Google Dorks Lab Assignment Report

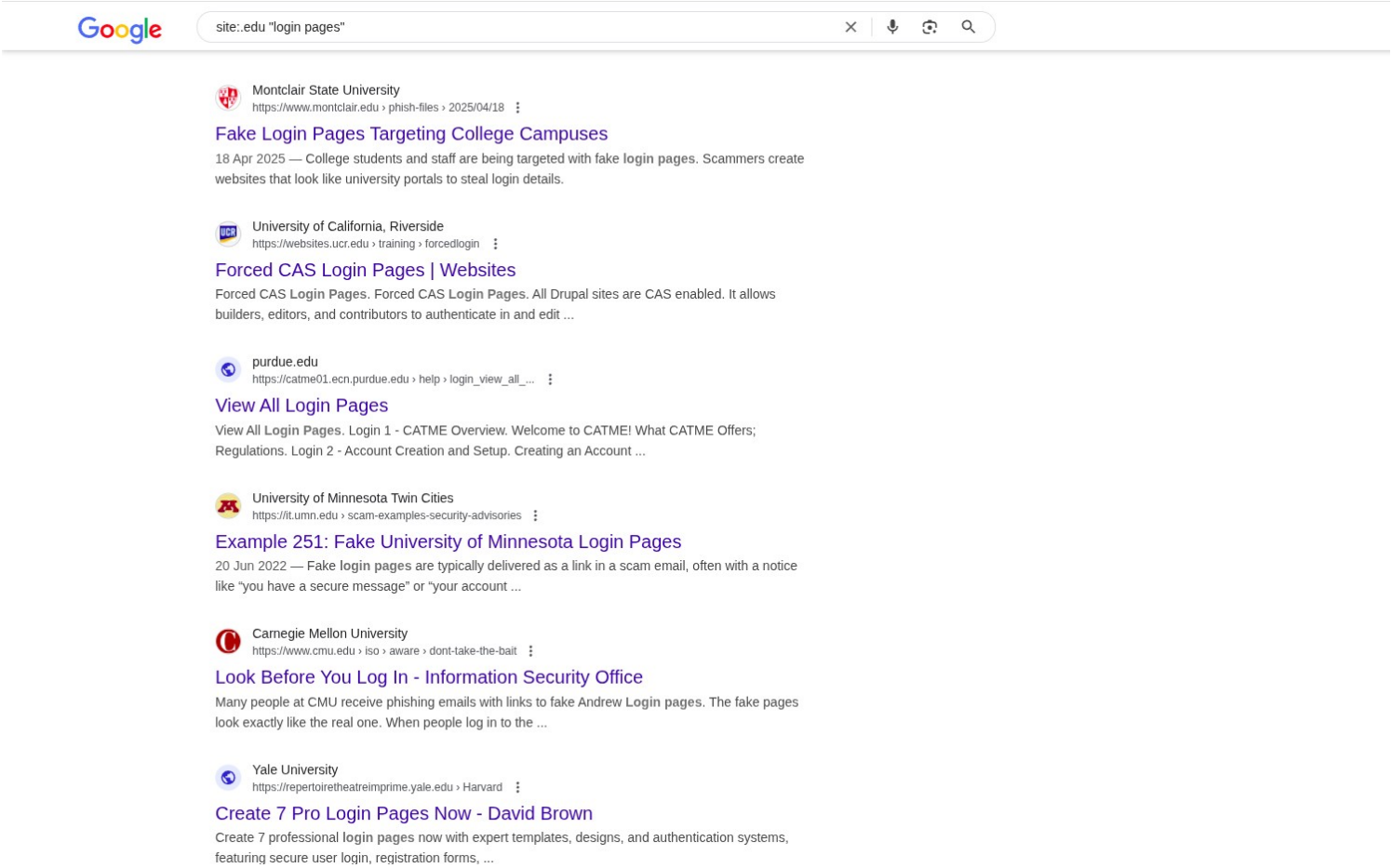
Introduction

This report documents the results of the Google Dorks lab, as outlined in the "GOOGLE DORKS lab manual.pdf". The objective is to use Google Dorks, an advanced search technique, to find hidden or sensitive information and vulnerabilities using Google search operators. The lab also involves running a Bash script to automate vulnerability searches. Below are the tasks performed, commands/queries used, their purpose, and placeholders for screenshots.

