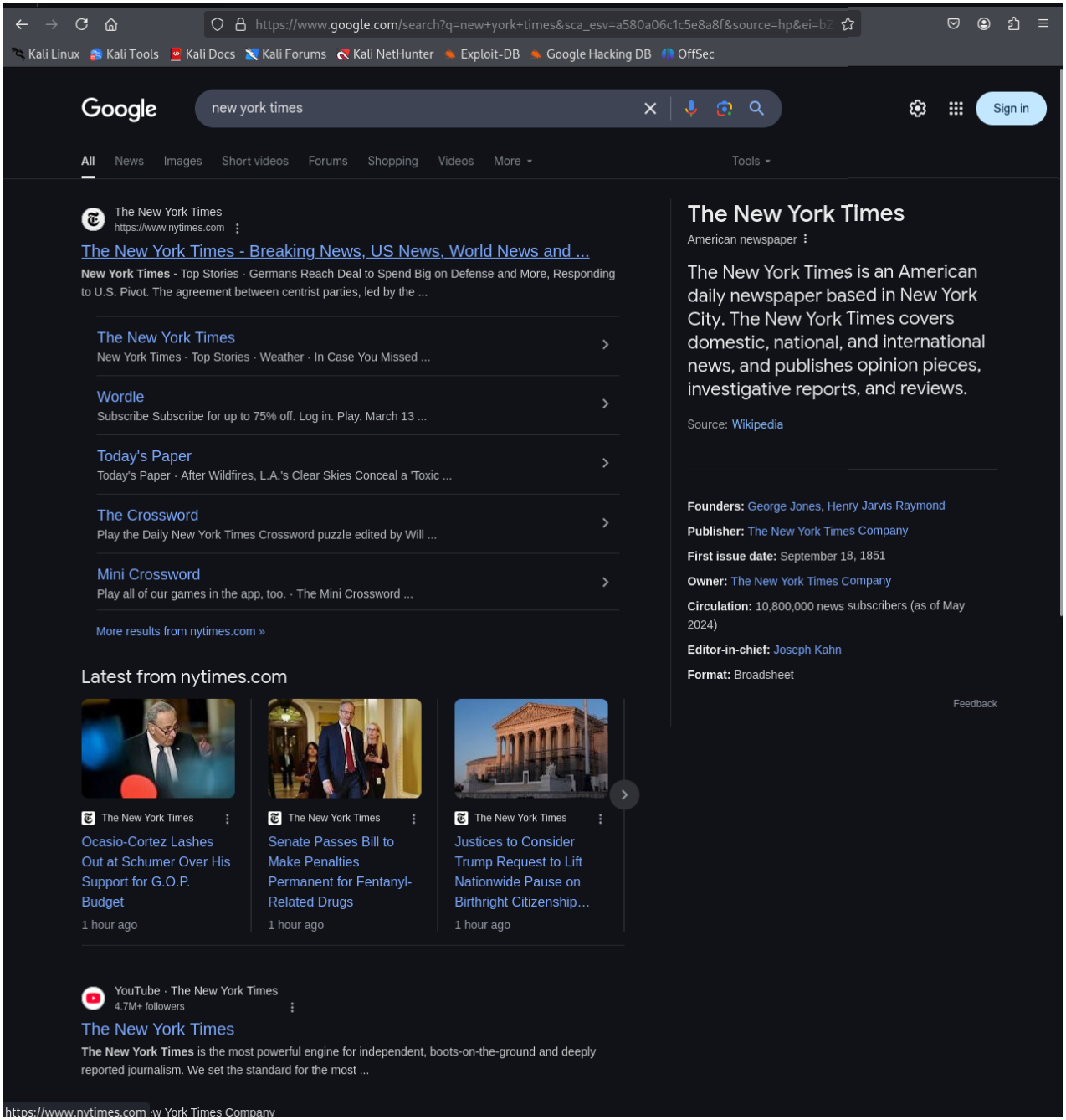
ETHICAL HACKING LAB 3

APARNAA MAHALAXMI ARULLJOTHI (A20560995)

Part 1: Explore Google Hacking Techniques

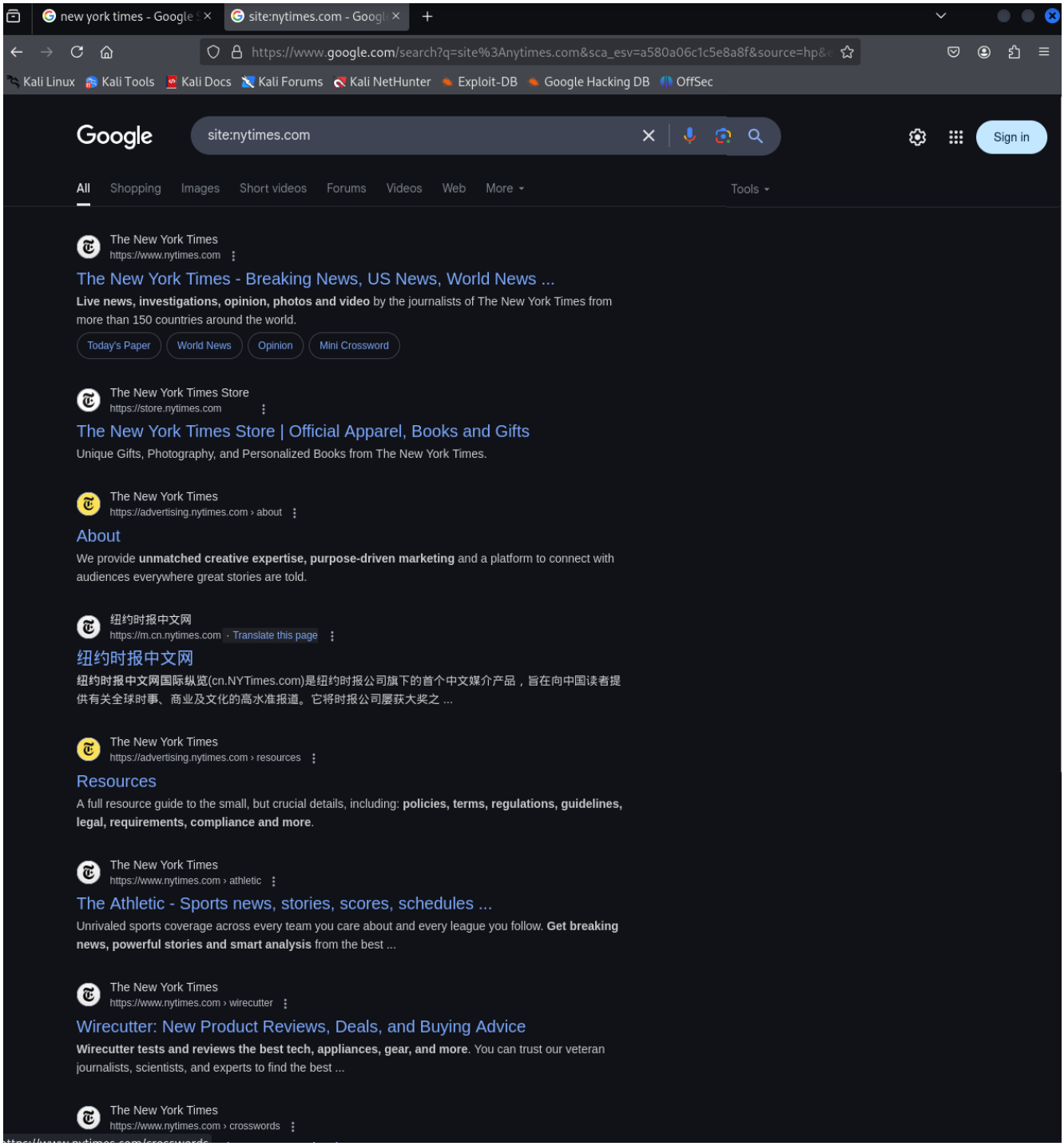
STEP 1,2,3-

In this task, I used the Firefox browser on my Kali Linux virtual machine to perform a basic Google search. I typed "**New York Times"** into the search bar to observe how search results are displayed. The top result was the official New York Times website, followed by related links and articles.



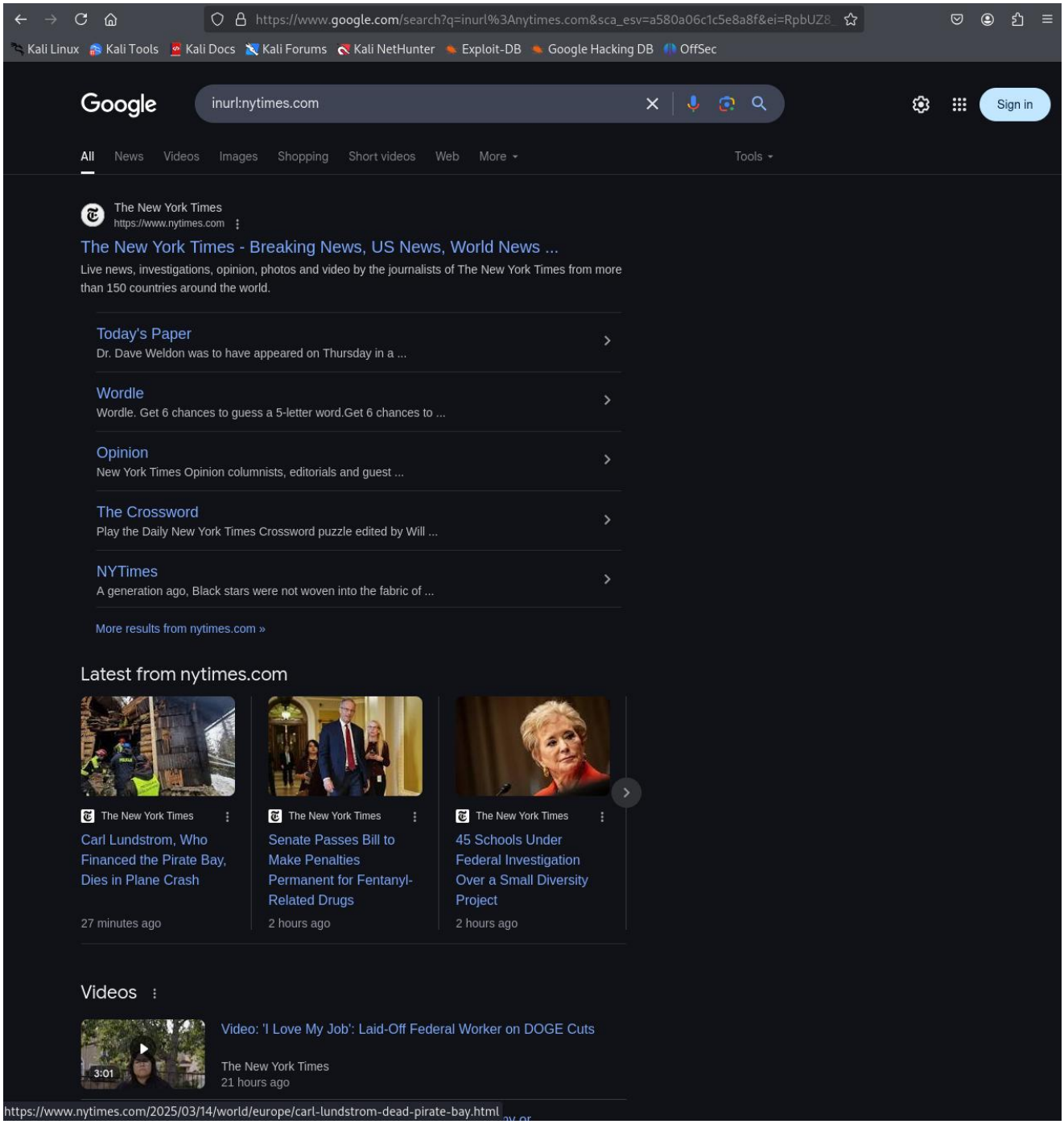
STEP 4,5-

I used the Google search operator **site:nytimes.com** to narrow down the search results strictly to pages within the official New York Times domain. By doing this, all the links shown were only from nytimes.com or its subdomains like cooking.nytimes.com or app.nytimes.com. This filters out unrelated content and focus only on the newspaper's own web pages.



