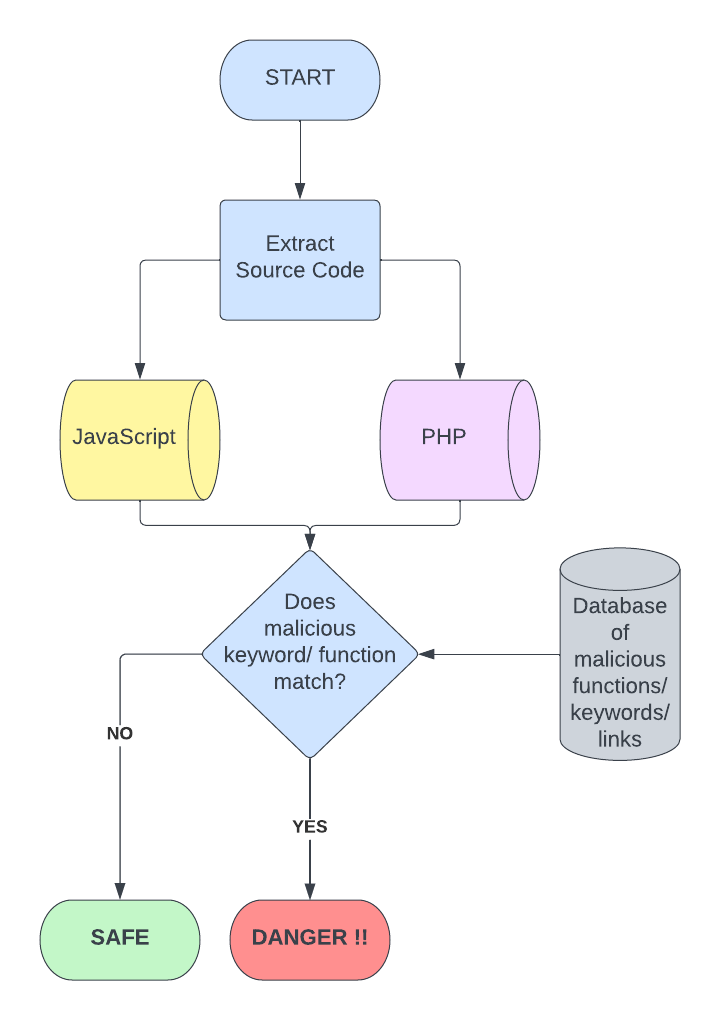
**Technology used:**

**MALICIOUS URL LINK DETECTOR: WEBSITE**

This program has been written in python and can be used as a Chrome extension that implements the detection of malicious websites in two methods:

First, it scans the source code of URLs and analyses its PHP and JS code

It uses various database of malicious functions, keywords, and links to analyse if the source code is suspicious.

**Working of program:**

1. **Extraction of source code:** The code is to be implemented as a chrome extension that can scan your webpage and extract their source code
2. **PHP and JS code analysis:** Then all PHP (<?php … ?>) and JS (<script> … </script>) code is extracted from the source codde and stored separately for analysis.
3. **Database:** A database of various malicious functions, links and keywords is maintained that is used to check the source code of the websites.
4. **Comparison:** The extension compares the database against the source code and provides an analysis of:
   1. **Status:** Whether the website is safe or not
   2. **Vulnerability:** What function or keyword has raised the alert
   3. **Severity:** This shows the severity of the potential exploit and threat
   4. **Remediation:** What next steps should the user take.

**How it can be improved:**

We can improve this technique by using a database that auto updates itself to make the malicious website detection more dynamic.

Recently discovered malware URLs can be appended to the database.

We can also enhance the ability to detect malware messages by using a more sophisticated language processing model that auto detects malicious words instead of using a small pool of words in the list.