Identifying Website Technologies

Identifying the technologies employed by a website can provide valuable insights into potential vulnerabilities, attack vectors, and defense mechanisms. By recognizing the content management systems (CMS), web servers, programming languages, and frameworks in use, we can tailor your reconnaissance efforts and develop targeted strategies for further exploration.

Site technologies Enumeration

- Builtwith
- Whatweb

```
whatweb zomato.com
```

- Wappalyzer
- Netcraft - https://sitereport.netcraft.com/
- Nerdy Data - https://www.nerdydata.com
- Platform discovery with Favicon - https://wiki.owasp.org/index.php/OWASP_favicon_database

Sometimes when frameworks are used to build a website, a favicon that is part of the installation gets leftover, and if the website developer doesn't replace this with a custom one, this can give us a clue on what framework is in use. OWASP host a database of common framework icons that we can use to check against the targets favicon

- use the curl command to download the favicon and get his MD5 hash.

```
curl https://example.com/favicon.ico | md5sum
```

- Compare it with OWASP favicon database to get the framework used in the website
- If hash ends with 427e, then curl failed.
