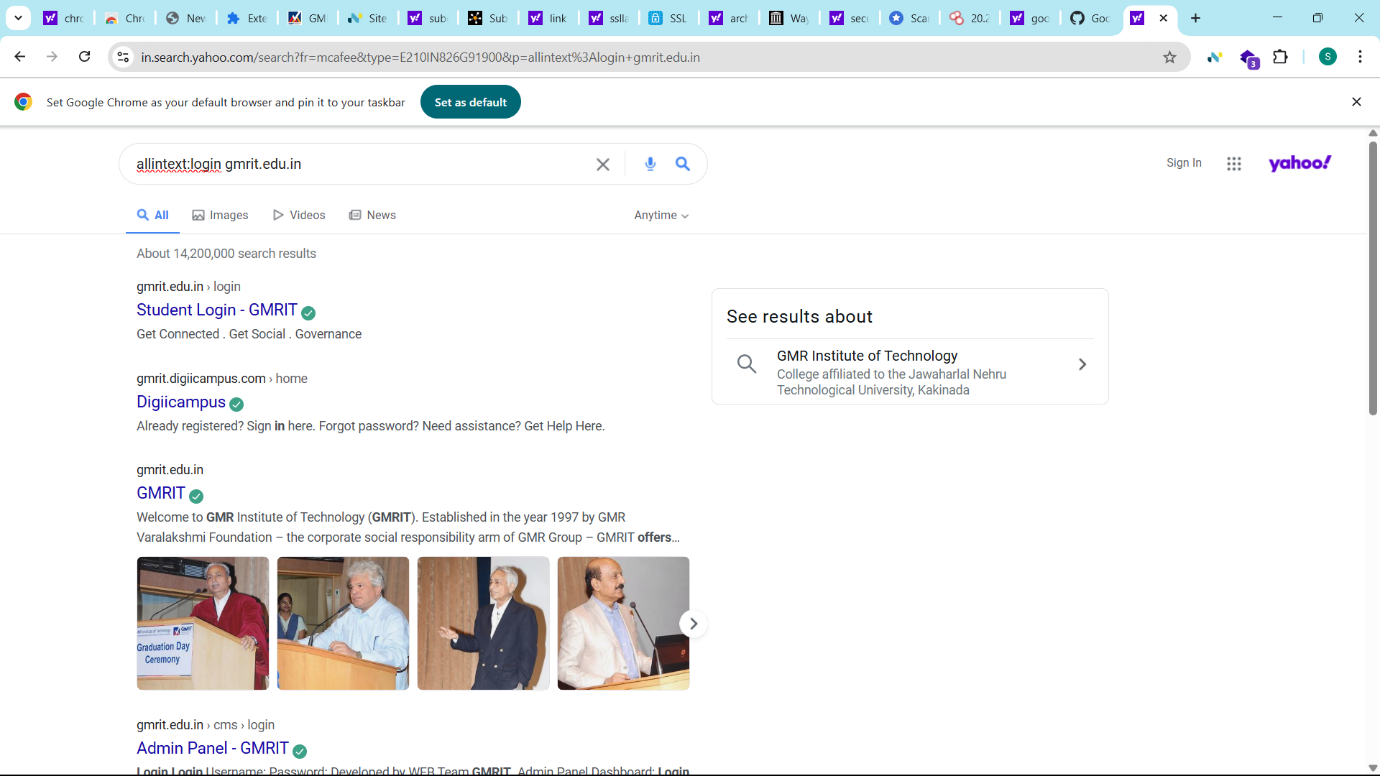
**What:** Use hacking-focused search engines to discover internet-connected devices, open ports, and vulnerabilities.  
**Why:** To identify exposed systems and weak points for security assessment or ethical hacking.  
**How:** Query tools like Shodan, Censys, and DuckDuckGo with specific filters or dorks to find hosts, services, and known vulnerabilities.



**3)Advance google search analytics(components):-**

**What:** Use advanced Google search techniques (Google dorks) to find specific information or vulnerabilities.  
**Why:** To uncover hidden data, sensitive files, or security flaws not easily found through regular searches.  
**How:** Apply special search operators (e.g., site:, filetype:, inurl:) and crafted queries to refine results.

