Experiment 07

AIM:
To use OSINT tools to identify the technologies and frameworks used by a website (such as CMS, server software, programming languages, or analytics tools) and to create vulnerability reports based on the findings.

Theory:

Every website is built on a combination of technologies, including:

- **CMS (Content Management System)** – e.g., WordPress, Joomla, Drupal.
- **Web Server Software** – e.g., Apache, Nginx.
- **Programming Languages & Frameworks** – e.g., PHP, Python, JavaScript (React, Angular, Vue).
- **Analytics Tools** – e.g., Google Analytics, Hotjar.
- **CDNs** – e.g., Cloudflare, Akamai.
- **Ad/Marketing Platforms** – e.g., Google Ads, Facebook Pixel.

Identifying these technologies helps in **profiling the target website** and detecting **possible vulnerabilities**. Attackers often exploit known flaws in outdated CMS plugins, server software misconfigurations, or insecure analytics/tracking setups.

WhatRuns is a commonly used OSINT tool for this purpose:

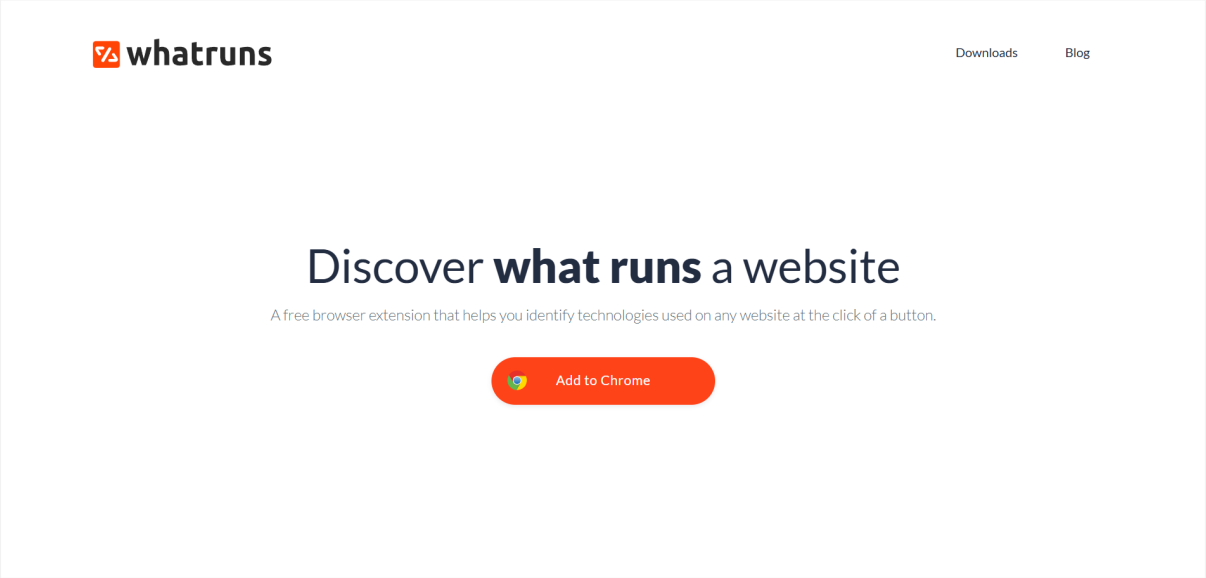
- It is a browser extension that detects the technologies behind websites.
- Once activated, it scans the webpage and displays the list of detected tools and frameworks.
- It provides insights into CMS, JavaScript libraries, fonts, analytics, ads, and server information.

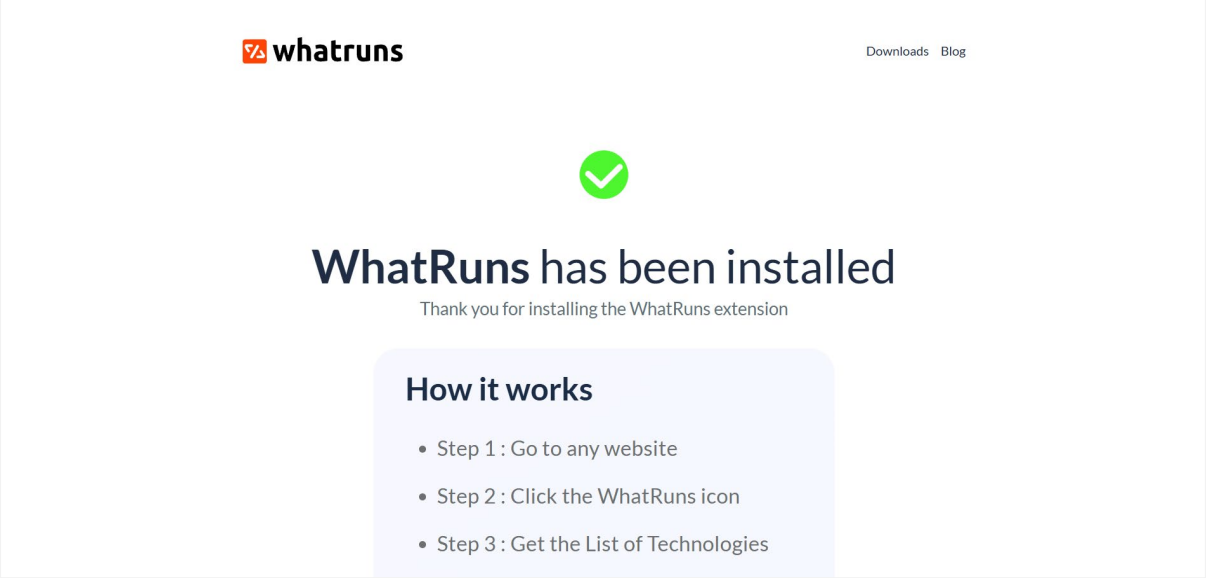
Requirements / Tools Used:

1. **WhatRuns Browser Extension** (available for Chrome/Firefox).
2. Test website (target of analysis).
3. Internet connectivity.