STEP 6,7-

On using the **inurl:nytimes.com** search operator on Google to filter results that contain "nytimes.com" anywhere in their URL. Unlike the site: operator, inurl: also brings in pages from subdirectories, not just subdomains. This helps to explore more specific sections within the New York Times website



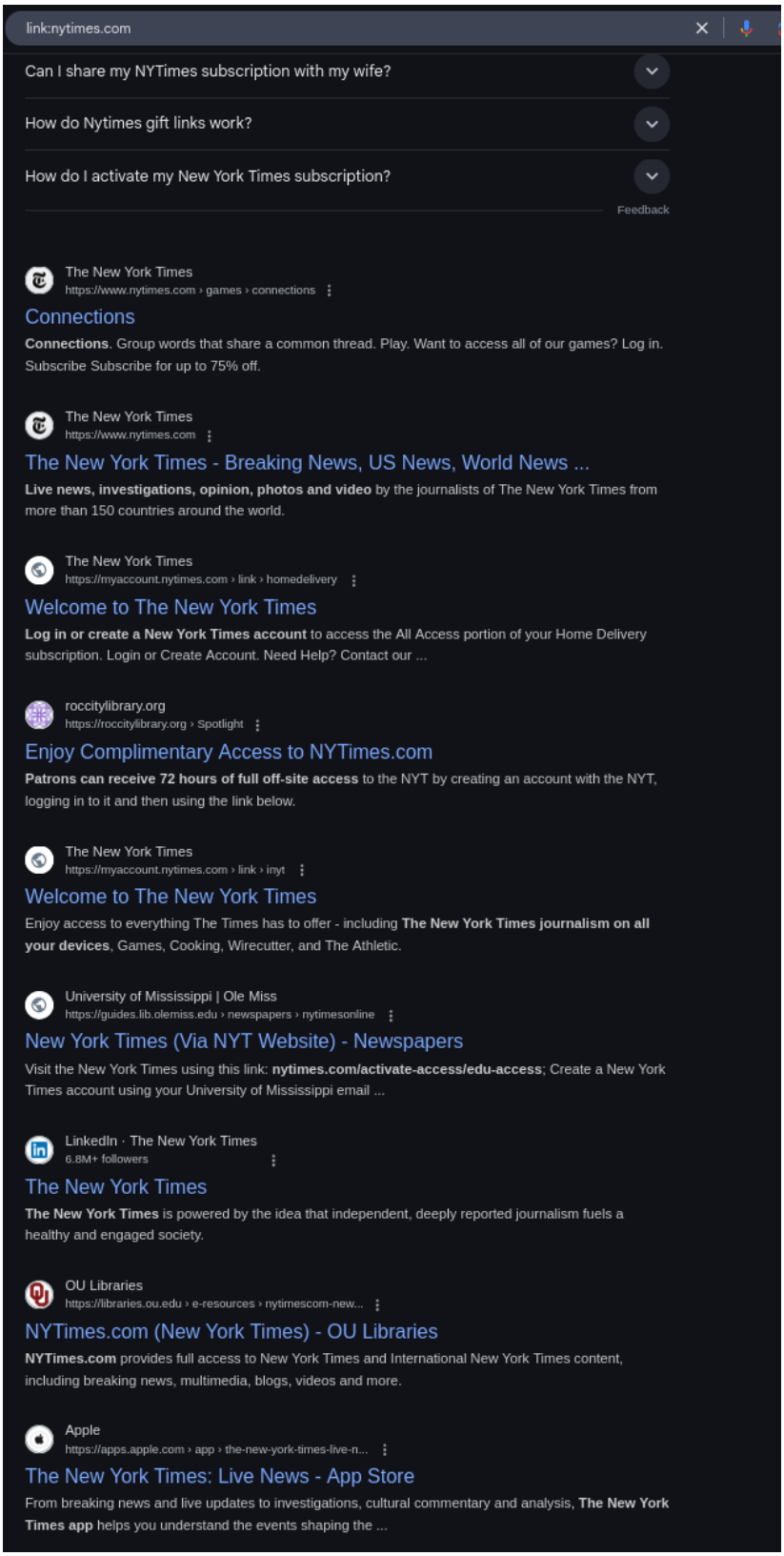
STEP 8,9-

The link: operator showed pages that link to the New York Times site, which is useful for identifying backlinks or references from other websites.

The related: operator displayed websites similar in content or structure to the New York Times, helping discover alternatives or competitors.

The info: operator provided a summary and quick links like cache, similar pages, and links to the site.

Link:nytimes.com



Related:nytimes.com

related:nytimes.com

All | News | Images | Videos | Short videos | Shopping | Forums | More | Tools

The New York Times
https://www.nytimes.com › spotlight › race

Race/Related

Welcome to **Race/Related**, a weekly newsletter focused on race, identity and culture.

Page 7 | Page 4 | Page 9 | 10

The New York Times
https://www.nytimes.com › games › connections

Connections

Connections. Group words that share a common thread. Play. Want to access all of our games? Log in. Subscribe Subscribe for up to 75% off.

Strands | Connections Bot | Connections Archive | Games Tips

People also ask

How do I access my Nytimes subscription?

How do I renew my nyt subscription?

How do I share my NYT subscription with family?

How do I cancel my New York Times subscription?

Feedback

The New York Times
https://www.nytimes.com › newsletters › race-related

Race/Related Newsletter

Race/Related. **Explore the countless ways race affects our lives**, with provocative reporting and discussion. Sent to Your Inbox Weekly; Read the Latest.

The New York Times
https://www.nytimes.com

The New York Times - Breaking News, US News, World News ...

Live news, investigations, opinion, photos and video by the journalists of The New York Times from more than 150 countries around the world.

Today's Paper | World News | Opinion | Mini Crossword

Wikipedia
https://en.wikipedia.org › wiki › The_New_York_Times

The New York Times

The New York Times (NYT) is an American daily newspaper based in New York City. The New York Times covers domestic, national, and international news, ...

Company | Times Building | Times Magazine | A. G. Sulzberger

The New York Times
https://www.nytimes.com › spotlight › race-racism-and-...

Race, Racism and Racial Justice Resources

Race, Racism and Racial Justice Resources: **Writing prompts, lesson plans and activities** to teach and learn about race-related issues.

Instagram · nytimes
18.8M+ followers

The New York Times (@nytimes)

19M Followers, 626 Following, 20K Posts - **The New York Times** (@nytimes) on Instagram: "We seek the truth and help people understand the world."

Info:nytimes.com

info:nytimes.com

All News Images Short videos Videos Shopping Forums More

The New York Times
https://help.nytimes.com › en-us › articles › 115015385...

Contact The New York Times - Help

Contact The New York Times Customer Care. For help with your subscription or account, get started through our Help Center.

Report a Newspaper Delivery... | Reader Submissions | The corrections process

The New York Times
https://help.nytimes.com › en-us

Help - The New York Times

Change Your Delivery Address · Reset Your Password · Report a Delivery Issue · Update Your Payment Information · Log in to Your Account · Cancel Your Subscription ...

People also ask

How do I email New York Times?

How do I cancel my subscription to The New York Times?

How do I contact the NYT billing?

How do I change my NYT subscription?

Feedback

The New York Times Company
https://www.nytco.com › contact

Contact

Contact ; **Business bizday@nytimes.com** ; Editorial editorial@nytimes.com ; Foreign foreign@nytimes.com ; Letter to the Editor letters@nytimes.com ; Metro metro@ ...

The New York Times
https://help.nytimes.com › en-us › categories › 115002...

Contact The New York Times - Help

Contact The New York Times · International Subscriber Contact Information · The New York Times Mailing Address · Contact The New York Times · Report a Security ...

The New York Times
https://www.nytimes.com

The New York Times - Breaking News, US News, World News ...

Live news, investigations, opinion, photos and video by the journalists of The New York Times from more than 150 countries around the world.

The New York Times
https://help.nytimes.com › en-us › requests › new

Contact Customer Care - Help - The New York Times

You can cancel your subscription to The New York Times any time. Visit our cancel your subscription page to select the best cancellation option.

Wikipedia
https://en.wikipedia.org › wiki › The_New_York_Times

The New York Times

The New York Times (NYT) is **an American** daily newspaper based in New York City. The New York Times covers domestic, national, and international news, ...

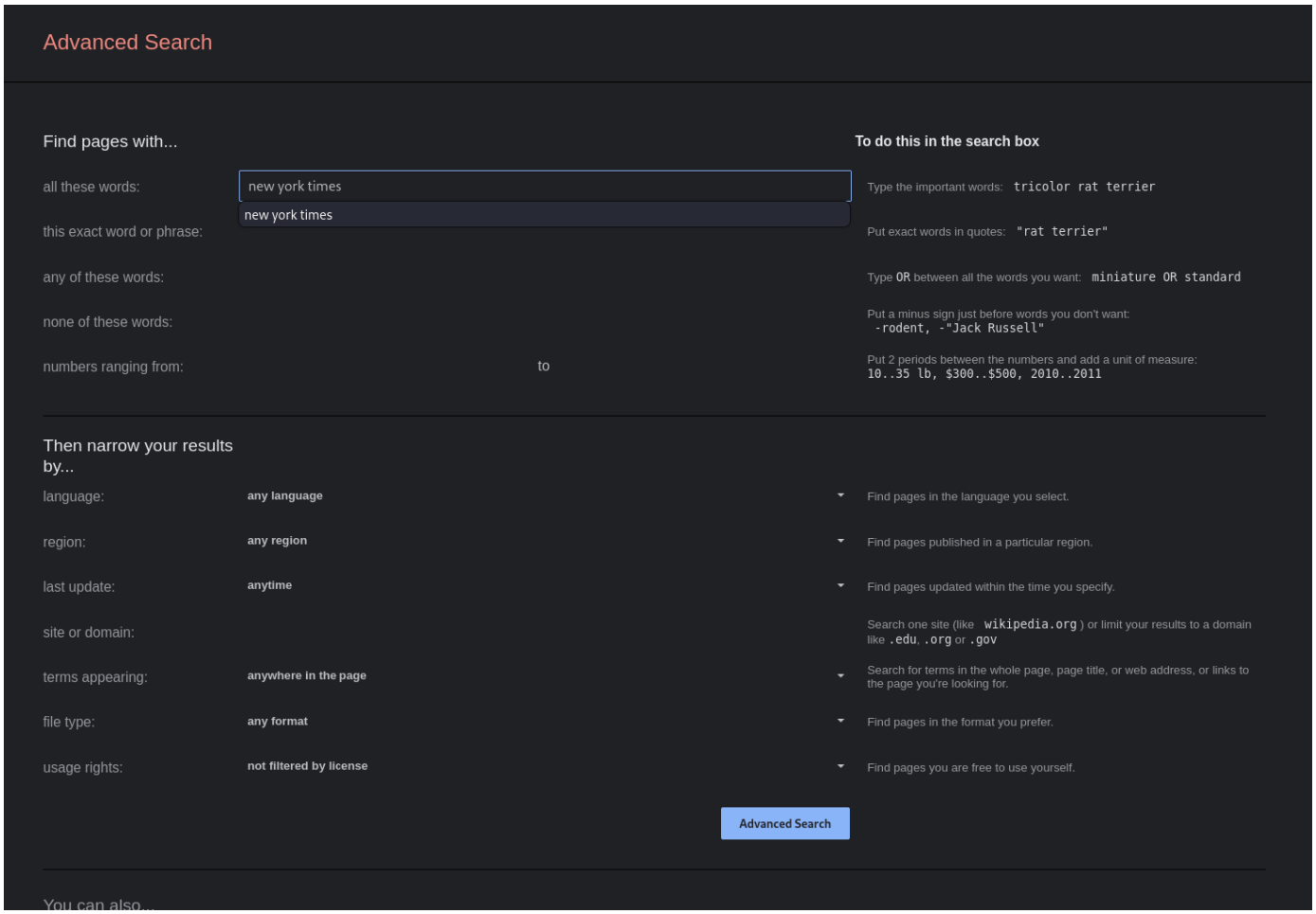
Facebook · The New York Times
20.4M+ followers

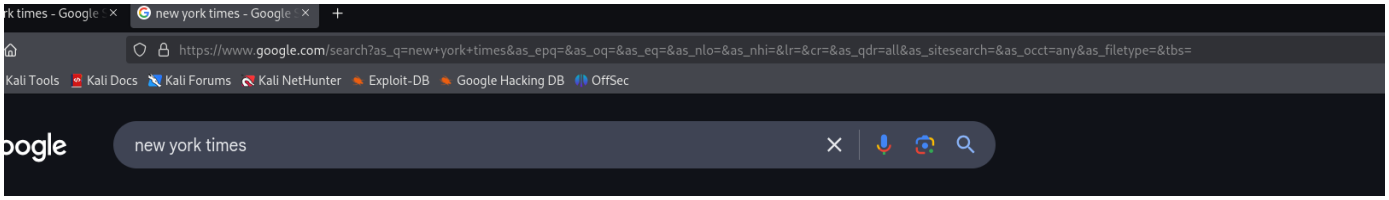
Profile for The New York Times

Part 2: Experiment with Google's Advanced Search Operators

STEP 1,2,3-

Here I used Google's Advanced Search feature by opening the advanced search page through Firefox on my VM. I typed "new york times" in the "all these words" box and observed how the search results were affected. This tool made it easy to search criteria without any operators. Here, Google encodes each field from the search form using variables like as_q, as_epq, as_eq, as_sitesearch, and others. Understanding this URL structure helps in crafting advanced search queries directly from the browser's address bar for quicker and more precise searches.