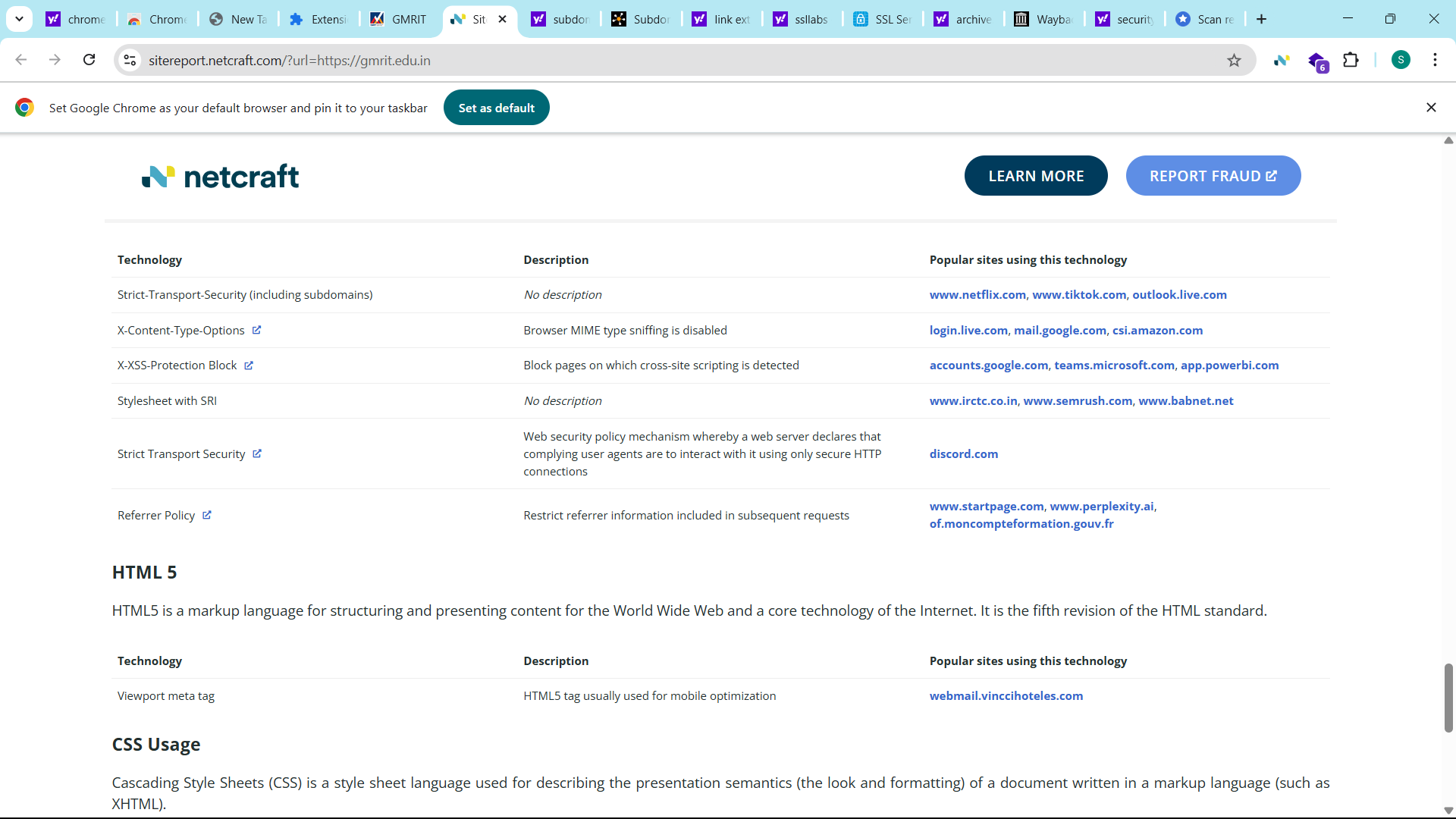


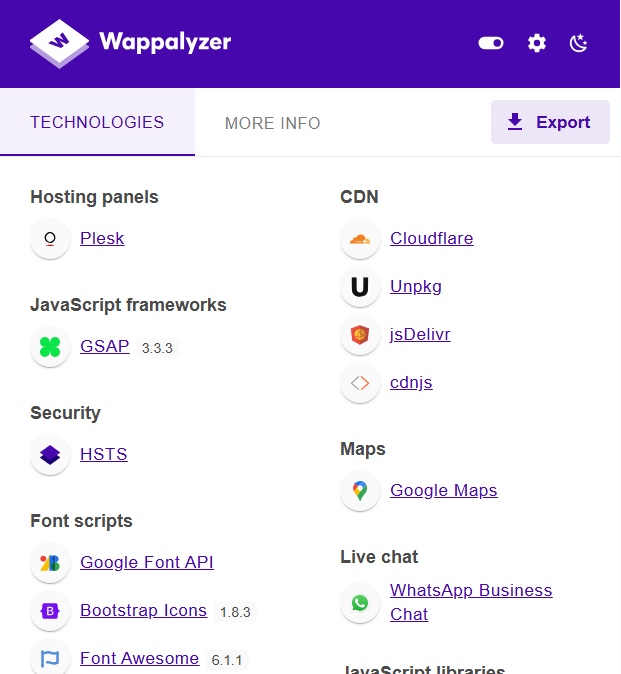


**Advance steps of the footprinting**

**1)Knowing the website technologies used on the target:-**

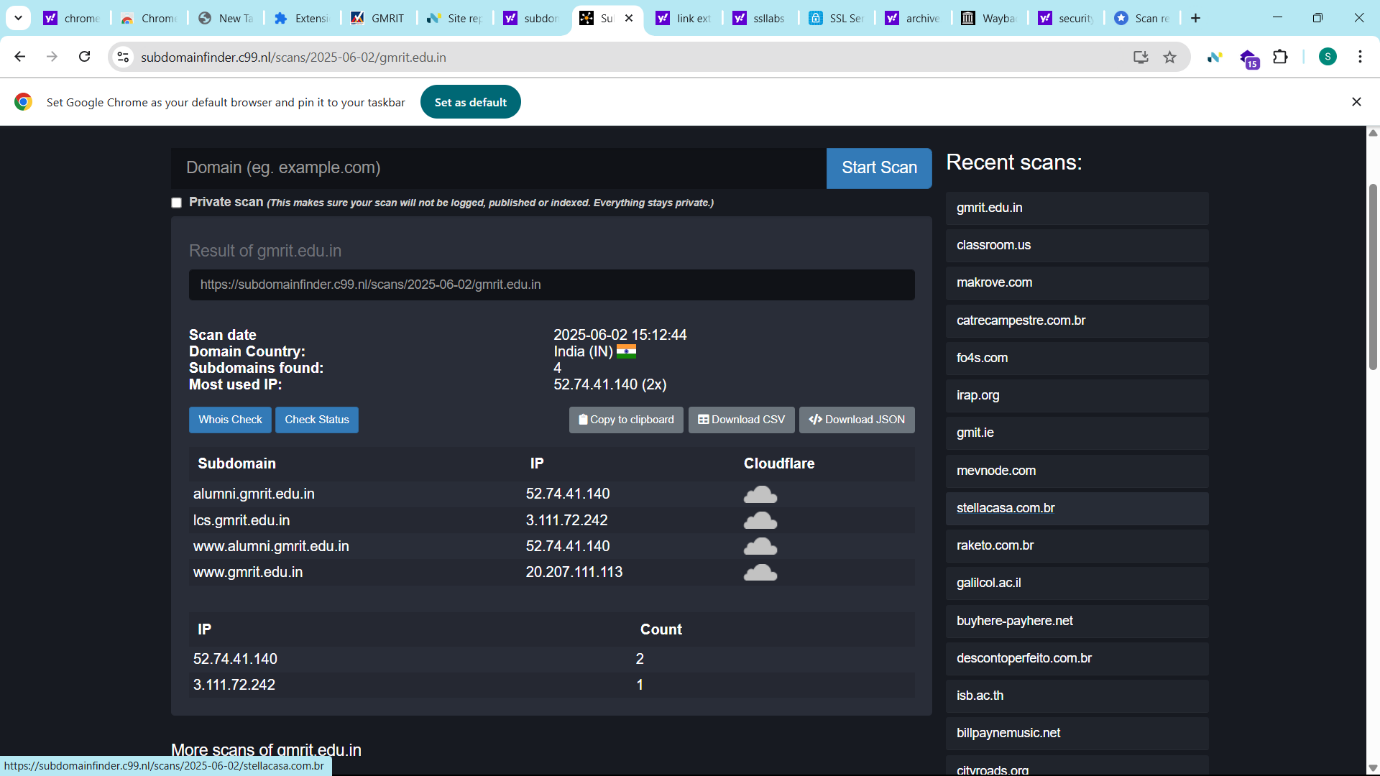
**What:** Identify the technologies a website uses.  
**Why:** To assess potential vulnerabilities, plan penetration testing, or understand site architecture.  
**How:** Use tools like Wappalyzer, Netcraft.





