Vulnerability scanning with nikto

Nikto is an open-source web server scanner that performs comprehensive tests against web servers, searching for outdated versions of software, misconfigured server settings, and other potential vulnerabilities that could be exploited by malicious actors. It's like having a highly skilled detective on your side, meticulously investigating every nook and cranny of your web applications to uncover any weaknesses.

So, let get started.

- To perform a basic scan first.

```
nikto -h IP
```

- To scan websites running on HTTPS (SSL/TLS)

```
nikto -h https://zomato.com --ssl
```

- To save the output in a text file

```
nikto -h IP -O scan_results.txt
```

- To perform scan on a list of websites.

```
nikto -h websites.txt
```

- The main issue with nmap is that it is very slow by default. But we can use options tuning and threads to speed up our scans.

```
nikto -h https://zomato.com --ssl -Tuning 10

nikto -h target.txt -threads 10
```