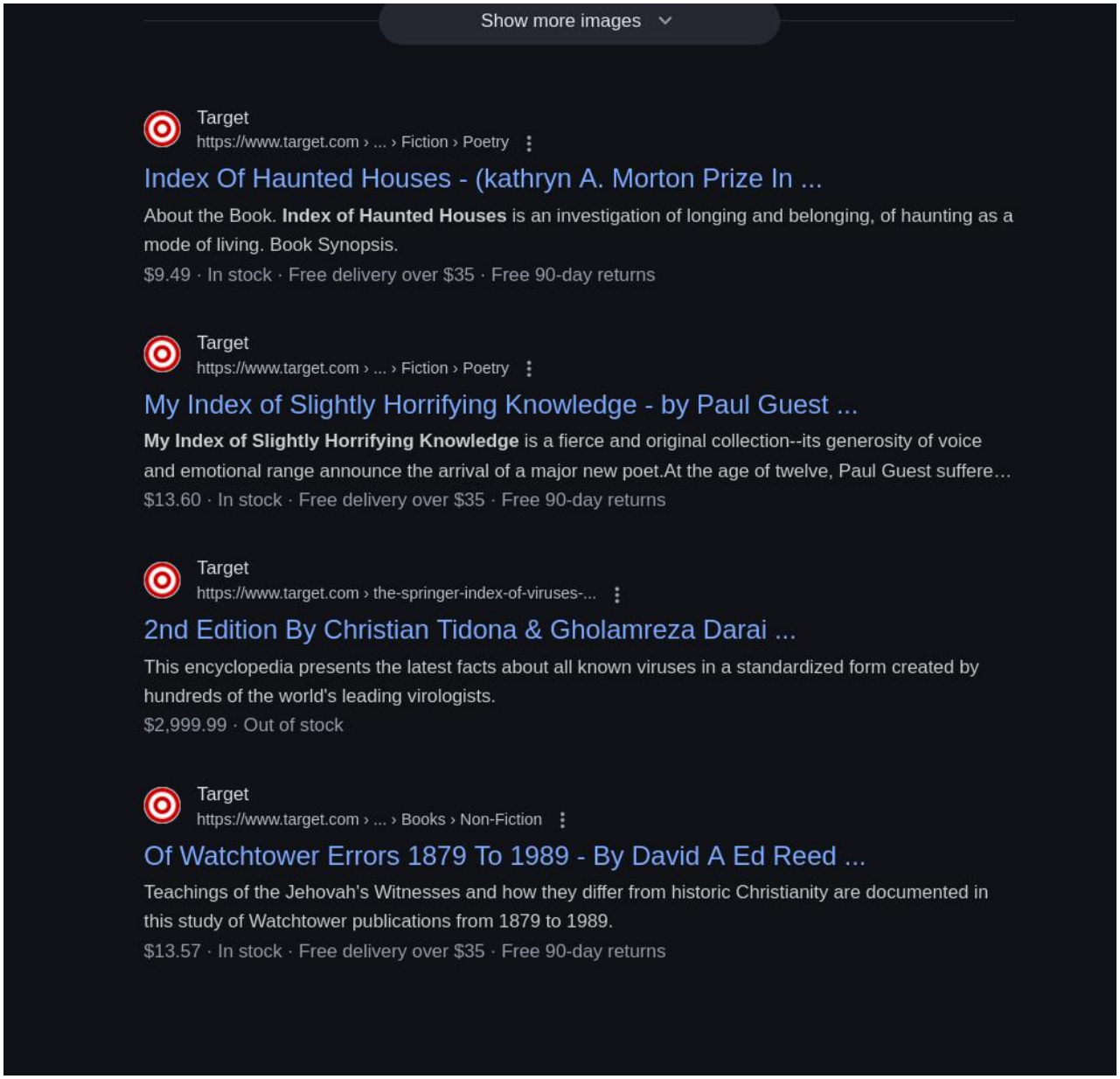


STEP 4,5,6,7-

FOR THESE TASKS I CHOOSE target.com as my Domain.

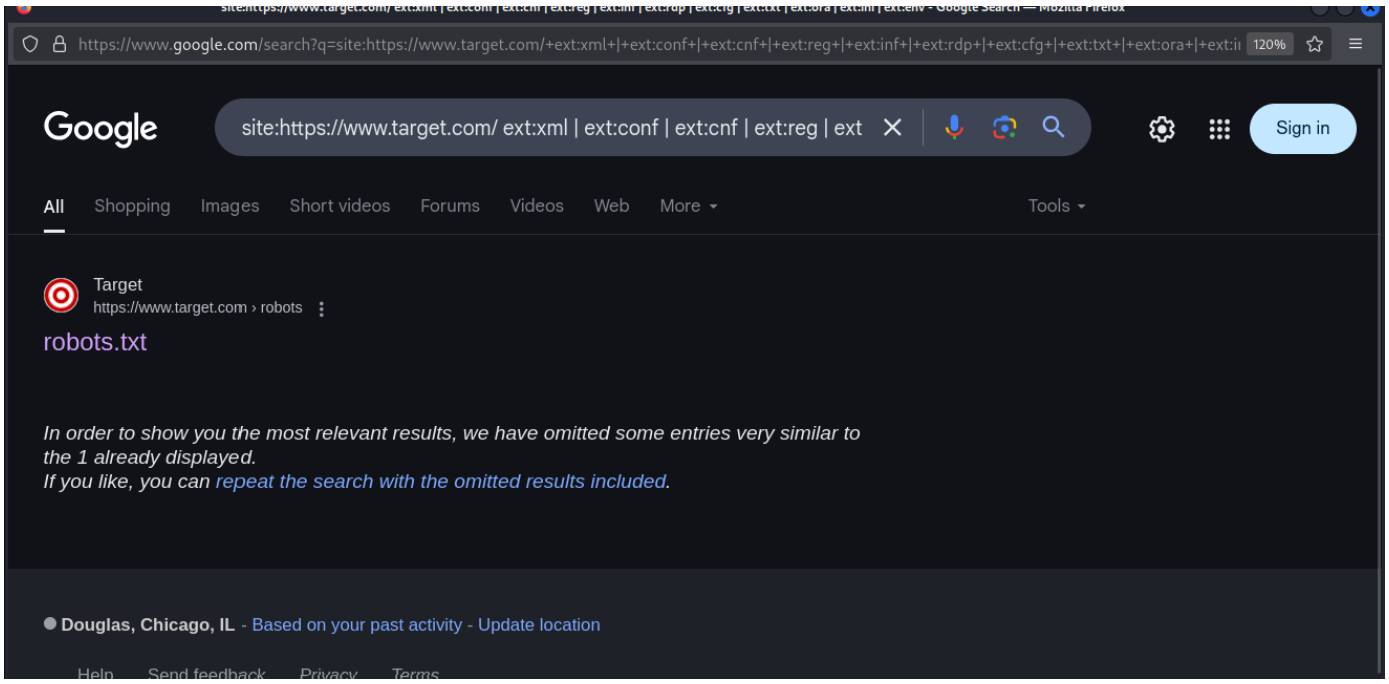
Option: Directory listing vulnerabilities

It contains just Normal product pages not the actual server directory listings, and contains no sensitive or exploitable information that could help a malicious hacker.



Option: configuration files exposed

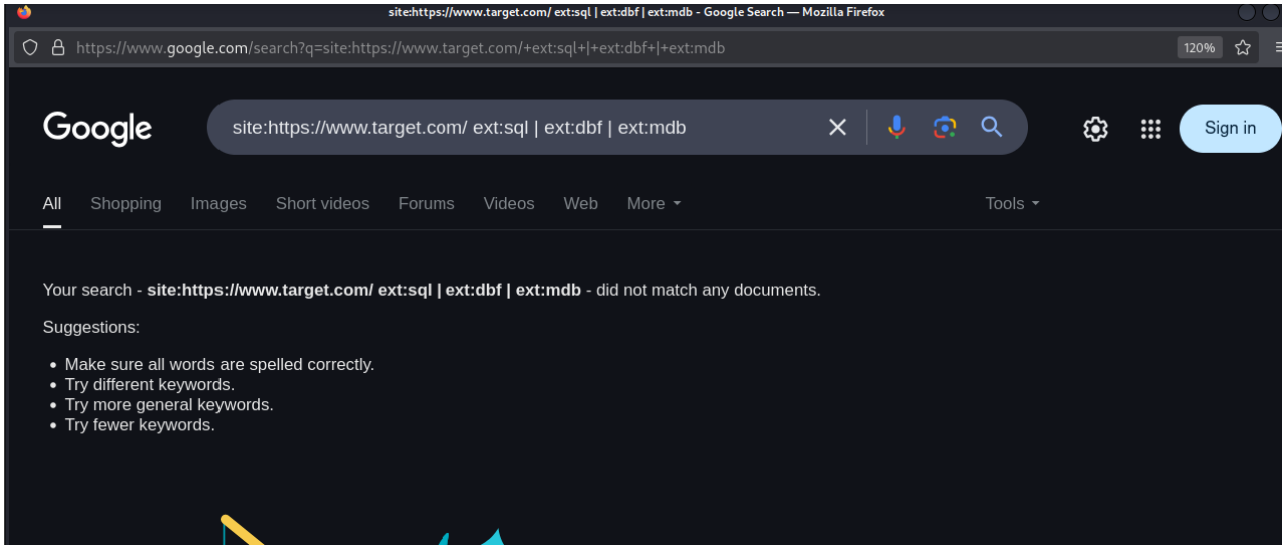
the robots.txt file in this case reveals several internal paths (like /admin, /config, /database/philboard.mdb) that can guide attackers in performing targeted enumeration or testing for misconfigurations. Even though these are not active vulnerabilities, the information disclosed here can help a hacker during the reconnaissance.




```
User-agent: *
Disallow: /*/Ntk
Disallow: /*/Ntt
Disallow: /*/Ntx
Disallow: /*%7Cd_
Disallow: /*/schoollist/
Disallow: /*BTWN
Disallow: /[path]/
Disallow: /7078046/
Disallow: /7079046/
Disallow: /AddToList
Disallow: /AddToRegistry
Disallow: /admin
Disallow: /advancedGiftRegistrySearchView
Disallow: /AjaxSearchNavigationView
Disallow: /Allons_voter
Disallow: /bp/c/
Disallow: /bp/guest_mfg_brand
Disallow: /bp/p/
Disallow: /CallToActionModalView
Disallow: /cgi-bin
Disallow: /cgi-local
Disallow: /Checkout
Disallow: /CheckoutEditItemsDisplayView
Disallow: /CheckoutOrderBillingView
Disallow: /CheckoutOrderShippingView
Disallow: /CheckoutSignInView
Disallow: /co-
Disallow: /common
Disallow: /coupons.
Disallow: /custom-reviews/
Disallow: /data
Disallow: /database/philboard.mdb
Disallow: /deals/
Disallow: /dir_on_server/
Disallow: /EmailCartView
Disallow: /EnlargedImageView
Disallow: /ESPDisplayOptionsViewCmd
Disallow: /ESPModal
Disallow: /ExitCheckoutCmd
Disallow: /FeaturedShowMoreOverlay
Disallow: /FetchProdRefreshContent
Disallow: /fiats
Disallow: /FiatsCmd
Disallow: /file
Disallow: /FreeGiftDisplayView
Disallow: /gam-
Disallow: /GenericRegistryPortalView
Disallow: /gc?k
Disallow: /GiftRegistrySearchViewCmd
Disallow: /gp/
Disallow: /GuestAsAnonymous
Disallow: /guestEmailNotificationView
Disallow: /HelpContent
Disallow: /icons/
Disallow: /igp
Disallow: /index.jhtml
Disallow: /keyword=
```