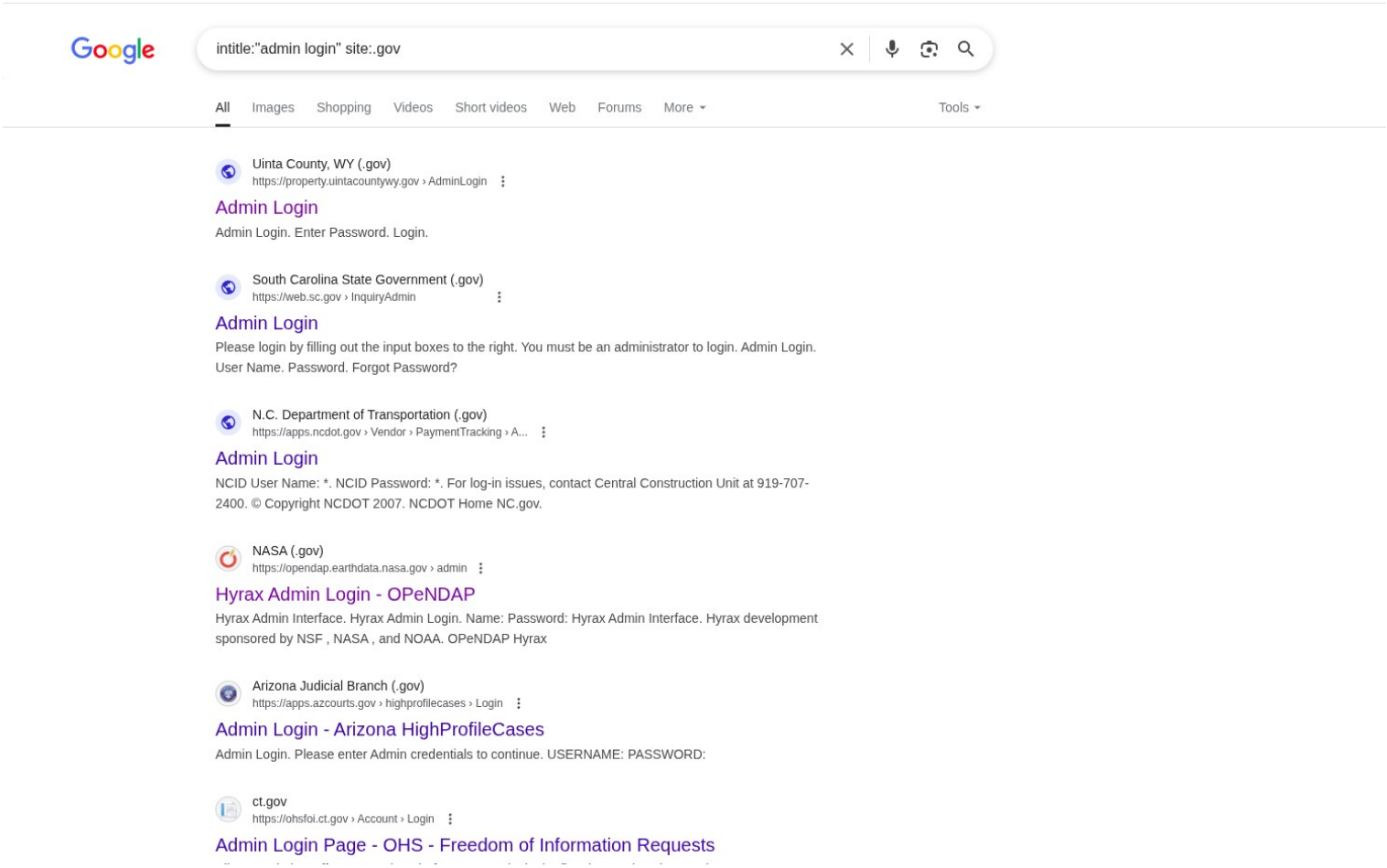
Lab Tasks and Results

1. Using site: Operator

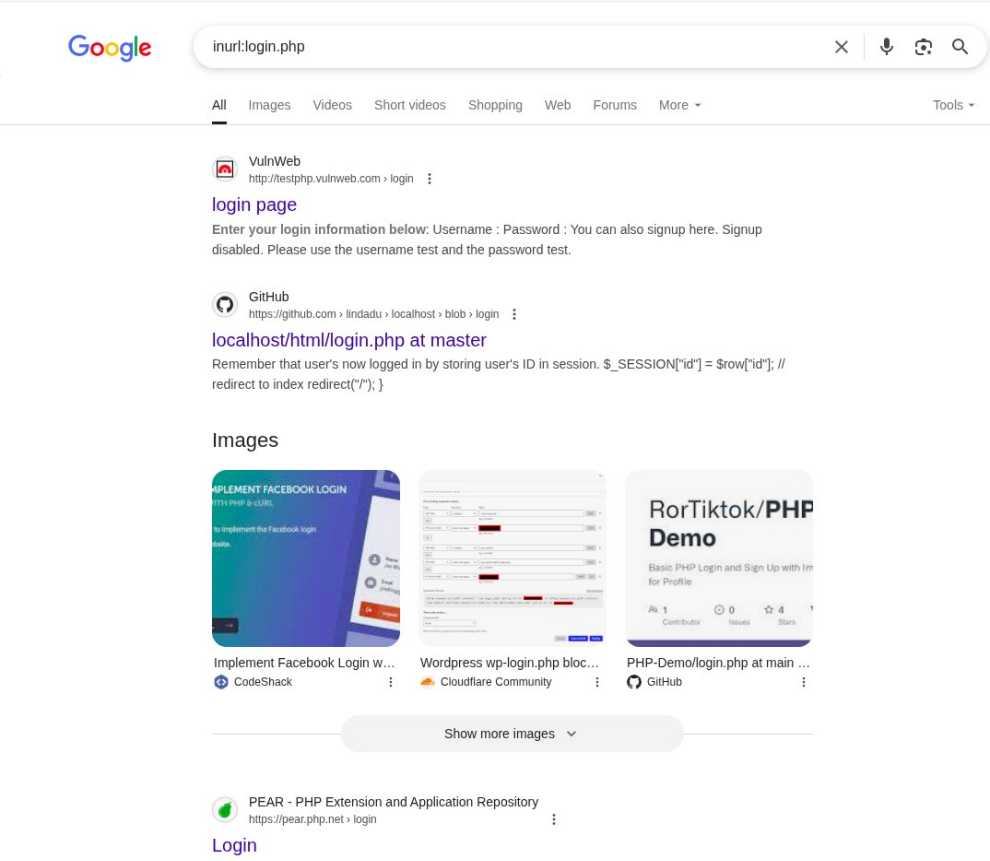
Purpose: Limit search results to a specific domain to find relevant pages.
Query: site:.edu "login pages"
Expected Output: List of login pages on edu domains.
