A logo with a person in a hoodie using a computer

AI-generated content may be incorrect.

**MISSION HACKERS**

**BANGLADESH**

**Assignment No-07**

**Assignment Title: Passive Reconnaissance**

**Course Title: Cybersecurity & Ethical Hacking**

**Submitted by:**

**Name: Istiak Alam**

**Phone: 01765376101**

**Submission Date: 08-07-25**

**Tools Task / Topic: Google Dork, DNSInfo, Maltego**

**Submitted to:**

**MD Sha Jalal**

**Founder of Mission Hackers Bangladesh**

**Google Dork :**

**Google Dorking** (also called Google Hacking) is the use of advanced search operators in Google to find **sensitive information** or **vulnerabilities** that are publicly exposed on the internet — often unintentionally.

✅ It's legal only if used for ethical hacking and with proper permission.

❌ It's illegal to exploit systems or data without consent.

## 🔍 Why is it used in Cybersecurity?

Ethical hackers and security researchers use it to:

* Find exposed login pages
* Discover open directories
* Locate vulnerable servers
* Uncover sensitive documents (PDFs, Excel sheets)
* Search camera feeds, passwords, config files, and more

## 🧪 Basic Syntax of Google Dorks

Here's a breakdown of commonly used **Google search operators**:

| Operator | Description | Example |
| --- | --- | --- |
| site: | Search only within a specific website | site:gov.bd |
| intitle: | Search words in the title of a webpage | intitle:"login page" |
| inurl: | Search keywords in the URL | inurl:admin |
| filetype: | Search specific file types (PDF, DOCX, XLSX...) | filetype:pdf "password" |
| ext: | Same as filetype: | ext:xls "confidential" |
| intext: | Finds a keyword in the body text | intext:"username=admin" |
| cache: | Show cached version of a page | cache:example.com |
| link: | Find pages that link to a specific URL | link:example.com |

## 💥 Google Dork Examples

| Goal | Dork |
| --- | --- |
| Find login pages | inurl:login or intitle:"Login Page" |
| Discover exposed admin panels | inurl:admin or intitle:"Admin Panel" |
| Find config files | filetype:env or filetype:xml "config" |
| Search for database dumps | filetype:sql "password" |
| Locate unsecured webcams | inurl:/view.shtml |
| Find Excel files with emails | filetype:xls intext:@gmail.com |
| PDFs containing passwords | filetype:pdf "username password" |
| Open directories | intitle:index.of |

## 🔐 Responsible Usage

✅ We will Use Google Dorking for:

* Cybersecurity research
* Bug bounty (if allowed by target's scope)
* Learning in our **lab environment**
* Penetration testing with permission

❌ Never:

* Exploit vulnerabilities that we discover
* Access unauthorized systems or data
* Share or sell discovered sensitive info

**More Advance Google Dork List :**

➢ Find all indexed pages

site:vulnweb.com

➢ Find login pages

site:vulnweb.com inurl:login

➢ Find admin panels

site:vulnweb.com inurl:admin

➢ Find config files

site:vulnweb.com ext:xml OR ext:conf

➢ Search for password in logs

site:vulnweb.com intext:password filetype:log

➢ Find backup files

site:vulnweb.com ext:bak OR ext:old OR ext:backup

➢ Search for SQL error messages

site:vulnweb.com intext:"You have an error in your SQL syntax"

➢ Find public documents

site:vulnweb.com filetype:pdf OR filetype:docx

➢ Find confidential info

site:vulnweb.com intext:"confidential" OR intext:"private"

