Google Dork Report

Cyber Security Bootcamp - µLearn x OWASP Kerala
Task 2 – Google Dorking
Name: Saniya Mary Jacob
GitHub Username: Zaniyahm

Aim

The objective is to use Google Dorks to identify publicly exposed documents or directories that may contain sensitive or interesting data. The search was limited to publicly available content indexed by Google, using advanced search operators like `site:`, `filetype:`, and `intitle:`.

Dork 1

Query Used: site:tesla.com filetype:pdf

Result:

- https://www.tesla.com/ownersmanual/modely/da_dk/Owners_Manual.pdf
- https://www.tesla.com/ownersmanual/modely/hu_hu/Owners_Manual.pdf

Dork 2

Query Used: intitle:"index of" "tesla"

Result:

No valid open directory result was found during this search. The query returned generic links not matching expected "index of" directory listings.

Dork 3

Query Used: site:tesla.com inurl:login

Result:

- https://solarbonds.tesla.com/a/login/

Summary

I explored the use of Google Dorking techniques to identify publicly exposed files or directories from target domains. Using advanced search operators like `site:`, `filetype:`, and `intitle:`, I was able to locate publicly accessible documents indexed by Google.