Screenshot:



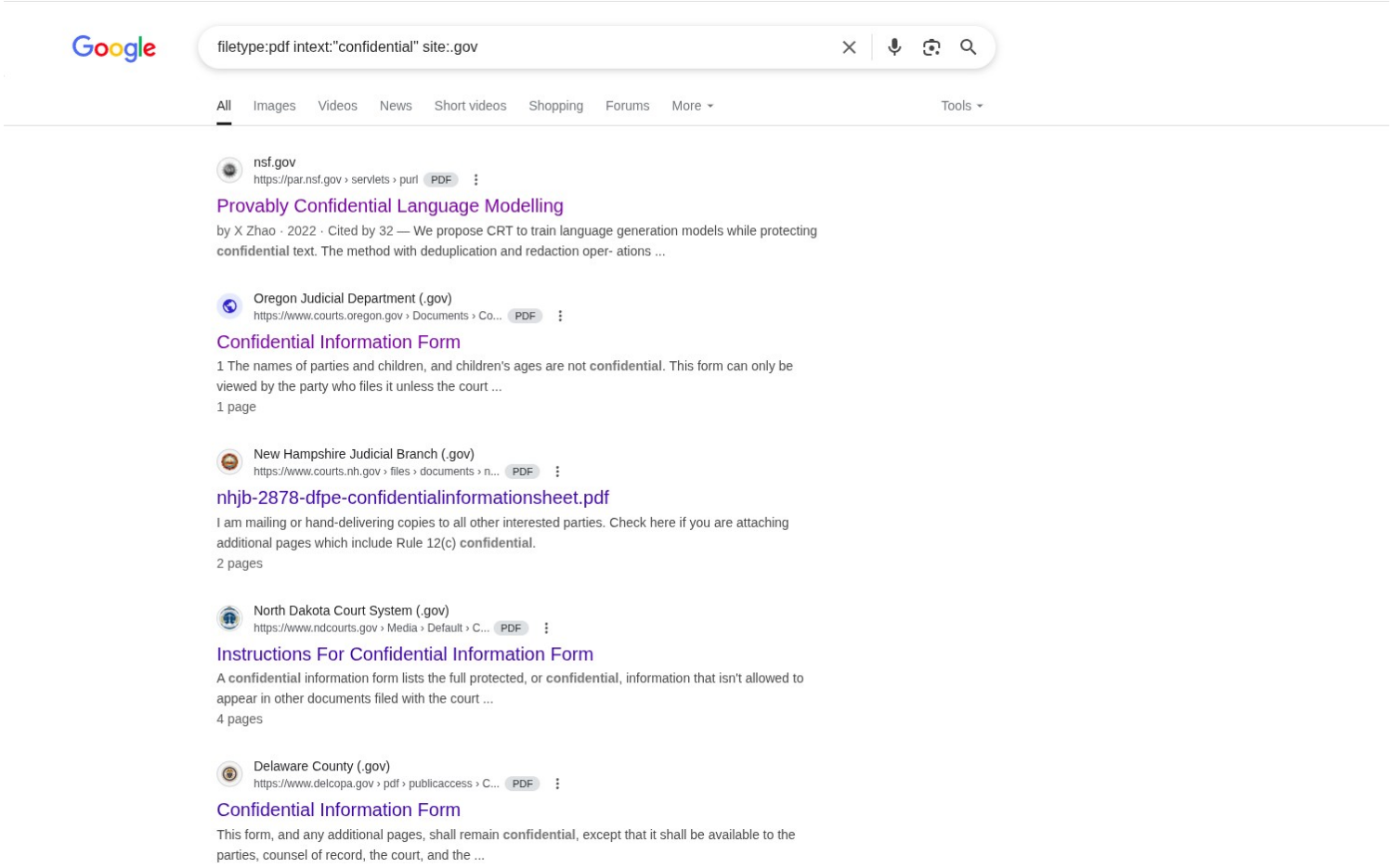
2. Using intitle: Operator
Purpose: Find pages with specific text in their HTML title, such as admin or login pages.
Query: intitle:"admin login" site:.gov
Expected Output: Admin login pages on .gov domains.
