

Experiment No. 5

Batch: A2**Roll No.:16010421073****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

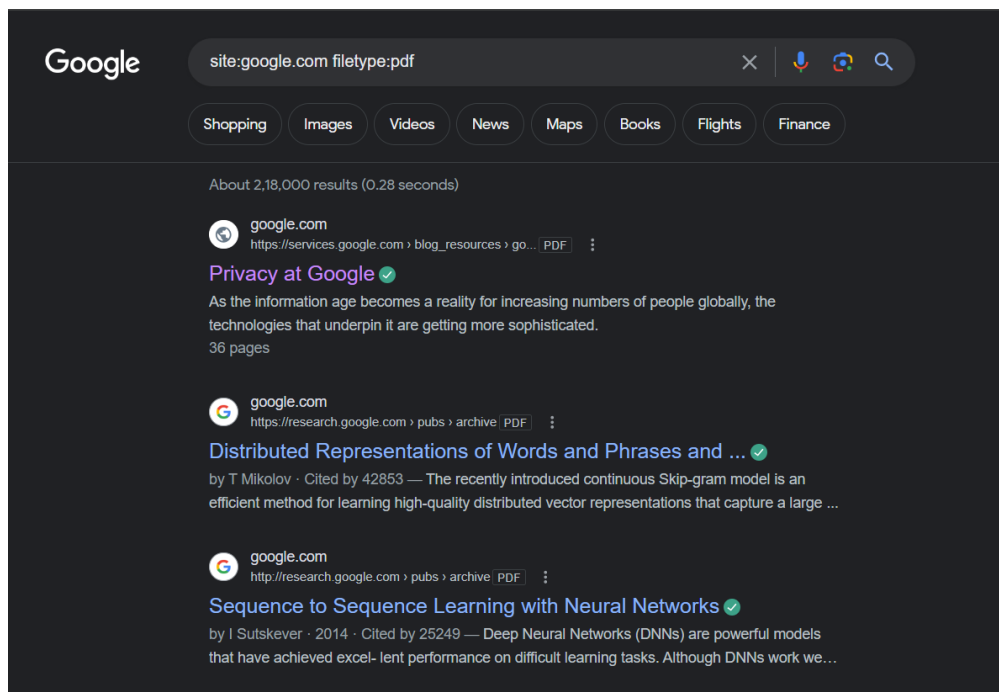
We are conducting a security assessment for a delivery service company called "Colis Express." Our purpose is to identify any publicly accessible sensitive

information or potential security risks on their website using google exploit-db

Step 2: Learn Google Dorking Operators:

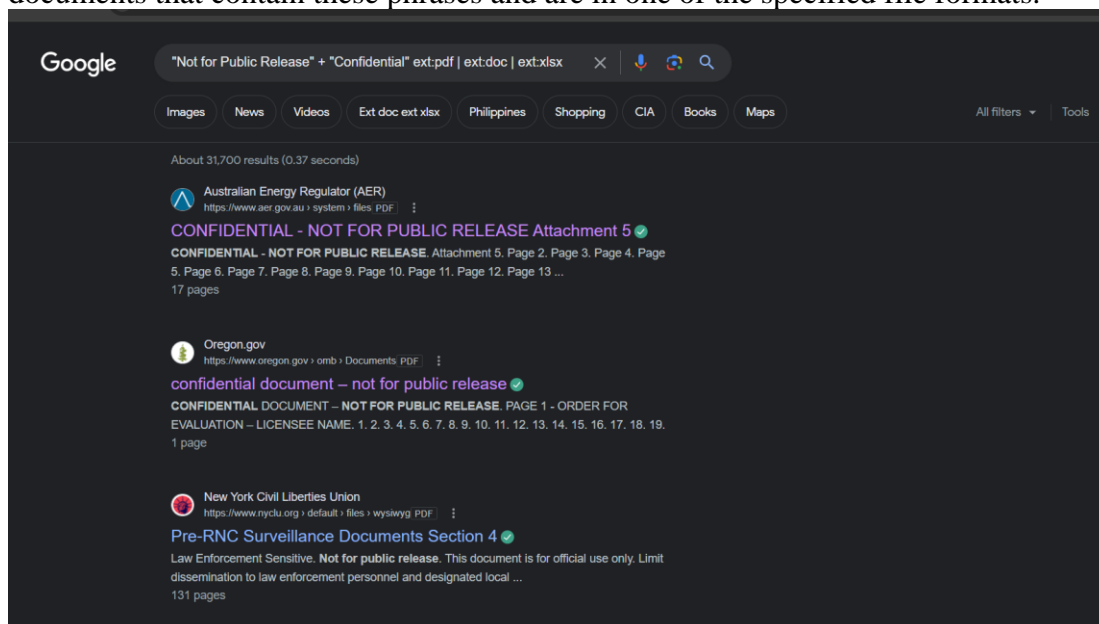
i. `site:google.com filetype:pdf`

- The Google Dork you provided, "site:google.com filetype:pdf", is a search query crafted to find PDF files specifically on the domain "google.com".



