Google Dorking

Lab 3: Recon using google Dorking

Google hacking DBs: It is a passive information gathering technique by the use of google. Hacker's gather information of target. Hackers invest 90% times of information gather (Recon).

We did fuzzing is the part of recon and it's came into the category of Active reconnaissance.

Reconnaissance types:

1. Active
2. Passing

Basic google Dorking

Google Dork: keywords to narrow down results.

google> hacking //Gives random result-article

google> intitle: hacking

google> intitle: hacking filetypes: pdf

with the use of this, we can filter out those websites who are unintentionally leaved .env file.

Exposing:

Google> filetype: env "DB_PASSWORD"

Note: double quotation is for exactly match the keyword specified.

It will list all those websites which disclose the environment file. It's a basic misconfiguration, done by developer (.env file exposed onto the server).

CCTV Camera Exposure

Use this for specific moboTix. Here URL for this will be "control/userimage.html"

This URL give us misconfigure cameras which mean where authentication not included. So, google can crawl & can filter out those targets.

- inurl: control/userimage.html
- intitle: "VNC viewer for JAVA"
- inurl: view.shtml //It's a service
- intext: "AXIS Q6155-E Network Camera" //Website who having this text.
- Inurl: .php? intext: CHARACTER_SETS, COLLATIONS intitle: phpMyAdmin //Misconfigured PHP my admin panel.
- Intext: "index of" ".sql" //Result who placed SQL files on server (by mistake) in Apache & ngX, these are directory in which we are visiting having the title as index of.