

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:

The screenshot shows a Google search interface with the query "site:.edu \"login pages\"". The search results list several educational institutions with links to login pages or security advisories. The results are as follows:

- Montclair State University**
https://www.montclair.edu > phish-files > 2025/04/18
Fake Login Pages Targeting College Campuses
18 Apr 2025 — College students and staff are being targeted with fake login pages. Scammers create websites that look like university portals to steal login details.
- University of California, Riverside**
https://websites.ucr.edu > training > forcedlogin
Forced CAS Login Pages | Websites
Forced CAS Login Pages. Forced CAS Login Pages. All Drupal sites are CAS enabled. It allows builders, editors, and contributors to authenticate in and edit ...
- purdue.edu**
https://catme01.ecn.purdue.edu > help > login_view_all_...
View All Login Pages
View All Login Pages. Login 1 - CATME Overview. Welcome to CATME! What CATME Offers; Regulations. Login 2 - Account Creation and Setup. Creating an Account ...
- University of Minnesota Twin Cities**
https://it.umn.edu > scam-examples-security-advisories
Example 251: Fake University of Minnesota Login Pages
20 Jun 2022 — Fake login pages are typically delivered as a link in a scam email, often with a notice like "you have a secure message" or "your account ...
- Carnegie Mellon University**
https://www.cmu.edu > iso > aware > dont-take-the-bait
Look Before You Log In - Information Security Office
Many people at CMU receive phishing emails with links to fake Andrew Login pages. The fake pages look exactly like the real one. When people log in to the ...
- Yale University**
https://repertoiretheatreimprime.yale.edu > Harvard
Create 7 Pro Login Pages Now - David Brown
Create 7 professional login pages now with expert templates, designs, and authentication systems, featuring secure user login, registration forms, ...

