Task 2: *Report on Google Dorking Findings and Confidential Information Exposure*

Date: 21/07/2025

Prepared For: MuLearn bootcamp

Prepared By: Atul H

Executive Summary

This report documents the use of Google Dorks to identify publicly exposed sensitive documents, as part of the MuLearn x OWASP Cyber Security Bootcamp's weekly task. The investigation focused on leveraging specific advanced search queries to uncover confidential files indexed by Google.

Introduction

Google Dorking is the technique of using advanced operators in Google Search to find information that is not readily visible or intended for public access. Cybersecurity professionals and researchers often utilize Google Dorks to identify unintentionally exposed sensitive files, misconfigured servers, or other public leaks as a part of responsible disclosure.

Goal: to identify publicly exposed confidential contents or files using google dorking.

Googles search engine is used for this dorking purpose(www.google.com)

Targeted domains: google.com, also tried Netflix.com but got no results.

Dorks used:

site:google.com intext:"confidential" filetype:pdf

- Searched for PDF files on the specified domain containing the word "confidential".-
- This query was repeated for "netflix.com", but no relevant results were found.

Findings:

https://services.google.com/fh/files/misc/self_cert_creator_guide.pdf

https://www.google.com/press/pdf/b_hurley_opp_declaration.pdf -- DECLARATION OF BRENT HURLEY IN OPPOSITION TO PLAINTIFFS' MOTIONS FOR SUMMARY JUDGMENT (marked highly confidential)

https://services.google.com/fh/files/misc/crr-rra-soy-form.pdf -- Google Registry-Registrar Agreement (.soy RRA form) (marked confidential in each pages.)

One file was marked highly confidential among them.

Risk identified: exposed document includes legal, internal or proprietary data.