Experiment No. 6

Batch:A2 **Roll No.:16010421073** **Experiment No.:6**

Aim: Conducting recon with OSINT tools.

Resources needed: OSINT Framework, Maltego, The OSINT Curious Project, Shodan, SpiderFoot, theHarvester, Recon-ng, Websites like public records databases, business registries, and government databases

---

Pre Lab/ Prior Concepts:
Students should know the Definition of OSINT, Legal and Ethical Considerations, Scope and Objectives, Public vs. Private Information, Tool Familiarity, Target Profiling, Understanding Search Operators, and Social Engineering Awareness.

Theory:
Open Source Intelligence (OSINT) is a critical facet of cybersecurity that involves collecting and analyzing publicly available information to gain insights into the online presence of individuals, organizations, or entities. Conducting reconnaissance with OSINT tools is a strategic process that unveils digital footprints, providing valuable data for threat intelligence, security assessments, and investigations.

Understanding OSINT: OSINT leverages publicly accessible information from social media, online forums, public records, and other openly available platforms. The key objective is to aggregate and analyze data to create a comprehensive profile of the target.

Legal and Ethical Considerations: Responsible conduct is paramount when engaging in OSINT activities. Practitioners must operate within legal boundaries and adhere to ethical standards, respecting privacy and avoiding any activities that might violate laws or infringe on individuals' rights.

Scope and Objectives: Defining the scope and objectives of OSINT activities is crucial. Whether it's gathering information about a potential threat, assessing the security posture of an organization, or investigating a specific incident, clear goals guide the reconnaissance process and ensure that efforts are focused and purposeful.

Tools of the Trade: Various OSINT tools facilitate the collection and analysis of information. Tools like Maltego, Shodan, theHarvester, and SpiderFoot automate data gathering, helping analysts visualize relationships between different data points and uncover hidden connections.

Information Validation: One of the critical aspects of OSINT is validating the obtained information. Analysts must employ techniques to verify the data's accuracy, relevance, and timeliness. Validation ensures that decisions based on OSINT findings are sound and reliable.

Target Profiling: OSINT enables the creation of detailed profiles of targets. Whether it's an

individual, a company, or a threat actor, profiling involves collecting data about online activities, affiliations, interests, and potential vulnerabilities. This information aids in risk assessment and strategic decision-making.

Procedure:

Procedure for Conducting Reconnaissance with OSINT Tools

Conducting reconnaissance with Open Source Intelligence (OSINT) tools involves systematically gathering and analyzing publicly available information to uncover digital insights. Here's a step-by-step procedure for conducting OSINT reconnaissance:

Step 1: Define Scope and Objectives: Clearly define the scope and objectives of OSINT activities. Determine the specific information to seek and the goals of reconnaissance. Whether it's profiling an individual, assessing an organization's online presence, or gathering threat intelligence, a well-defined scope guides the process.

Step 2: Identify Target: Identify the target for reconnaissance. This could be an individual, an organization, or a specific topic of interest. Understanding the target helps tailor OSINT efforts to gather relevant information.

Step 3: Select OSINT Tools: Choose appropriate OSINT tools based on the nature of target and objectives. Common OSINT tools include:

- Maltego: For visualizing relationships between different data points.
- Shodan: To search for internet-connected devices.
- theHarvester: For email and domain information gathering.
- SpiderFoot: An OSINT automation tool for comprehensive data collection.

Step 4: Craft Search Queries: Create specific search queries or tasks based on the information gathered and the chosen OSINT tools. Craft queries that leverage the functionalities of the selected tools to obtain relevant results.