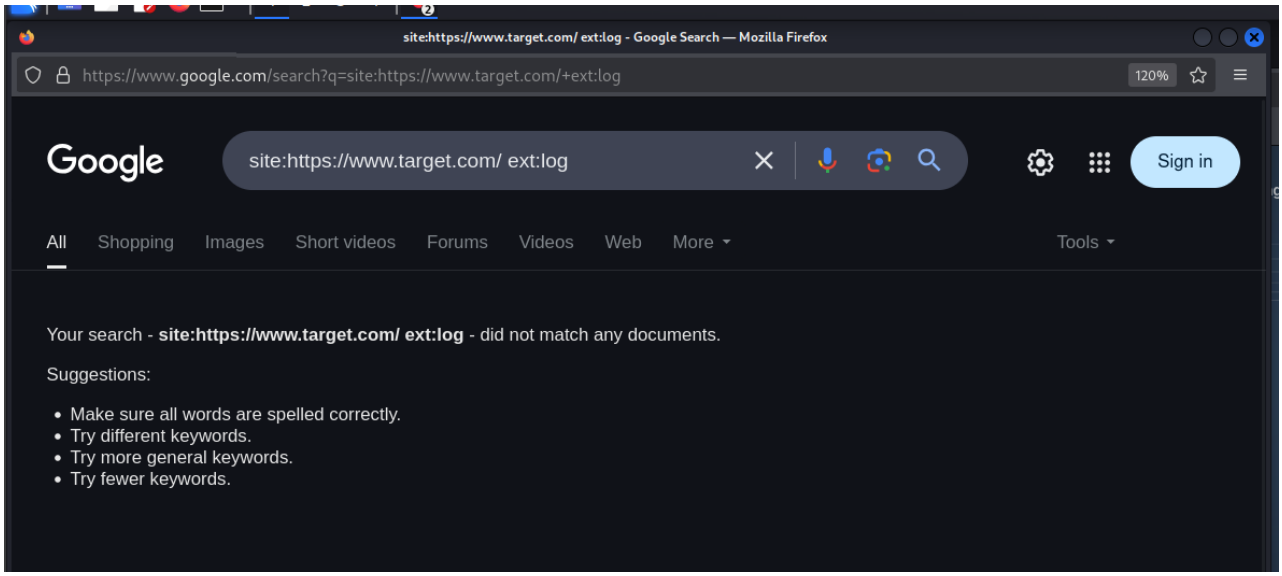
Option : database files exposed

No database files are exposed. Databases store important stuff like customer information, orders, or internal records. If exposed, this data can be stolen or misused.



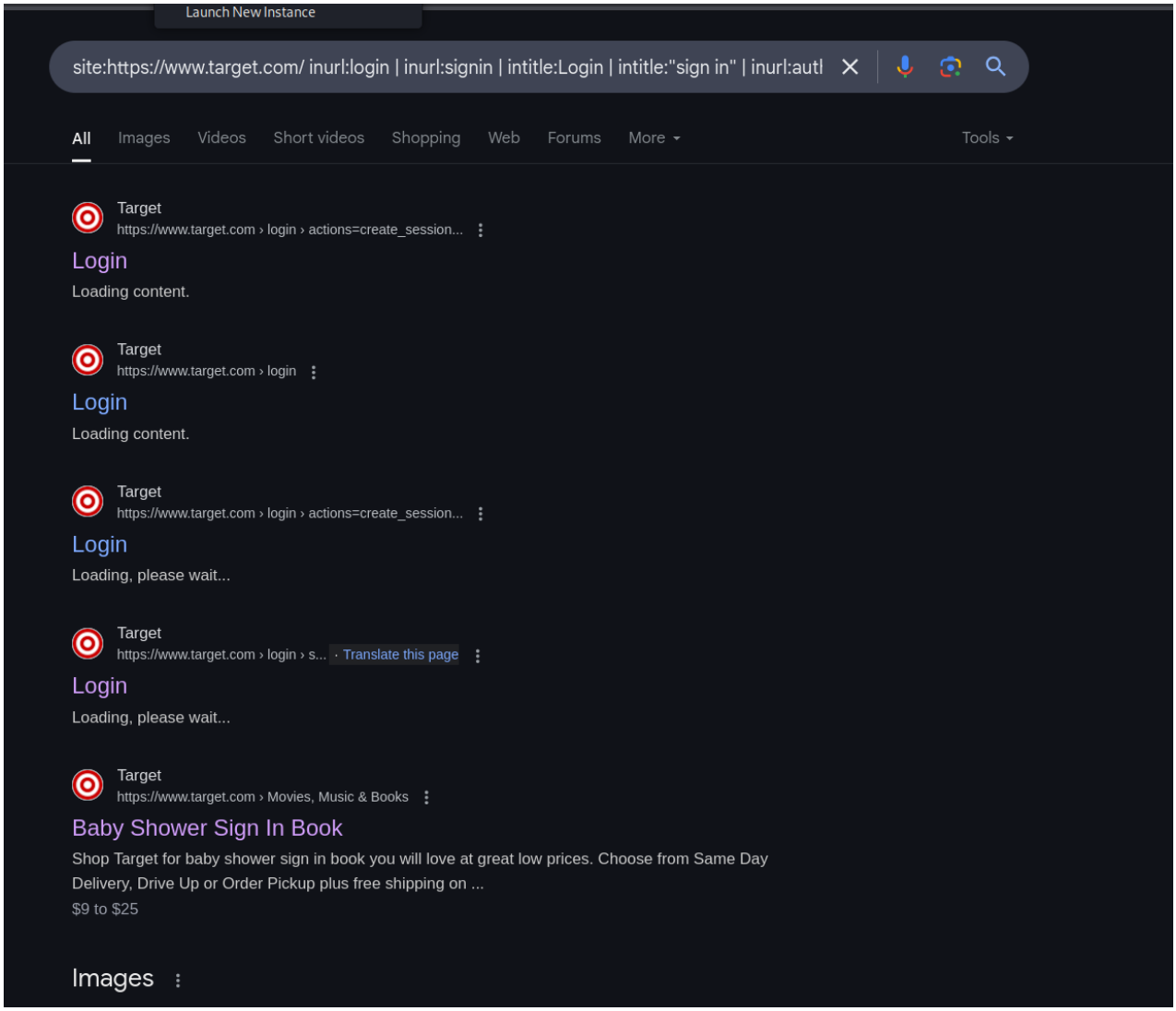
OPTION: Log files exposed

No log files exposed. Logs show what's happening behind the scenes—errors, user actions, system behavior. Hackers can use this to understand how your system works and where it might be weak.



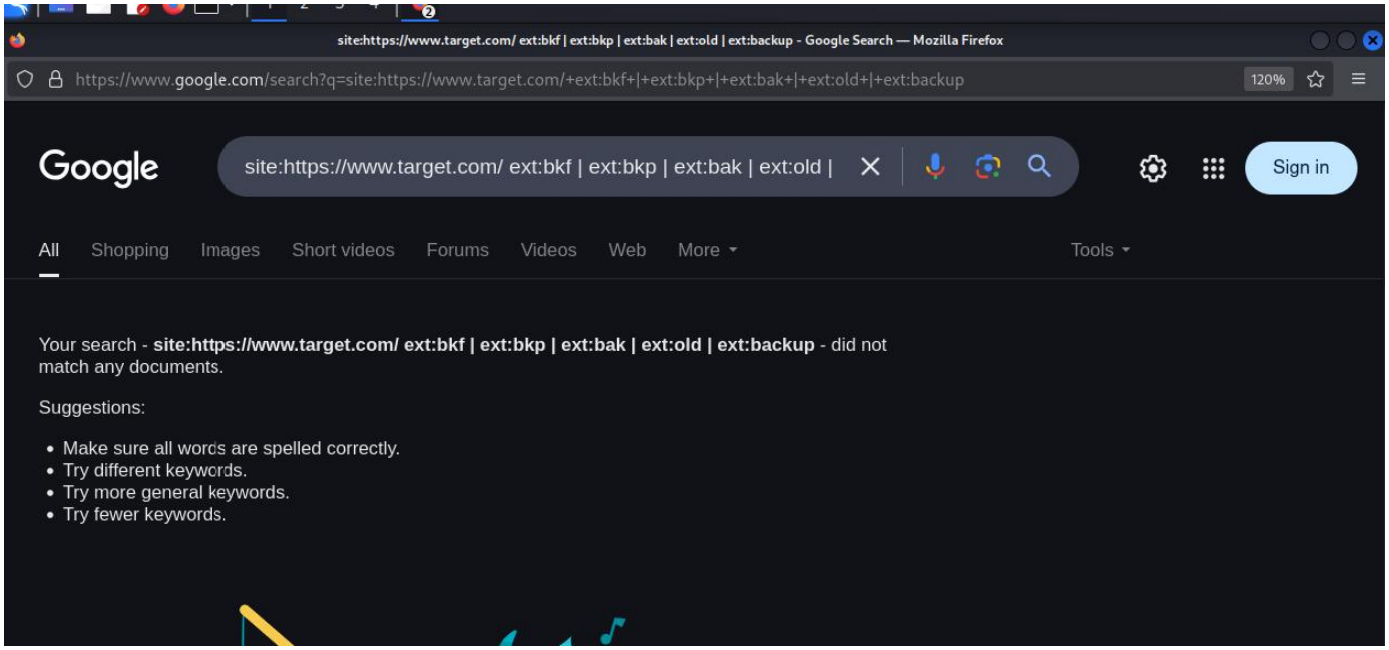
OPTION: Login pages

Login pages knows the location of the login endpoints. Also the attacker can automate login attempts multiple times. They may also manipulate URL parameters. From this search I was able to see critical entry points to the site's authentication system. Although no passwords or user credentials were exposed, the visibility of such URLs can help an attacker identify login flows, attempt brute-force or credential-stuffing attacks. The presence of query parameters like action=create_session can also indicate backend logic that may be further probed for session fixation or injection vulnerabilities.



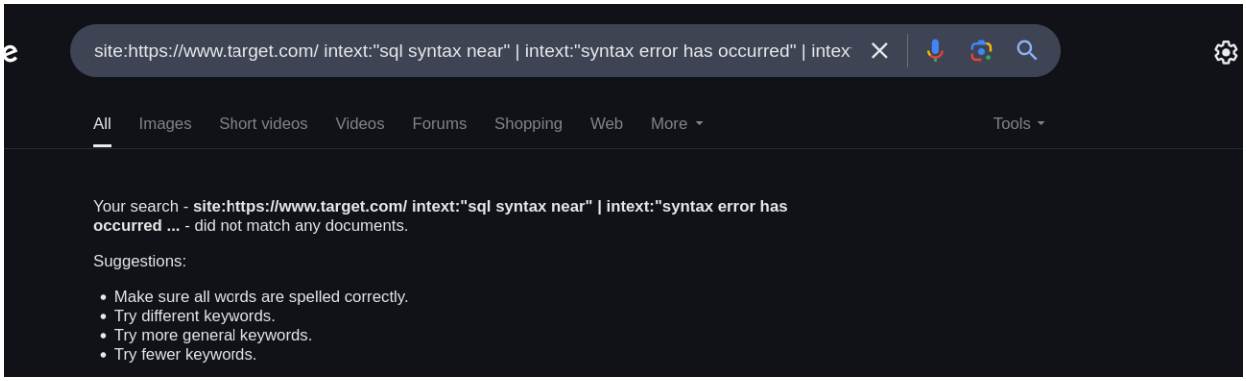
Option: Backup and old files

No backup files are available. Backups and outdated files may seem harmless, but they often contain useful data or old code that attackers can dig through to find vulnerabilities.



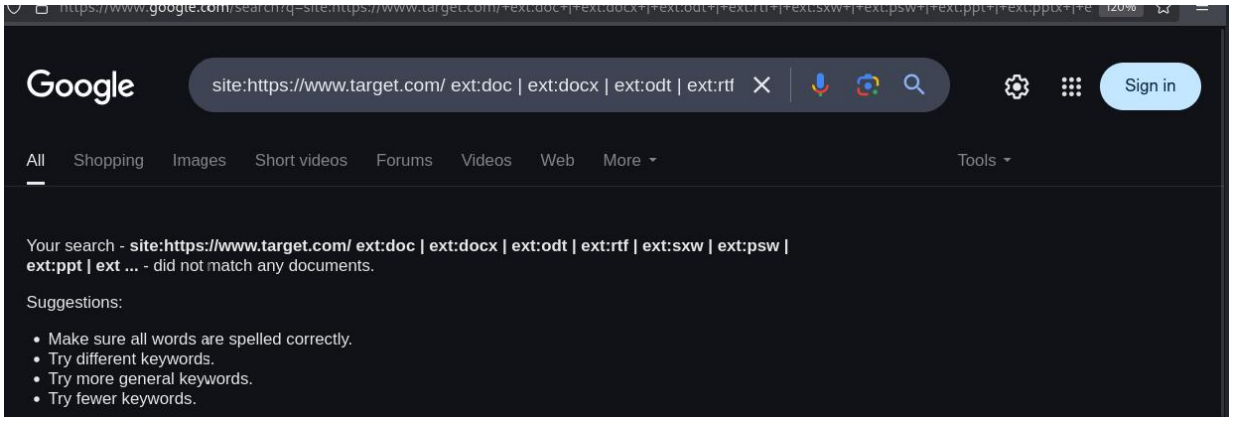
Option : sql errors

No sql errors found. When websites accidentally show database error messages, it can give attackers clues about how the database is structured, helping them launch SQL injection attacks.



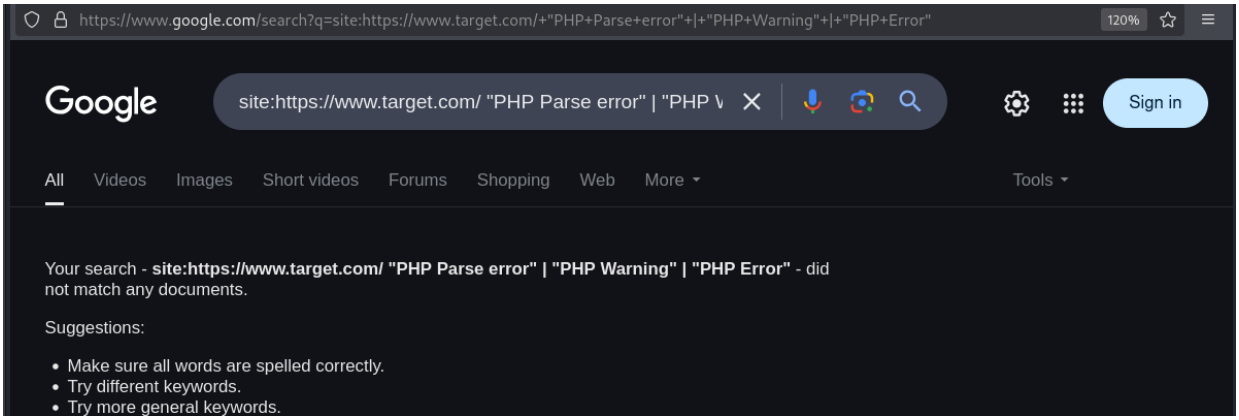
Option: Publicly exposed documents

Does not any publicly exposed documents. Sometimes internal documents like PDFs or reports are unintentionally made public. These could contain private or sensitive information.



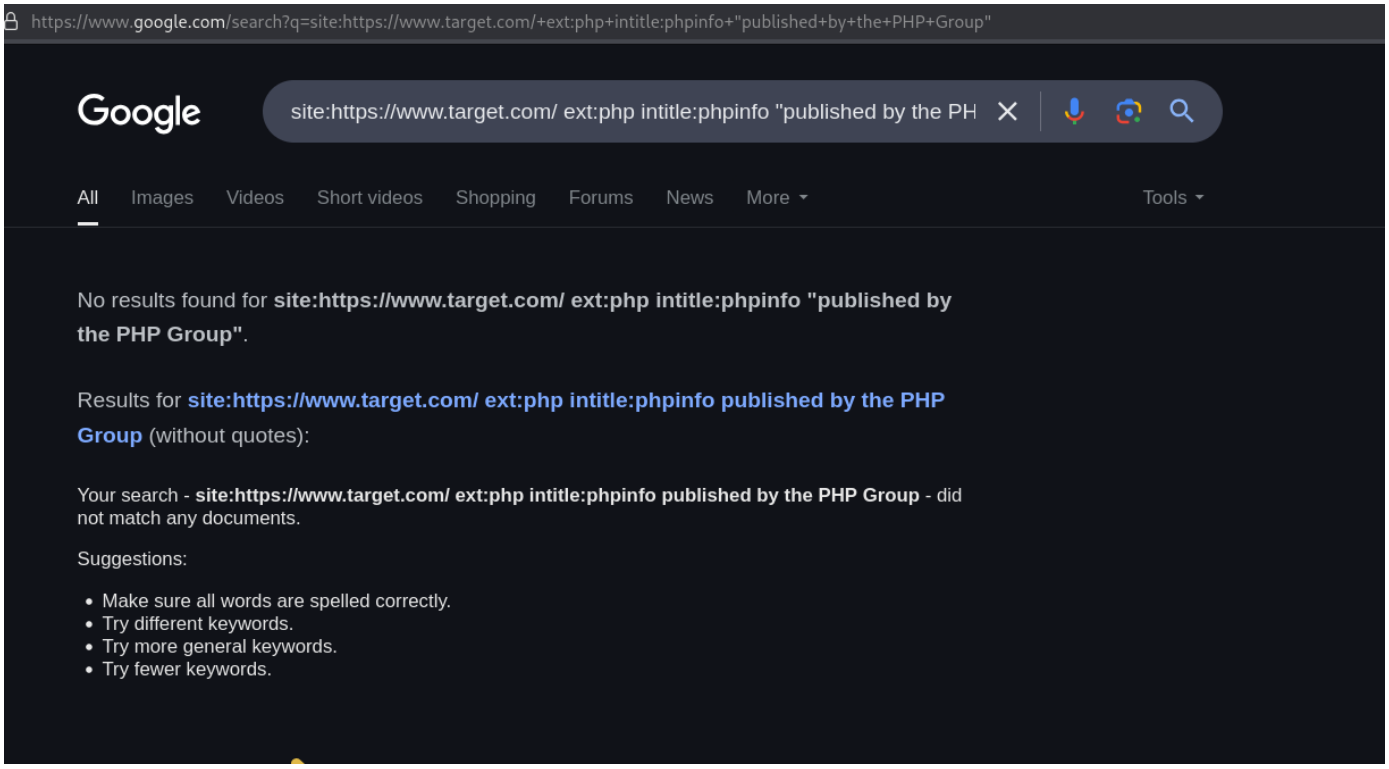
Option: PHP errors / warnings:

No PHP errors or warnings found. If the system shows technical error messages, it might reveal things like file locations or parts of the code, which can help attackers find ways to exploit the system.



Option: Phpinfo ()

No phpinfo are found. This page shows detailed information about how the server is set up. While it's useful for developers, it's also valuable to hackers looking for weak spots.



Part 3: Explore the WHOIS Database

STEP 1,2,3,4-

GoDaddy Corporate Domains, LLC	
Whois Server	whois.brandsight.com
Referral URL	http://gcd.com
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited serverTransferProhibited https://icann.org/epp#serverTransferProhibited serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Important Dates	
Expires On	2028-01-01
Registered On	1997-01-02
Updated On	2023-06-01
Name Servers	
ns5-65.akam.net	184.85.248.65
ns7-64.akam.net	96.7.49.64
ns4-65.akam.net	84.53.139.65
ns1-168.akam.net	193.108.91.168
Similar Domains	

targe-ay.info | targe-chauffeurs.com | targe-checkbalance.space | targe-china.com | targe-enargy.com | targe-energy.com | targe-env.co.uk | targe-env.com | targe-market.co.il | targe-marketing.info | targe-miroiterie-lyon.fr | targe-of-gordon.de | targe-of-gordon.org | targe-point.it | targe-sa.fr | targe-security.com | targe-security.info | targe-t.com | targe-tier.com | targe.asso.fr |

Similar Domains

targe-ay.info | targe-chauffeurs.com | targe-checkbalance.space | targe-china.com | targe-enargy.com | targe-energy.com | targe-env.co.uk | targe-env.com | targe-market.co.il | targe-marketing.info | targe-miroiterie-lyon.fr | targe-of-gordon.de | targe-of-gordon.org | targe-point.it | targe-sa.fr | targe-security.com | targe-security.info | targe-t.com | targe-tier.com | targe.asso.fr |

Registrar Data

Make Private Now

We will display stored WHOIS data for up to 30 days.

```
Registrant Contact Information:
Name:                                   Brandsight Privacy Customer 243552
Organization:
Address Line 1:                         PO Box 190899
Address Line 2:
City:                                   Boise
State/Province:                         ID
Postal Code:                            83719
Country:                                US
Phone:                                  +1.2084252575
Fax:
Email:                                  243552@brandsightprivacy.com
Full Address:                           PO Box 190899, Boise, ID, 83719, US

Tech Contact Information:
Name:                                   Brandsight Privacy Customer 243552
Organization:
Address Line 1:                         PO Box 190899
Address Line 2:
City:                                   Boise
State/Province:                         ID
Postal Code:                            83719
Country:                                US
Phone:                                  +1.2084252575
Fax:
Email:                                  243552@brandsightprivacy.com
Full Address:                           PO Box 190899, Boise, ID, 83719, US

Information Updated: 2025-03-14 16:31:41.520717+00
```

Here I used who.is and perform a WHOIS lookup for the domain **target.com**. The WHOIS results provided details about the domain's technical and registration details. I found that the **registrar** is GoDaddy Corporate Domains, LLC, and the domain's status is set to clientTransferProhibited, which means the domain cannot be transferred without explicit authorizatio- this is a security measure to prevent hijacking.

I also noted important dates such as:

- Domain Registered On: 1997-01-02
- Last Updated On: 2023-06-01
- Expiry Date: 2028-01-01

The WHOIS record also displayed the DNS server names and their respective IP addresses, for example:

- ns5-65.akam.net → 184.85.248.65
- ns7-64.akam.net → 96.7.49.64
- ns4-65.akam.net → 84.53.139.65
- ns1-168.akam.net → 193.108.91.168

Additionally, it included Registrant and Technical Contact Information, although the actual owner's identity was masked using a privacy protection service (Brandsight Privacy Customer 243552). It also showed the mailing address (Boise, Idaho, US), contact phone number, and email used for administrative purposes.