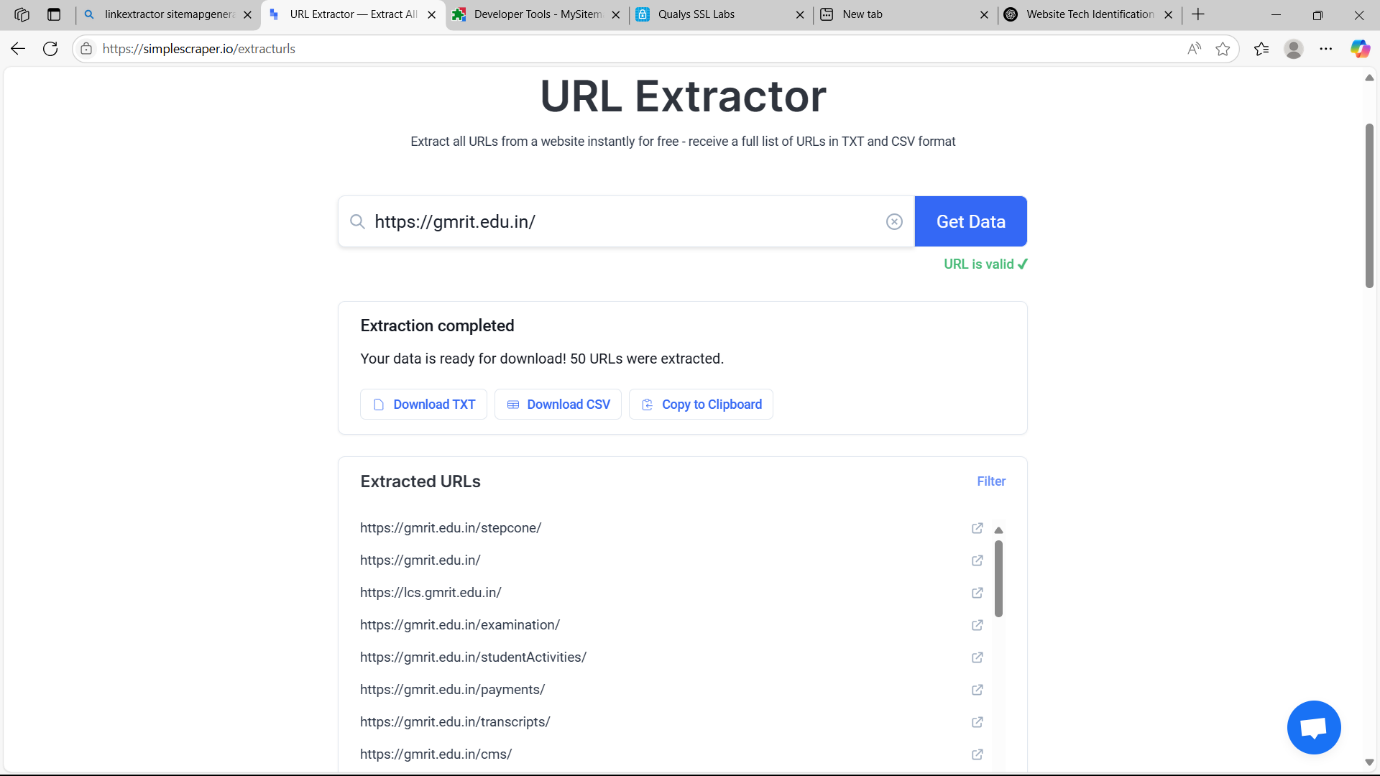
**2)Find the subdomain of a website:-**

**What:** Discover subdomains of a target website.  
**Why:** To uncover hidden or vulnerable services and expand the attack surface.  
**How:** Use tools like Subdomain finder.