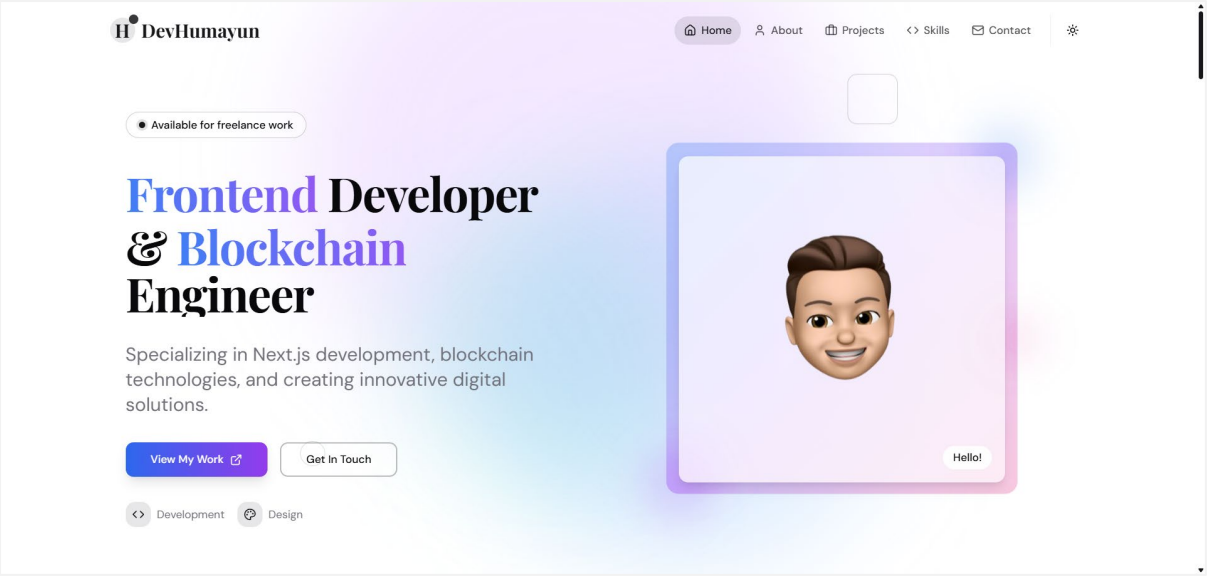
Procedure

1. **Install WhatRuns**
   - Open your browser's extension store.
   - Search for **WhatRuns** and add it to the browser.

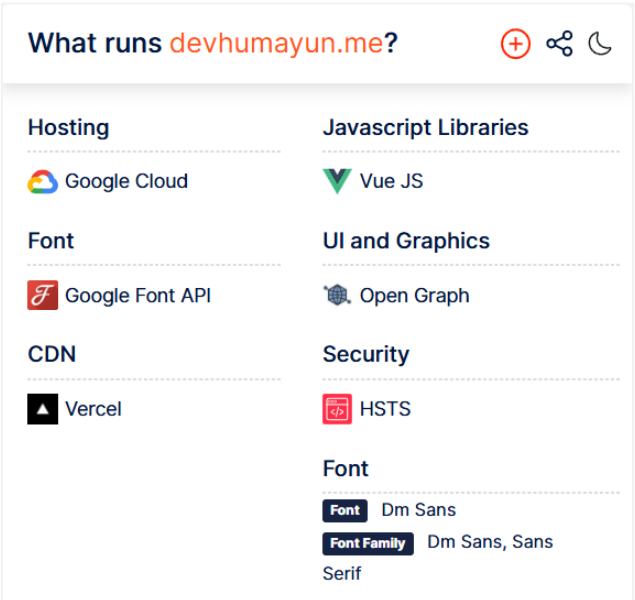




2. **Visit Target Website**
   - Navigate to the website you want to analyze.
   - www.devhumayun.me



3. **Activate WhatRuns**
   - Click on the WhatRuns icon in the browser toolbar & The extension scans the current site.
4. **View Technology Stack**
   - The extension displays detected technologies under categories:
     - Server software
     - JavaScript libraries/frameworks
     - Analytics tools
     - Fonts and UI libraries
     - CDN services



5. **Document the Findings**
    - Note down the complete technology stack detected.
    - DevHumayun:
        - Hosting → Google Cloud
        - Font → Google Font API
        - CDN → Vercel
        - JavaScript Libraries → Vue JS
        - UI and Graphics → Open Graph
        - Security → HSTS

Observations

- The WhatRuns tool provides a **clear overview of the tech stack** of the target site.
- It highlights multiple categories, making it easier to perform **technology fingerprinting**.
- Example vulnerabilities may include:
    - Outdated WordPress plugins (susceptible to XSS/SQLi).
    - Old Apache/Nginx versions with security flaws.
    - Exposed analytics tools leaking user behavior.

Conclusion

We have successfully used OSINT Tools to identify the technologies and frameworks used by the website, such as content management systems (CMS), server software, programming languages, or analytics tools and create vulnerability reports.