**DAY 34**

sql map – in kali linux – automated sql injection vulnerability testing.

Command for sqlmap:

#sqlmap -u <http://berkeleyrecycling.org/page.php?id=1>

This command is used to find out any kind of sql injection vulnerabilities using the id parameter.

#sqlmap -u <url with id parameter> --level=(1,2,3,4,5) –risk=(1,2,3) –current-db –current-user …..

Do not use dump command

Google dorks:

Google dorks are advanced search queries which are used to provide exact context from website(s)

Official link: <https://exploit-db.com>

Google dorks are used by ethical hackers to find out vulnerable links and endpoints to test on those vulnerabilities.

Why do ethical hacker needs to enumerate sub-domains?

🡪base domain may not be vulnerable so the ethical hacker goes with sub domains.

🡪Consider sub domains aren’t vulnerable now the ethical hacker goes with sub-sub-domains.

Because the ethical hacker need to look into every nook and corner of the target the ethical hacker need to enumerate sub domains

Note: We should enumerate both active and inactive sub domains

Open source platforms to enumerate sub domains:

1. virustotal.com

2. crt.sh

Github tools:

1. sublist3r

2. subbrute

3. amass sub domain enumerator