Part 4 - Using Domain Dossier Whois Function

STEP 1,2,3,4,5,6-

Domain : mit.edu

I entered "**mit.edu**" in the search bar, selected the "domain whois record" option, and clicked the "Go" button. The tool provided detailed WHOIS information about the domain owned by mit.edu. It displayed the IP addresses associated with the domain, including 23.204.2.14 and 2600:140e:6:ab3::255e, as well as a list of name servers like EUR5.AKAM.NET, USW2.AKAM.NET, and others. The WHOIS section also included the registrant, administrative, and technical contact details, along with email addresses and phone numbers. Additionally, I noted that the domain was activated on 23-May-1985, last updated on 15-Jan-2025, and is set to expire on 31-Jul-2025.

Domain Dossier Investigate domains and IP addresses

domain or IP address: mit.edu

☑ domain whois record ☐ DNS records ☐ traceroute

☐ network whois record ☐ service scan go

user: anonymous [208.59.151.147]
balance: 48 units
log in | account info

CentralOps.net

To obtain Whois data redacted because of the GDPR or privacy services, try ICANN's RDRS. [more information]

Address lookup

canonical name **mit.edu.**

aliases

addresses **23.204.2.14**
2600:140e:6:ab3::255e
2600:140e:6:a83::255e

Domain Whois record

Queried **whois.educause.net** with "**mit.edu**"...

```
Domain Name: MIT.EDU

Registrant:
        Massachusetts Institute of Technology
        77 Massachusetts Ave
        Cambridge, MA 02139
        USA

Administrative Contact:
        Mark Silis
        Massachusetts Institute of Technology
        MIT Room W92-167, 77 Massachusetts Avenue
        Cambridge, MA 02139-4307
        USA
        +1.6173245900
        mark@mit.edu

Technical Contact:
        MIT Network Operations
        Massachusetts Institute of Technology
        MIT Room W92-167, 77 Massachusetts Avenue
        Cambridge, MA 02139-4307
        USA
        +1.6172538400
        noc@mit.edu

Name Servers:
        EUR5.AKAM.NET
        USW2.AKAM.NET
        ASIA1.AKAM.NET
        USE5.AKAM.NET
        USE2.AKAM.NET
        ASIA2.AKAM.NET
        NS1-173.AKAM.NET
        NS1-37.AKAM.NET

Domain record activated:    23-May-1985
Domain record last updated: 15-Jan-2025
Domain expires:             31-Jul-2025

-- end --
```

URL for this output | return to CentralOps.net, a service of Hexillion

STEP 7-

Domain: iit.edu

I used iit.edu, which provided detailed registrant and technical contact details, including names, addresses, and email IDs. The IP addresses listed were 174.143.130.167 and 2001:4800:7819:104:be76:4eff:fe04:88c6, and the name servers included entries like DDA-RS2.IIT.EDU and DNS.ENT.IIT.EDU. I also noted that the domain was activated on 07-Apr-1988, last updated on 02-Oct-2024, and set to expire on 31-Jul-2027.

Domain Dossier Investigate domains and IP addresses

domain or IP address: iit.edu

☑ domain whois record ☐ DNS records ☐ traceroute

☐ network whois record ☐ service scan go

user: anonymous [208.59.151.147]
balance: 47 units
log in | account info

CentralOps.net

To obtain Whois data redacted because of the GDPR or privacy services, try ICANN's RDRS. [more information]

Address lookup

canonical name **iit.edu.**

aliases

addresses **174.143.130.167**
2001:4800:7819:104:be76:4eff:fe04:88c6

Domain Whois record

Queried **whois.educause.net** with "**iit.edu**"...

```
Domain Name: IIT.EDU

Registrant:
        Illinois Institute of Technology
        Office of Technology Services
        10 West 31st Street,
        Chicago, IL 60616
        USA

Administrative Contact:
        Ibukun Oyewole
        Illinois Institute of Technology
        10 West 31st St
        Chicago, IL 60616
        USA
        +1.3125675809
        oyewole@iit.edu

Technical Contact:
        Technology Infrastructure
        Illinois Institute of Technology
        10 West 31st St
        Chicago, IL 60616
        USA
        +1.3125675809
        oyewole@iit.edu

Name Servers:
        DDA-RS2.IIT.EDU
        DNS.ENT.IIT.EDU
        DNS2.ENT.IIT.EDU

Domain record activated:    07-Apr-1988
Domain record last updated: 02-Oct-2024
Domain expires:             31-Jul-2027
```

-- end --

URL for this output | return to CentralOps.net, a service of Hexillion

Domain: target.com

Although the technical details like name servers and domain dates were shown, most of the contact details were masked using Brandsight Privacy Services, reflecting a more privacy-conscious approach. Instead of individual names, only a general privacy customer identity and address were displayed.

Address lookup

canonical name sites.target.map.fastly.net.

aliases www.target.com

addresses 151.101.162.187

Domain Whois record

Queried whois.internic.net with "dom target.com"...

```
   Domain Name: TARGET.COM
   Registry Domain ID: 117595_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.brandsight.com
   Registrar URL: http://gcd.com
   Updated Date: 2023-06-01T04:16:02Z
   Creation Date: 1997-01-02T05:00:00Z
   Registry Expiry Date: 2028-01-01T05:00:00Z
   Registrar: GoDaddy Corporate Domains, LLC
   Registrar IANA ID: 3786
   Registrar Abuse Contact Email: abuse@gcd.com
   Registrar Abuse Contact Phone: +1.5189669187
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1-168.AKAM.NET
   Name Server: NS4-65.AKAM.NET
   Name Server: NS5-65.AKAM.NET
   Name Server: NS7-64.AKAM.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-03-14T16:55:26Z <<<
```

Queried whois.brandsight.com with "target.com"...

```
Domain Name: target.com
Registry Domain ID: 117595_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.brandsight.com
Registrar URL: https://gcd.com
Updated Date: 2023-06-01T04:16:02Z
Creation Date: 1997-01-02T05:00:00Z
Registrar Registration Expiration Date: 2028-01-01T05:00:00Z
Registrar: GoDaddy Corporate Domains, LLC
Registrar IANA ID: 3786
Registrar Abuse Contact Email: abuse@gcd.com
Registrar Abuse Contact Phone: +1.5188315864
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Brandsight Privacy Customer 243552
Registrant Organization:
Registrant Street: PO Box 190899
Registrant City: Boise
Registrant State/Province: ID
Registrant Postal Code: 83719
Registrant Country: US
Registrant Phone: +1.2084252575
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: 243552@brandsightprivacy.com
Registry Tech ID: Not Available From Registry
Tech Name: Brandsight Privacy Customer 243552
Tech Organization:
Tech Street: PO Box 190899
Tech City: Boise
Tech State/Province: ID
Tech Postal Code: 83719
Tech Country: US
Tech Phone: +1.2084252575
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: 243552@brandsightprivacy.com
Name Server: NS1-168.AKAM.NET
Name Server: NS4-65.AKAM.NET
Name Server: NS5-65.AKAM.NET
Name Server: NS7-64.AKAM.NET
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2025-03-14T16:55:39Z <<<
```

-- end --

URL for this output | return to CentralOps.net, a service of Hexillion

5. Part 5 - DNS Reconnaissance

5.1. Host:

STEP 1,2-

I used the **host** command in my Kali Linux terminal to retrieve DNS information for facebook.com. This simple command displayed the IPv4 address (31.13.66.35) and IPv6 address (2a03:2880:f103:83:face:b00c:0:25de) associated with the domain. It also showed that Facebook's mail is handled by smtpin.vvv.facebook.com, which is the server responsible for managing incoming emails

```
┌──(kali㉿kali)-[~]
└─$ host facebook.com
facebook.com has address 31.13.66.35
facebook.com has IPv6 address 2a03:2880:f103:83:face:b00c:0:25de
facebook.com mail is handled by 10 smtpin.vvv.facebook.com.
```

STEP 3,4-

In this step, I used the host command again, but this time to perform a reverse DNS lookup by entering Facebook's IP address 31.13.66.35. The result revealed the domain name associated with this IP, which was edge-star-mini-shv-01-iad3.facebook.com.

```
┌──(kali㉿kali)-[~]
└─$ host 31.13.66.35
35.66.13.31.in-addr.arpa domain name pointer edge-star-mini-shv-01-iad3.facebook.com.

┌──(kali㉿kali)-[~]
```

STEP 5-

In this step, I used the host **-v** facebook.com command in the Kali Linux terminal to enable **verbose** output while performing the DNS lookup. This provided a detailed breakdown of the query process, including the header info, question section, and answer section. It showed the IPv4 address (31.13.66.35), IPv6 address (2a03:2880:f103:83:face:b00c:0:25de), and the mail exchange (MX) server - smtpin.vvv.facebook.com.

```
┌──(kali㉿kali)-[~]
└─$ host -v facebook.com
Trying "facebook.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56218
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;facebook.com.                  IN      A

;; ANSWER SECTION:
facebook.com.           44      IN      A       31.13.66.35

Received 46 bytes from 192.168.0.1#53 in 44 ms
Trying "facebook.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54693
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;facebook.com.                  IN      AAAA

;; ANSWER SECTION:
facebook.com.           43      IN      AAAA    2a03:2880:f103:83:face:b00c:0:25de

Received 58 bytes from 192.168.0.1#53 in 20 ms
Trying "facebook.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24245
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;facebook.com.                  IN      MX

;; ANSWER SECTION:
facebook.com.           3600    IN      MX      10 smtpin.vvv.facebook.com.

Received 69 bytes from 192.168.0.1#53 in 16 ms
```

STEP 6,7-

In this step, I used the **host -t ns facebook.com** command in my Kali Linux terminal to find out the name servers responsible for handling DNS queries for facebook.com. The -t ns option specifically queries for NS (Name Server) records. The output showed four name servers: a.ns.facebook.com, b.ns.facebook.com, c.ns.facebook.com, and d.ns.facebook.com.

```
┌──(kali㉿kali)-[~]
└─$ host -t ns  facebook.com
facebook.com name server b.ns.facebook.com.
facebook.com name server a.ns.facebook.com.
facebook.com name server d.ns.facebook.com.
facebook.com name server c.ns.facebook.com.
```

STEP 8,9-

In this step, I performed a DNS query using a specific DNS server instead of relying on the system's default. I used the command **host -t ns facebook.com** 8.8.8.8, which directed the query to Google's public DNS server (8.8.8.8). The result returned the same list of Facebook's name servers: a.ns.facebook.com, b.ns.facebook.com, c.ns.facebook.com, and d.ns.facebook.com. This method is helpful when local DNS is not trustable or want to verify results using a known and reliable DNS provider like Google.

```
┌──(kali㉿kali)-[~]
└─$ host -t ns facebook.com 8.8.8.8
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:

facebook.com name server c.ns.facebook.com.
facebook.com name server d.ns.facebook.com.
facebook.com name server a.ns.facebook.com.
facebook.com name server b.ns.facebook.com.

┌──(kali㉿kali)-[~]
└─$
```

5.4. Find DNS Records

STEP 1-

In this step, I used the host command again to retrieve the IP addresses and MX records (mail servers) for the domain **target.com**. The output showed multiple IP addresses including 151.101.194.187, 151.101.130.187, 151.101.66.187, and 151.101.2.187, which are all part of Target's content delivery network. Additionally, the MX records revealed that emails for the domain are handled by mxa-0020ab02.gslb.pphosted.com and mxb-0020ab02.gslb.pphosted.com. This demonstrated how host can be used to quickly extract DNS details like web server IPs and mail server configurations for any domain.

```
┌──(kali㉿kali)-[~]
└─$ host target.com
target.com has address 151.101.194.187
target.com has address 151.101.130.187
target.com has address 151.101.66.187
target.com has address 151.101.2.187
target.com mail is handled by 5 mxa-0020ab02.gslb.pphosted.com.
target.com mail is handled by 5 mxb-0020ab02.gslb.pphosted.com.
```

STEP 2,3-

I used the **host -t MX target.com** command to specifically query the MX (Mail Exchange) records for the domain target.com. The output showed that Target's email is handled by two mail servers: mxa-0020ab02.gslb.pphosted.com and mxb-0020ab02.gslb.pphosted.com. This command helps in identifying the email infrastructure used by an organization.

```
┌──(kali㉿kali)-[~]
└─$ host -t MX target.com
target.com mail is handled by 5 mxa-0020ab02.gslb.pphosted.com.
target.com mail is handled by 5 mxb-0020ab02.gslb.pphosted.com.
```

STEP 4,5-

In this step, I used the **host -t ns target.com** command to retrieve the NS (Name Server) records for the domain target.com. The output listed four name servers: ns7-64.akam.net, ns4-65.akam.net, ns5-65.akam.net, and ns1-168.akam.net, which are part of Akamai's DNS infrastructure. This shows that Target's domain is managed through a globally distributed content delivery network

```
┌──(kali㉿kali)-[~]
└─$ host -t ns target.com
target.com name server ns7-64.akam.net.
target.com name server ns4-65.akam.net.
target.com name server ns5-65.akam.net.
target.com name server ns1-168.akam.net.
```

STEP 6,7-

Here I used the **host -t txt target.com** command to retrieve the TXT records for the domain target.com. TXT records usually contain important domain-related information such as SPF (Sender Policy Framework) records, domain verification strings, and site ownership confirmations. The output displayed several entries, including SPF records for email validation, Google site verification, Apple, Stripe, OpenAI, and Atlassian domain verifications, and other identifiers like NS_monitor and Brevo-code.

```
┌──(kali㉿kali)-[~]
└─$ host -t txt target.com
target.com descriptive text "v=spf1 include:%{ir}.%{v}.%{d}.spf.has.pphosted.com include:aspmx.pardot.com ~all"
target.com descriptive text "extensis-domain-verification=3911f3c0-e69c-4d75-aa8a-33afa0520d00"
target.com descriptive text "dGFyZ2V0"
target.com descriptive text "9rHeUd6AiQ30jFgENxeGX6CKgbSmFB/NeV5oCOQS5PbafVN66NOLFLcsuixmOo1krFPgHLMt7TCEL3iJOUF1mQ=="
target.com descriptive text "stripe-verification=c52e56dae78932924b24e718a7850f861712da65458f8c40bab37393ccb56854"
target.com descriptive text "1bsEs7Bmn7dTcejJKXlqr9CnnnHXScqfcjGCUs5JitlqKhuQG9jYszZ91XH+Q9LcoOY52FUopROI8LYUz5YeYQ=="
target.com descriptive text "brevo-code:7e6bbbf1fc671ea0755795690d17ba46"
target.com descriptive text "MS=ms72649311"
target.com descriptive text "apple-domain-verification=oc-ywTgysCFxVjoVZ7Alg51HbTSY0D7HhKU_9om-EFg"
target.com descriptive text "openai-domain-verification=dv-75YwqS2p7WZUZtnEA4VQmZpn"
target.com descriptive text "google-site-verification=2saealyvcdakrTY4LOg3GjblevTIYAJ4p_Ihwf3OrbU"
target.com descriptive text "NS_monitor"
target.com descriptive text "stripe-verification=916f40ab1d809d427b07435525ec8efcd0fc24be25674d3cc1067de63aa0021c"
target.com descriptive text "atlassian-domain-verification=PrIDM+2UNKNbpMDoD3mux5NL3XcTt2tisHloieySUpQAJXBPCtBzvw2WP7tRzUvd"
```

STEP 8,9-

The **host -t cname target.com** command to check for CNAME (Canonical Name) records associated with the domain target.com. The result indicated that target.com has no CNAME record. CNAME records are typically used to alias one domain name to another

```
┌──(kali㉿kali)-[~]
└─$ host -t cname target.com
target.com has no CNAME record
```

STEP 10,11-

The **host -t soa target.com** command to retrieve the SOA (Start of Authority) record for the domain target.com. The SOA record provides administrative information about the domain, including the primary name server (ns1-168.akam.net) and the responsible party's email (hostmaster.target.com). It also includes key configuration values like serial number, refresh time, retry time, expiry time, and minimum TTL

```
┌──(kali㉿kali)-[~]
└─$ host -t soa target.com
target.com has SOA record ns1-168.akam.net. hostmaster.target.com. 2005143630 3600 3600 2419200 900
```

5.5. dig Command.

STEP 1-

The **dig target.com** command to resolve the domain name and retrieve its A records (IP addresses). The output provided detailed information about the query, showing multiple IP addresses associated with target.com, including 151.101.2.187, 151.101.66.187, 151.101.130.187, and 151.101.194.187. The response also included additional technical details such as query time, server used, and response message size.

```
┌──(kali㉿kali)-[~]
└─$ dig target.com

; <<>> DiG 9.20.2-1-Debian <<>> target.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25861
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;target.com.                    IN      A

;; ANSWER SECTION:
target.com.             3396    IN      A       151.101.2.187
target.com.             3396    IN      A       151.101.66.187
target.com.             3396    IN      A       151.101.130.187
target.com.             3396    IN      A       151.101.194.187

;; Query time: 4 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Fri Mar 14 19:21:48 EDT 2025
;; MSG SIZE  rcvd: 103
```

STEP 2-

In this step, I used the **dig target.com +nocomments** command to perform a DNS lookup while removing unnecessary comment lines from the output

```
┌──(kali㉿kali)-[~]
└─$ dig target.com +nocomments

; <<>> DiG 9.20.2-1-Debian <<>> target.com +nocomments
;; global options: +cmd
;target.com.                    IN      A
target.com.             3391    IN      A       151.101.194.187
target.com.             3391    IN      A       151.101.2.187
target.com.             3391    IN      A       151.101.66.187
target.com.             3391    IN      A       151.101.130.187
;; Query time: 8 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Fri Mar 14 19:21:54 EDT 2025
;; MSG SIZE  rcvd: 103
```

STEP 3-

the **dig mx target.com** command to find out which mail servers handle email delivery for the domain target.com. The response showed two MX records, indicating that email for this domain is routed through mxa-0020ab02.gslb.pphosted.com and mxb-0020ab02.gslb.pphosted.com

```
┌──(kali㉿kali)-[~]
└─$ dig mx target.com

; <<>> DiG 9.20.2-1-Debian <<>> mx target.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14104
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;target.com.                    IN      MX

;; ANSWER SECTION:
target.com.             16      IN      MX      5 mxb-0020ab02.gslb.pphosted.com.
target.com.             16      IN      MX      5 mxa-0020ab02.gslb.pphosted.com.

;; Query time: 20 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Fri Mar 14 19:23:09 EDT 2025
;; MSG SIZE  rcvd: 111
```

STEP 4-

the **dig ns target.com** command to retrieve the Name Server (NS) records for the domain target.com. The response listed four authoritative name servers: ns7-64.akam.net, ns1-168.akam.net, ns4-65.akam.net, and ns5-65.akam.net. The output also included their corresponding IP addresses in the additional section, such as 84.53.139.65, 184.85.248.65, and 96.7.49.64.

```
┌──(kali㉿kali)-[~]
└─$ dig ns target.com

; <<>> DiG 9.20.2-1-Debian <<>> ns target.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55006
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 11baac6e8bda5c220100000067d4ba752d883e985d07bf78 (good)
;; QUESTION SECTION:
;target.com.                    IN      NS

;; ANSWER SECTION:
target.com.             3357    IN      NS      ns7-64.akam.net.
target.com.             3357    IN      NS      ns1-168.akam.net.
target.com.             3357    IN      NS      ns4-65.akam.net.
target.com.             3357    IN      NS      ns5-65.akam.net.

;; ADDITIONAL SECTION:
ns4-65.akam.net.        142021  IN      A       84.53.139.65
ns5-65.akam.net.        141790  IN      A       184.85.248.65
ns7-64.akam.net.        142021  IN      A       96.7.49.64

;; Query time: 16 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Fri Mar 14 19:23:32 EDT 2025
;; MSG SIZE  rcvd: 208
```

STEP 5,6 -

the **dig target.com +short** command to get a clean and simplified output that displays only the IP addresses of the domain target.com. This option filters out all extra technical details and returns just the essential information

```
┌──(kali㉿kali)-[~]
└─$ dig target.com +short
151.101.130.187
151.101.194.187
151.101.2.187
151.101.66.187

┌──(kali㉿kali)-[~]
```

STEP 7,8-

the **dig target.com +trace** command to perform a DNS trace, which allowed me to follow the full path of the DNS query resolution process. The +trace option initiates iterative queries, starting from the root name servers, then moving down the top-level domain (TLD) servers, and finally reaching the authoritative name servers for target.com. This method provides a clear picture of how DNS resolution works

```
└─$ dig target.com +trace

; <<>> DiG 9.20.2-1-Debian <<>> target.com +trace
;; global options: +cmd
.                       80605   IN      NS      a.root-servers.net.
.                       80605   IN      NS      h.root-servers.net.
.                       80605   IN      NS      j.root-servers.net.
.                       80605   IN      NS      e.root-servers.net.
.                       80605   IN      NS      d.root-servers.net.
.                       80605   IN      NS      c.root-servers.net.
.                       80605   IN      NS      g.root-servers.net.
.                       80605   IN      NS      m.root-servers.net.
.                       80605   IN      NS      l.root-servers.net.
.                       80605   IN      NS      f.root-servers.net.
.                       80605   IN      NS      b.root-servers.net.
.                       80605   IN      NS      i.root-servers.net.
.                       80605   IN      NS      k.root-servers.net.
.                       80605   IN      RRSIG   NS 8 0 518400 20250327170000 20250314160000 26470 . RNBi4rY553YVDa8DjWj786NTjL+qEUUAq86K4PMhoU/oqH0R16wJpCXN osD1nR7Zj65
Skp0pSqS/RNSx7yfGjSvEaefPSrYcMjeo0Ue/gtET1a1Z IZLH7wUEV/GUHPJ6NzsAgbS0AWyjTZfbcht23EMYIbyu3/cRNoRhQoey T2idHQmodQgAWsVVCJcuipoR1QFrhM0KQE0dTWq2joQOgyYbq7CVYuC1 +InuzZMb
dPCFIo2z5d5SnLqAJSb25kwcV04V8u0OCRqGheGu0PebKspR 1AqJhCrexsX6682p6WSj1Q3DlFE6F8V+amRxpHciD9/paTDNMvwg0YgU mRPQkw==
;; Received 525 bytes from 192.168.0.1#53(192.168.0.1) in 16 ms

com.                    172800  IN      NS      m.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    86400   IN      DS      19718 13 2 8ACBB0CD28F41250A80A491389424D341522D946B0DA0C0291F2D3D7 71D7805A
com.                    86400   IN      RRSIG   DS 8 1 86400 20250327170000 20250314160000 26470 . Q14qWW5hfHLBR153R+oJtiF/9Uc9bHPEZxl1dfNIO7igac1R1NcsEAI2 c1NDzmPTEc4T
54UW4g5W0Ba7pQuJq9OZzA8SzxdzoDuXoqIYt/GkELDO N83TWT85X9L8e8HotSM5IrnOTKOiejLrZQ7nuDsXmUug/pI1Rtn6SAdM fGMF6lS20wFzEZU1rXVOU0ozFPH6IJfYux9lcG8Kz4qZNiV8oh5u4+eK I9Zey02XY
ZI58MbjFXYGWNde+p5THzT5G2Oxqcuvz1TMFE8QPfndtS3K YUID1whzSGavZZ9G7UBhT3pJnoT9bxLM/7m8aH1+qElULM9Nxi82jKWF VPLK1g==
;; Received 1198 bytes from 192.112.36.4#53(g.root-servers.net) in 20 ms
```

```
target.com.             172800  IN      NS      ns1-168.akam.net.
target.com.             172800  IN      NS      ns4-65.akam.net.
target.com.             172800  IN      NS      ns5-65.akam.net.
target.com.             172800  IN      NS      ns7-64.akam.net.
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 900 IN NSEC3 1 1 0 - CK0Q3UDG8CEKKAE7RUKPGCT1DVSSH8LL NS SOA RRSIG DNSKEY NSEC3PARAM
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 900 IN RRSIG NSEC3 13 2 900 20250320002631 20250312231631 23202 com. OCYuQBeQH/LgOwKDB+rY0ImHhZ4Li7cFur436MWEpR87DMrs7sn60ERk rjOP
fpyr3JjyJFKPOlPD57cV8NydNA==
DI4FD9IHTUGNT7LT1HGGVNK6D7G24Q2Q.com. 900 IN NSEC3 1 1 0 - DI4FREEVODGA3U973CBMI5T1N5CJS44V NS DS RRSIG
DI4FD9IHTUGNT7LT1HGGVNK6D7G24Q2Q.com. 900 IN RRSIG NSEC3 13 2 900 20250319005243 20250311234243 23202 com. LVG32+eyunUl42PpQrSXX2e58bLun6P4NwGC7ZO+cOS3F6SKPmM2lF2T emmd
COQsHe26Zl0Jq3QjwbWKQGQ/bA==
;; Received 489 bytes from 192.41.162.30#53(l.gtld-servers.net) in 16 ms

target.com.             3600    IN      A       151.101.66.187
target.com.             3600    IN      A       151.101.130.187
target.com.             3600    IN      A       151.101.2.187
target.com.             3600    IN      A       151.101.194.187
;; Received 103 bytes from 184.85.248.65#53(ns5-65.akam.net) in 28 ms


┌──(kali㉿kali)-[~]
```