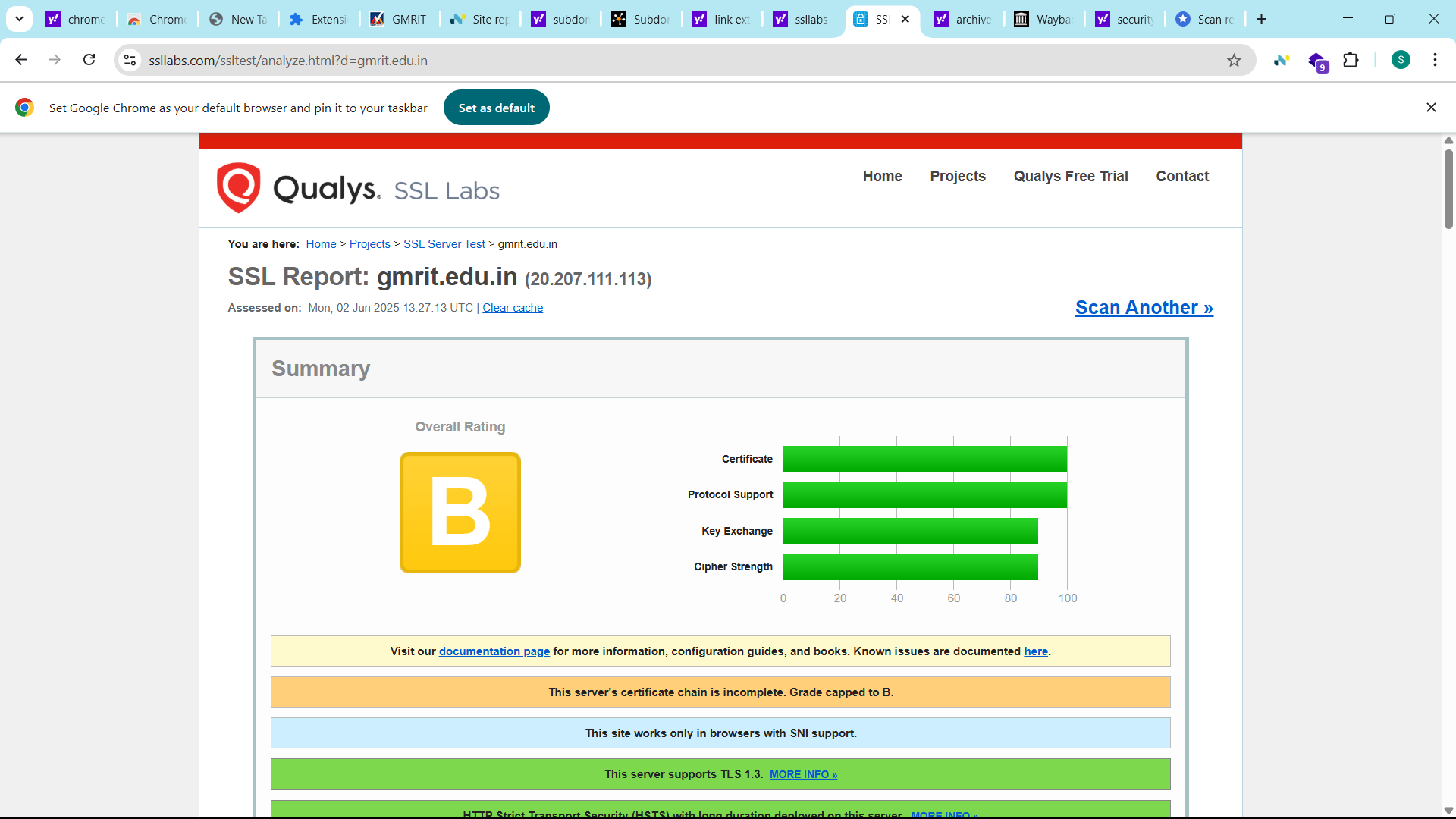
**3)Finding all the url’s of a website:-**

**What:** Gather all accessible URLs of a website.  
**Why:** To map the attack surface and identify hidden or sensitive endpoints.  
**How:** Use tools like Linkextractor.