Screenshot:



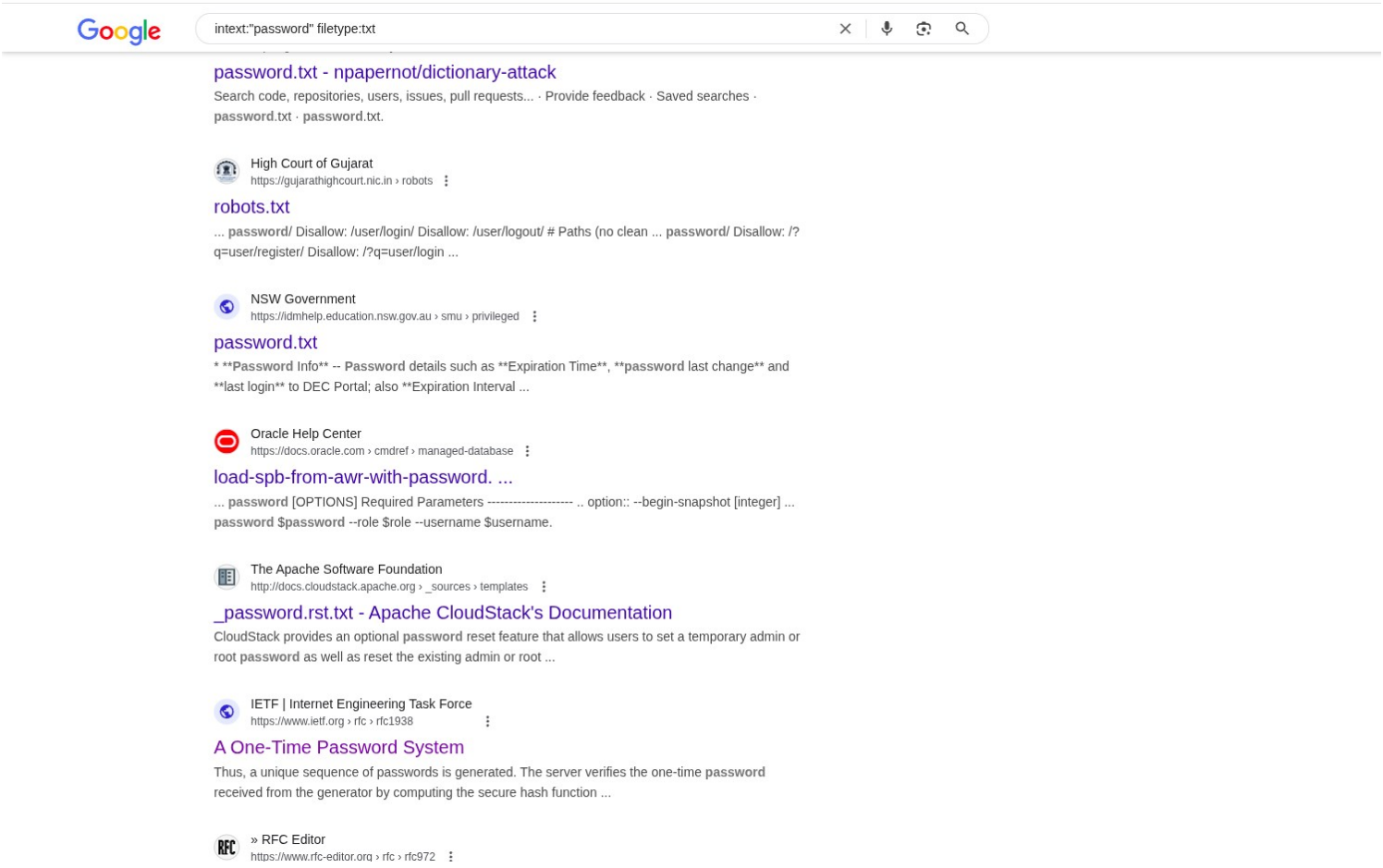
3. Using inurl: Operator
Purpose: Find pages with specific text in their URL, such as login or admin panels.
Query: inurl:login.php
Expected Output: Pages with "login.php" in their URL, likely login portals.