➢ Check for SQL injection points

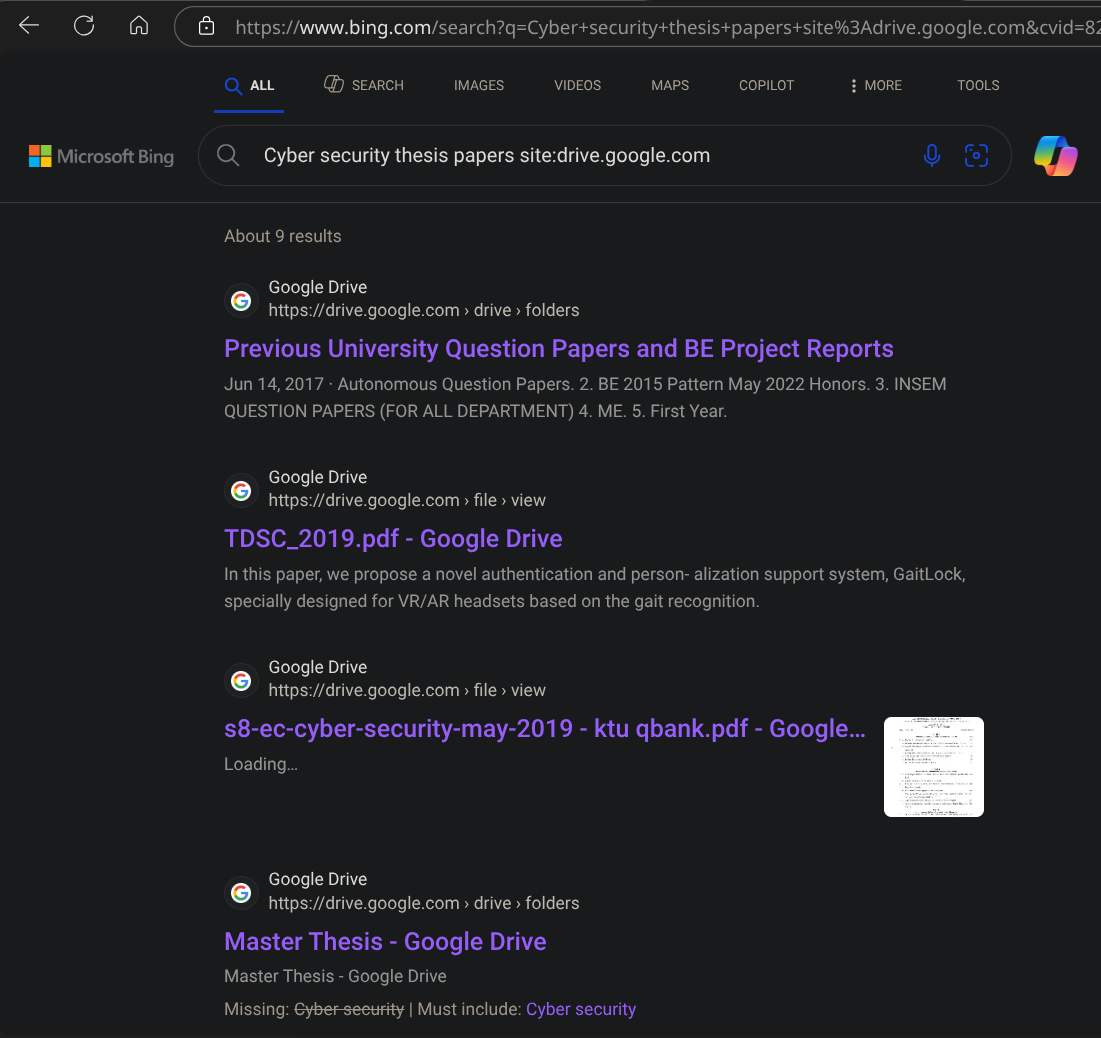
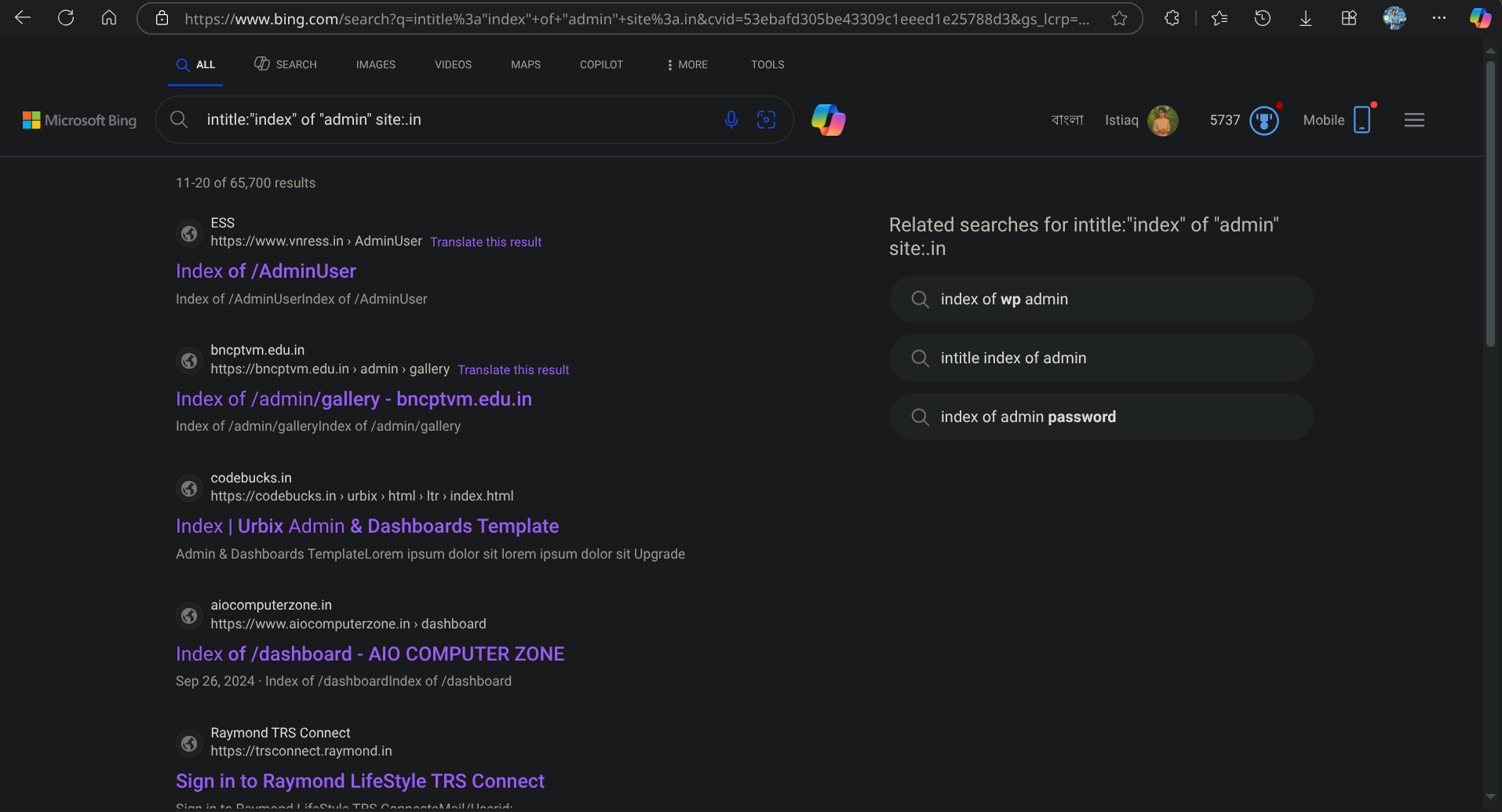
site:vulnweb.com inurl:"id=" intext:"sql"

**SQL Injection →**

**Username : 1’or’1’=’1**

**Password : 1’or’1’=’1**

Examples :

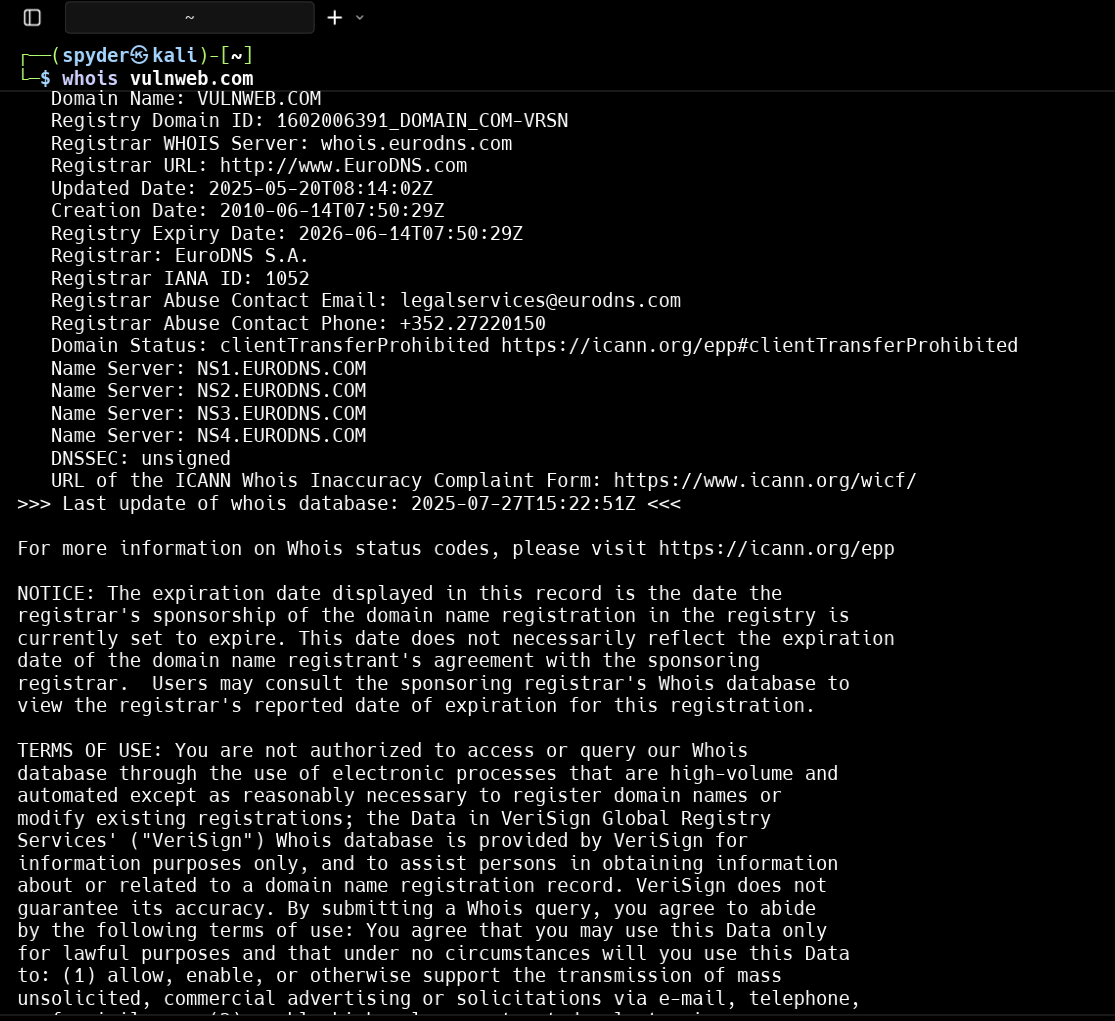


First of all we need to get information of any web server.

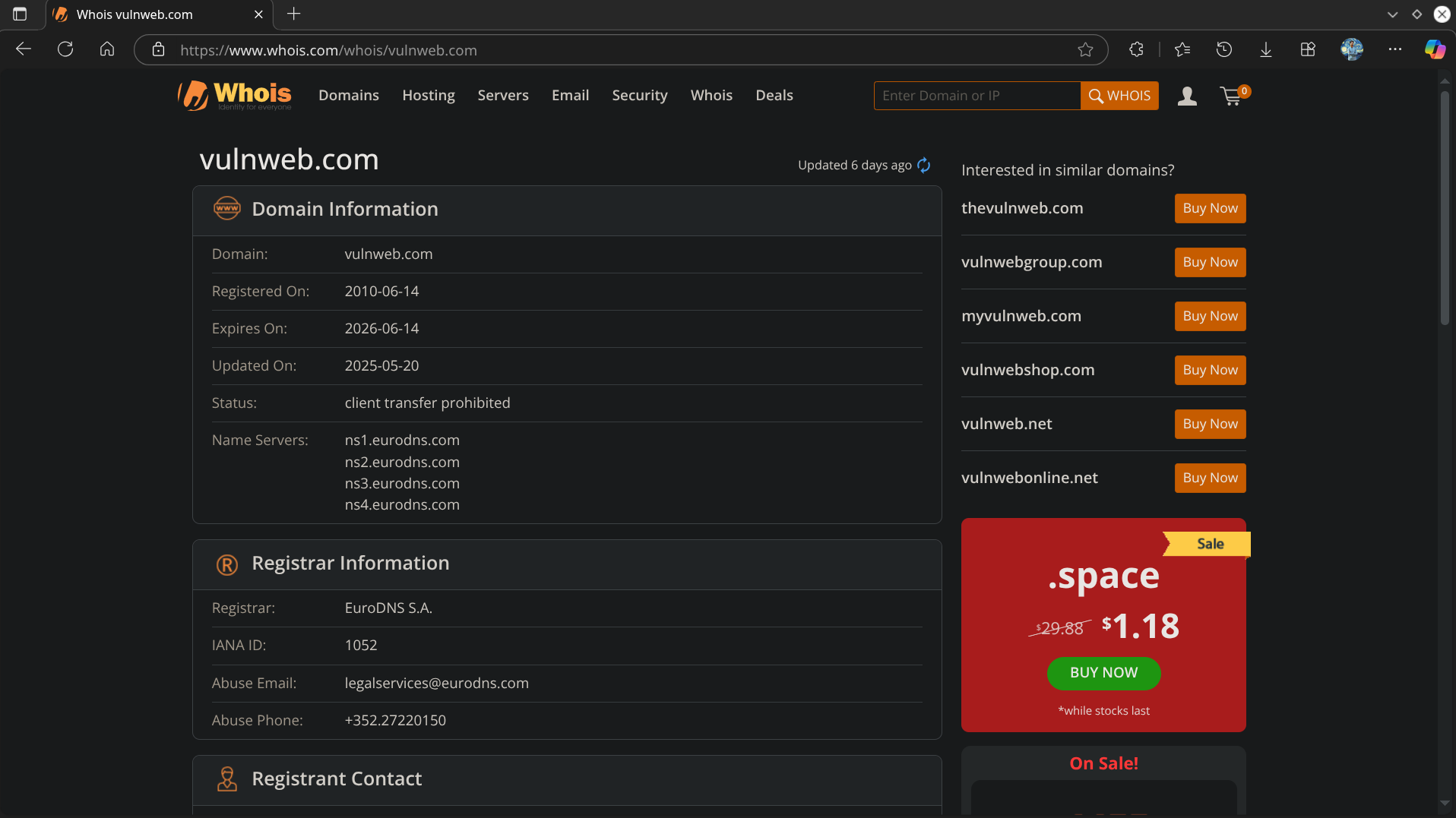
So, we will seek information of any website using **Whois :**

Open Terminal [ctrl+alt+t] and run whois <website>

**whois vulnweb.com**

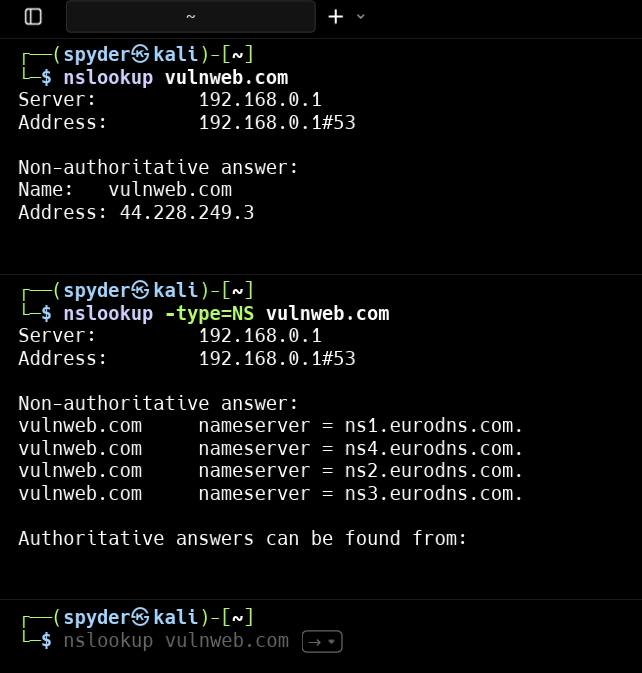


Using GUI website :



Taking Name Server info using nslookup :

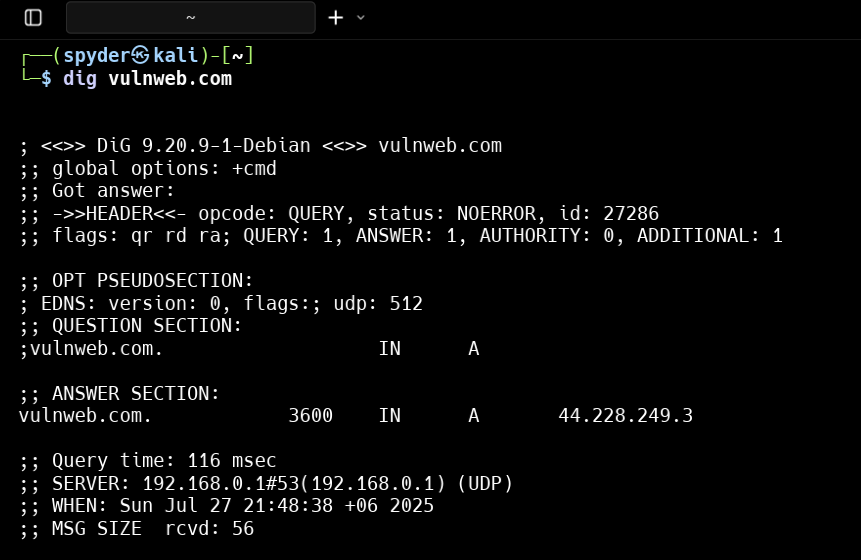
**nslookup vulnweb.com**



**DIG (Domain Information Groper) :**

Open Terminal and run :

**dig vulnweb.com**



**Automatic Scripting Tools [dnsinfo]**

Open terminal and clone <https://github.com/ShajalalCSE/dnsinfo.git>

┌──(kali㉿kali)-[~]

└─$ ./dnsinfo.sh vulnweb.com

[+] Starting advanced DNS recon for: vulnweb.com

--------------------------------------------

[\*] Basic DNS Records:

vulnweb.com. 3600 IN HINFO "RFC8482" ""

ns4.eurodns.com.

ns1.eurodns.com.

ns3.eurodns.com.

ns2.eurodns.com.

"google-site-verification=4LQORV-lTi-d4GPxtBEQWmFnwff7UAazQc9gZvHukbw"

"v=spf1 -all"

[\*] A & AAAA Records:

44.228.249.3

[\*] Zone Transfer Attempt:

[>] Trying AXFR on ns4.eurodns.com.

; <<>> DiG 9.20.9-1-Debian <<>> @ns4.eurodns.com. vulnweb.com AXFR

; (2 servers found)

;; global options: +cmd

; Transfer failed.

[>] Trying AXFR on ns2.eurodns.com.

; <<>> DiG 9.20.9-1-Debian <<>> @ns2.eurodns.com. vulnweb.com AXFR

; (2 servers found)

;; global options: +cmd

; Transfer failed.

[>] Trying AXFR on ns1.eurodns.com.

; <<>> DiG 9.20.9-1-Debian <<>> @ns1.eurodns.com. vulnweb.com AXFR

; (2 servers found)

;; global options: +cmd

; Transfer failed.

[>] Trying AXFR on ns3.eurodns.com.

; <<>> DiG 9.20.9-1-Debian <<>> @ns3.eurodns.com. vulnweb.com AXFR

; (2 servers found)

;; global options: +cmd

; Transfer failed.

[\*] DNSSEC Status:

;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

; EDNS: version: 0, flags: do; udp: 512

[\*] Brute-force Subdomains:

www.vulnweb.com has address 44.228.249.3

mail.vulnweb.com has address 44.228.249.3

ftp.vulnweb.com has address 44.228.249.3

dev.vulnweb.com has address 44.228.249.3

admin.vulnweb.com has address 44.228.249.3

test.vulnweb.com has address 44.228.249.3

staging.vulnweb.com has address 44.228.249.3

beta.vulnweb.com has address 44.228.249.3

blog.vulnweb.com has address 44.228.249.3

api.vulnweb.com has address 44.228.249.3

portal.vulnweb.com has address 44.228.249.3

webmail.vulnweb.com has address 44.228.249.3

cpanel.vulnweb.com has address 44.228.249.3

vpn.vulnweb.com has address 44.228.249.3

[\*] dnsrecon Scan:

[\*] std: Performing General Enumeration against: vulnweb.com...

[!] Wildcard resolution is enabled on this domain

[!] It is resolving to 44.228.249.3

[!] All queries will resolve to this list of addresses!!

[\*] Checking for Zone Transfer for vulnweb.com name servers

[\*] Resolving SOA Record

[+] SOA ns1.eurodns.com 199.167.66.107

[+] SOA ns1.eurodns.com 2610:1c8:b002::107

[\*] Resolving NS Records

[\*] NS Servers found:

[+] NS ns2.eurodns.com 104.37.178.107

[+] NS ns2.eurodns.com 2610:1c8:b001::107

[+] NS ns4.eurodns.com 104.37.178.108

[+] NS ns4.eurodns.com 2610:1c8:b001::108

[+] NS ns3.eurodns.com 199.167.66.108

[+] NS ns3.eurodns.com 2610:1c8:b002::108

[+] NS ns1.eurodns.com 199.167.66.107

[+] NS ns1.eurodns.com 2610:1c8:b002::107

[\*] Removing any duplicate NS server IP Addresses...

[\*]

[\*] Trying NS server 2610:1c8:b001::108

[-] Zone Transfer Failed for 2610:1c8:b001::108!

[-] Port 53 TCP is being filtered

[\*]

[\*] Trying NS server 199.167.66.108

[+] 199.167.66.108 Has port 53 TCP Open

[-] Zone Transfer Failed (Zone transfer error: REFUSED)

[\*]

[\*] Trying NS server 2610:1c8:b002::107

[-] Zone Transfer Failed for 2610:1c8:b002::107!

[-] Port 53 TCP is being filtered

[\*]

[\*] Trying NS server 104.37.178.107

[+] 104.37.178.107 Has port 53 TCP Open

[-] Zone Transfer Failed (Zone transfer error: REFUSED)

[\*]

[\*] Trying NS server 199.167.66.107

[+] 199.167.66.107 Has port 53 TCP Open

[-] Zone Transfer Failed (Zone transfer error: REFUSED)

[\*]

[\*] Trying NS server 2610:1c8:b002::108

[-] Zone Transfer Failed for 2610:1c8:b002::108!

[-] Port 53 TCP is being filtered

[\*]

[\*] Trying NS server 2610:1c8:b001::107

[-] Zone Transfer Failed for 2610:1c8:b001::107!

[-] Port 53 TCP is being filtered

[\*]

[\*] Trying NS server 104.37.178.108

[+] 104.37.178.108 Has port 53 TCP Open

[-] Zone Transfer Failed (Zone transfer error: REFUSED)

[\*] Checking for Zone Transfer for vulnweb.com name servers

[\*] Resolving SOA Record

[+] SOA ns1.eurodns.com 199.167.66.107

[+] SOA ns1.eurodns.com 2610:1c8:b002::107

[\*] Resolving NS Records

[\*] NS Servers found:

[+] NS ns2.eurodns.com 104.37.178.107

[+] NS ns2.eurodns.com 2610:1c8:b001::107

[+] NS ns3.eurodns.com 199.167.66.108

[+] NS ns3.eurodns.com 2610:1c8:b002::108

[+] NS ns1.eurodns.com 199.167.66.107

[+] NS ns1.eurodns.com 2610:1c8:b002::107

[+] NS ns4.eurodns.com 104.37.178.108

[+] NS ns4.eurodns.com 2610:1c8:b001::108

[\*] Removing any duplicate NS server IP Addresses...

[\*]

[\*] Trying NS server 2610:1c8:b001::108

[-] Zone Transfer Failed for 2610:1c8:b001::108!

[-] Port 53 TCP is being filtered

[\*]

[\*] Trying NS server 199.167.66.108

[+] 199.167.66.108 Has port 53 TCP Open

[-] Zone Transfer Failed (Zone transfer error: REFUSED)

[\*]

[\*] Trying NS server 2610:1c8:b002::107

[-] Zone Transfer Failed for 2610:1c8:b002::107!

[-] Port 53 TCP is being filtered

[\*]

[\*] Trying NS server 104.37.178.107

[+] 104.37.178.107 Has port 53 TCP Open

[-] Zone Transfer Failed (Zone transfer error: REFUSED)

[\*]

[\*] Trying NS server 199.167.66.107

[+] 199.167.66.107 Has port 53 TCP Open

[-] Zone Transfer Failed (Zone transfer error: REFUSED)

[\*]

[\*] Trying NS server 2610:1c8:b002::108

[-] Zone Transfer Failed for 2610:1c8:b002::108!

[-] Port 53 TCP is being filtered

[\*]

[\*] Trying NS server 2610:1c8:b001::107

[-] Zone Transfer Failed for 2610:1c8:b001::107!

[-] Port 53 TCP is being filtered

[\*]

[\*] Trying NS server 104.37.178.108

[+] 104.37.178.108 Has port 53 TCP Open

[-] Zone Transfer Failed (Zone transfer error: REFUSED)

[-] DNSSEC is not configured for vulnweb.com

[\*] SOA ns1.eurodns.com 199.167.66.107

[\*] SOA ns1.eurodns.com 2610:1c8:b002::107

[\*] NS ns2.eurodns.com 104.37.178.107

[\*] NS ns2.eurodns.com 2610:1c8:b001::107

[\*] NS ns3.eurodns.com 199.167.66.108

[\*] NS ns3.eurodns.com 2610:1c8:b002::108

[\*] NS ns4.eurodns.com 104.37.178.108

[\*] NS ns4.eurodns.com 2610:1c8:b001::108

[\*] NS ns1.eurodns.com 199.167.66.107

[\*] NS ns1.eurodns.com 2610:1c8:b002::107

[\*] A vulnweb.com 44.228.249.3

[\*] TXT vulnweb.com v=spf1 -all

[\*] TXT vulnweb.com google-site-verification=4LQORV-lTi-d4GPxtBEQWmFnwff7UAazQc9gZvHukbw

[\*] TXT \_dmarc.vulnweb.com v=spf1 -all

[\*] TXT \_domainkey.vulnweb.com v=spf1 -all

[\*] TXT \_dmarc.\_domainkey.vulnweb.com v=spf1 -all

[\*] Enumerating SRV Records

[-] No SRV Records Found for vulnweb.com

[\*] Amass Passive Subdomain Enum:

testaspnet.vulnweb.com (FQDN) --> a\_record --> 44.238.29.244 (IPAddress)

testasp.vulnweb.com (FQDN) --> a\_record --> 44.238.29.244 (IPAddress)

rest.vulnweb.com (FQDN) --> a\_record --> 18.215.71.186 (IPAddress)

localhost.vulnweb.com (FQDN) --> a\_record --> 127.0.0.1 (IPAddress)

44.224.0.0/11 (Netblock) --> contains --> 44.238.29.244 (IPAddress)

16509 (ASN) --> managed\_by --> AMAZON-02 - Amazon.com, Inc. (RIROrganization)

16509 (ASN) --> announces --> 44.224.0.0/11 (Netblock)

18.208.0.0/13 (Netblock) --> contains --> 18.215.71.186 (IPAddress)

127.0.0.0/8 (Netblock) --> contains --> 127.0.0.1 (IPAddress)

14618 (ASN) --> managed\_by --> AMAZON-AES - Amazon.com, Inc. (RIROrganization)

14618 (ASN) --> announces --> 18.208.0.0/13 (Netblock)

0 (ASN) --> managed\_by --> Reserved Network Address Blocks (RIROrganization)

0 (ASN) --> announces --> 127.0.0.0/8 (Netblock)

The enumeration has finished

[\*] CNAME Records:

[\*] Email Security Records:

- SPF:

"v=spf1 -all"

- DKIM (default selector):

"v=spf1 -all"

- DMARC:

"v=spf1 -all"

[\*] Reverse DNS Check:

1.249.228.44.in-addr.arpa domain name pointer ec2-44-228-249-1.us-west-2.compute.amazonaws.com.

2.249.228.44.in-addr.arpa domain name pointer ec2-44-228-249-2.us-west-2.compute.amazonaws.com.

3.249.228.44.in-addr.arpa domain name pointer ec2-44-228-249-3.us-west-2.compute.amazonaws.com.

4.249.228.44.in-addr.arpa domain name pointer ec2-44-228-249-4.us-west-2.compute.amazonaws.com.

5.249.228.44.in-addr.arpa domain name pointer ec2-44-228-249-5.us-west-2.compute.amazonaws.com.

[\*] Checking Wildcard DNS:

[\*] DNS Cache Snooping Test (on 8.8.8.8):

vulnweb.com. 3600 IN A 44.228.249.3

[+] Recon Complete!

## ✅ **Summary of DNS Reconnaissance on vulnweb.com**

### 🔍 **1. Zone Transfer Vulnerability**

* Zone Transfer (AXFR) was **attempted on all listed nameservers**:
  + ns1.eurodns.com
  + ns2.eurodns.com
  + ns3.eurodns.com
  + ns4.eurodns.com
* **Result**: All attempts were **refused or failed**. This means:
  + 🔒 **GOOD**: Zone transfer is **not allowed**, which is secure.
  + ❗ **BUT**: Some NS servers showed **open TCP port 53**, which is worth monitoring (but not a direct vulnerability on its own).

✅ No Zone Transfer vulnerability found – this is a **positive** result from a security standpoint.

### 🌐 **2. Wildcard DNS Configuration**

* The domain uses **Wildcard DNS**, meaning:
  + All subdomain queries resolve to the **same IP address**: 44.228.249.3
* This often hides **real subdomains**, and might be used:
  + By devs for convenience
  + To confuse attackers or tools
* ❗ **Risk**: Can **interfere with subdomain enumeration**, and may hide unused or legacy subdomains still pointing to sensitive services.

### 📛 **3. Subdomain Enumeration**

Brute-force and passive methods revealed multiple valid subdomains:

| Example Subdomains | Observed Behavior |
| --- | --- |
| admin.vulnweb.com | Exists → Possible Admin Panel |
| test.vulnweb.com / staging.vulnweb.com | Used for testing → Often misconfigured |
| localhost.vulnweb.com | Points to 127.0.0.1 → **Critical Misconfiguration** |

⚠️ **Misconfigured DNS (localhost.vulnweb.com)**  
This entry **resolves to the loopback address** 127.0.0.1, which is dangerous because:

* It can cause **denial-of-service** on internal services
* Can be abused in **SSRF (Server-Side Request Forgery)** attacks
* It exposes the internal logic or test entries in public DNS

### 🔒 **4. DNSSEC Not Configured**

* The domain does **not use DNSSEC** (Domain Name System Security Extensions).
* ❗ **Risk**: DNS records can be spoofed or manipulated in MITM attacks.

🔐 Recommendation: Enable DNSSEC for tamper-proof DNS queries.

### ✉️ **5. Email Security Misconfigurations**

* SPF, DKIM, and DMARC records all show:

**v=spf1 -all**

* Meaning:
  + No authorized mail servers exist for sending email
  + Could prevent **spoofing**, but also means:
    - **Email services may be misconfigured** or **non-existent**
    - Email delivery from domain might fail entirely

⚠️ Indicates **incomplete or defensive-only email config**, often a placeholder.

### 🧠 **6. Reverse DNS Findings**

* Shows reverse lookup records for IPs under:
  + ec2-44-228-249-x.us-west-2.compute.amazonaws.com
* Hints that the server is hosted on **Amazon AWS**
* Not a vulnerability, but useful **infrastructure info**

## 🛡️ **Conclusion:**

| Area | Status | Summary |
| --- | --- | --- |
| **Zone Transfer** | ✅ Secure | No AXFR allowed (good) |
| **Wildcard DNS** | ⚠️ Risky | Can confuse tools, hide misconfigurations |
| **Subdomains** | ⚠️ Risky | Many sensitive entries found (admin, localhost) |
| **DNSSEC** | ❌ Missing | DNS not cryptographically validated |
| **Email Records** | ⚠️ Defensive / Incomplete | SPF/DKIM present but misused |
| **Localhost Record** | ❌ Critical Misconfig | Maps public domain to 127.0.0.1 (bad) |

## 🔧 Recommendations:

1. ✅ No urgent DNS server vulnerability — but still:
2. 🔒 **Enable DNSSEC**
3. 🧹 **Remove or fix** localhost.vulnweb.com
4. 📧 **Review Email TXT records** for SPF/DKIM/DMARC
5. 🔍 **Monitor wildcard DNS behavior** (or remove it if not needed)
6. 👀 Check subdomains like admin, test, staging for exposed panels

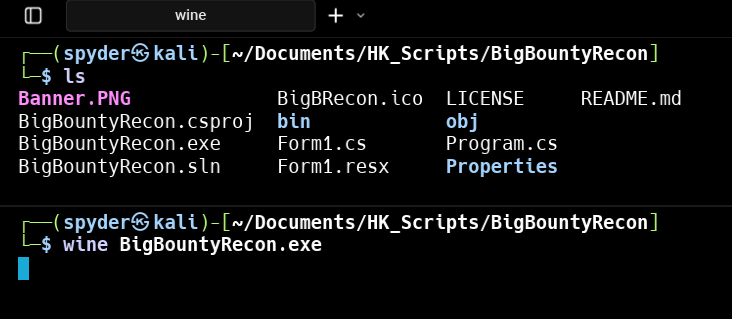
**Reconnaissance Using Automation Tool :**

[BigBountyRecon](https://github.com/Viralmaniar/BigBountyRecon.git) Recon Setup :

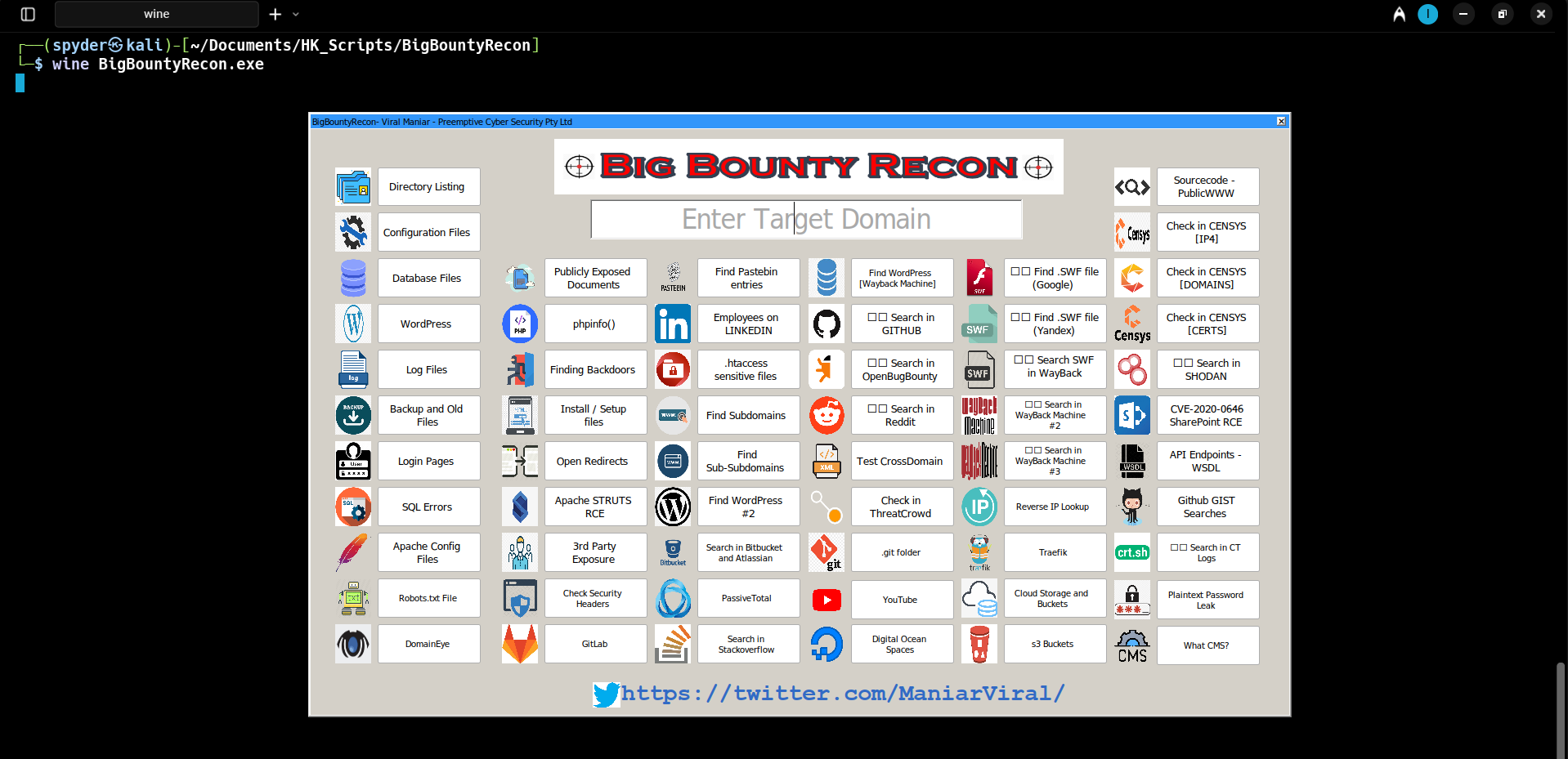
Step 1 : Open the Url [BigBountyRecon](https://github.com/Viralmaniar/BigBountyRecon.git) and download the latest binary

Step 2 : Open Terminal in the BigBountyRecon folder and run

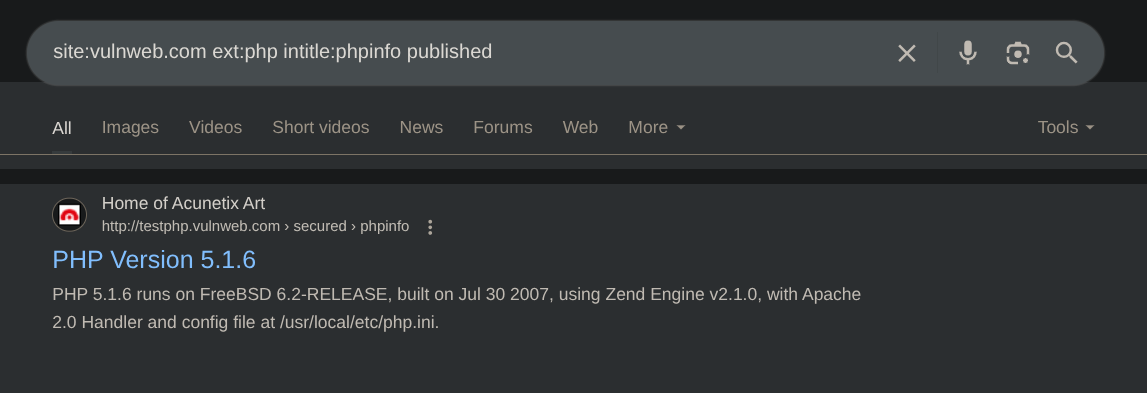
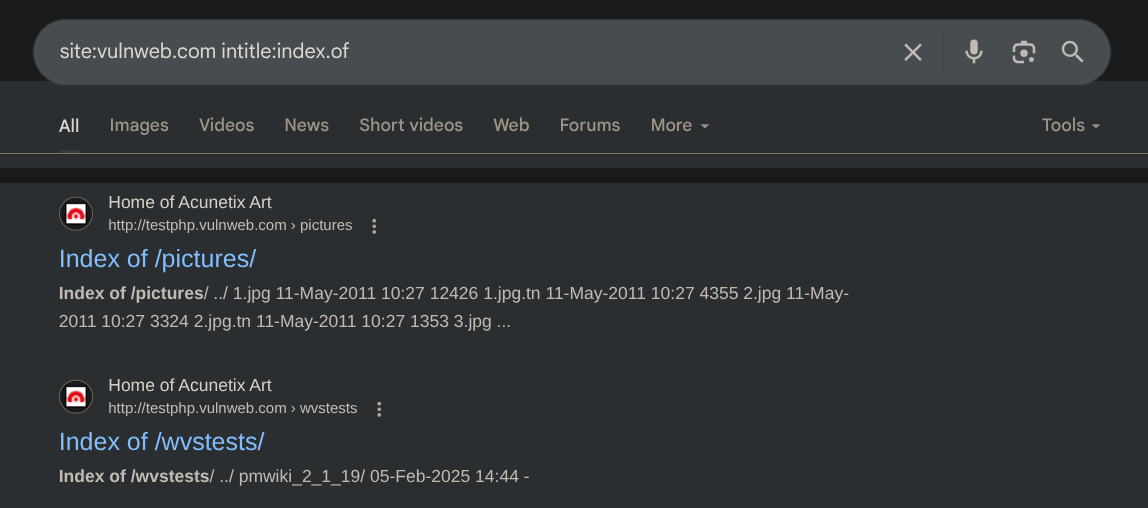
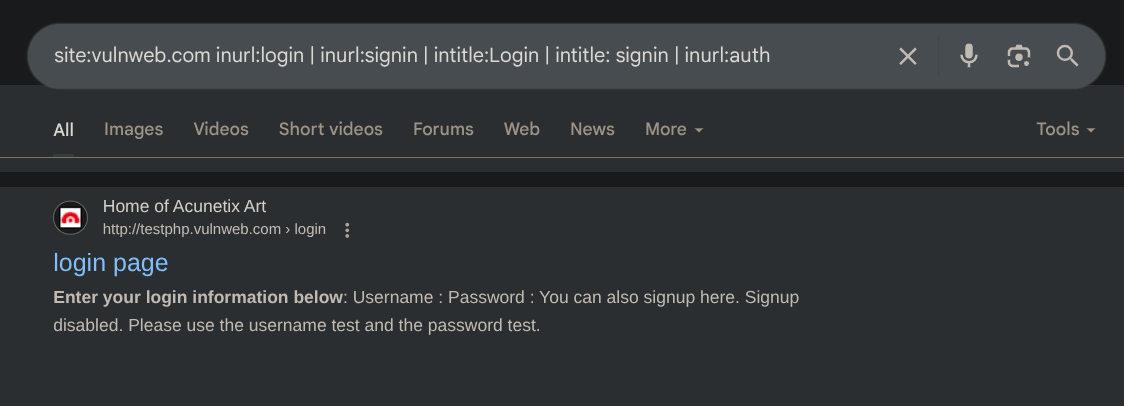
wine BigBountyRecon.exe



Then the BigBountyRecon will open :



After that We can select option for Google dork and it will redirect it to the Browser. Just we need to enter the website / Domain. Such as, “vulnweb.com”



This is how we can automation the Google Dork for a particular website…

**Maltego Tool**

Open-source intelligence (OSINT) tool for graphical link analysis. ✓ Features:

❖ Visual map of relationships

❖ Entities: Domains, IPs, People, Emails, etc.

❖ Transform-based querying

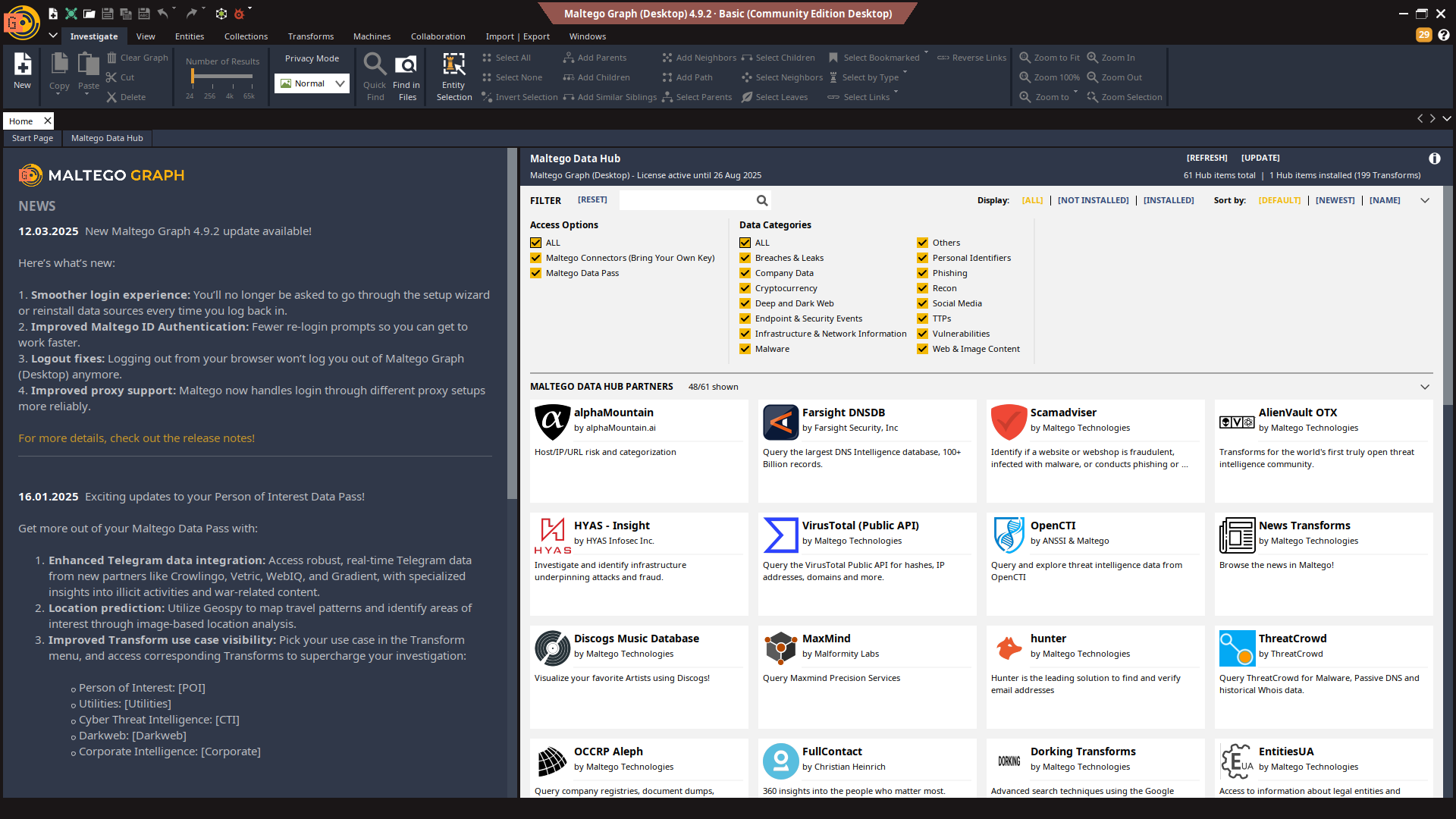
✓ Use: Analyze social networks, domains, organizations

1. Create Maltego-ID from [Maltego](https://app.maltego.com/) Website

2. Login into website

3. Open Maltego App and login using browser

4. After setup everything it should be like this



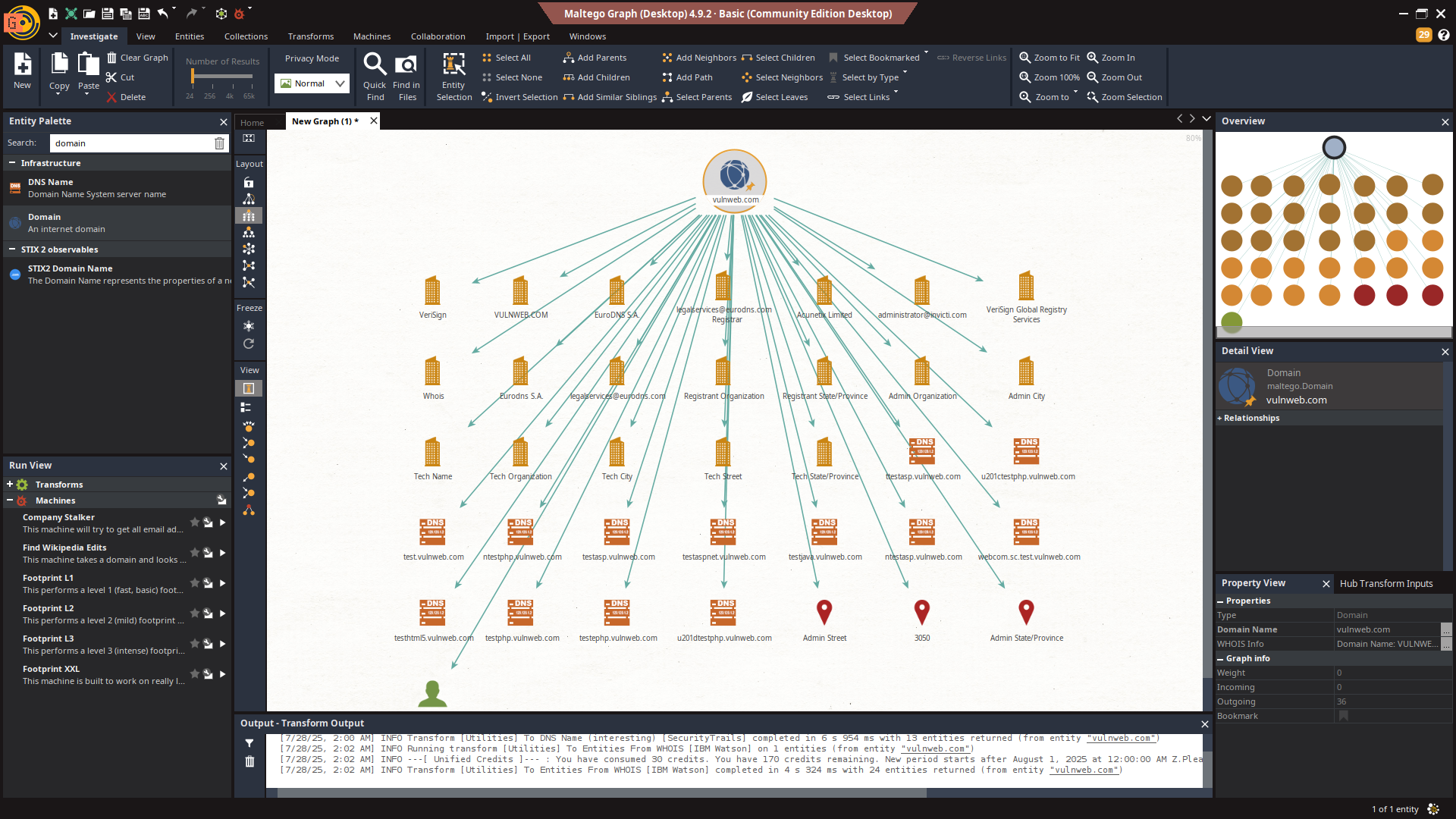
5. Open a New File it will show an empty New Graph

6. In the search for **Domain** and Drag drop it into Graph

7. Right Click on the Domain and edit the Domain name [vulnweb]

8. Then Right Click on the Domain graph and select here multiple options, for get info..

such as, we Click on Domain Owner Details and we get :



9. If I want to get information about more.. then we can Select one of those options



This is how we get information about any kind of website or domain…