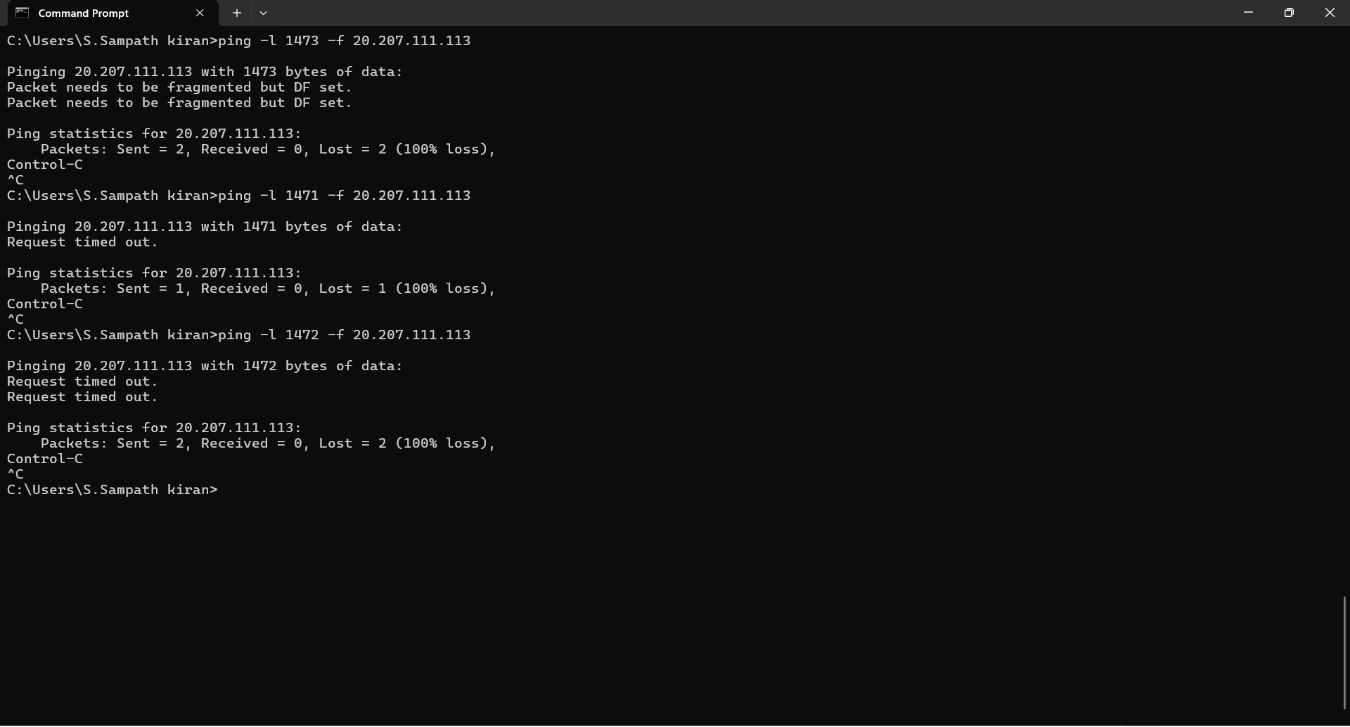
**4)Testing SSL/TLS:-**

**What:** Assess the SSL/TLS configuration of a website.  
**Why:** To identify weaknesses like outdated protocols or weak ciphers that could compromise data security.  
**How:** Use tools like SSL Labs.