Screenshot:



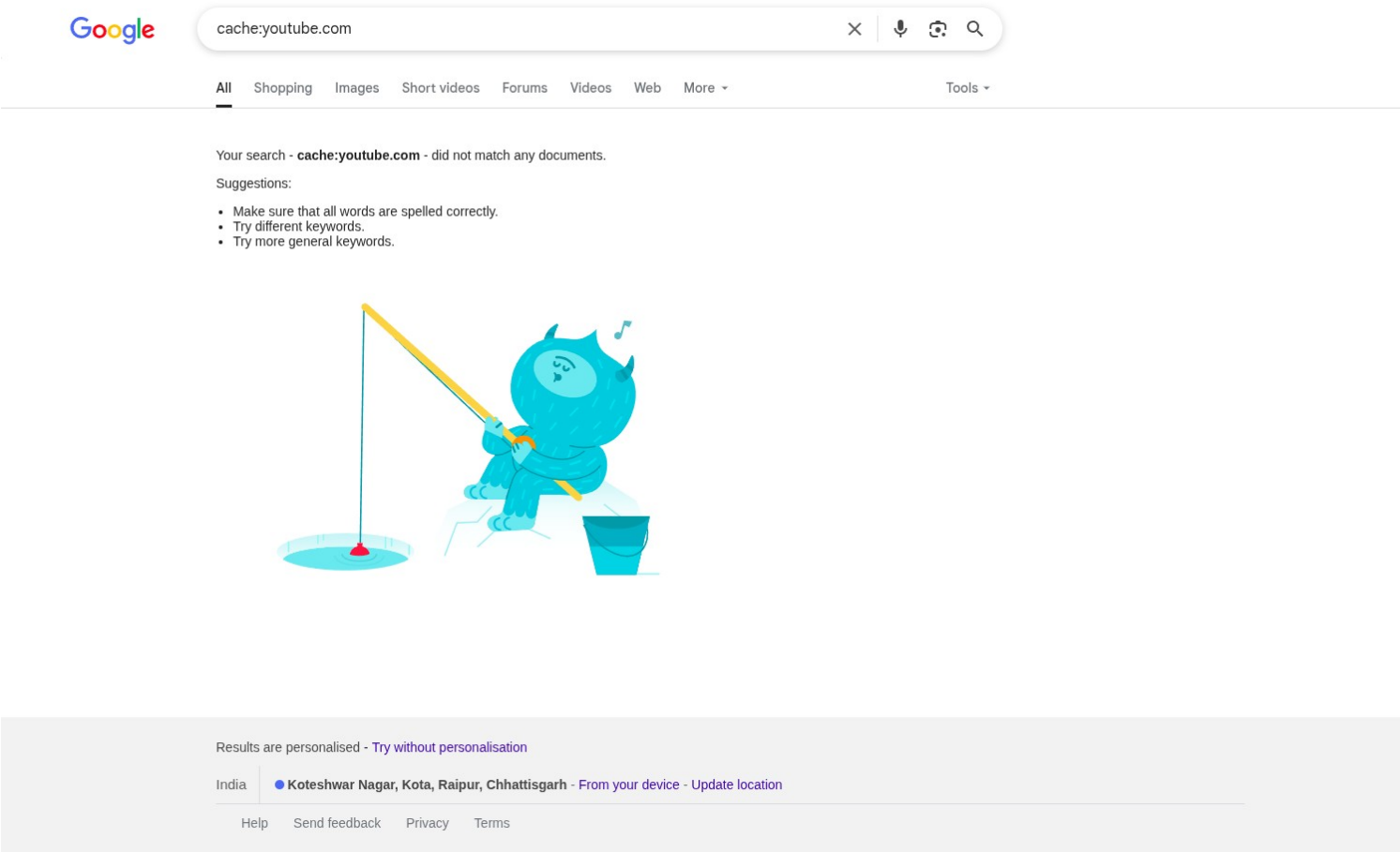
4. Using filetype: or ext: Operator
Purpose: Search for specific file types that may contain sensitive information.
Query: filetype:pdf intext:"confidential" site:.org
Expected Output: PDF files containing "confidential" on .org domains.
