Finding Hidden parameters and endpoints

During the reconnaissance phase of security assessments, identifying and analyzing JavaScript files can reveal valuable information about the target's infrastructure, including the existence of undocumented or hidden endpoints.

We'll explore techniques for finding and enumerating JavaScript endpoints associated with a target website or web application.

Hidden endpoints of the website can be used to perform Penetration Testing on the domain. Detection of these endpoints is difficult if we are using a manual way. So we need to have an automated script that can detect the endpoints of JavaScript links. LinkFinder is an automated tool developed in the Python language which detects the endpoints and their parameters on the target domain.

- Use LinkFinder to find JS endpoints

```
python3 linkfinder.py -i https://paytm.com
```

Next, we have Arjun. This tool is also designed specifcally to find hidden HTTP and JS parameters.

- Use Arjun to find hidden parameters & endpoints

```
arjun -u https://paytm.com
```