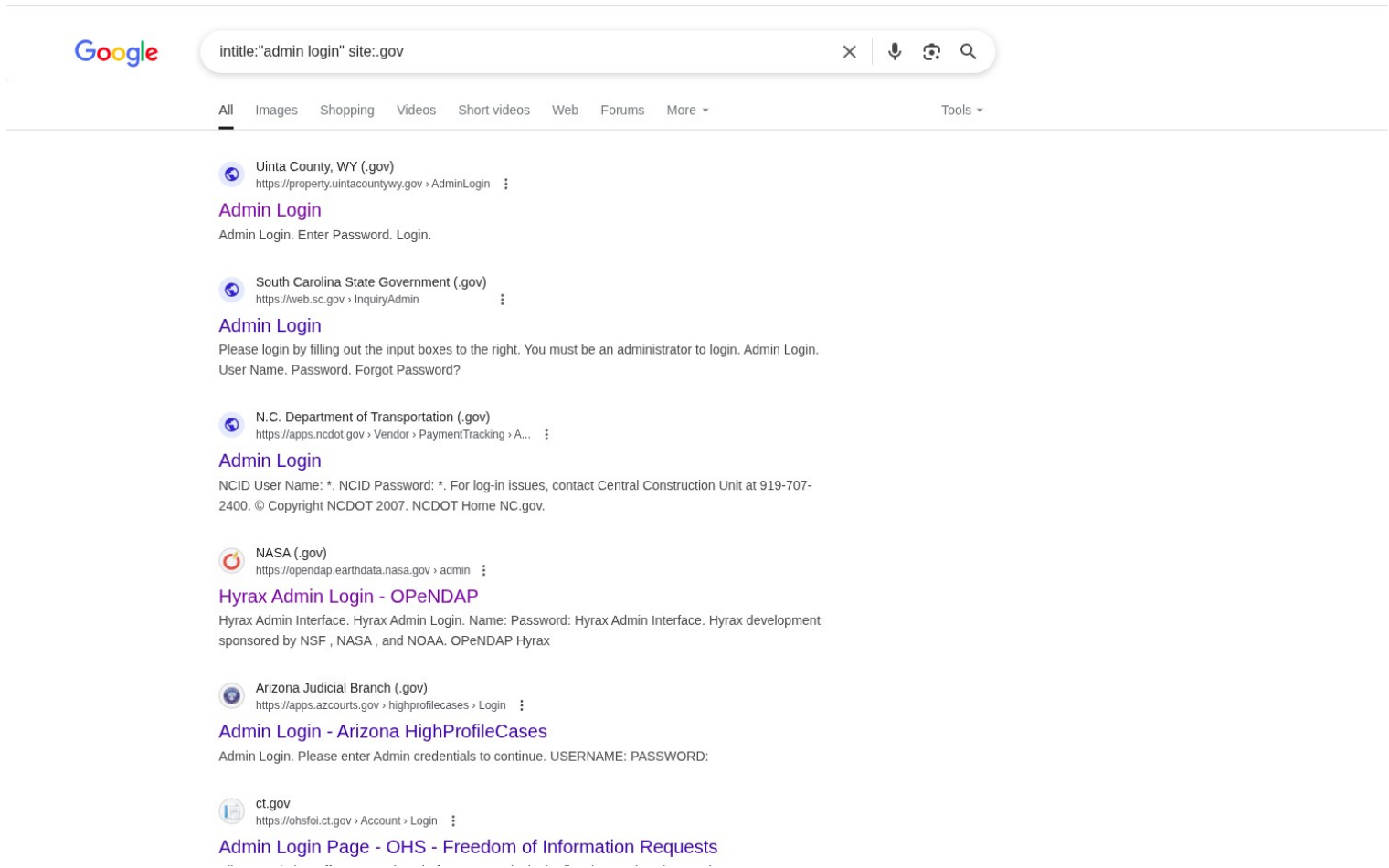
2. Using intitle: Operator

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:



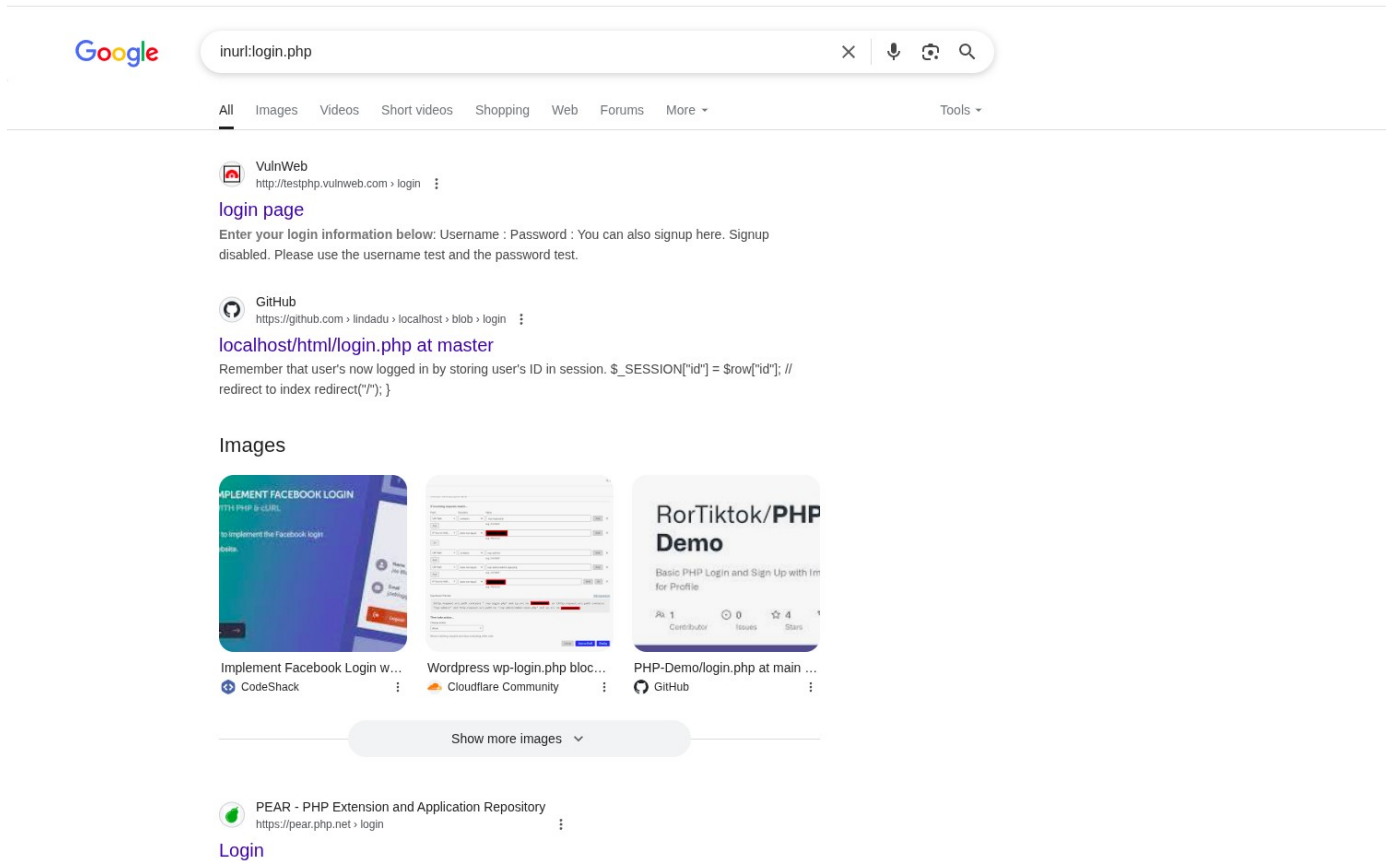
3. Using inurl: Operator

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:



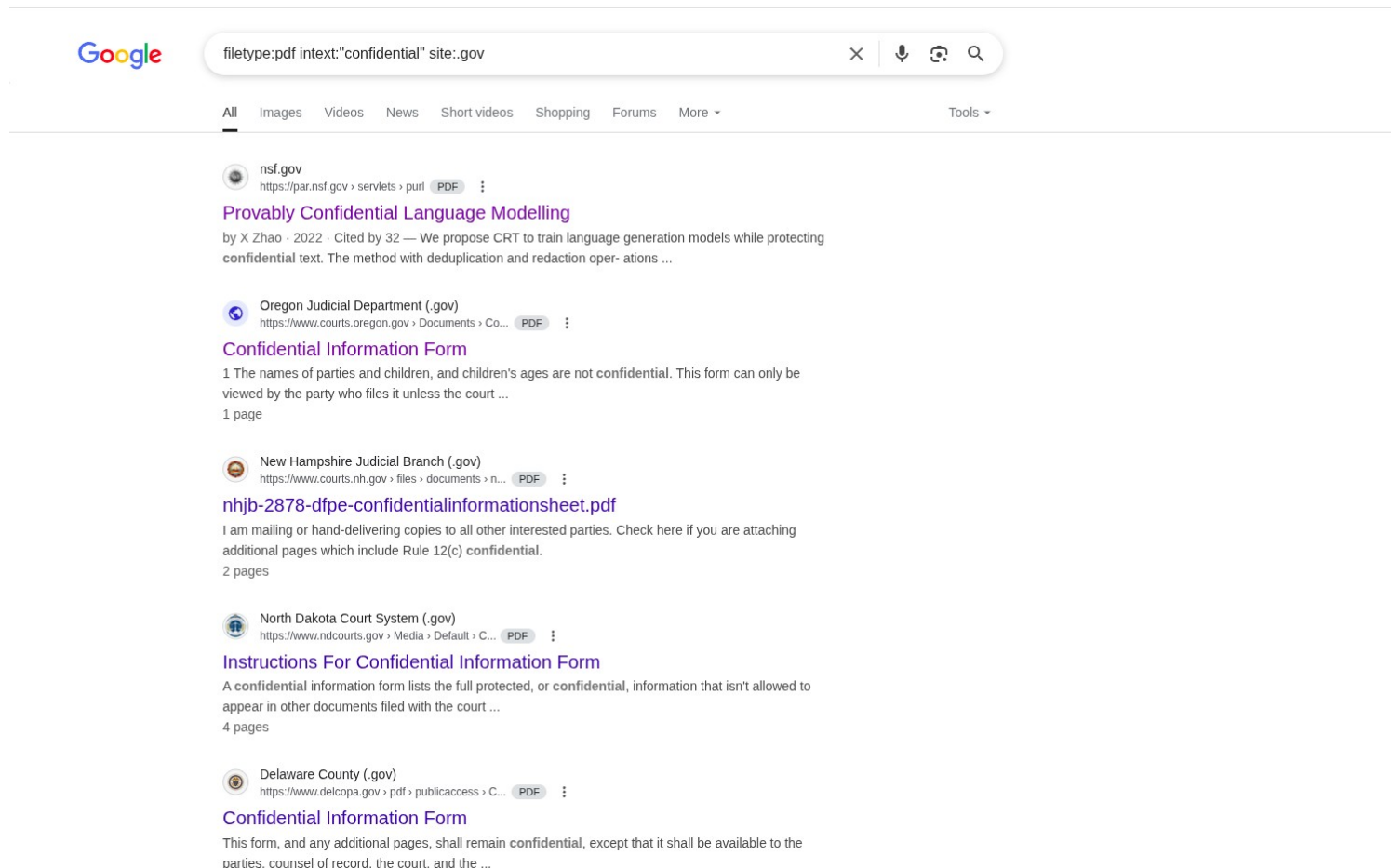
4. Using filetype: or ext: Operator

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:



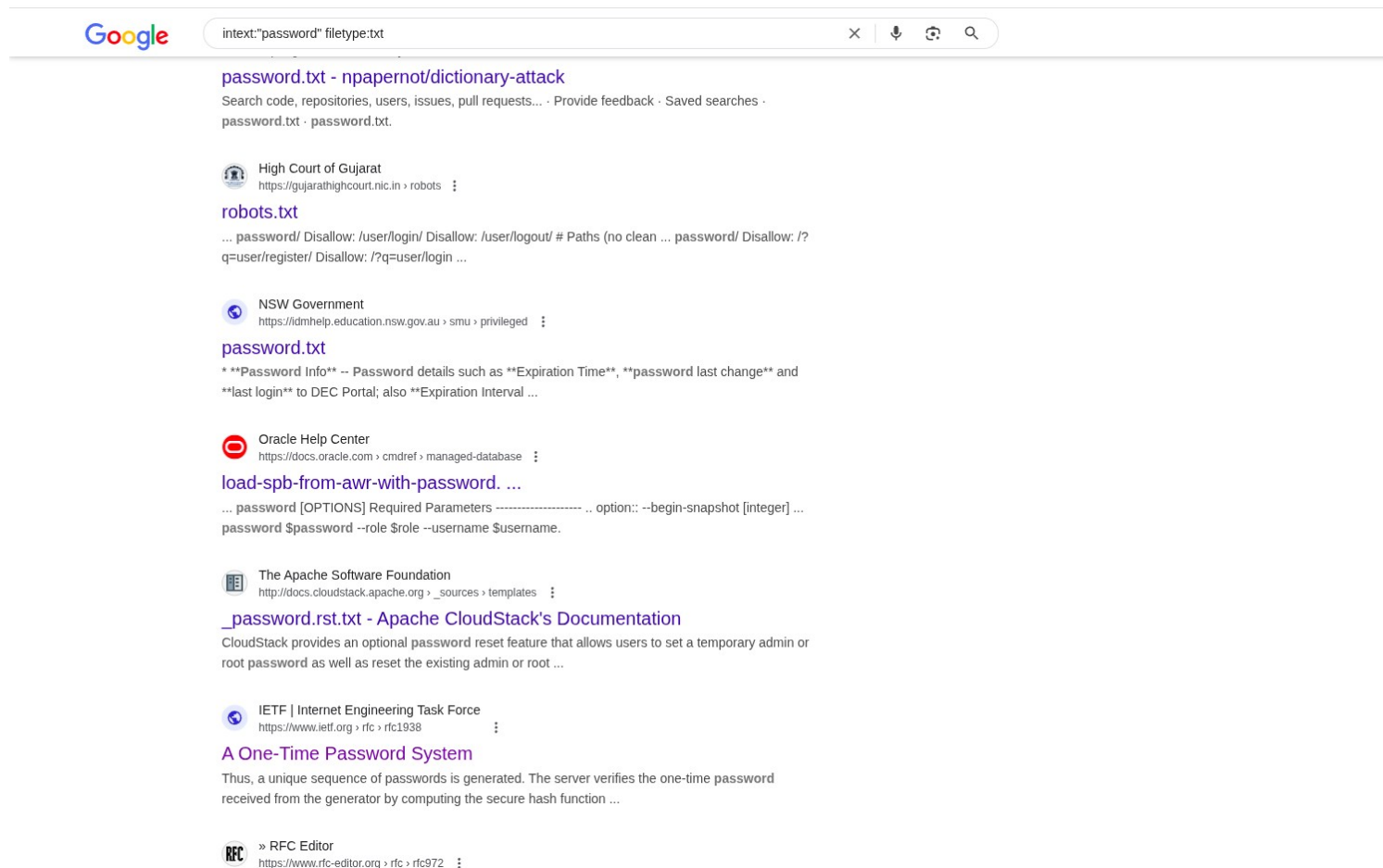
5. Using intext: Operator

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:



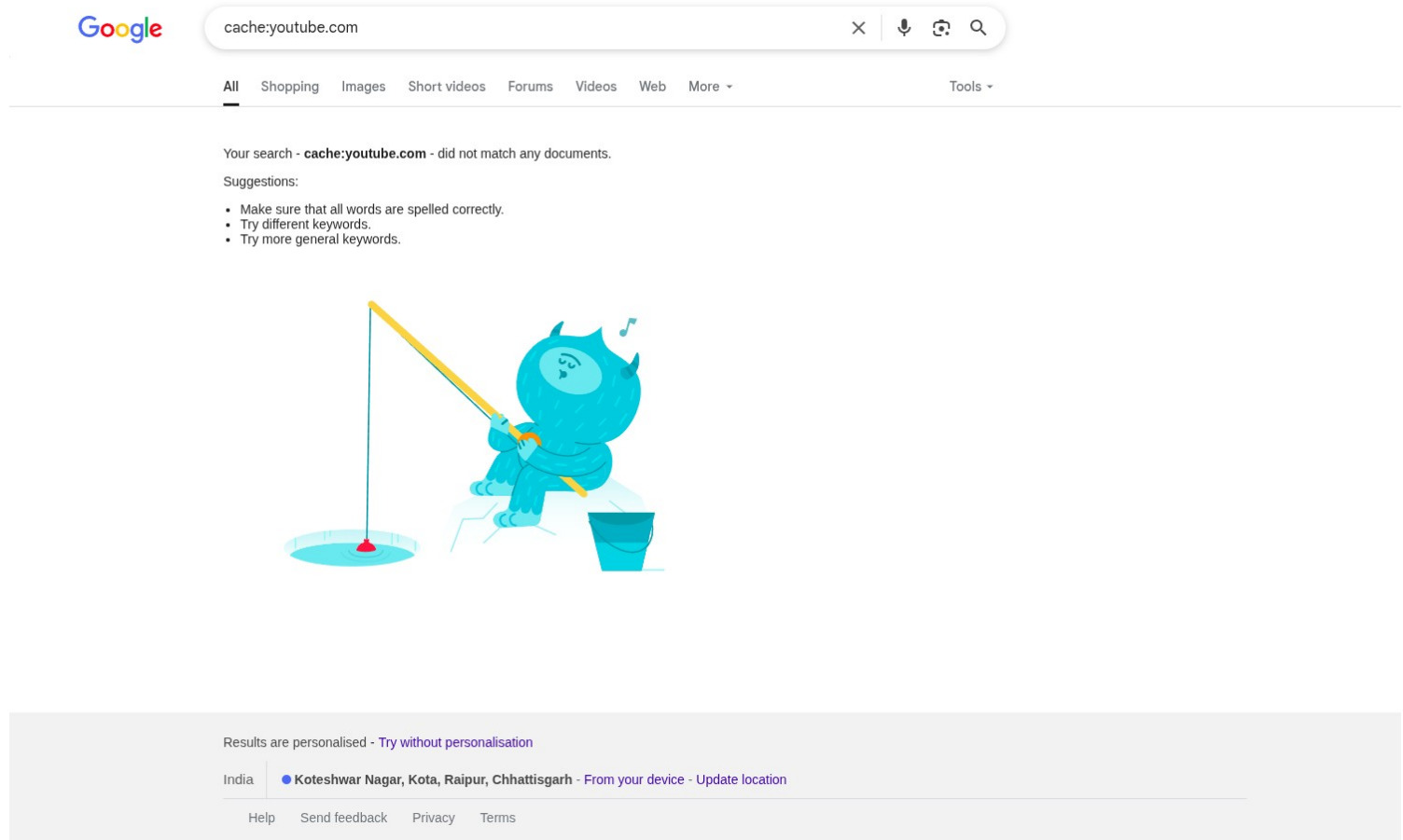
6. Using cache: Operator

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:



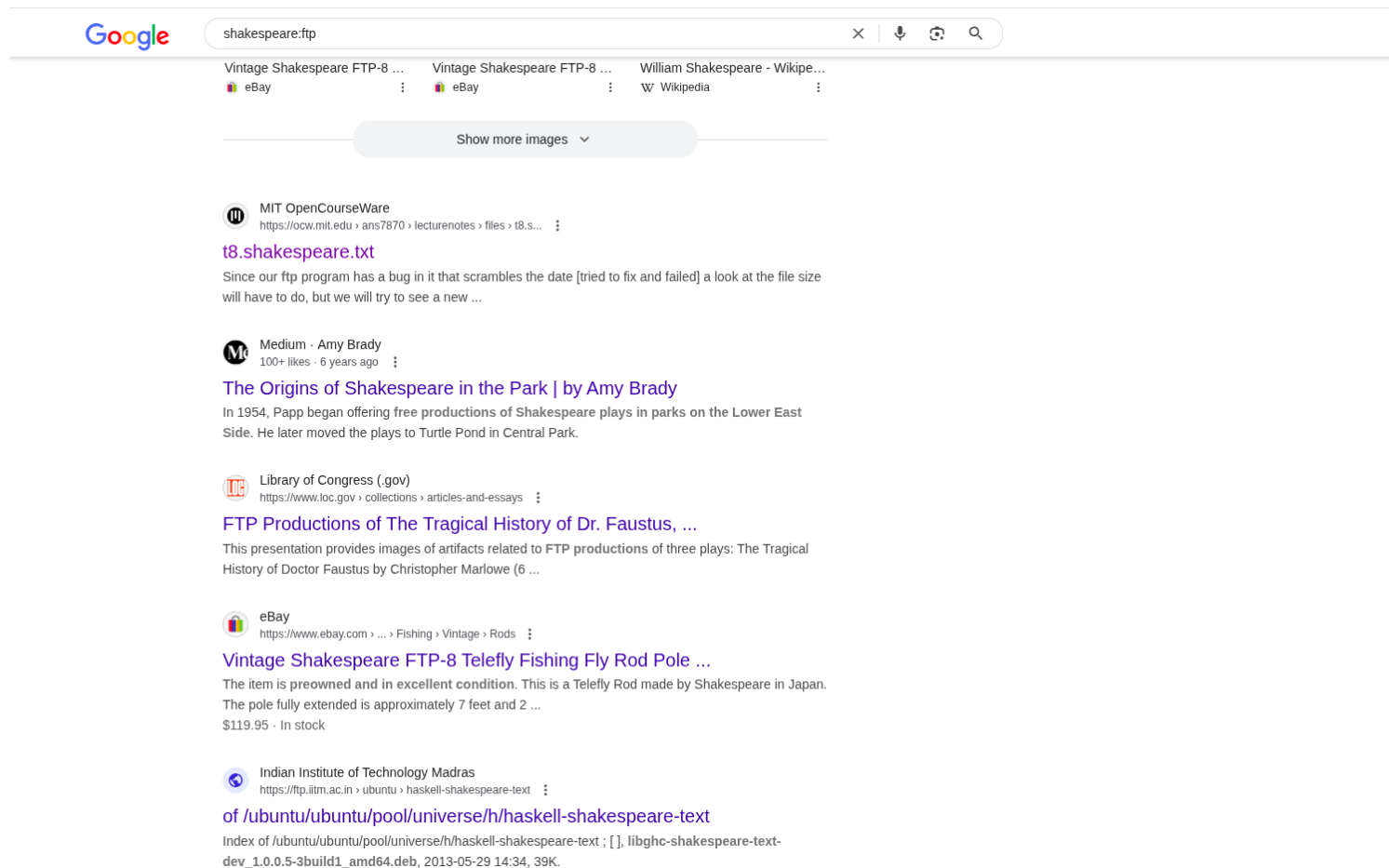
7. Using ftp Search

Purpose: Find FTP servers hosting files.

Query: `shakespeare:ftp`

Expected Output: FTP servers with Shakespeare-related files.

Screenshot:



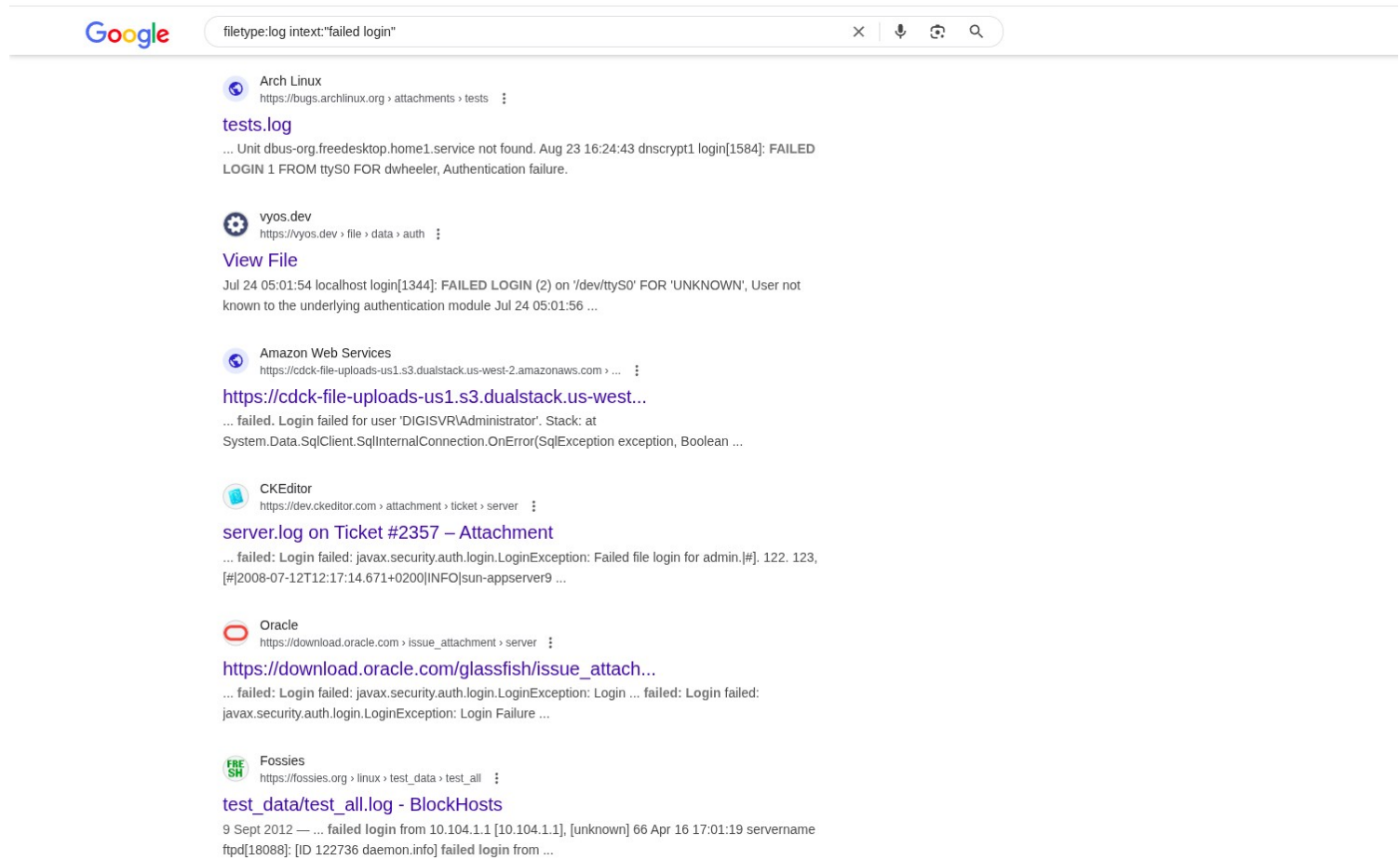
8. Using filetype:log

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 didn'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: