Open Source code reconnaissance

Open source code reconnaissance involves searching for and analyzing publicly available source code, configuration files, and other artifacts related to the target organization or its products and services.

This technique can provide insights into the technologies, frameworks, and libraries used by the target, as well as potential security flaws or misconfigurations.

- We can use open source repos like Github, Github Gist, Gitlab and Sourceforge to reveal some sensitive info.

Enumeration using Github search

- Go to Github search.
- Check for files of a given owner.

```
owner:megacorpone path:users
```

So, sometimes what happen is that, while pushing the code, developers forget to remove the hardcoded credentials or API keys from it. If we get something juicy like this, that is no less than a lottery.

We can use these credentials later at our exploitation phase of the penetration test giving us an easy access to the target environment.