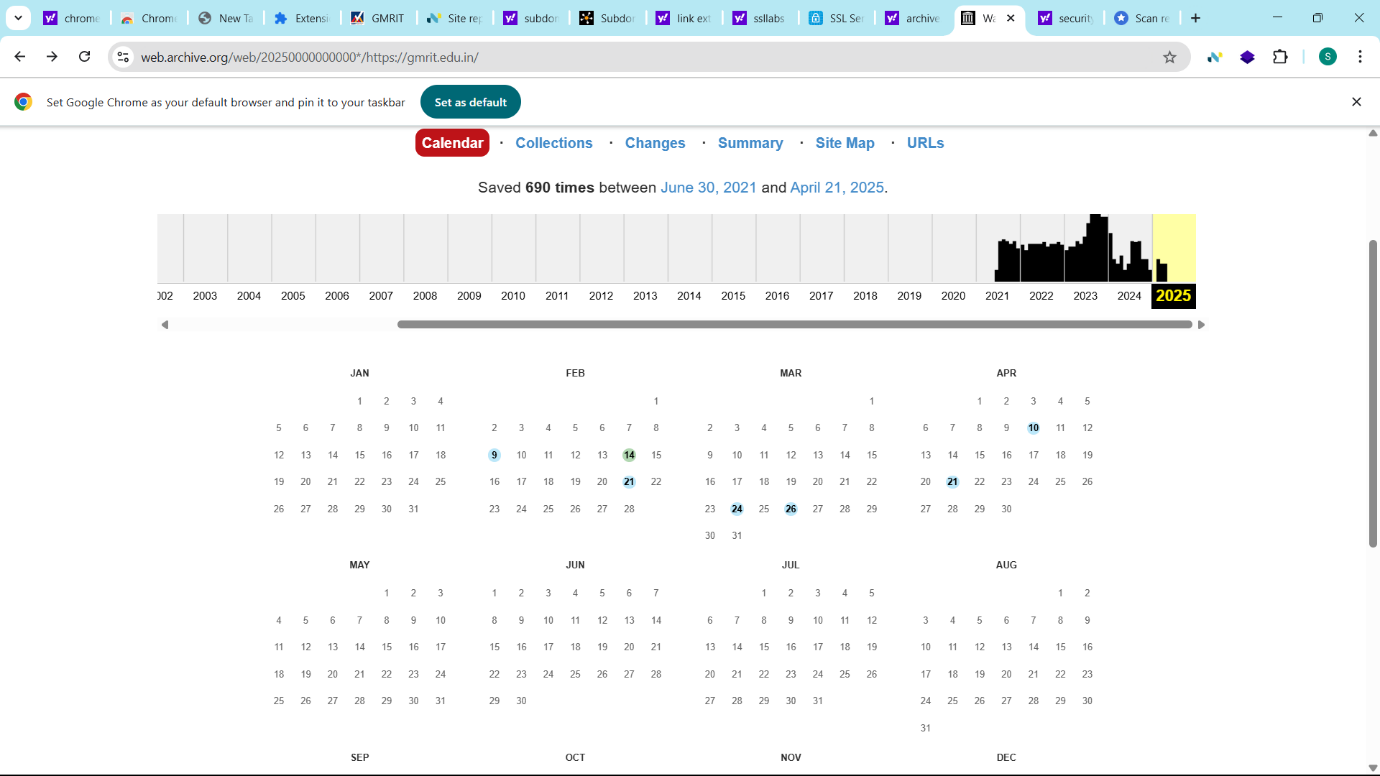
**5)Finding the buffer size of a website:-**

**What:** Determine the buffer size a web application can handle before causing overflow or crashes.  
**Why:** To identify potential buffer overflow vulnerabilities exploitable for code execution.  
**How:** Send progressively larger payloads using tools like fuzzers or scripts until the application crashes or behaves abnormally.



