**Experiment – 2**

**Aim :** Explore Burp Suite, archieve.org, HTTrack, Mx analyser, Email Lookup, Harvester.

**Description** :

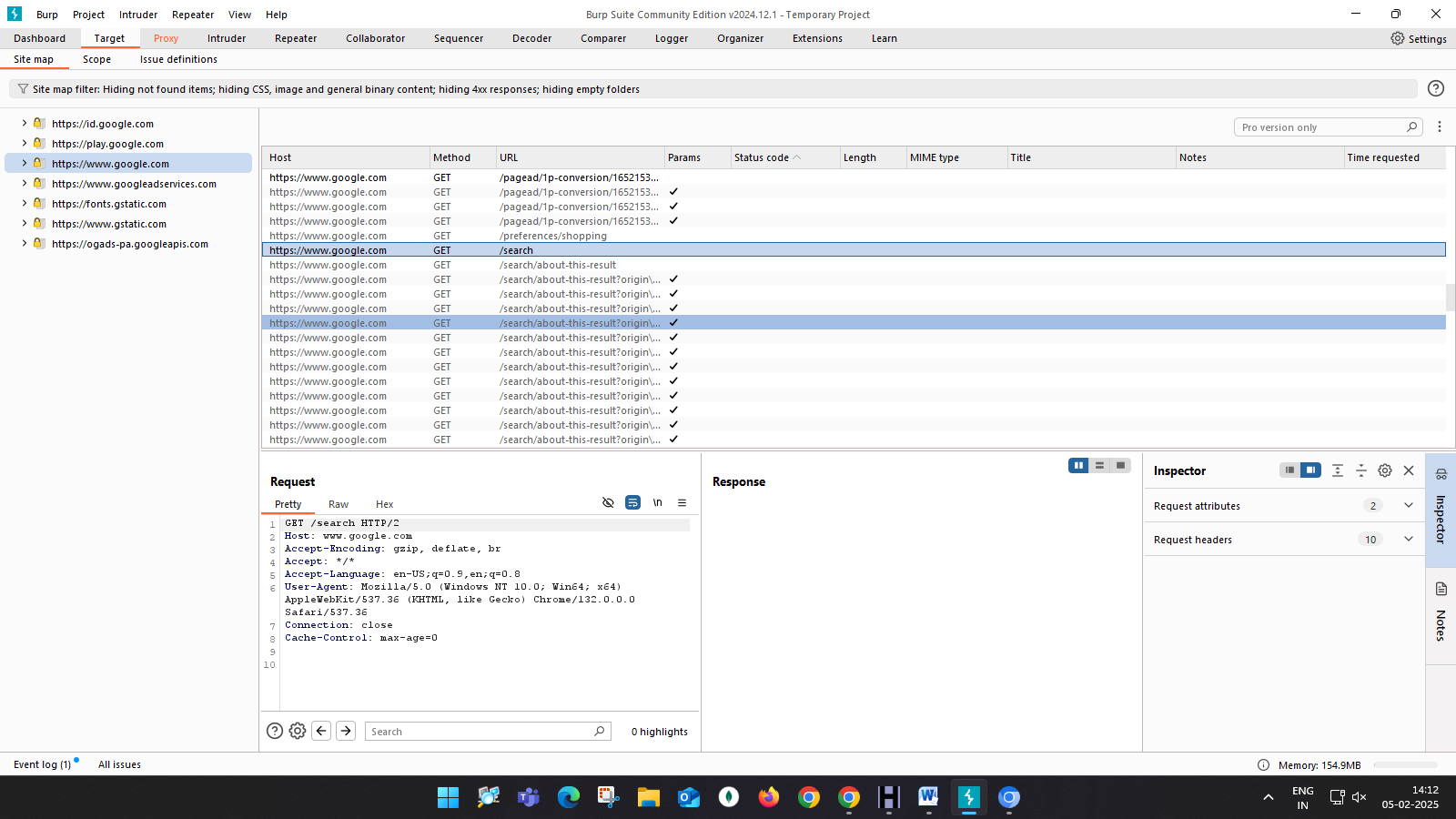
1.**Burp Suite:**

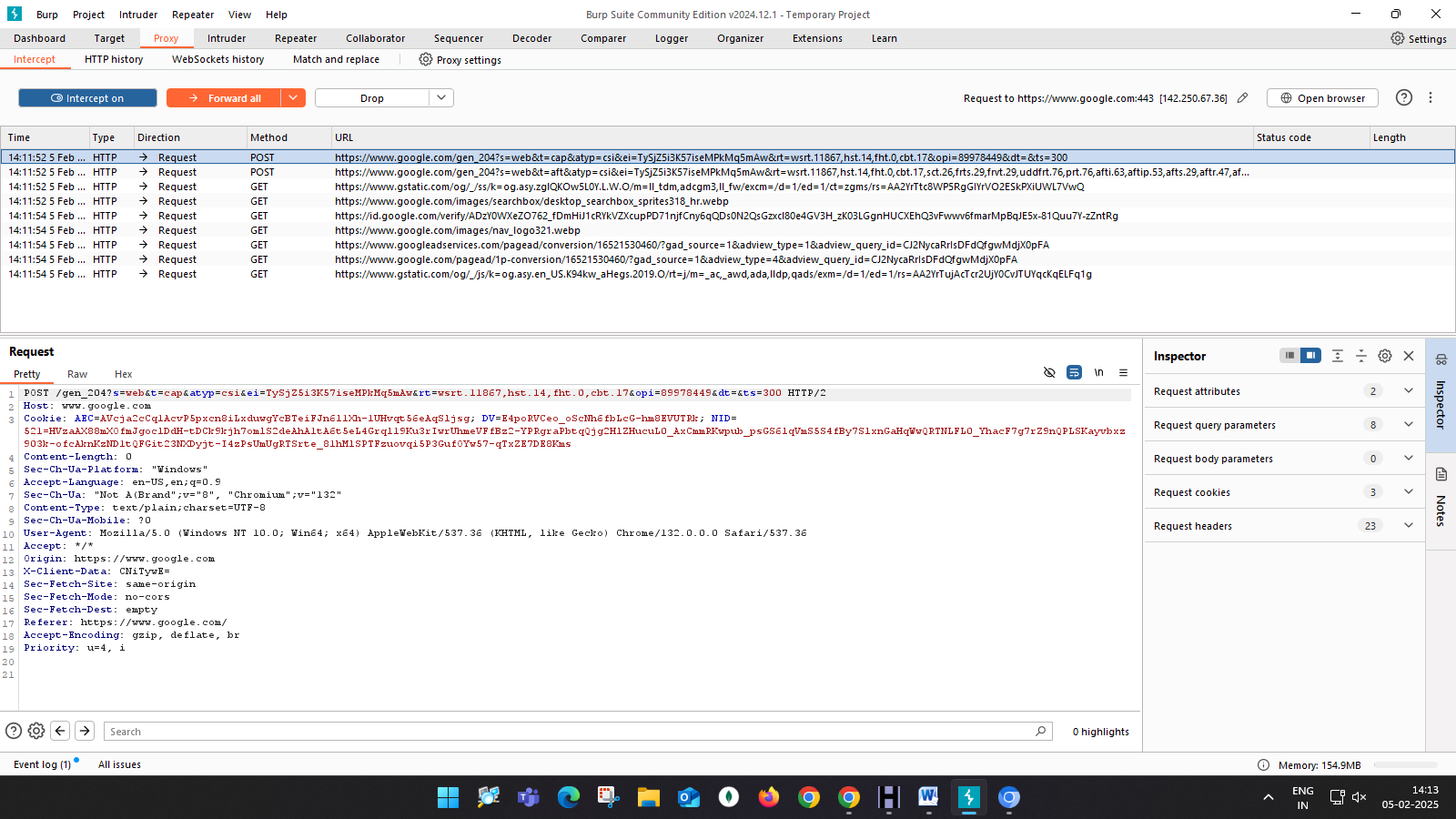
Burp Suite is a comprehensive platform for web application security testing. It’s used for scanning, crawling, and manipulating HTTP/S traffic between a browser and a web server, making it a powerful tool for penetration testers.

 **Task**: Intercept and modify HTTP requests using Burp Suite.

 **Steps**:

1. Launch Burp Suite and set up the proxy.
2. Configure your browser (e.g., Firefox) to use 127.0.0.1:8080 as its proxy.
3. Browse a simple website (e.g., <https://google.com>).
4. In Burp Suite, go to the "Proxy" tab and intercept the request.
5. Modify the request (e.g., change the value of a parameter) and forward it.
6. Observe the website’s response to the modified request.