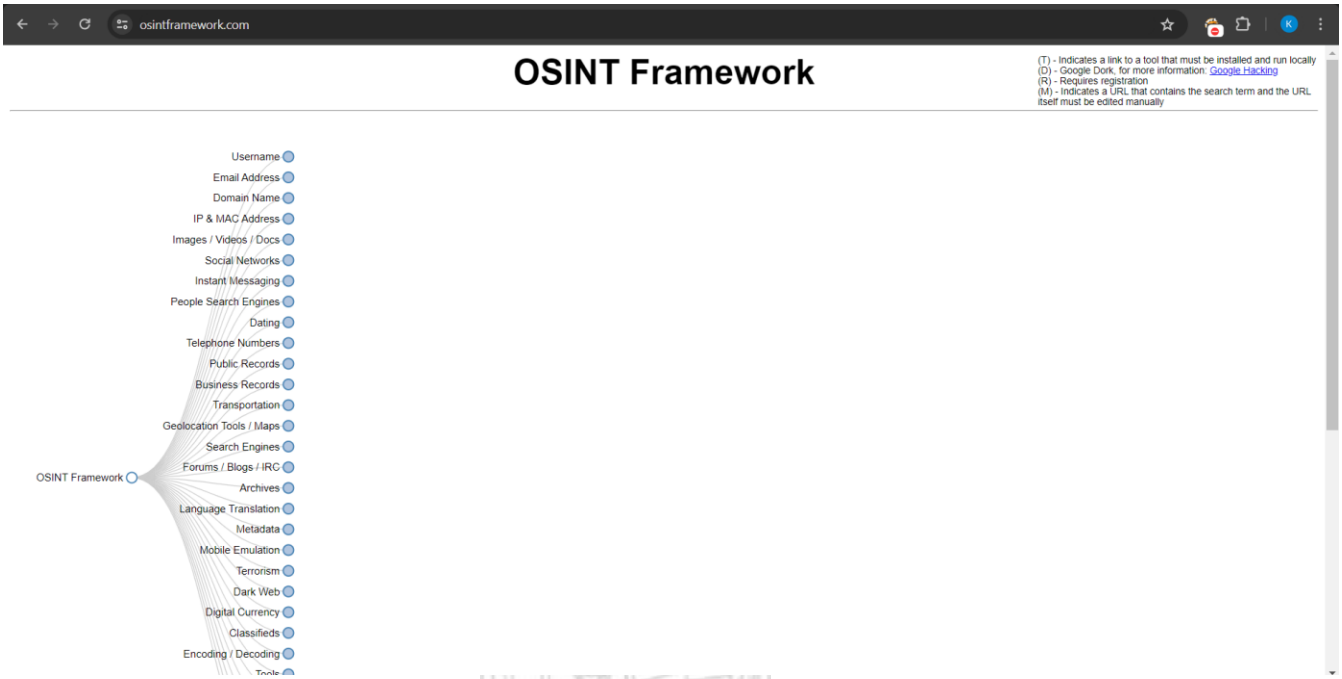
Step 5: Execute OSINT Tools: Execute the chosen OSINT tools and queries to collect information. Use tools to search for data across various sources, including social media platforms, online forums, public records, and websites.

Step 6: Validate Information: Validate the collected information's accuracy, relevance, and timeliness. Cross-reference data obtained from different sources to ensure consistency and reliability. Validation is crucial to avoid relying on misinformation.

Step 7: Analyze and Correlate Data: Analyze the gathered data for meaningful insights. Correlate different data points to create a comprehensive profile of the target. Look for patterns, connections, and potential areas of interest.

Output (Code with result Snapshot)

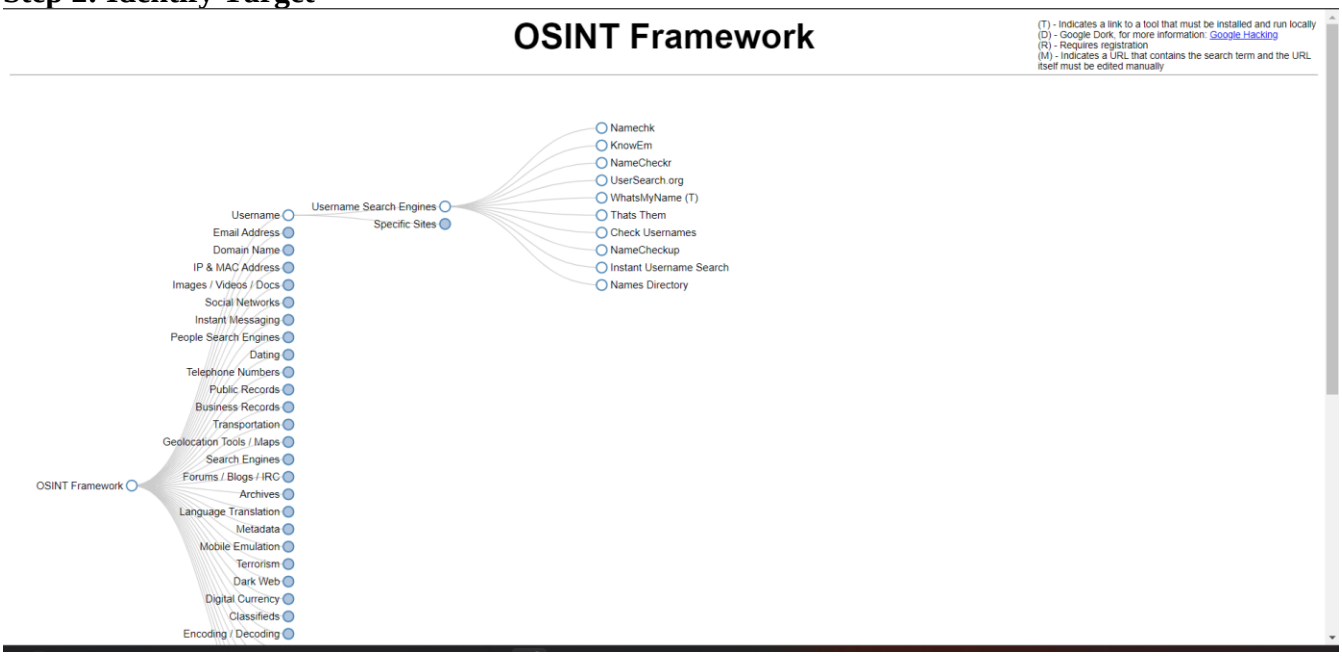
OSINT Framework where we are going to use OSINT Tool username.



Step 1: Define Scope and Objectives

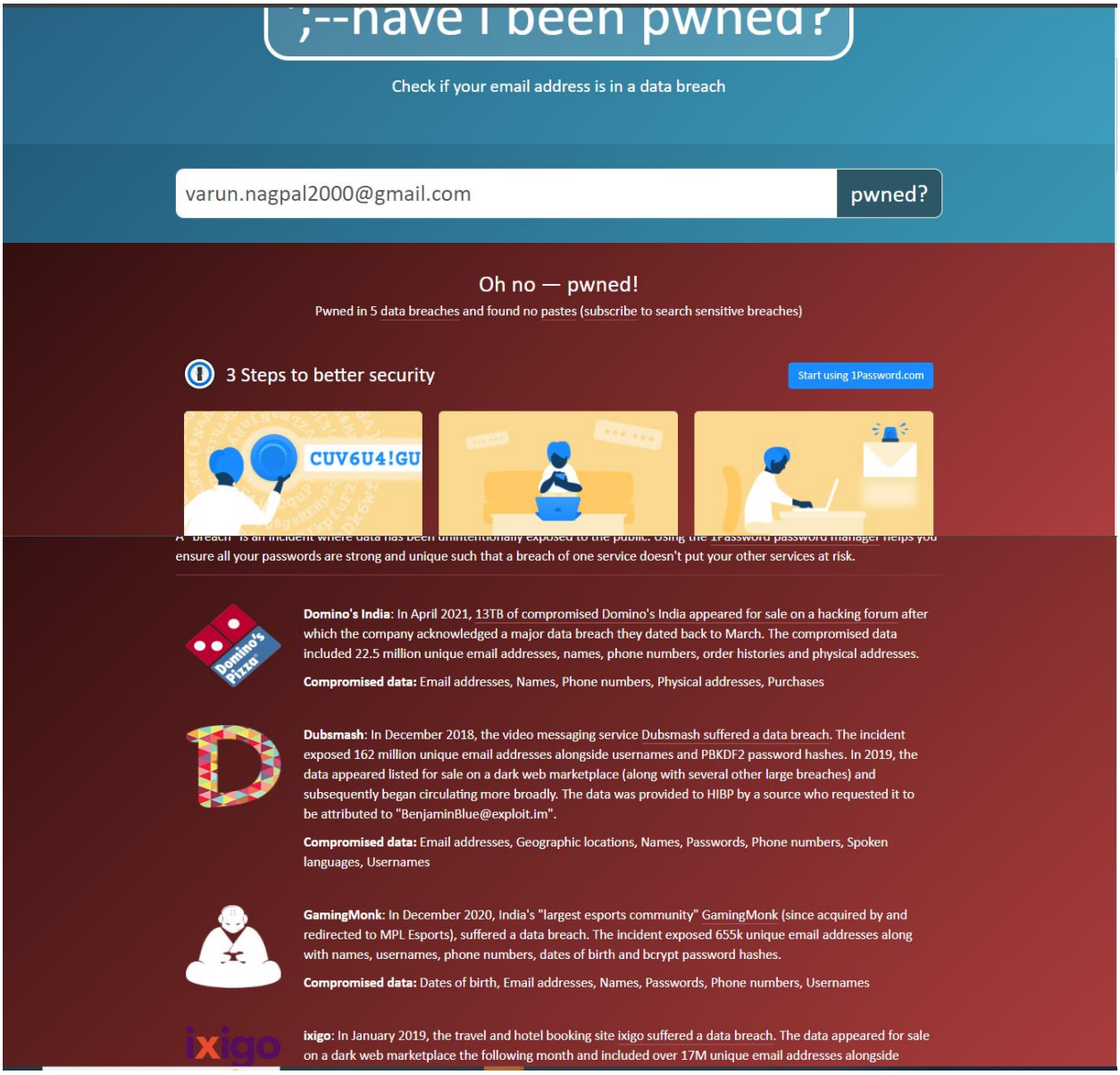
Searching for the username across various online platforms, social media sites, forums, and databases to gather information about the person's online presence and activity.

Step 2: Identify Target

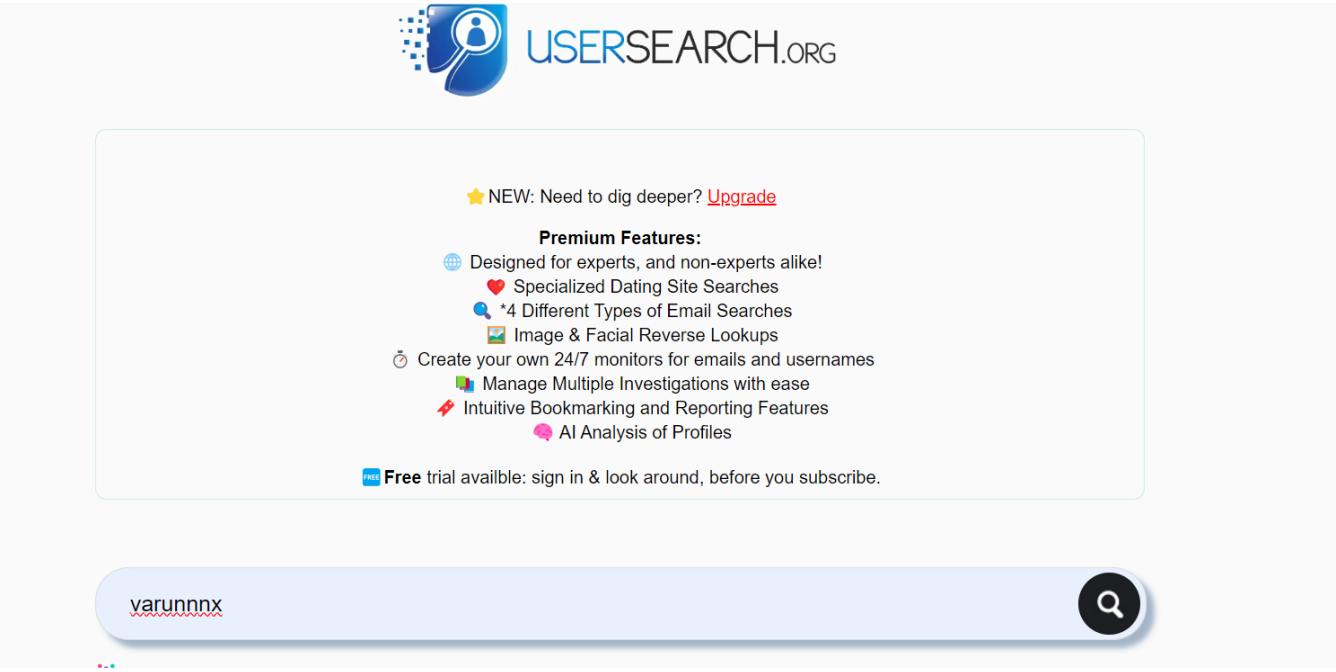


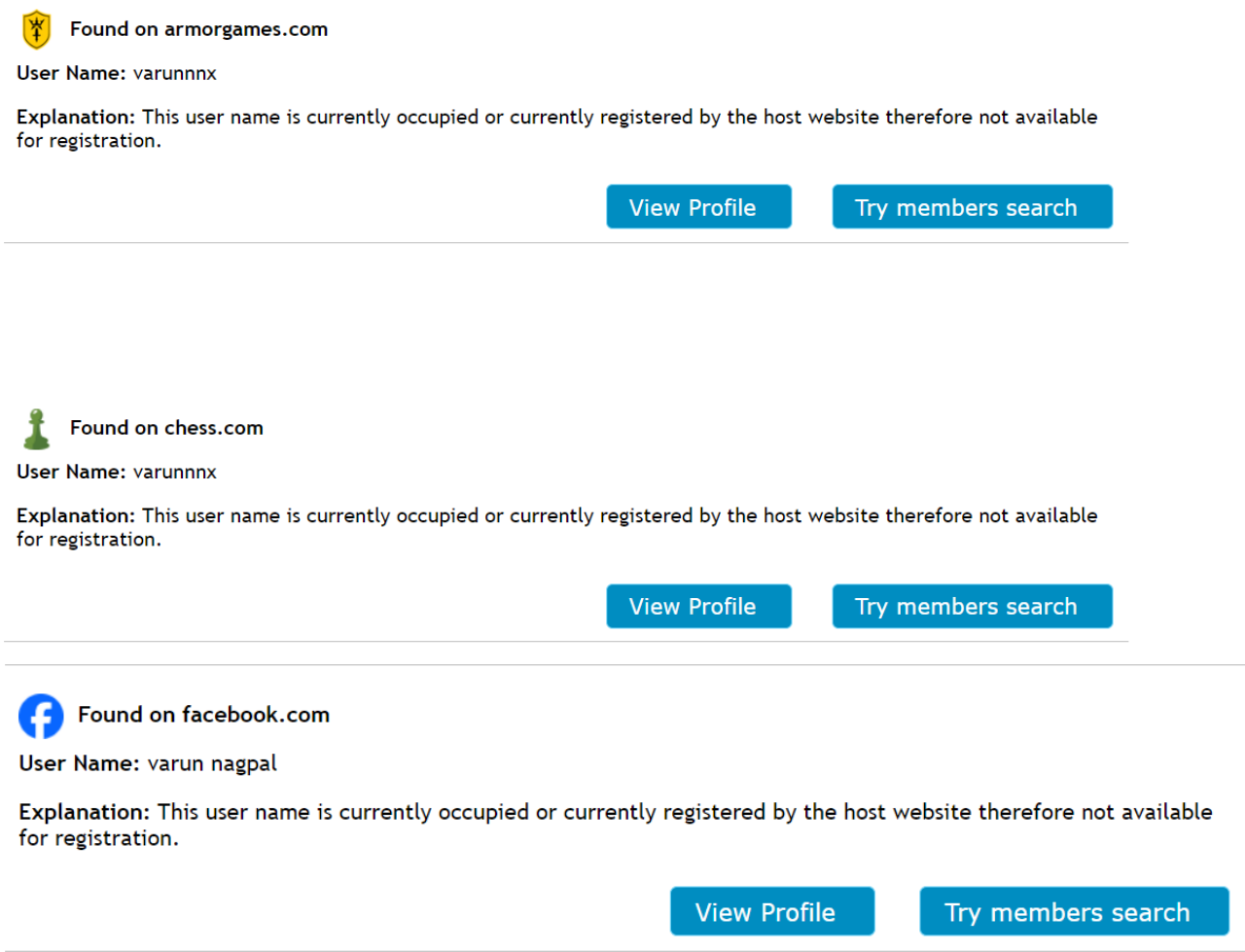
Step 3: Select OSINT Tools

- **OSINT Tools used in data gathering are 'have I been pwned' for email breach.**

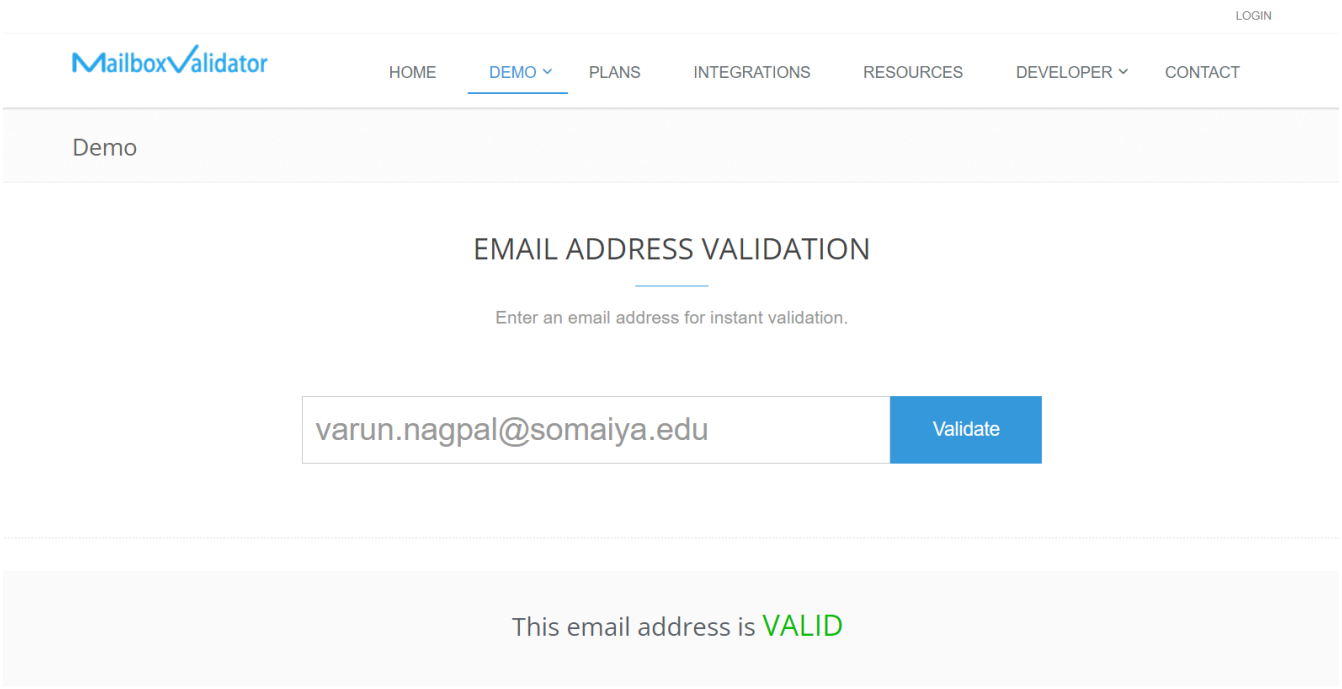


Step 4: Craft Search Queries:
Using User Search.org

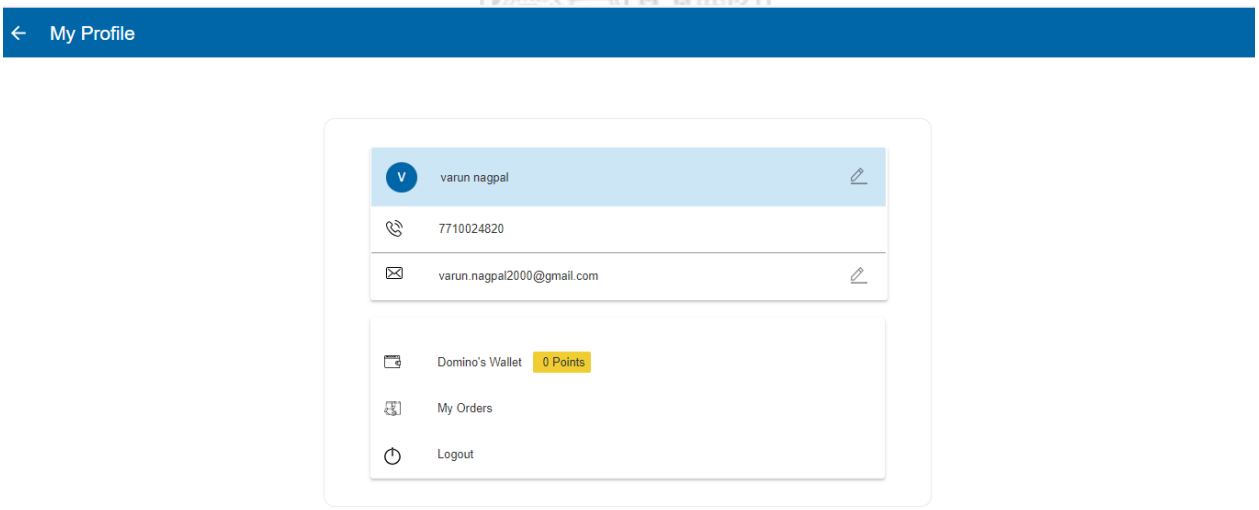




Step 5: Execute OSINT Tools:



Step 6: Validate Information:
Validating for dominos account data breach .



Step 7: Analyze and Correlate Data:

Post Lab Questions: -

1. **Evaluate the effectiveness of the OSINT tools used in the reconnaissance. Which tools proved most valuable, and how did they contribute to achieving the defined objectives?**

Ans: When evaluating the effectiveness of OSINT tools used for username reconnaissance related to a specific person, here are some key points to consider:

- **Pipl.com**
  This tool can be quite valuable as it aggregates data from various public sources and directories. For a username, it may reveal the real name, location, images and other details about the associated person. However, the depth of results can vary.
- **Spokeo.com**
  While designed more for physical address/phone searches, Spokeo can sometimes surface social media, online profiles and websites tied to a username which aids in identifying the person behind it.
- **Webmix.ru**
  This Russian engine has proven effective for finding forum posts, blog comments, and other niche sources where a username is used, which can provide useful context about the person's interests and activities online.

2. **Assess your documentation practices. What information did you include in your records, and how would your documentation aid in analysis, reporting, or collaboration with other team members?**

Ans:

- **Description of Functionality:** A detailed explanation of what the tool does and its purpose, such as identifying and gathering information about a specific person based on their username.
- **Technical Specifications:** Information on the technical aspects of the tool, including programming languages, frameworks, or libraries used, database structures, APIs utilized, and any other relevant technical details.
- **Data Sources:** Documentation on the sources of data the tool accesses or interacts with, such as social media platforms, public databases, or other online sources.

Outcomes: CO2 Comprehend purpose of Anonymity and Foot printing

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)
Successfully conducted recon for a particular username along with data breaches.

Signature of faculty in charge with date

References:

1. https://securitytrails.com/blog/osint-tools
2. https://www.codecademy.com/article/passive-active-reconnaissance
3. https://www.csnp.org/post/using-osint-reconnaissance-to-protect-your-organization