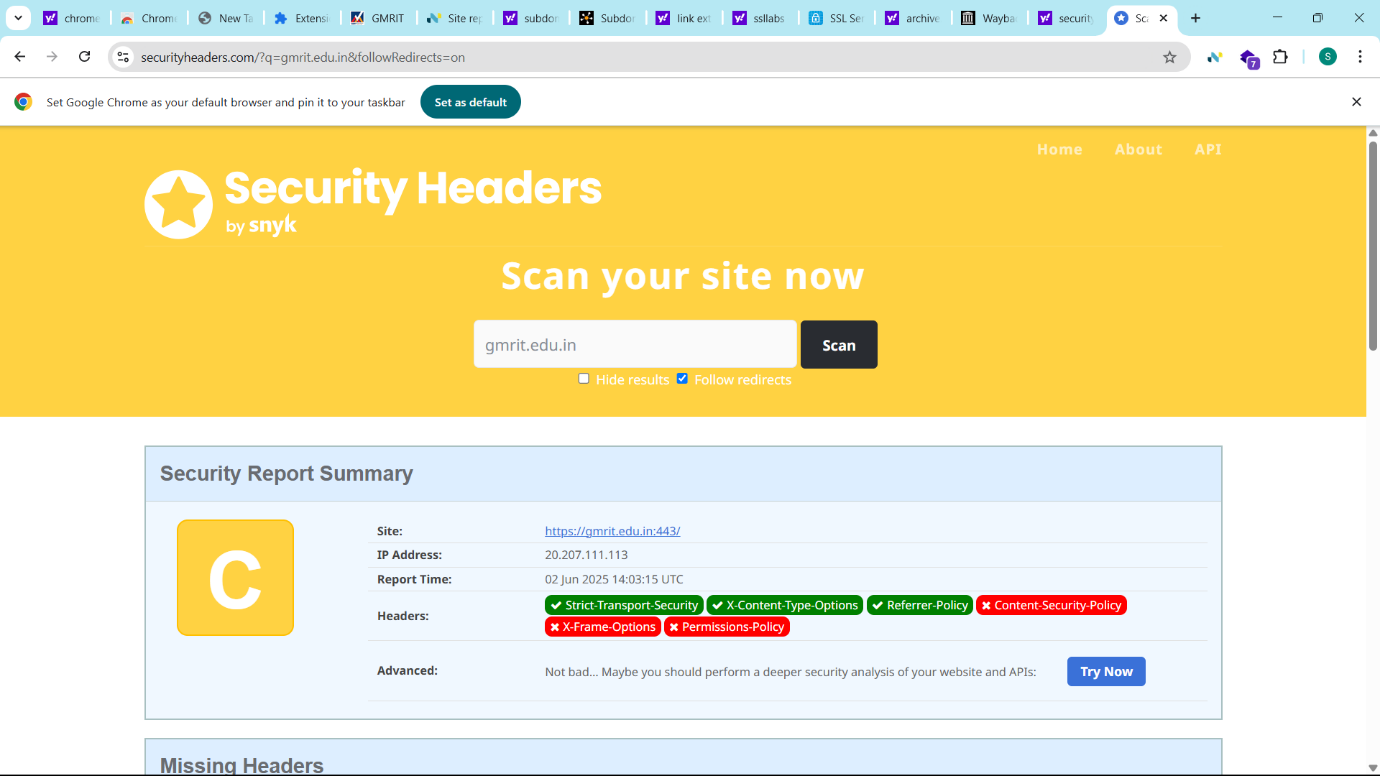
**6)Wayback machine:-**

**What:** View archived versions of a website using the Wayback Machine.  
**Why:** To discover removed pages, old endpoints, or sensitive data once publicly available.  
**How:** Search the target domain on Archive.org.



**7)Finding the missing security headers of a website:-**

**What:** Identify absent security-related HTTP headers on a website.  
**Why:** To detect misconfigurations that may expose the site to attacks like XSS, clickjacking, or content sniffing.  
**How:** Use tools like SecurityHeaders.com, curl, or browser developer tools to inspect response headers.



**Summary of Footprinting:-**

To gather detailed information about a target, use social networks and advanced search engines like Shodan or Censys to find exposed devices, open ports, and vulnerabilities. Employ Google dorks for precise searches to uncover hidden data and potential security flaws. Analyze website technologies, subdomains, URLs, and SSL/TLS setups to map the target’s attack surface. Utilize tools like the Wayback Machine to view archived content and check for missing security headers to identify misconfigurations. These steps collectively form a comprehensive footprinting process for effective security assessment.