Screenshot:



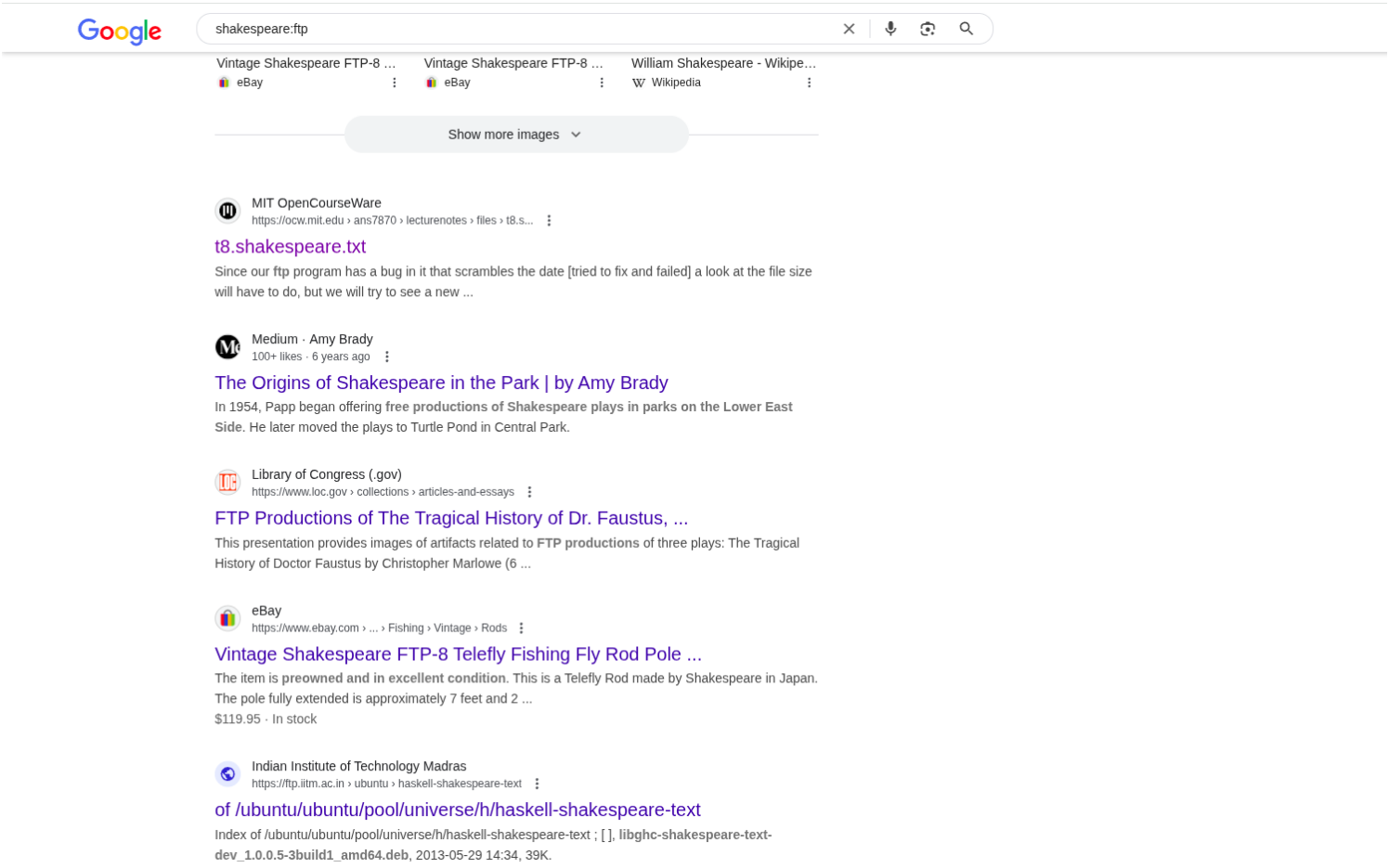
5. Using intext: Operator
Purpose: Search for pages containing specific keywords in their content.
Query: intext:"password =" filetype:txt
Expected Output: Text files containing "password =" in their content.
