**Information Gathering of Website(Whatweb)**

In this section, we will discuss various techniques to gather information about the client using the Whois Lookup, Netcraft, and Robtex. Then we will see how we can attack a server by targeting websites that are hosted on that server. Moving towards the information gathering section, we will learn about subdomain and how they can be useful for performing attacks. Later we are going to look for files on the target system to gather some information and also analyze that data.

Now, we will do information gathering before we start trying to exploit. Therefore, we are going to gather as much information as we can about the IP of the target, the technology that is used on the website, the domain name info, which programming language is used, what kind of server is installed on it, and what kind of database is being used. We will gather the company's information and its DNS records. We will also see subdomains that are not visible to other people and we can also find any files that are not listed. Now we can use any of the information gathering tools that we used before, for example, we can use Maltego and just insert an entity as a website, and start running actions. We can also use Nmap, or even Nexpose, and test the infrastructure of the website and see what information we can gather from that.

How to use whatweb?

Copy the given code in linux/termux software

whatweb –v website(any website you want to get information about)

**Repositorylink:** [**https://github.com/Pragyesh1212/websiteinformation.git**](https://github.com/Pragyesh1212/websiteinformation.git)