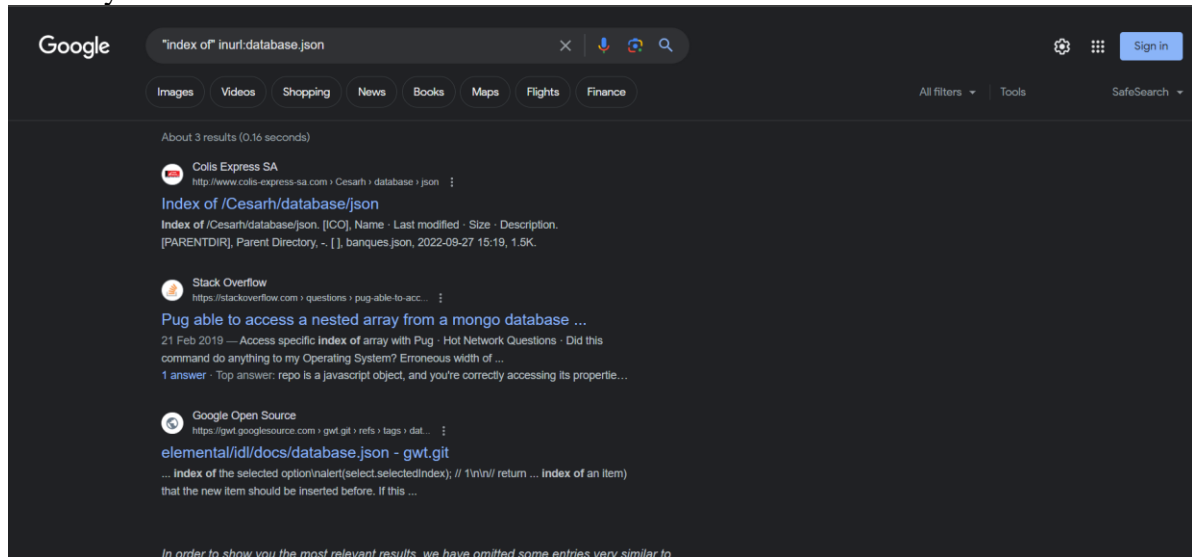
ii. `"Not for Public Release" + "Confidential" ext:pdf | ext:doc | ext:xlsx`

- It is a search query crafted to find documents with specific phrases ("Not for Public Release" and "Confidential") in their content, and with file extensions either PDF, DOC, or XLSX. When entered into the Google search bar and executed, it will return documents that contain these phrases and are in one of the specified file formats.

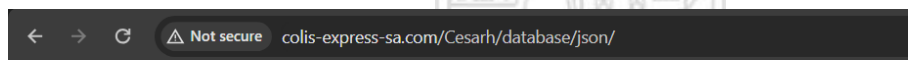


Step 3: Identify the Target,crafting and executing on google dorks:

- “index of” inurl:database.json
- This search query is commonly used in reconnaissance to discover openly accessible databases that may contain sensitive information.



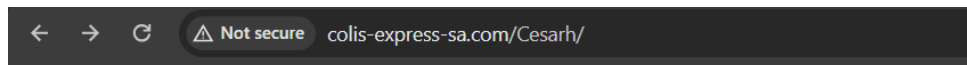
- This is the index of colis express website containing database of json type.
- It contains database information for bankaccount,birthdate,employee info etc.



Index of /Cesarh/database/json

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
banks.json	2022-09-27 15:19	1.5K	
bankaccount.json	2022-09-27 15:19	49K	
conges.json	2022-09-30 07:38	9.5K	
birthdate.json	2022-09-27 15:19	22K	
employees.json	2022-09-27 15:19	127K	
functions.json	2022-09-27 15:19	4.9K	
grilles.json	2022-09-27 15:19	739	
localites.json	2022-09-27 15:19	5.4K	
surcharges.json	2022-09-30 07:17	5.3K	
reminderSeptember.json	2022-09-30 09:03	18K	

- This is the main directory of website



Index of /Cesarh

Name	Last modified	Size	Description
Parent Directory		-	
app/	2022-09-26 09:47	-	
artisan	2022-09-26 09:46	1.6K	
bootstrap/	2022-09-26 09:47	-	
composer.json	2022-09-30 01:26	2.1K	
composer.lock	2022-10-03 15:15	366K	
config/	2022-10-03 15:15	-	
database/	2022-09-26 14:48	-	
error_log	2022-10-04 04:24	3.0K	
lang/	2022-09-26 09:47	-	
odoo/	2022-10-07 10:25	-	
package-lock.json	2022-10-03 15:15	230K	
package.json	2022-09-26 09:47	1.1K	
phpunit.xml	2022-10-06 14:41	1.2K	
pint.json	2022-09-26 09:47	27	
postcss.config.js	2022-09-26 09:47	140	
public/	2022-09-26 09:47	-	
resources/	2022-09-26 09:47	-	
routes/	2022-10-04 08:33	-	
storage/	2022-09-26 09:46	-	



- This is the Employee.json file in database directory containing information such as registration number,name,gender,address,children,date of birth and first name.

```

{
  "matricule": "0012",
  "nom": "RAKOTOTSIFERANA",
  "grille": "5B-Gr.III",
  "date_embauche": "1995-11-05",
  "adresse": "Lot VF 76 Volotara",
  "enfants": 4,
  "cin": "117171002640",
  "cnaps": "75101010039E",
  "fonction_id": 58,
  "localite_id": 6,
  "genre": 1,
  "prenom": "JEAN NOEL"
},
{
  "matricule": "0019",
  "name": "RANDRIATSIMIALA",
  "grille": "3B-Gr.II",
  "date_embauche": "1996-07-10",
  "adresse": "Lot 5F282 Andranomainty",
  "enfants": 2,
  "cin": "210011009884",
  "cnaps": "730625000302",
  "fonction_id": 78,
  "localite_id": 79,
  "genre": 1,
  "prenom": "NIRINA"
},
{
  "matricule": "0022",
  "name": "RAZAFINDRAPAOLY",
  "grille": "3B-Gr.II",
  "date_embauche": "1996-10-14",
  "adresse": "LOT 26 B73 ANT SIRABE",
  "enfants": 2,
  "cin": "204091001682",
  "cnaps": "740823000379",
  "fonction_id": 78,
  "localite_id": 38,
  "genre": 1,
  "prenom": "NASOLO"
}
],
[
  {
    "matricule": "0005",
    "nom": "ANDRIANOMENJANAHARY",
    "grille": "HC-Gr.IV",
    "date_embauche": "2021-01-01",
    "adresse": "COLIS EXPRESS",
    "enfants": 2,
    "cin": "204321008409",
    "cnaps": "59092040001U",
    "fonction_id": 56,
    "localite_id": 1,
    "genre": 1,
    "prenom": "HERISOA"
  },
  {
    "matricule": "0006",
    "nom": "ANDRIANALIMANANA",
    "grille": "5B-Gr.III",
    "date_embauche": "1994-09-01",
    "adresse": "Lot III D 30 bis",
    "enfants": 2,
    "cin": "101251056743",
    "cnaps": "66061010012Q",
    "fonction_id": 86,
    "localite_id": 20,
    "genre": 1,
    "prenom": "ROLAND"
  },
  {
    "matricule": "0010",
    "nom": "RAKOTOARINIASY",
    "grille": "HC-Gr.IV",
    "date_embauche": "1995-10-01",
    "adresse": "CHEZ COLIS EXPRESS",
    "enfants": 0,
    "cin": "201991052769",
    "cnaps": "66042010002A",
    "fonction_id": 33,
    "localite_id": 1,
    "genre": 1,
    "prenom": "JEAN HUBERT"
  }
]

```

- **"matricule"**: This represent a unique identifier or code associated with each delivery or package.
 - **"montant"**: This could represent the amount paid for each delivery or package.
- So each entry in the JSON data corresponds to a delivery or package, with the "matricule" being a unique identifier for that delivery and the "montant" being the amount paid for it. This data might be used by the delivery service to track and manage deliveries, invoices, or payments.

- reminderSeptember.json

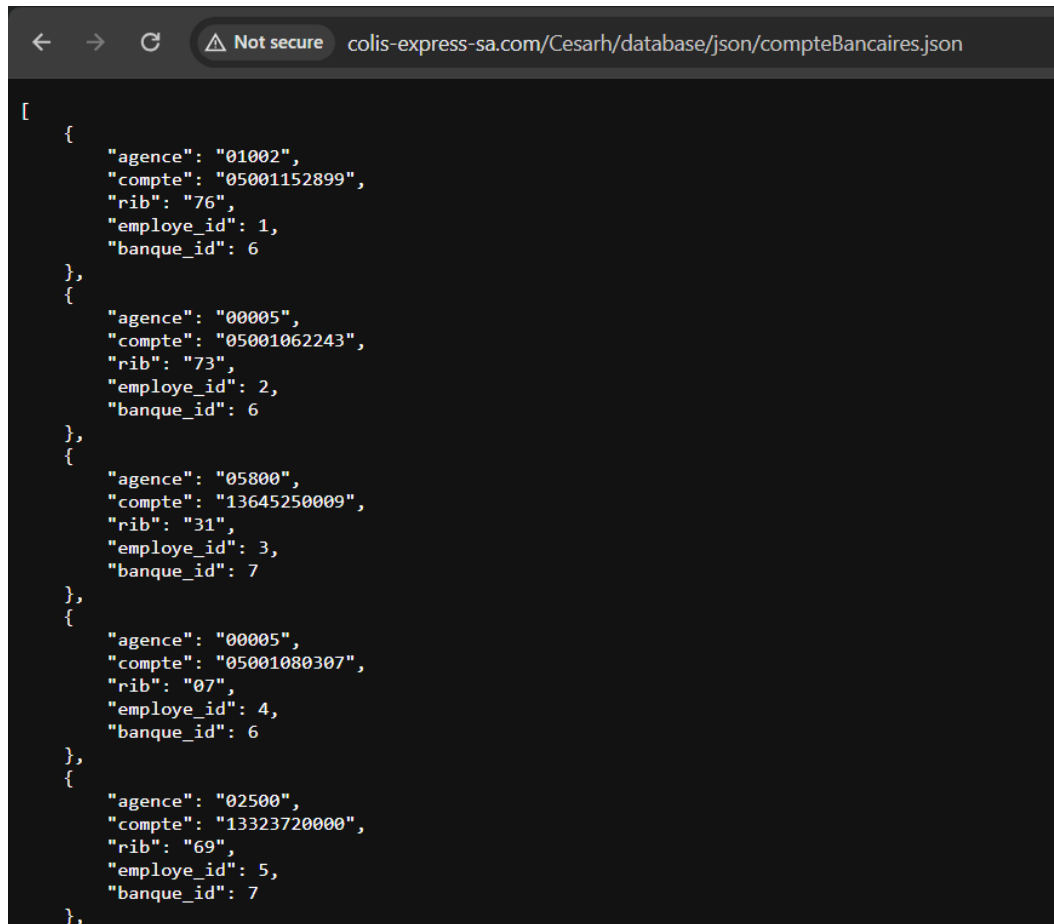
Index of /Cesarh/database/json

Name	Last modified	Size	Description
 Parent Directory		-	
 banks.json	2022-09-27 15:19	1.5K	
 bankaccount.json	2022-09-27 15:19	49K	
 conges.json	2022-09-30 07:38	9.5K	
 birthdate.json	2022-09-27 15:19	22K	
 employees.json	2022-09-27 15:19	127K	
 functions.json	2022-09-27 15:19	4.9K	
 grilles.json	2022-09-27 15:19	739	
 localites.json	2022-09-27 15:19	5.4K	
 surcharges.json	2022-09-30 07:17	5.3K	
 reminderSeptember.json	2022-09-30 09:03	18K	



```
[
  {
    "matricule": "0019",
    "montant": "22197.78"
  },
  {
    "matricule": "0022",
    "montant": "20291.76"
  },
  {
    "matricule": "0028",
    "montant": "29221.24"
  },
  {
    "matricule": "0033",
    "montant": "30472.20"
  },
  {
    "matricule": "0035",
    "montant": "33293.80"
  },
  {
    "matricule": "0040",
    "montant": "24571.40"
  },
  {
    "matricule": "0044",
    "montant": "30472.20"
  },
  {
    "matricule": "0051",
    "montant": "25235.50"
  },
  {
    "matricule": "0052",
    "montant": "20291.76"
  },
  {
    "matricule": "0072",
    "montant": "33293.80"
  },
]
```


- This is the **bankaccount.json** file consisting of agent number,account number,employee id,bank id.



```
[
  {
    "agence": "01002",
    "compte": "05001152899",
    "rib": "76",
    "employe_id": 1,
    "banque_id": 6
  },
  {
    "agence": "00005",
    "compte": "05001062243",
    "rib": "73",
    "employe_id": 2,
    "banque_id": 6
  },
  {
    "agence": "05800",
    "compte": "13645250009",
    "rib": "31",
    "employe_id": 3,
    "banque_id": 7
  },
  {
    "agence": "00005",
    "compte": "05001080307",
    "rib": "07",
    "employe_id": 4,
    "banque_id": 6
  },
  {
    "agence": "02500",
    "compte": "13323720000",
    "rib": "69",
    "employe_id": 5,
    "banque_id": 7
  },
]
```

- This is the banks.json file consisting of bank code,name of bank and acronym for bank for transaction by customers.

```
[
  {
    "code": "00001",
    "nom": "Bank of Africa Madagascar",
    "ref": "BOA"
  },
  {
    "code": "00004",
    "nom": "Banque Malgache de l'Océan Indien",
    "ref": "BMOI"
  },
  {
    "code": "00005",
    "nom": "BNI Madagascar",
    "ref": "BNI"
  },
  {
    "code": "00006",
    "nom": "The Mauritius Commercial Bank (Madagascar) SA",
    "ref": "MCB"
  },
  {
    "code": "00007",
    "nom": "SBM Madagascar",
    "ref": "SBM"
  },
  {
    "code": "00008",
    "nom": "BFV-Soci t  G n rale",
    "ref": "BFV"
  },
  {
    "code": "00009",
    "nom": "Bank of Africa Madagascar",
    "ref": "BOA"
  },
  {
    "code": "00011",
    "nom": "Acc s Banque Madagascar",
    "ref": "ABM"
  },
  {
    "code": "00012",
    "nom": "BGFIBank Madagascar",
    "ref": "BGFI"
  },
]
```

Step 6: Analyze Results:

- This delivery service website is vulnerable as it exposes(public info) the sensitive information of transactions made by customers in json format.

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:

- **Exposure of Bank Details:** If the delivery service website is exposing bank details, it could lead to financial fraud, unauthorized transactions, and compromise of customers' financial accounts. This could severely damage the trust and reputation of the delivery service.
- **Exposure of Transaction Details:** Exposing transaction details made by customers can lead to privacy violations, identity theft, and financial loss for customers.
- **Exposure of Basic Employee Information:** If basic employee information is exposed, it can lead to targeted attacks, identity theft, or social engineering attempts against employees. This could compromise the security of internal systems and sensitive company data.

Recommendations:

- **Review Website Configuration:** Ensure that directory listings are disabled to prevent unintentional exposure of sensitive files and directories to search engines.
 - **Regular Google Dorking Audits:** Conduct regular audits using Google Dorking techniques to proactively identify any inadvertently exposed sensitive information.
 - **Implement Access Controls:** Implement access controls and authentication mechanisms to restrict access to sensitive directories and files.
 - **Encrypt Sensitive Data:** Encrypt sensitive data stored on the website to mitigate the impact of unauthorized access in case of a breach.
2. If vulnerabilities were discovered, discuss the approach you would take for responsible disclosure. What considerations would guide communication with the affected parties?

Ans:

Here's an approach for responsible disclosure and considerations for communication with affected parties:

- **Verify the Vulnerability:** Before disclosing the vulnerability, ensure that it is indeed valid and poses a genuine security risk. Verify the vulnerability through testing and analysis to understand its scope and potential impact.
- **Identify the Responsible Party:** Determine who is responsible for addressing the vulnerability. This could be the website owner, the organization's security team, or a third-party vendor

responsible for website maintenance and security.

- **Prepare a Detailed Report:** Document the vulnerability thoroughly, including its description, impact, affected systems, and potential mitigation strategies. Provide clear steps for reproducing the vulnerability to help the responsible party understand and address it.
- **Contact the Responsible Party:** Reach out to the responsible party directly through secure communication channels, such as encrypted email or a secure contact form on their website. Provide a summary of the vulnerability and offer to share the detailed report privately.
- **Establish a Disclosure Timeline:** Work with the responsible party to establish a timeline for addressing the vulnerability. Consider factors such as the severity of the vulnerability, the complexity of mitigation, and any potential mitigating factors that may require additional time.
- **Offer Support and Assistance:** Offer your support and assistance to the responsible party in understanding and addressing the vulnerability. This could include providing additional information, clarification, or guidance on mitigation strategies.
- **Maintain Confidentiality:** Respect the confidentiality of the vulnerability until it has been adequately addressed and publicly disclosed. Avoid disclosing information about the vulnerability publicly or to unauthorized parties before it has been mitigated.

Outcomes:

CO2: Comprehend purpose of Anonymity and Foot printing.

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

Thus we learnt about the google dorking commands for using passive reconnaissance on a vulnerable website.

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>