Screenshot:



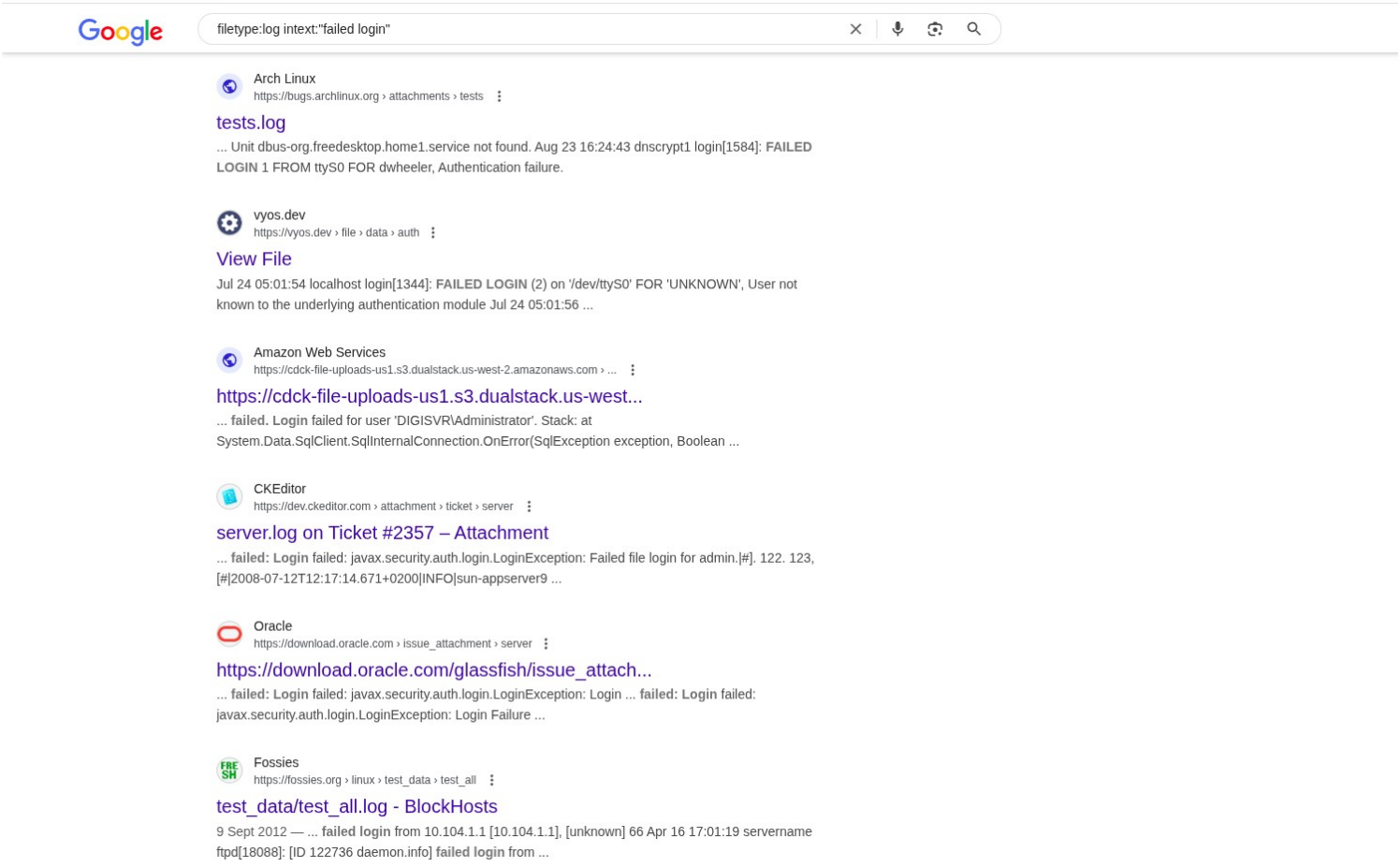
6. Using cache: Operator
Purpose: View cached versions of websites to access old or removed content.
Query: cache:youtube.com
Expected Output: Cached version of youtube homepage. *I tried many website but same result did not mach any document*
Screenshot:



7. Using ftp Search
Purpose: Find FTP servers hosting files.
Query: shakespeare:ftp
Expected Output: FTP servers with Shakespeare-related files.
Screenshot:



8. Using filetype:log
Purpose: Find log files that may contain sensitive information like credentials.
Query:filetype:log intext:"failed login"
Expected Output: Log files with failed login attempts.
Screenshot:



9. Running the Bash Script
I did't find any script file . But if I founded that script file I followed this step
Purpose: Automate Google Dorks searches to find vulnerabilities.
Command: chmod +x google_dorks.sh
./google_dorks.sh
Expected Output: List of vulnerabilities or sensitive information found (e.g., exposed files, login pages).
Screenshot: