Experiment No. 5

Title: Conducting recon with Google Dorking

Batch: A3 **Roll No.: 16010421119** **Experiment**

No.:5 Aim: Conducting recon with Google Dorking.

Resources needed: Google Hacking Database (GHDB), Google Dorks Cheat Sheet, Google Operators Reference, Online Tutorials and Blog Posts, Dork Searcher, GooDork, OWASP WebGoat, DVWA (Damn Vulnerable Web Application)

Pre Lab/ Prior Concepts:

Students should have prior knowledge of Search Engine Basics, Google Search Operators, HTTP Protocol and Web Technologies, Web Application Architecture, Ethical Hacking Principles, Web Application Security Fundamentals, Legal and Ethical Considerations, Data Protection, and Privacy Laws.

Theory:

Google Dorking, also known as Google hacking, is a technique used by cybersecurity professionals and ethical hackers to refine search queries on Google to uncover sensitive information that is not typically visible in conventional searches. This practice relies on leveraging advanced search operators to narrow down search results, revealing specific details that may inadvertently expose vulnerabilities or sensitive data.

Google Dorking Basics:

At its core, Google Dorking involves using special search operators that allow users to customize their queries for more targeted results. Some common operators include:

site: Limits the search to a specific site or domain.

Example: site:example.com filetype: pdf searches for PDF files within the example.com domain.

filetype: Specifies a particular file type.

Example: filetype: SQL password looks for SQL files containing the term

"password." intitle: Searches for a specific word or phrase in the title of web pages.

Example: intitle: "index of" password aims to find directories containing files with the term "password."

Purpose of Google Dorking:

1. **Information Gathering:** Google Dorking is a powerful reconnaissance tool for collecting information about a target. By crafting specific queries, security professionals can unveil details such as directory structures, exposed files, or even sensitive information inadvertently disclosed on publicly accessible web servers.
2. **Vulnerability Discovery:** Ethical hackers use Google Dorking to identify potential vulnerabilities. This may include discovering exposed databases, misconfigured servers, or files containing sensitive data. By understanding how information is indexed, security practitioners can pinpoint areas that require attention.
3. **Security Assessments:** Google Dorking is an integral part of security assessments. By comprehensively searching for patterns indicative of security issues, analysts can assess the robustness of a target's web presence and identify potential weaknesses before malicious actors do.

Responsible Use of Google Dorking:

While Google Dorking is a valuable tool for ethical hacking and security testing, it's essential to approach it responsibly:

Legal Compliance: Ensuring VAPT actions comply with local and international laws. Unauthorized access or exploitation is unethical and can lead to legal consequences.

Obtain Authorization: Before conducting any reconnaissance activities, obtain proper authorization and ensure permission to assess and analyze the target.

Ethical Considerations: Adhere to ethical guidelines and principles. Use Google Dorking for legitimate and ethical purposes, focusing on improving security rather than engaging in malicious activities.

Procedure:

Reconnaissance with Google Dorking involves using advanced search operators to uncover information that might not be readily available through conventional searches. Here's a step-by-step procedure for conducting reconnaissance using Google Dorking:

Step 1: Understand the Scope and Purpose: Before starting reconnaissance, clearly define the scope and purpose of activities. Determine what specific information to seek and why. Ensuring reconnaissance efforts align with ethical and legal standards.

Step 2: Learn Google Dorking Operators: Familiarize with various Google Dorking operators to craft precise search queries. Key operators include site:, filetype:, intitle:, and others. Understand how these operators can be combined for more targeted results.

Step 3: Identify the Target: Define the target for reconnaissance. This could be a specific domain, website, or information to look for.

Step 4: Craft Google Dorks: Create specific Google Dorks by combining operators to refine the search. For example:

site:example.com filetype: pdf searches for PDF files on example.com.

intitle:"index of" password looks for directories containing files with the term "password."

Step 5: Execute Google Dorks: Enter the crafted Google Dorks into the Google search bar and execute the queries. Review the search results for information that aligns with reconnaissance goals. Pay attention to details in titles, URLs, and snippets.

Step 6: Analyze Results: Carefully analyze the search results to extract relevant information. Look for exposed directories, sensitive files, or any data that might pose a security risk. Document findings and maintain a record of the URLs and details discovered.

Step 7: Verify and Cross-Reference: Verify the accuracy of the information obtained by cross-referencing it with other sources if possible. Ensure that the information is current and relevant to your reconnaissance objectives. Cross-referencing helps in confirming the authenticity of findings.

Output (Code with result Snapshot)

Step 1: Understand the Scope and Purpose:

Before commencing reconnaissance, it's crucial to establish the scope and purpose of our activities. In this case, our objective is to identify any potential security vulnerabilities or sensitive information exposed on examplewebsite.com. Our reconnaissance efforts strictly adhere to ethical and legal standards.

Step 2: Learn Google Dorking Operators:

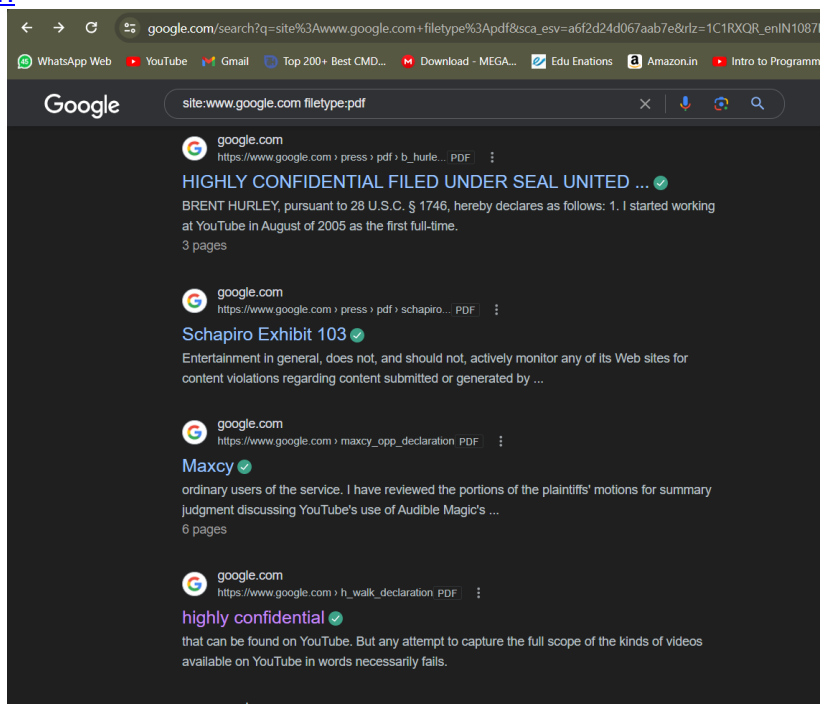
We are familiar with various Google Dorking operators, including site:, filetype:, and intitle:. These operators enable us to construct precise search queries to uncover specific types of information.

Step 3: Identify the Target

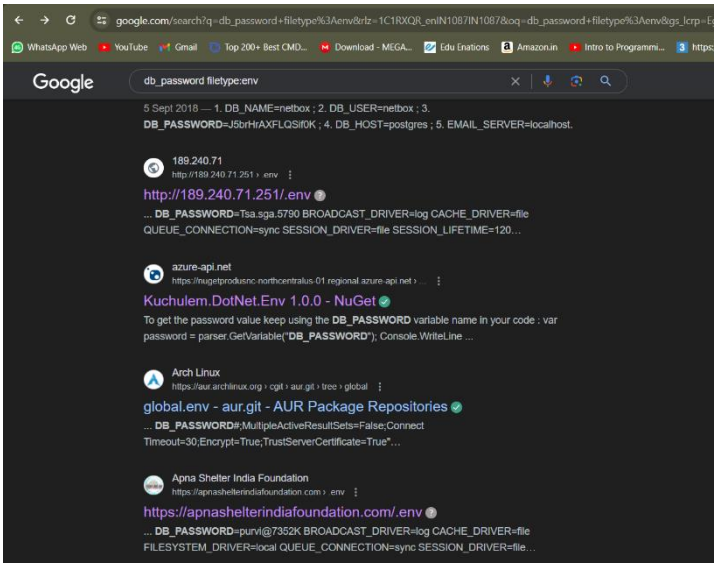
Our target for reconnaissance are websites with Open Databases which includes sensitive information. We aim to identify any sensitive files, directories, or information that may be publicly accessible.

Step 4: Craft Google Dorks:

site:www.google.com filetype:pdf: This query searches for PDF files specifically on www.google.com



intitle:"index of" password : Searches for directories containing files with the term "password" specifically within examplewebsite.com.

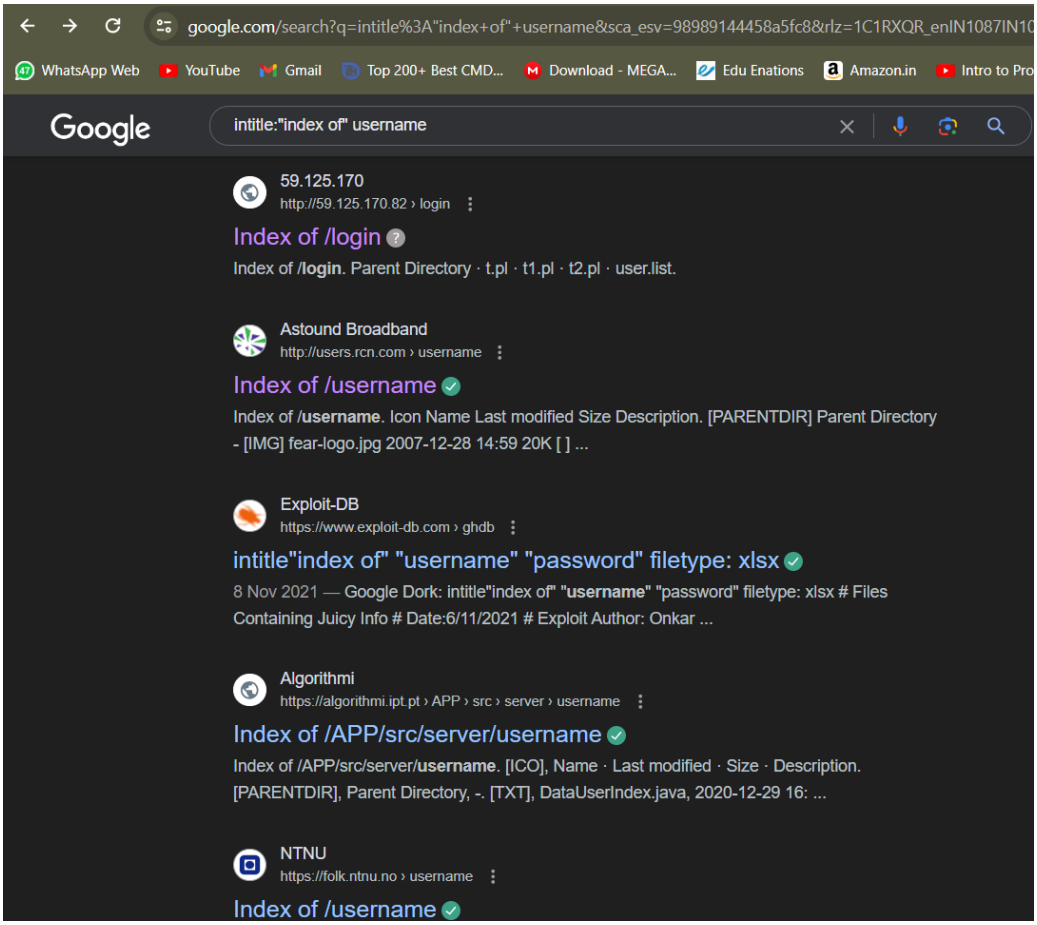


Here, db_password helps this dork to surf around databases containing password while the filetype:env sets individual user environment variables that override the variables set. individual user environment variables can override the variables set globally, allowing users to customize certain aspects of the

application environment according to their preferences or needs. As the result, various .env file can be seen which are publicly available

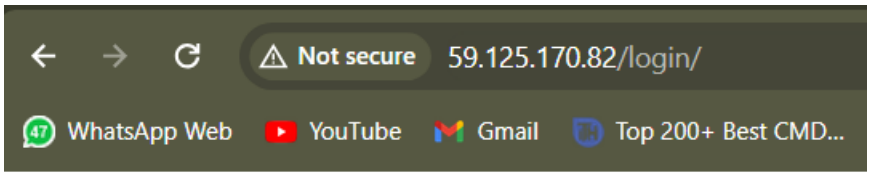
Step 5: Execute Google Dorks

We entered the crafted Google Dorks into the Google search bar and executed the queries. The search results were carefully reviewed for information relevant to our reconnaissance goals.



The Google Dork "intitle:"index of" username" is crafted to search for web directories containing the term "index of" in their title, indicative of open directory indexing. The term "username" suggests that the search is aimed at finding directories that might expose files or resources related to user accounts. This dork is often used to uncover publicly accessible directories containing sensitive information like user lists or login credentials, posing potential security risks if left unsecured.

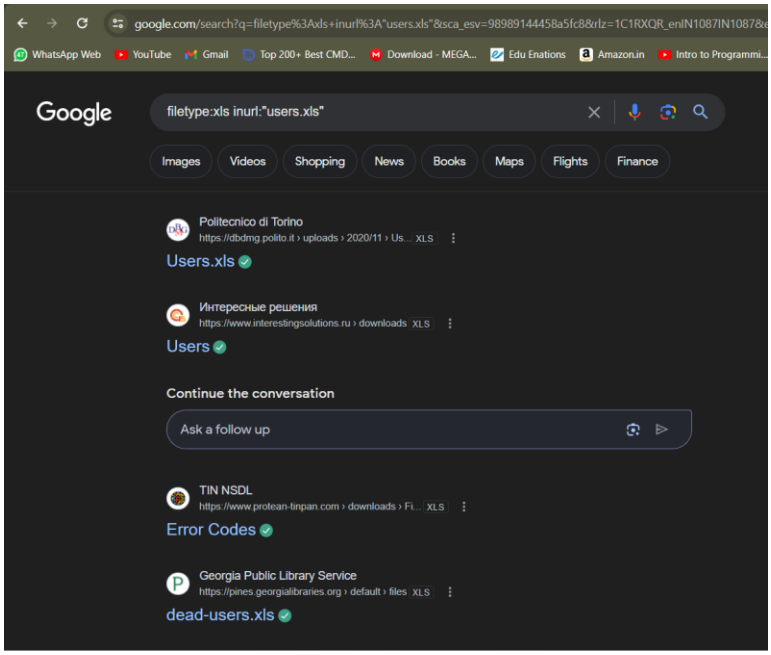
Step 6: Analyze Results:

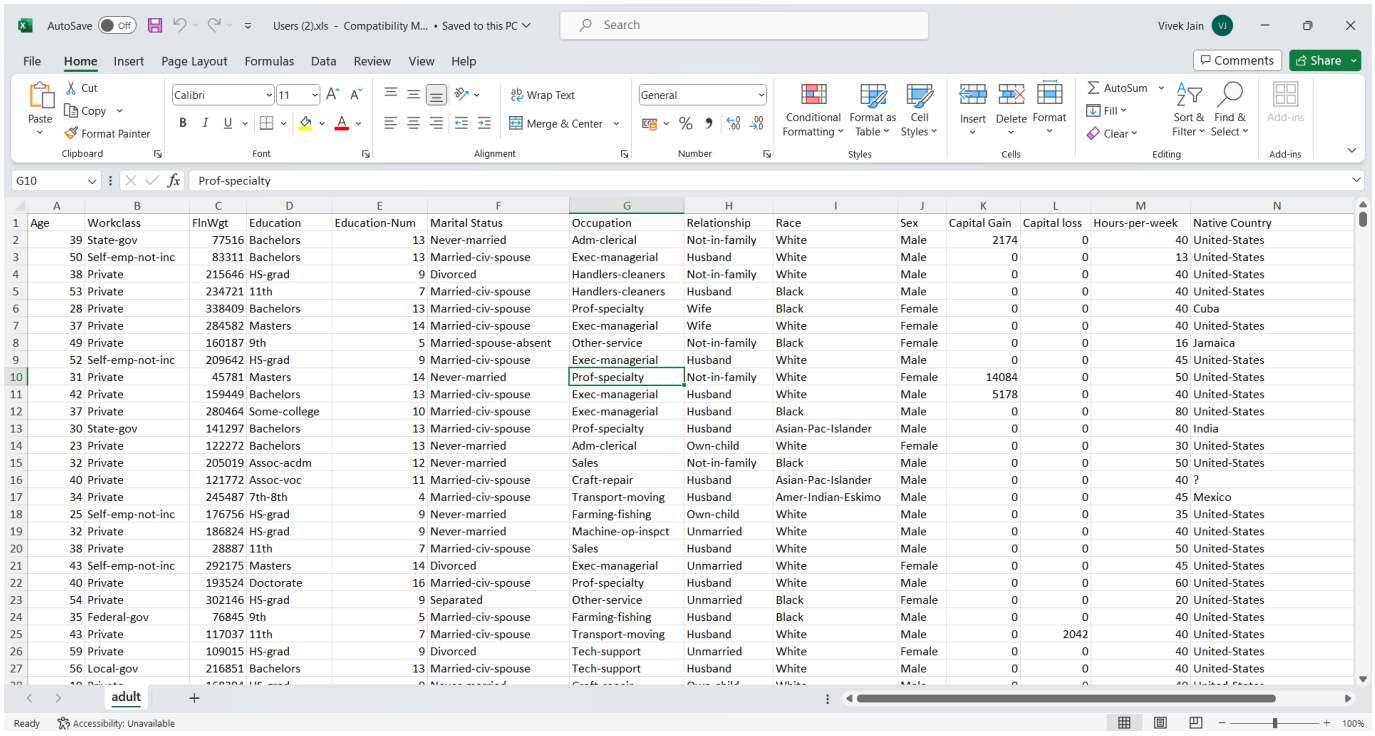


Index of /login

- Parent Directory
- t.pl
- t1.pl
- t2.pl
- user.list

After viewing all the directories including parent directory, we found out that an xls file is publicly on internet so we we use our next crafted dork filetype:xls inurl:"users.xls" so surf for xls file that contain users information.





Age	Workclass	FlnWgt	Education	Education-Num	Marital Status	Occupation	Relationship	Race	Sex	Capital Gain	Capital loss	Hours-per-week	Native Country
39	State-gov	77516	Bachelors	13	Never-married	Adm-clerical	Not-in-family	White	Male	2174	0	40	United-States
50	Self-emp-not-inc	83311	Bachelors	13	Married-civ-spouse	Exec-managerial	Husband	White	Male	0	0	13	United-States
38	Private	215646	HS-grad	9	Divorced	Handlers-cleaners	Not-in-family	White	Male	0	0	40	United-States
53	Private	234721	11th	7	Married-civ-spouse	Handlers-cleaners	Husband	Black	Male	0	0	40	United-States
28	Private	338409	Bachelors	13	Married-civ-spouse	Prof-specialty	Wife	Black	Female	0	0	40	Cuba
37	Private	284582	Masters	14	Married-civ-spouse	Exec-managerial	Wife	White	Female	0	0	40	United-States
49	Private	160187	9th	5	Married-spouse-absent	Other-service	Not-in-family	Black	Female	0	0	16	Jamaica
52	Self-emp-not-inc	209642	HS-grad	9	Married-civ-spouse	Exec-managerial	Husband	White	Male	0	0	45	United-States
31	Private	45781	Masters	14	Never-married	Prof-specialty	Not-in-family	White	Female	14084	0	50	United-States
42	Private	159449	Bachelors	13	Married-civ-spouse	Exec-managerial	Husband	White	Male	5178	0	40	United-States
37	Private	280464	Some-college	10	Married-civ-spouse	Exec-managerial	Husband	Black	Male	0	0	80	United-States
30	State-gov	141297	Bachelors	13	Married-civ-spouse	Prof-specialty	Husband	Asian-Pac-Islander	Male	0	0	40	India
23	Private	122272	Bachelors	13	Never-married	Adm-clerical	Own-child	White	Female	0	0	30	United-States
32	Private	205019	Assoc-acdm	12	Never-married	Sales	Not-in-family	Black	Male	0	0	50	United-States
40	Private	121772	Assoc-voc	11	Married-civ-spouse	Craft-repair	Husband	Asian-Pac-Islander	Male	0	0	40	?
34	Private	245487	7th-8th	4	Married-civ-spouse	Transport-moving	Husband	Amer-Indian-Eskimo	Male	0	0	45	Mexico
25	Self-emp-not-inc	176756	HS-grad	9	Never-married	Farming-fishing	Own-child	White	Male	0	0	35	United-States
32	Private	186824	HS-grad	9	Never-married	Machine-op-inspct	Unmarried	White	Male	0	0	40	United-States
38	Private	28887	11th	7	Married-civ-spouse	Sales	Husband	White	Male	0	0	50	United-States
43	Self-emp-not-inc	292175	Masters	14	Divorced	Exec-managerial	Unmarried	White	Female	0	0	45	United-States
40	Private	193524	Doctorate	16	Married-civ-spouse	Prof-specialty	Husband	White	Male	0	0	60	United-States
54	Private	302146	HS-grad	9	Separated	Other-service	Unmarried	Black	Female	0	0	20	United-States
35	Federal-gov	76845	9th	5	Married-civ-spouse	Farming-fishing	Husband	Black	Male	0	0	40	United-States
43	Private	117037	11th	7	Married-civ-spouse	Transport-moving	Husband	White	Male	0	2042	40	United-States
59	Private	109015	HS-grad	9	Divorced	Tech-support	Unmarried	White	Female	0	0	40	United-States
56	Local-gov	216851	Bachelors	13	Married-civ-spouse	Tech-support	Husband	White	Male	0	0	40	United-States

This excel file contains private and sensitive data of the employees including Age , Workclass, Education, Education-Num, Marital Status, Occupation, Relationship, Race, Sex, Capital Gain, Capital loss, Hours-per-week, Native Country, Class.
This data can be easily used by anyone in illegal ways.

Step 7: Verify and Cross-Reference:
To ensure the accuracy of our findings, we cross-referenced the discovered information with other sources. We verified the authenticity of the exposed data and confirmed its relevance to our reconnaissance objectives.
Using this xls file and the sources like company official website we can ensure the data is highly accurate and updated.

Post Lab Questions: -

1. Describe any vulnerabilities or sensitive information identified during the reconnaissance. How might these findings impact the target's security posture, and what recommendations should be proposed?

ANS:- While using dorks, I found out various directories that has sensitive data and the excel (.xls) file we found at the end had almost 1000+ employee details with various imformation like Age , Workclass, Education, Education-Num, Marital Status, Occupation, Relationship, Race, Sex, Capital Gain, Capital loss, Hours-per-week, Native Country, Class which is not a good practice.

2. If vulnerabilities were discovered, discuss the approach you would take for responsible disclosure. What considerations would guide communication with the affected parties?

ANS:- In the event of discovering a .xls file containing sensitive employee details, responsible disclosure entails promptly notifying the website owner/administrator of the vulnerability. Offering clear guidance and recommendations for mitigating the risk, setting a reasonable timeline for resolution, and transparently communicating with affected parties about the potential impact and necessary precautions. Additionally, coordinating with relevant authorities, if warranted, ensures comprehensive protection of user data and fosters a culture of cybersecurity diligence and accountability.

Outcomes: CO2 Comprehend purpose of Anonymity and Foot printing

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

Google dorks are very helpful for finding accurate results but at the same time, illegal use of google dorks leads to leaking of private and sensitive data of any person or company

Signature of faculty in charge with date

References:

1.https://blog.glugmvit.com/Google-Dorks-for-Recon/

2.https://www.stationx.net/google-dorking-commands/

3.https://www.hackthebox.com/blog/What-Is-Google-Dorking