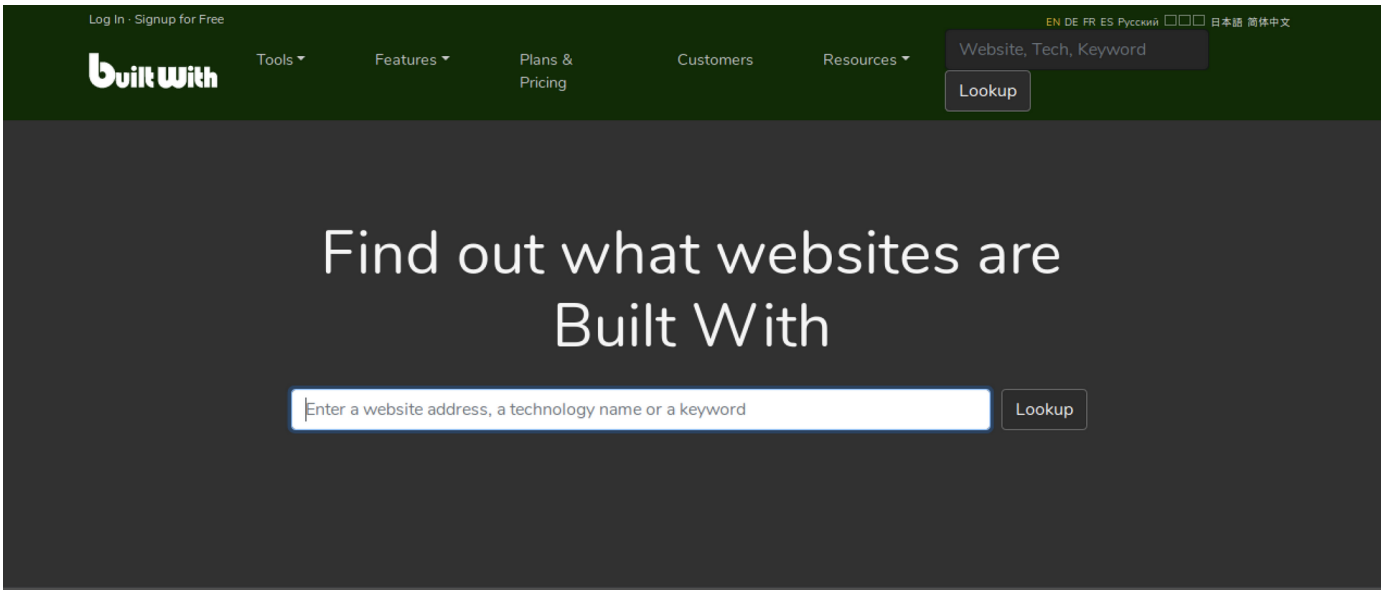
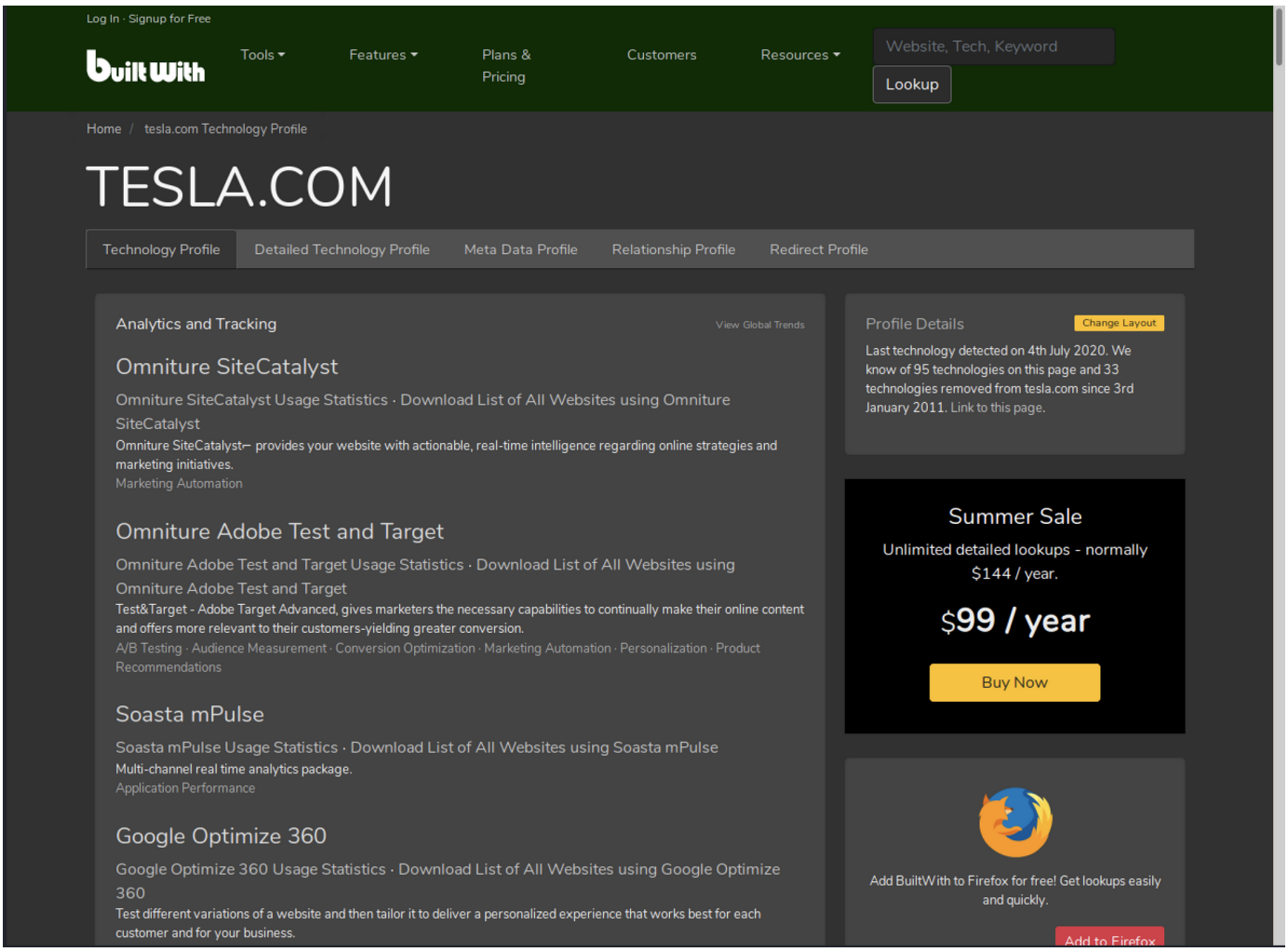
Identifying Website Technologies

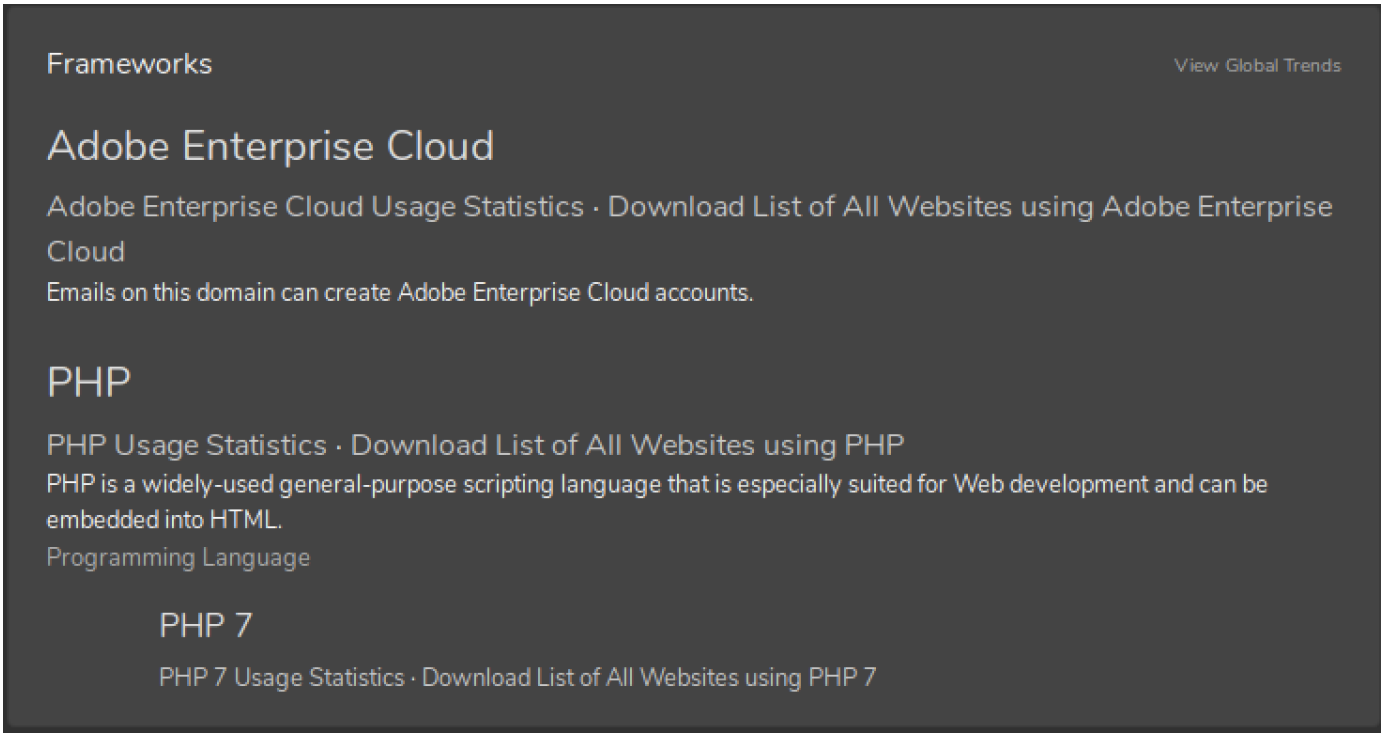
We will be trying to identify the underlying technology behind web applications. We will use an online tool called "BuiltWith" which can be found at https://builtwith.com/ shown below:

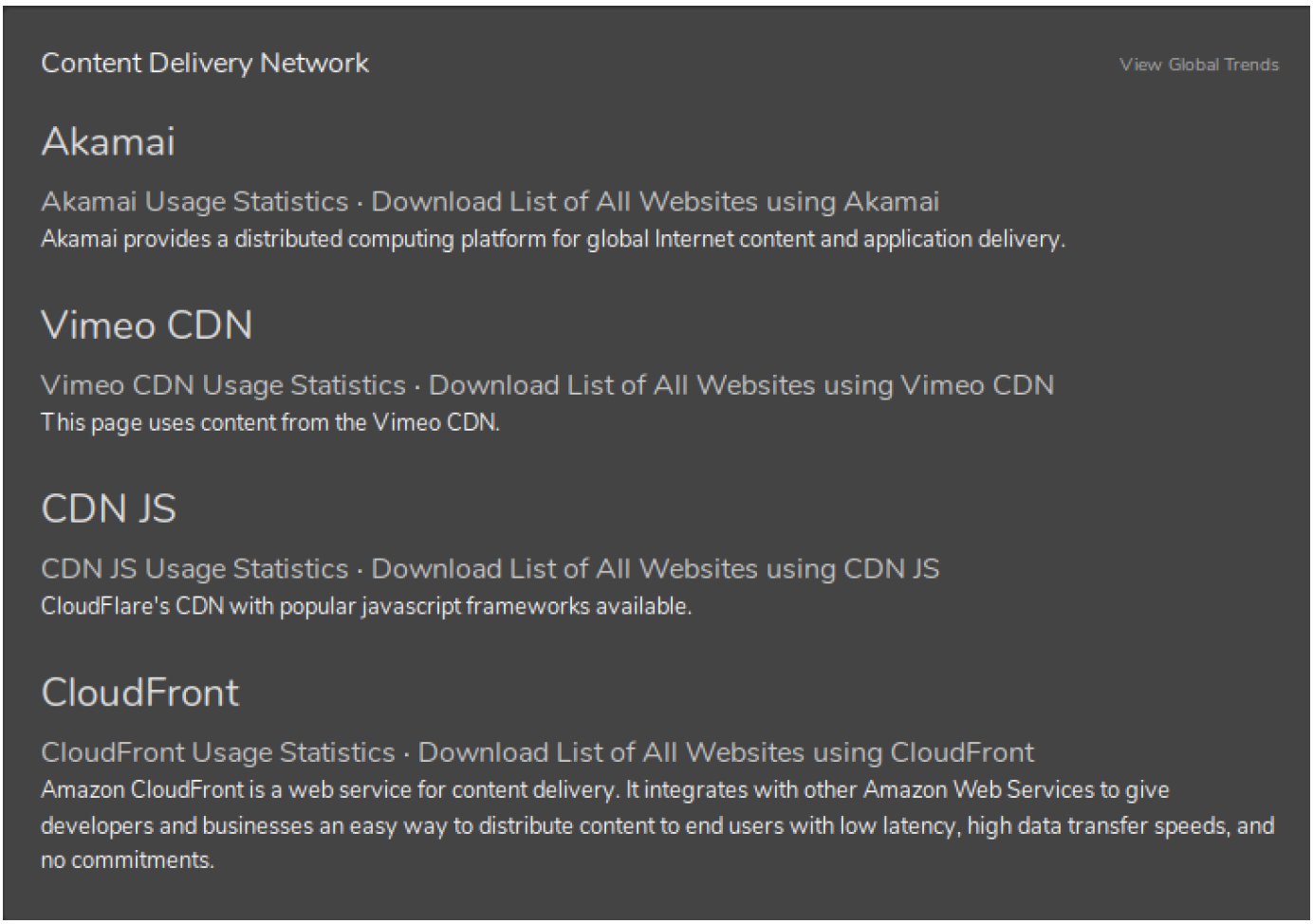


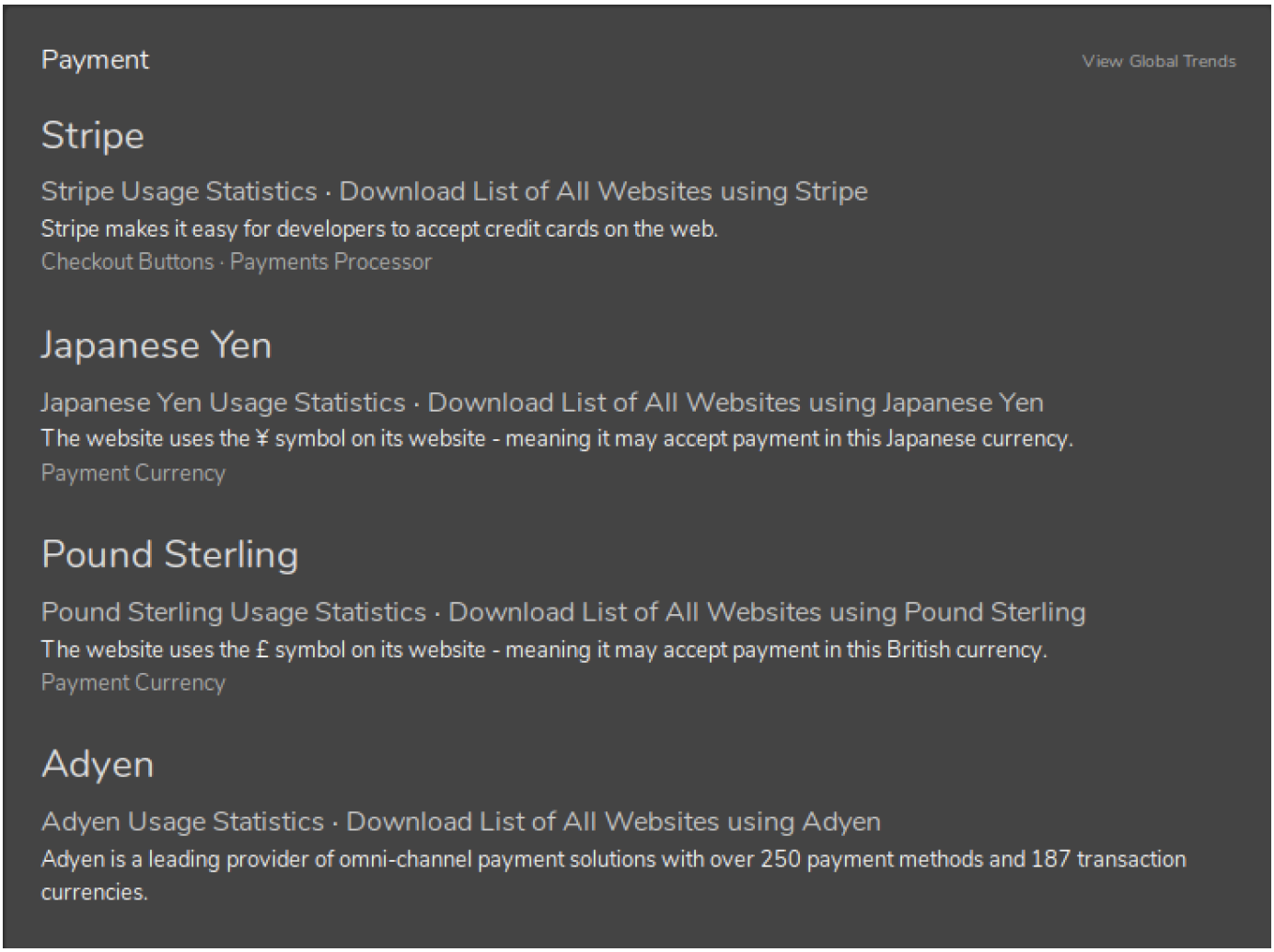
In the lookup text box, we can search for a domain e.g `tesla.com` as shown below:

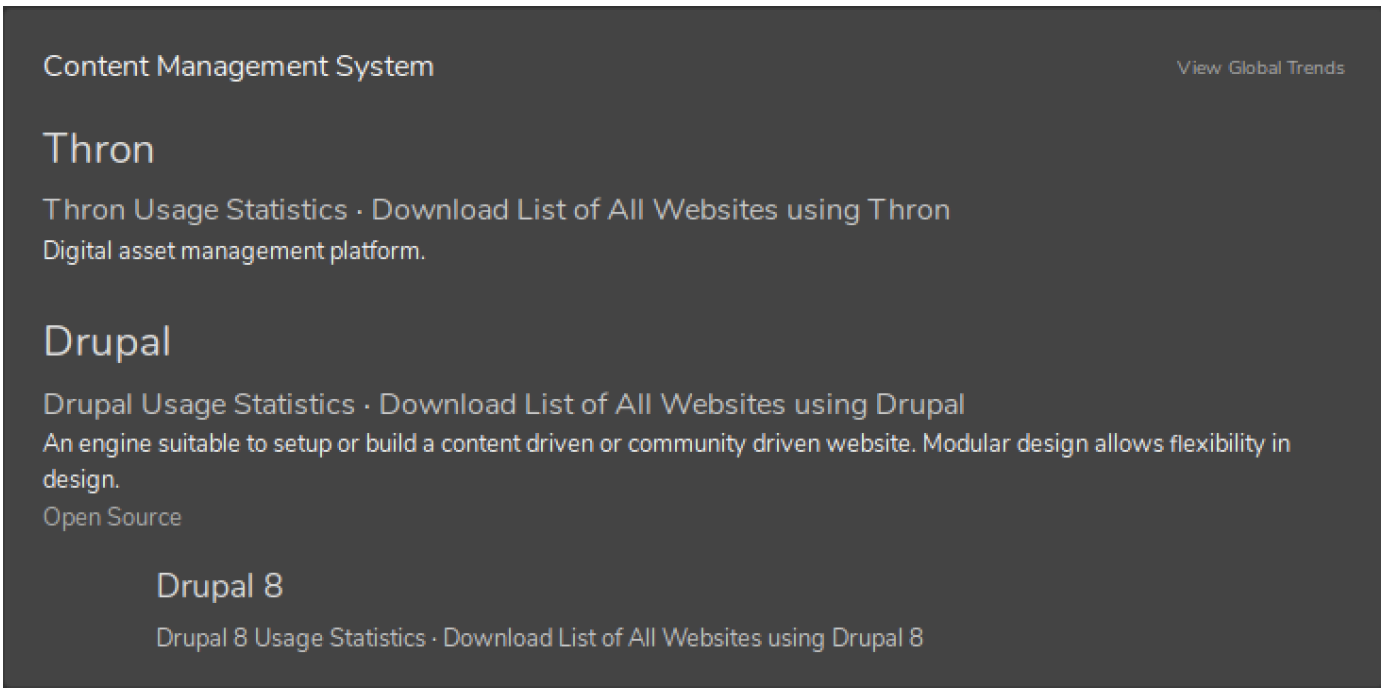


While scrolling through the page, we notice that there are various sections such as "Analytics and Tracking", "Widgets", etc. We are more interested in sections such as "Frameworks", "Content Delivery Network", "Payment", "Content Management System" shown below:

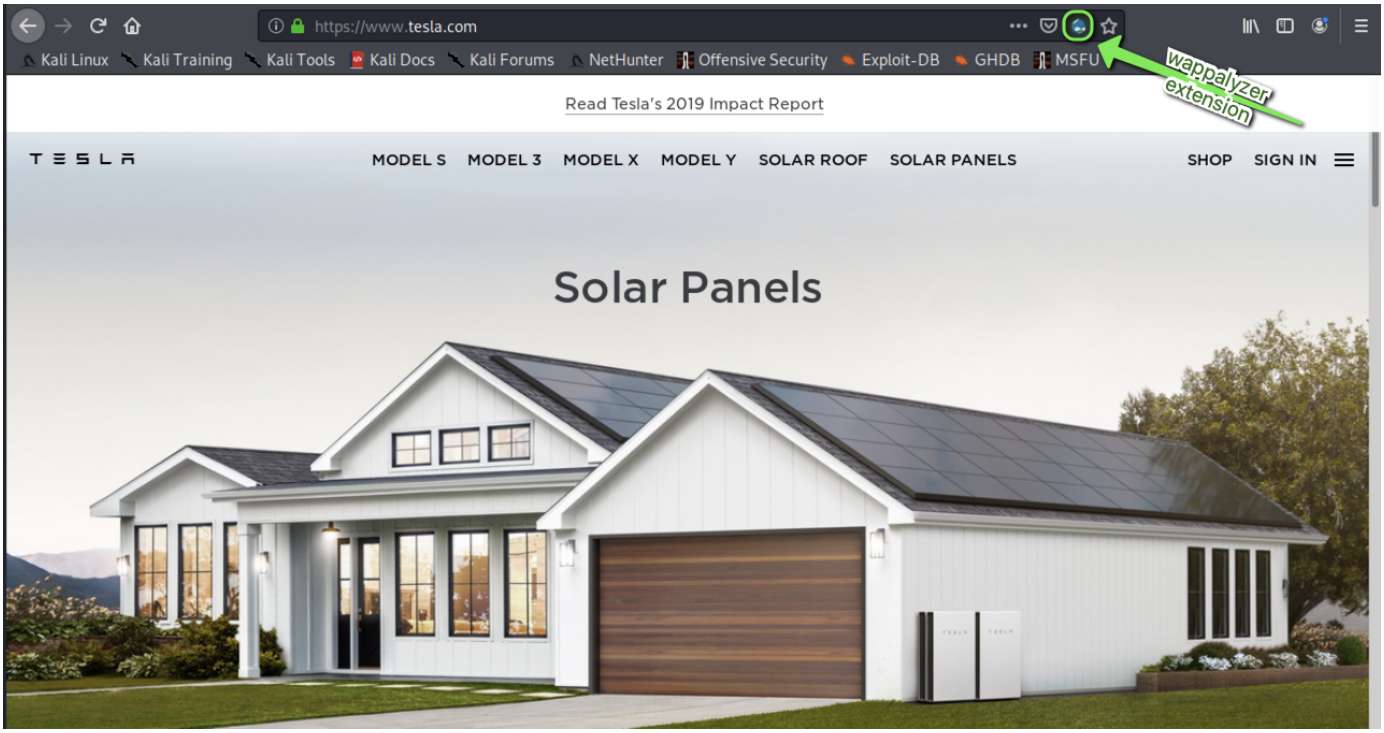


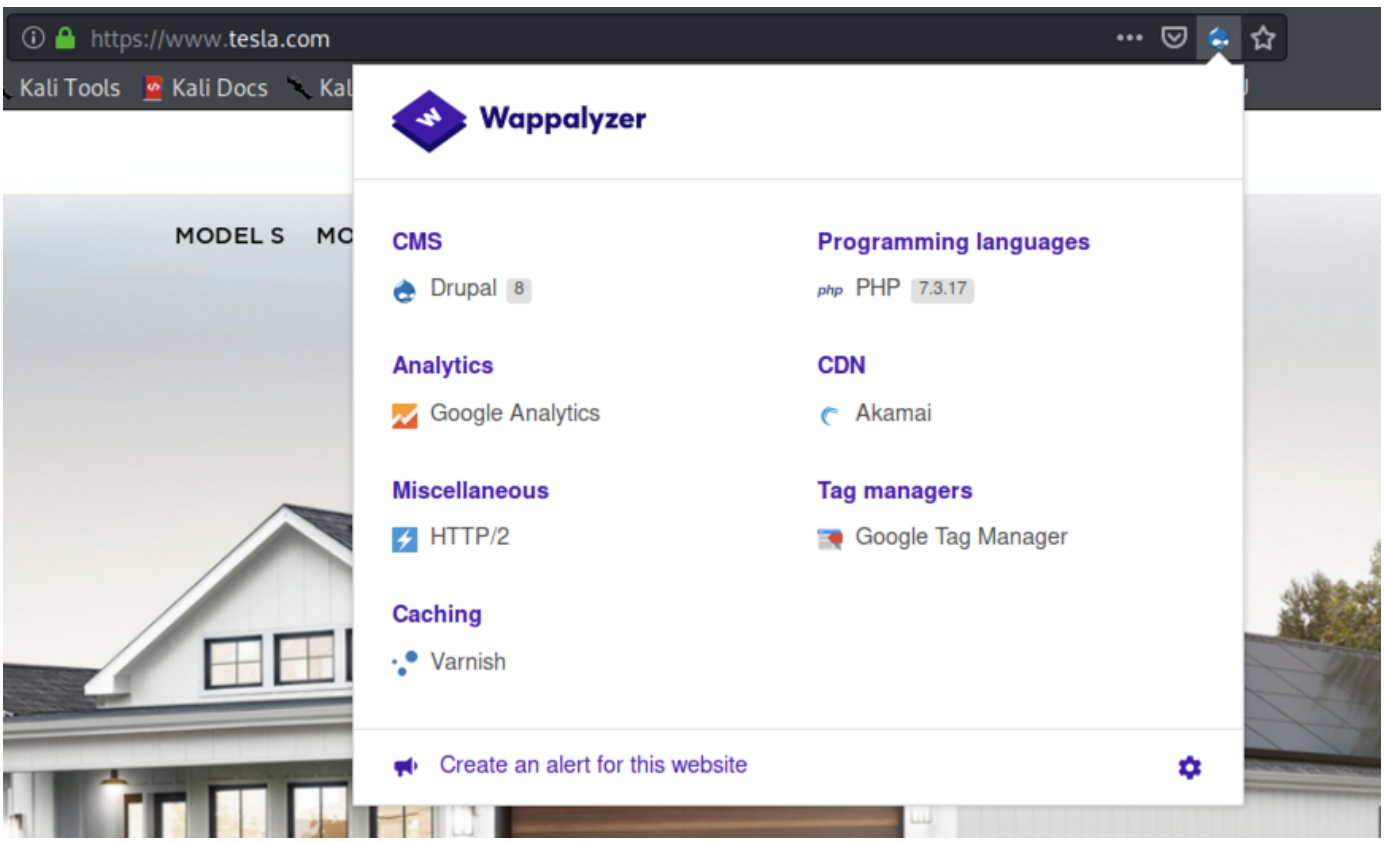






We can also use a tool called "wappalyzer firefox". It functions as a browser extension that analyzes the frameworks that support a website. An example is shown below:



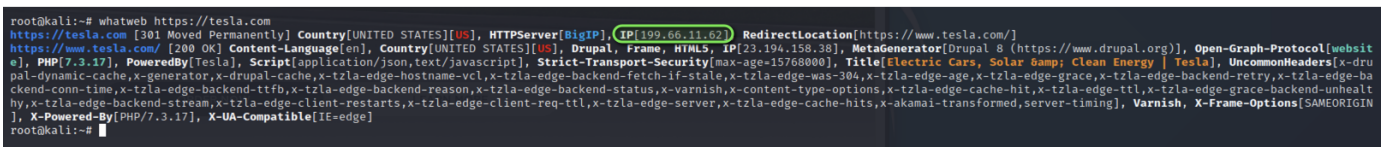


The wappalyzer tool does not do any in-depth "active" scanning. It basically gives a summary of the easily detectable services running on a website. It still provides some helpful insight to give us an idea of the potential vulnerabilities in a system. For example, the result from the `tesla.com` page shows that it is running on `PHP` and `Drupal`. If there's a known vulnerability in that version of `PHP` or `Drupal`, we could hypothesize that website exploitation is possible.

We also have another tool called `whatweb` shown below. It's a tool that's native to Kali Linux.

```
root@kali:~# whatweb

.$$$     $.                                  .$$$     $.
$$$$     $$. .$$$  $$$ .$$$$$$.  .$$$$$$$$$$. $$$$     $$. .$$$$$$$. .$$$$$$.
$ $$     $$$ $ $$  $$$ $ $$$$$$. $$$$$ $$$$$$ $ $$     $$$ $ $$   $$ $ $$$$$$.
$ `$     $$$ $ `$  $$$ $ `$  $$$ $$' $ `$ `$$ $ `$     $$$ $ `$      $ `$  $$$'
$. $     $$$ $. $$$$$$ $. $$$$$$ `$  $. $  :' $. $     $$$ $. $$$$   $. $$$$$.
$::$  .  $$$ $::$  $$$ $::$  $$$      $::$     $::$  .  $$$ $::$      $::$  $$$$
$;;$ $$$ $$$ $;;$  $$$ $;;$  $$$      $;;$     $;;$ $$$ $$$ $;;$      $;;$  $$$$
$$$$$$ $$$$$ $$$$  $$$ $$$$  $$$      $$$$     $$$$$$ $$$$$ $$$$$$$$$ $$$$$$$$'


WhatWeb - Next generation web scanner version 0.5.2.
Developed by Andrew Horton (urbanadventurer) and Brendan Coles (bcoles)
Homepage: https://www.morningstarsecurity.com/research/whatweb

Usage: whatweb [options] <URLs>

  <TARGETs>                     Enter URLs, hostnames, IP addresses, filenames or
                                IP ranges in CIDR, x.x.x-x, or x.x.x.x-x.x.x.x
                                format.
  --input-file=FILE, -i         Read targets from a file.

  --aggression, -a=LEVEL        Set the aggression level. Default: 1.
  1. Stealthy                   Makes one HTTP request per target and also
                                follows redirects.
  3. Aggressive                 If a level 1 plugin is matched, additional
                                requests will be made.

  --list-plugins, -l            List all plugins.
  --info-plugins, -I=[SEARCH]   List all plugins with detailed information.
                                Optionally search with a keyword.

  --verbose, -v                 Verbose output includes plugin descriptions.

Note: This is the short usage help. For the complete usage help use -h or --help.

root@kali:~#
```

Here is a sample run of the tool shown below:



In the sample run, we can see that it retrieved some information such as the IP address (hiighlighted), and some services and other information.