****

****

**Key Features:**

**Proxy Intercept:** Allows you to intercept, inspect, and modify HTTP and HTTPS requests and responses in real-time between a browser and web server.

**Web Application Scanner:** Identifies security vulnerabilities like SQL injection, XSS, and other web application issues by scanning the web application's traffic.

**Spidering**: Automatically maps out a website by crawling and analyzing links, directories, and resources.

**Intruder**: Automates attacks such as brute force, fuzzing, and parameter manipulation to find vulnerabilities in web applications.

**Repeater**: Sends modified requests and replays them to test responses and application behavior.

**Sequencer**: Analyzes the randomness of tokens and sessions to find weaknesses in web application security.

**Extensibility**: Supports extensions that enhance functionality, including various plugins and custom scripts via the Burp Extender API.

**Collaborator**: A service for detecting out-of-band (OOB) interactions in web applications**.**

**Conclusion:**

Burp Suite is an essential tool for web application security testing. By intercepting and modifying HTTP/S traffic, it allows security professionals to assess the vulnerabilities of web applications. The ability to capture, manipulate, and analyze requests and responses is critical for identifying potential security flaws such as SQL injection, XSS (Cross-Site Scripting), and other vulnerabilities. Burp Suite is widely regarded as one of the most powerful tools in penetration testing, and familiarity with it enhances the ability to test and protect web applications effectively.

### ****2. archive.org****

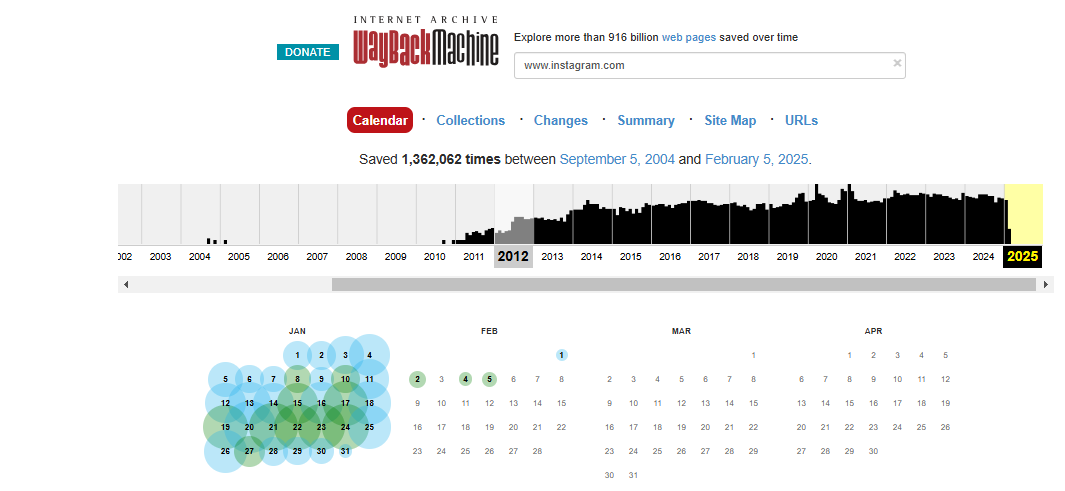
#### ****Purpose:****

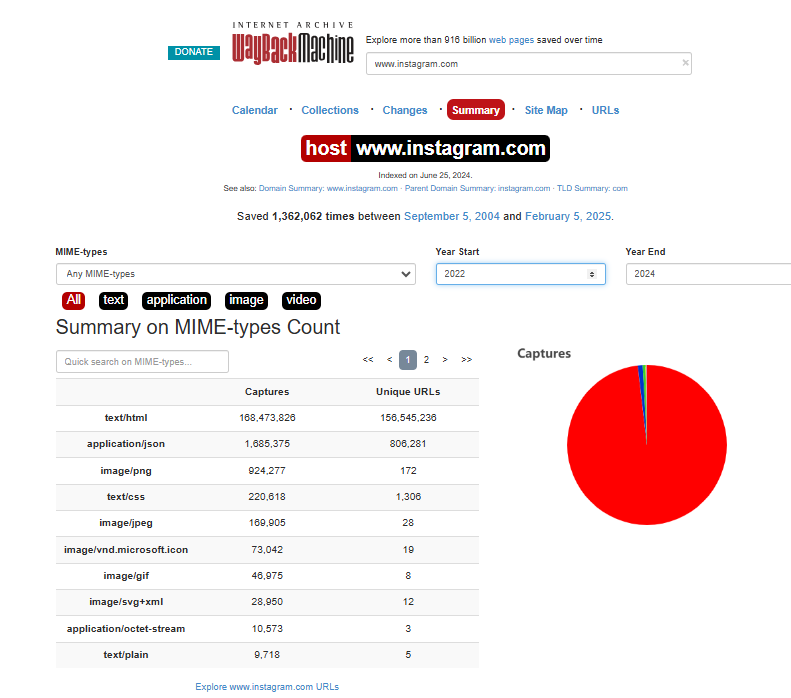
archive.org, also known as the Wayback Machine, is an online tool that lets you view archived versions of websites. This is useful for researching past versions of a site, finding removed content, or performing OSINT (Open Source Intelligence) gathering.

**Task**: Retrieve historical versions of a website.

**Steps**:

* Go to archive.org/web/.
* Enter the URL of a website (e.g., <http://google.com>).
* Browse through different archived dates.
* Compare how the website has evolved over time, including changes to its content and structure.







#### ****Key Features:****

* **Website Archiving**: Allows users to view historical snapshots of websites taken at different points in time.
* **Searchable Database**: Provides an easy way to search archived content by URL, date, or site category.
* **Access to Removed Content**: Lets you view content that has been removed or altered on websites, helping in forensics and digital investigations.
* **Wide Coverage**: Archives millions of websites across multiple years, offering insights into website structures, content, and design changes over time.
* **Downloadable Content**: Enables users to download archived websites for offline browsing and analysis.
* **No Authentication Required**: You can access archived websites without needing any account or credentials.
* **Public Data Collection**: Gathers data for public use, making it a valuable tool for researchers, historians, and investigators.

#### ****Conclusion:****

The Wayback Machine (archive.org) is a valuable resource for retrieving historical data from websites. It’s useful in cases where content has been deleted, or when trying to understand how a website has evolved over time. Additionally, it can be a vital tool for digital forensics and Open Source Intelligence (OSINT) gathering. Understanding its capabilities is critical for anyone involved in web research or investigating online content changes over time. It also helps in retrieving information that might no longer be available on the live web.

### ****3. HTTrack****

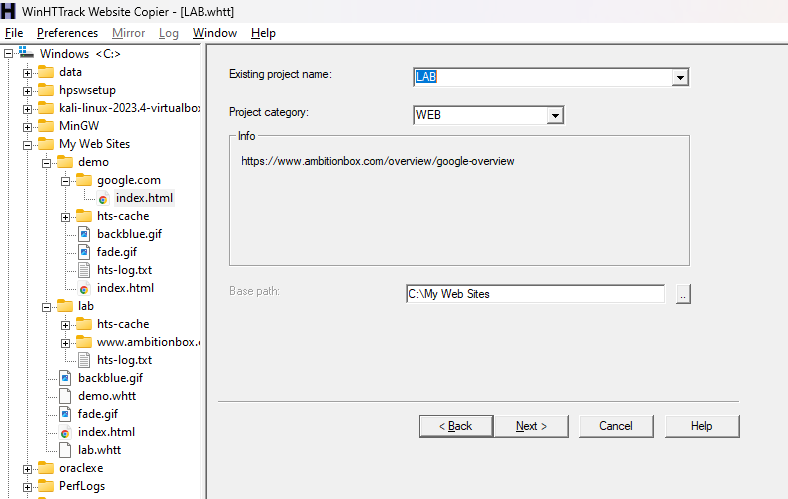
#### ****Purpose:****

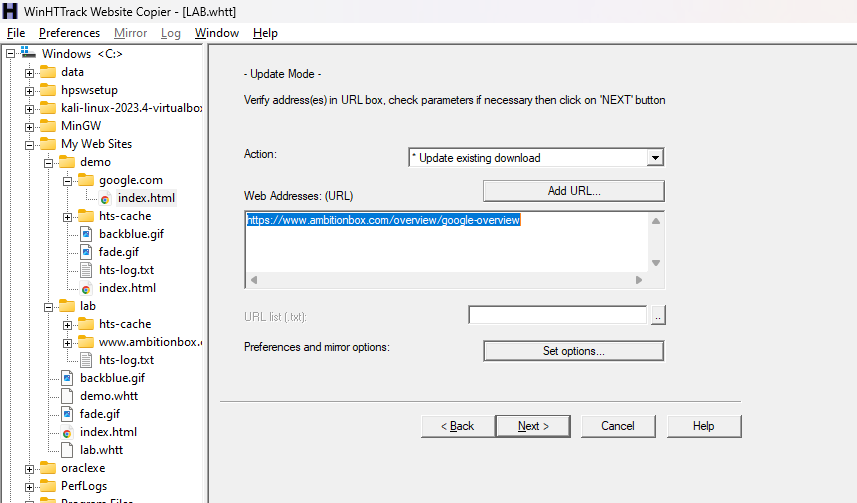
HTTrack is an open-source web crawler that allows you to download a website from the Internet to your local hard drive, enabling offline browsing of the site.

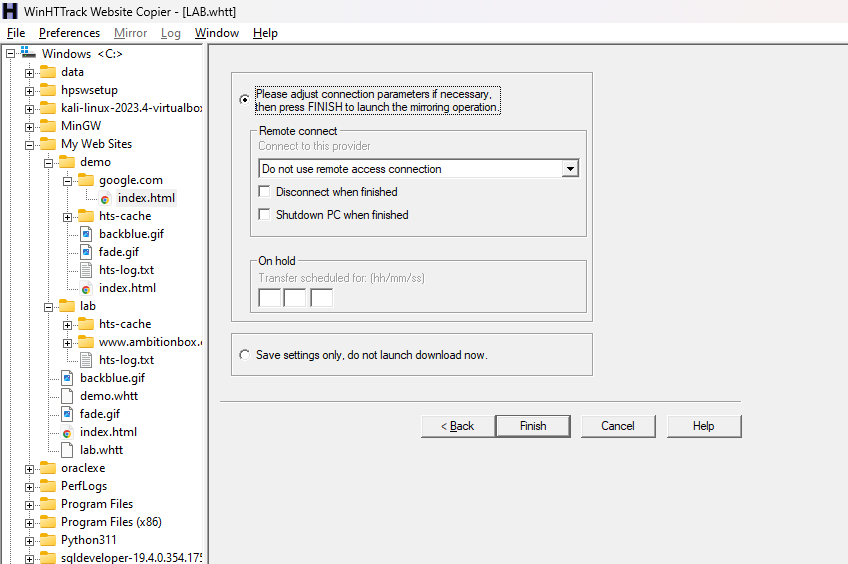
**Task**: Mirror a website for offline analysis.

**Steps**:

* 1. Open HTTrack and choose "Create a new project."
  2. Enter a project name, category, and choose the directory where you want to save the website.
  3. Enter the URL of the website to download.
  4. Start the mirroring process.
  5. After completion, browse the website offline by opening the index.html file in the directory.









#### ****Key Features:****

* **Website Mirroring**: Downloads entire websites, including images, HTML, and other assets, for offline browsing.
* **Customization Options**: Allows users to define download parameters, such as limiting download size, file types, or the depth of crawl.
* **Resume Downloads**: If a download process is interrupted, it can be resumed from where it left off.
* **Automatic Link Adjustments**: After downloading, HTTrack adjusts links so that the website can be browsed offline as if it were the live version.
* **Supports Multiple Platforms**: Available for Windows, Linux, and macOS.
* **User-Agent Customization**: Allows users to change the user-agent string to mimic different browsers or devices.
* **Mirroring Multiple Sites**: Supports downloading multiple websites simultaneously.

#### ****Conclusion:****

HTTrack is an excellent tool for mirroring websites and enabling offline browsing. This tool is useful for data collection, website archiving, and offline analysis. It’s valuable for anyone needing to perform analysis on a website's structure and content without having to be constantly connected to the internet. It can also be used to back up websites or create offline copies for analysis or review, making it a powerful tool in the arsenal of web researchers and penetration testers.

### ****4. Mx Analyzer****

#### ****Purpose:****

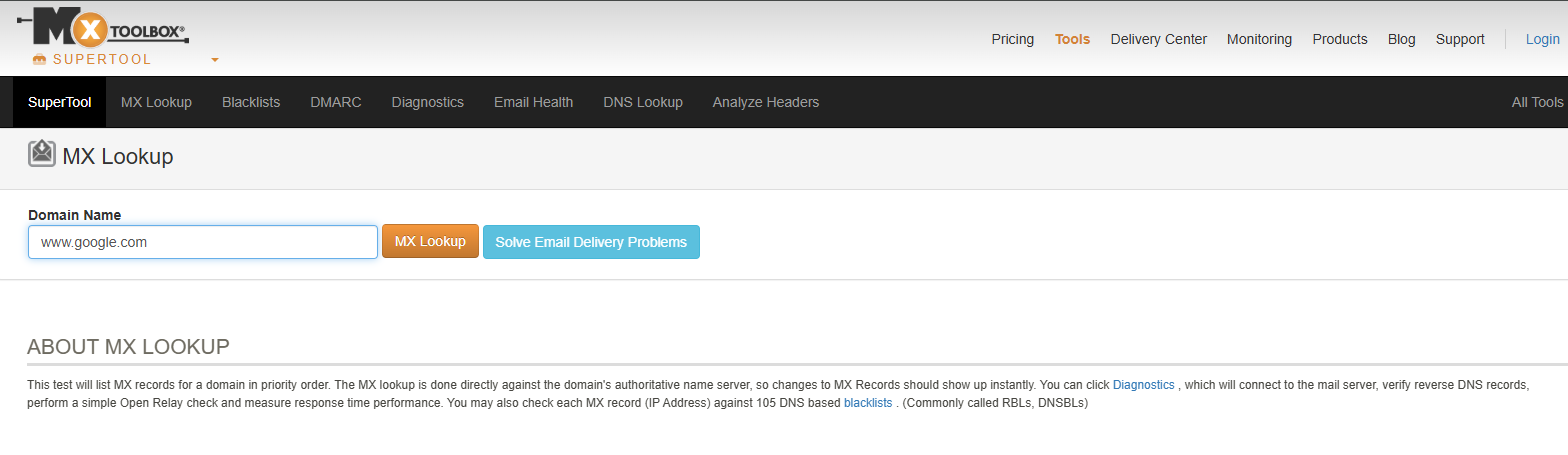
MX Analyzer is a tool used to analyze Mail Exchange (MX) records to ensure proper email server configuration, security, and to diagnose potential email delivery issues.

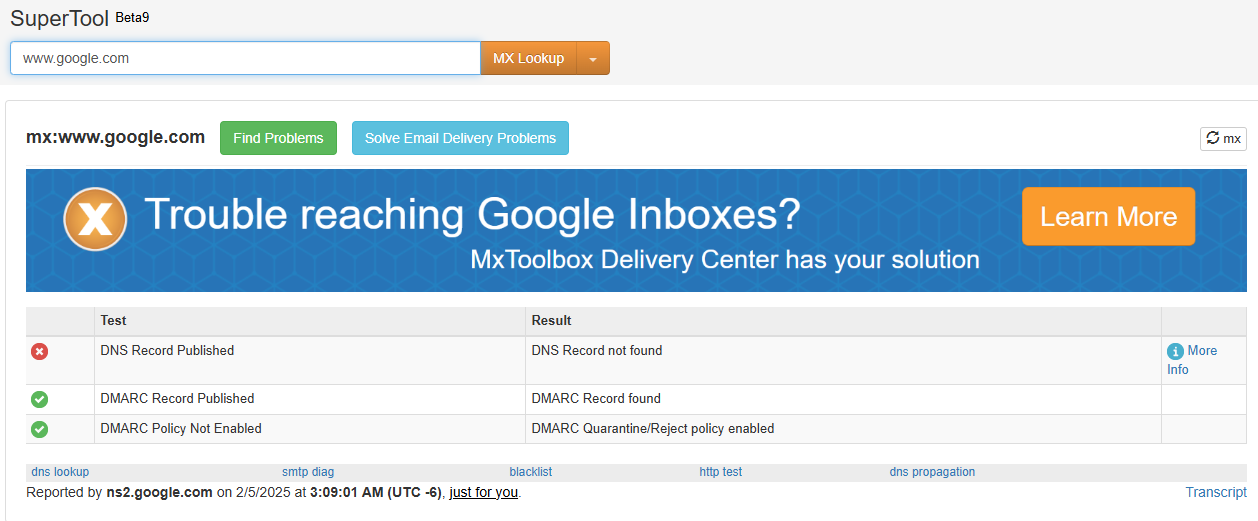
#### ****Lab Example:****

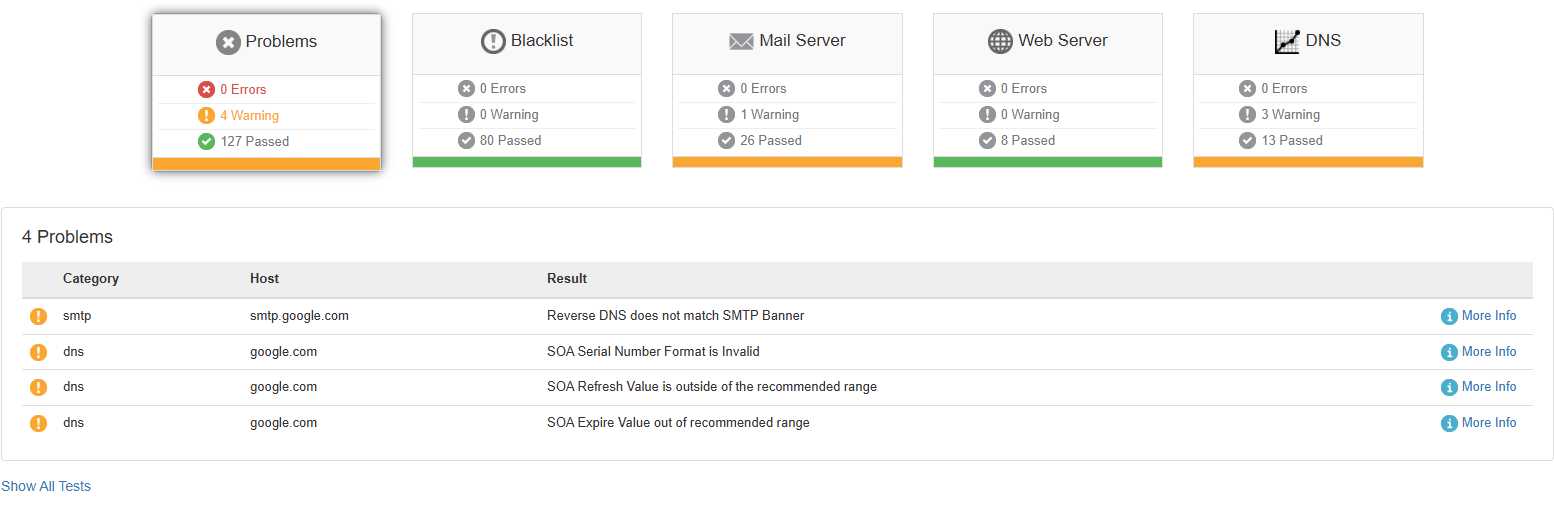
**Task**: Analyze the MX records of a domain.

**Steps**:

* Go to [MXToolbox](https://mxtoolbox.com/).
* Enter a domain name (e.g., google.com) into the search bar.
* Select the "MX Lookup" option.
* Review the MX records, including the mail servers and their IP addresses.
* Analyze the security and configuration of the email system.







#### ****Key Features:****

* **MX Record Lookup**: Allows you to check the Mail Exchange (MX) records of a domain, which are essential for routing emails.
* **Blacklist Check**: Checks if an email server's IP address is listed in blacklists, which can affect email deliverability.
* **DNS Record Lookup**: Provides additional insights into DNS records, such as A, AAAA, CNAME, and SPF records.
* **SMTP Test**: Helps test the connectivity and functionality of an SMTP server to diagnose email delivery issues.
* **Email Health Report**: Offers detailed reports on the health and configuration of an email system, highlighting potential issues or vulnerabilities.
* **Relay Test**: Checks if an SMTP server allows open relays, which can lead to spam issues.
* **Monitoring Alerts**: Some MX analyzers allow you to set up alerts if an MX record or server status changes.

#### ****Conclusion:****

MX Analyzer tools like MXToolbox are essential for diagnosing email server configurations and ensuring that MX records are correctly set up. They help in identifying potential misconfigurations in email infrastructure, which could lead to issues like undelivered emails or even security vulnerabilities like email spoofing. Proper analysis of MX records is critical for maintaining the security and functionality of an organization's email system, making these tools a necessary resource for system administrators and security professionals.

### ****5. Email Lookup****

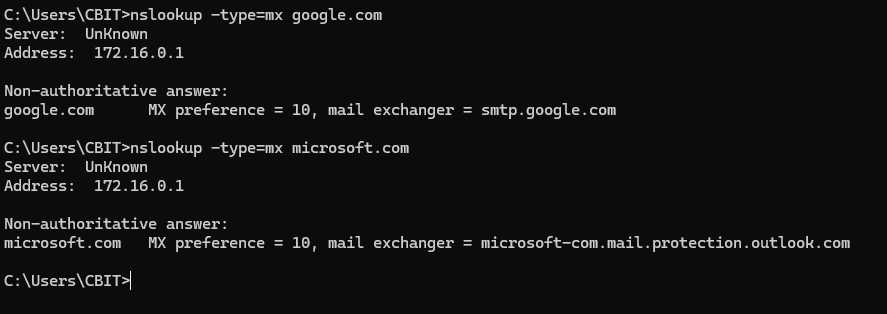
#### ****Purpose:****

Email Lookup tools are used to gather information about an email address, such as the domain, the owner, and sometimes even the social profiles or associated websites.

**Task**: Find the owner and associated domain of an email address.

**Steps**:

* Go to [Hunter.io](https://hunter.io/).
* Enter the email address you want to look up.
* Analyze the results, including information about the email’s associated domain and other public information.
* If available, check for social media or company links associated with the email address.



#### ****Conclusion:****

Email Lookup tools are powerful for gathering information about email addresses, such as domain ownership and social media profiles linked to the email. These tools help in the OSINT (Open Source Intelligence) process by revealing more information about individuals or organizations associated with an email address. They are invaluable for security analysts and investigators who are conducting background checks or identifying potential security risks through email-related data.

**6. The Harvester**

#### ****Purpose:****

The Harvester is a tool used for gathering email addresses, subdomains, and other valuable information about a target through various search engines and online sources. It’s popular in OSINT (Open Source Intelligence) investigations.

#### ****Setup Instructions:****

1. **Installation**: The Harvester is a Python-based tool, so it can be installed using pip.
2. git clone https://github.com/laramies/theHarvester
3. cd theHarvester
4. pip install -r requirements.txt

 **Task**: Gather email addresses and subdomains of a domain.

 **Steps**:

1. Open a terminal and navigate to the theHarvester directory.
2. Run the following command to gather emails from a domain (e.g., example.com):
3. python3 theHarvester.py -d example.com -b google
4. Analyze the output, including email addresses and subdomains discovered.
5. Use additional flags (e.g., -l for limiting results) to refine the search.

#### ****Key Features:****

* **Email Enumeration**: Gathers email addresses associated with a target domain through multiple public sources, such as search engines, social media, and websites.
* **Subdomain Discovery**: Identifies subdomains linked to a domain using search engines, DNS records, and other public sources.
* **Search Engine Integration**: Uses search engines (Google, Bing, etc.) to extract publicly available email addresses and domain-related information.
* **Public Data Sources**: Collects data from a wide range of sources, including PGP key servers, LinkedIn, and other public databases.
* **File Output Options**: The tool can output results in a variety of formats, such as HTML, CSV, or plain text, making it easy to analyze or store the results.
* **Search Customization**: Offers options for customizing the number of results, search engines used, and the types of data harvested.
* **Open Source**: Being an open-source tool, it is free to use and can be modified or extended by users for their needs.

#### ****Conclusion:****

The Harvester is an effective tool for gathering valuable information from public sources about email addresses, subdomains, and other domain-related data. It aids in conducting OSINT investigations by gathering critical data that could be used for further security testing or cyberattacks, such as phishing campaigns. By utilizing The Harvester, security professionals can gain insights into an organization's digital footprint and discover publicly available information that could help identify vulnerabilities or threats. It’s an essential tool for penetration testers and anyone involved in cybersecurity research.