5.6. Zone Transfer.

STEP 1-

the **dig -t ns zonetransfer.me +short** command to identify the name servers for the domain zonetransfer.me. The result showed two DNS servers: nsztm1.digi.ninja and nsztm2.digi.ninja, which are authoritative for this domain.

```
┌──(kali㉿kali)-[~]
└─$ dig -t ns zonetransfer.me +short
nsztm1.digi.ninja.
nsztm2.digi.ninja.
```

STEP 2,3,4-

The **dig axfr zonetransfer.me @nsztm2.digi.ninja** performs a DNS zone transfer from the name server nsztm2.digi.ninja. The query successfully returned a complete list of DNS records, including SOA, A, MX, NS, TXT, AAAA, CNAME, and others. This kind of result shows all publicly exposed DNS information on the zone, such as subdomains, internal hostnames, and email servers. Zone transfers like this should generally be restricted by administrators, but when left open they can expose sensitive infrastructure details

```
File  Actions  Edit  View  Help
└─$ dig axfr zonetransfer.me @nsztm2.digi.ninja

; <<>> DiG 9.20.2-1-Debian <<>> axfr zonetransfer.me @nsztm2.digi.ninja
;; global options: +cmd
zonetransfer.me.        7200    IN      SOA     nsztm1.digi.ninja. robin.digi.ninja. 2019100801 172800 900 1209600 3600
zonetransfer.me.        301     IN      TXT     "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"
zonetransfer.me.        7200    IN      MX      0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      A       5.196.105.14
zonetransfer.me.        7200    IN      NS      nsztm1.digi.ninja.
zonetransfer.me.        7200    IN      NS      nsztm2.digi.ninja.
zonetransfer.me.        300     IN      HINFO   "Casio fx-700G" "Windows XP"
_acme-challenge.zonetransfer.me. 301 IN TXT     "6Oa05hbUJ9xSsvYy7pApQvwCUSSGgxvrbdizjePEsZI"
_sip._tcp.zonetransfer.me. 14000 IN     SRV     0 0 5060 www.zonetransfer.me.
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me. 7200 IN PTR www.zonetransfer.me.
asfdbauthdns.zonetransfer.me. 7900 IN   AFSDB   1 asfdbbox.zonetransfer.me.
asfdbbox.zonetransfer.me. 7200  IN      A       127.0.0.1
asfdbvolume.zonetransfer.me. 7800 IN    AFSDB   1 asfdbbox.zonetransfer.me.
canberra-office.zonetransfer.me. 7200 IN A      202.14.81.230
cmdexec.zonetransfer.me. 300    IN      TXT     "; ls"
contact.zonetransfer.me. 2592000 IN     TXT     "Remember to call or email Pippa on +44 123 4567890 or pippa@zonetransfer.me when making DNS changes"
dc-office.zonetransfer.me. 7200 IN      A       143.228.181.132
deadbeef.zonetransfer.me. 7201  IN      AAAA    dead:beaf::
dr.zonetransfer.me.     300     IN      LOC     53 20 56.558 N 1 38 33.526 W 0.00m 1m 10000m 10m
DZC.zonetransfer.me.    7200    IN      TXT     "AbCdEfG"
email.zonetransfer.me.  2222    IN      NAPTR   1 1 "P" "E2U+email" "" email.zonetransfer.me.zonetransfer.me.
email.zonetransfer.me.  7200    IN      A       74.125.206.26
Hello.zonetransfer.me.  7200    IN      TXT     "Hi to Josh and all his class"
home.zonetransfer.me.   7200    IN      A       127.0.0.1
Info.zonetransfer.me.   7200    IN      TXT     "ZoneTransfer.me service provided by Robin Wood - robin@digi.ninja. See http://digi.ninja/projects/zonetransferme.php fo
r more information."
internal.zonetransfer.me. 300   IN      NS      intns1.zonetransfer.me.
internal.zonetransfer.me. 300   IN      NS      intns2.zonetransfer.me.
intns1.zonetransfer.me. 300     IN      A       81.4.108.41
intns2.zonetransfer.me. 300     IN      A       167.88.42.94
office.zonetransfer.me. 7200    IN      A       4.23.39.254
ipv6actnow.org.zonetransfer.me. 7200 IN AAAA    2001:67c:2e8:11::c100:1332
owa.zonetransfer.me.    7200    IN      A       207.46.197.32
robinwood.zonetransfer.me. 302  IN      TXT     "Robin Wood"
rp.zonetransfer.me.     321     IN      RP      robin.zonetransfer.me. robinwood.zonetransfer.me.
sip.zonetransfer.me.    3333    IN      NAPTR   2 3 "P" "E2U+sip" "!^.*$!sip:customer-service@zonetransfer.me!" .
sqli.zonetransfer.me.   300     IN      TXT     "' or 1=1 --"
sshock.zonetransfer.me. 7200    IN      TXT     "() { :]}; echo ShellShocked"
staging.zonetransfer.me. 7200   IN      CNAME   www.sydneyoperahouse.com.
alltcpportsopen.firewall.test.zonetransfer.me. 301 IN A 127.0.0.1
testing.zonetransfer.me. 301    IN      CNAME   www.zonetransfer.me.
vpn.zonetransfer.me.    4000    IN      A       174.36.59.154
www.zonetransfer.me.    7200    IN      A       5.196.105.14
xss.zonetransfer.me.    300     IN      TXT     "'><script>alert('Boo')</script>"
zonetransfer.me.        7200    IN      SOA     nsztm1.digi.ninja. robin.digi.ninja. 2019100801 172800 900 1209600 3600
;; Query time: 120 msec
;; SERVER: 5.196.105.10#53(nsztm2.digi.ninja) (TCP)
;; WHEN: Fri Mar 14 19:30:18 EDT 2025
;; XFR size: 50 records (messages 1, bytes 2085)
```

Part 6: Collect Information with theHarvester

STEP 1,2,3,4-

In this step, I used the command **theHarvester -d target.com -b** google to perform email and subdomain enumeration using theHarvester tool on my Kali Linux terminal. The tool returned an "Invalid source" error

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d target.com -b google
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
*******************************************************************
*  _   _                                                          *
* | |_| |__   ___    ^  /\__ _ _ ___   _____   __| |_ ___ _ __   *
* | __|  _ \ / _ \  / /_/ / _` | '_\ \ / / _ v  __| __/ _ \ '_| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |   *
*  \__|_| |_|\___| v /_/ \__,_|_|    \_/ \___||___/\__\___|_|     *
*                                                                 *
* theHarvester 4.6.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[!] Invalid source.
```

STEP 5,6,7-

I used **theHarvester -d target.com -l 500 -b** all to gather maximum publicly available information on the domain target.com. The -l 500 option was used to limit the search results to the first 500 entries, and -b all told the tool to collect data from all available sources. The tool began querying various engines, but displayed messages indicating that API keys were missing for some services. This search could reveal information such as LinkedIn users, email addresses, and hostnames

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d target.com -l 500 -b all
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
*******************************************************************
*  _   _                                                          *
* | |_| |__   ___    ^  /\__ _ _ ___   _____   __| |_ ___ _ __   *
* | __|  _ \ / _ \  / /_/ / _` | '_\ \ / / _ v  __| __/ _ \ '_| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |   *
*  \__|_| |_|\___| v /_/ \__,_|_|    \_/ \___||___/\__\___|_|     *
*                                                                 *
* theHarvester 4.6.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: target.com

Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for bevigil.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for binaryedge.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for bufferoverun.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for Censys ID and/or Secret.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for criminalip.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for fullhunt.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for Github.
```

```
My current iter_url: http://www.sitedossier.com/parentdomain/target.com/101
An exception has occurred: 500, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url='https://api.threatminer.org/v2/domain.php?q=target.com&rt=5'
In total found: 100
{'studiored.target.com', 'item.target.com', 'imgsvc.target.com', 'sendasmoochie.target.com', 'corporategiftcards.target.com', 'originpky-www.target.com', 'fresh.target.com', 'targetcareers.target.com', 'hereforgood.target.com', 'supplierregistration.tar
get.com', 'india.target.com', 'fallingforyou.target.com', 'mig.target.com', 'onestar.target.com', 'mytargetweekly.target.com', 'home.target.com', 'sellpathext.target.com', 'startsomething.target.com', 'sitemap.target.com', 'pdzone.target.com', 'home.cat
alogs.target.com', 'target.com', 'confluence.target.com', 'mail.target.com', 'careers.target.com', 'pdpw.target.com', 'grs.target.com', 'seclogin.target.com', 'm.weeklyad.target.com', 'mobileconnect.target.com', 'pets.target.com', 'patio.catalogs.target
.com', 'sites.target.com', 'custom.target.com', 'investors.target.com', 'community.target.com', 'print.coupons.target.com', 'coupons.target.com', 'smithandhawken.catalogs.target.com', 'redirect.target.com', 'college.target.com', 'style.target.com', 'rec
ipes.target.com', '2day.target.com', 'babycatalog.target.com', 'health.target.com', 'nro01.target.com', 'mobilerx.target.com', 'targetfieldtripgrants.target.com', 'news.target.com', 'redcard.target.com', 'reading.target.com', 'selipointext.target.com',
'ns3.target.com', '2daysale.target.com', 'originscs-www.target.com', 'bookmarked.target.com', 'm.college.target.com', 'corporate.target.com', 'racing.target.com', 'dailydeals.target.com', 'catalogs.target.com', 'star.target.com', 'cinemared.target.com',
'kpm.target.com', 'target.com.', 'checkcard.target.com', 'roommates.target.com', 'hrportal.target.com', 'shop.target.com', 'csvta.target.com', 'holidaymusicstream.target.com', 'jira.target.com', 'givewith.target.com', 'marketingresources.target.com',
communitydev.target.com', 'podfodder.target.com', 'prefs.target.com', 'spiderman3.target.com', 'ns4.target.com', 'samples.target.com', 'metrics.target.com', 'targetrewards.target.com', 'exemplumext.target.com', 'beta.target.com', 'm.target.com', 'grscat
.target.com', 'cartwheel-secure.target.com', 'download.target.com', 'targetbabycatalog.target.com', 'catalog.target.com', 'holidaymusic.target.com', 'designforall.target.com', 'bullseye.target.com', 'fstl.target.com', 'cartwheel.target.com', 'pressroom.
target.com', 'rcam.target.com', 'rcamc.target.com', 'estatement.target.com'}
[*] Searching Sitedossier.
An exception has occurred: 429, message='Attempt to decode JSON with unexpected mimetype: text/html', url='https://urlscan.io/api/v1/search/?q=domain:target.com'
[*] Searching Yahoo.
An exception has occurred: 'NoneType' object has no attribute 'find'
[*] Searching Rapiddns.

[*] LinkedIn Links found: 0

[*] IPs found: 233

104.130.110.237
104.17.59.65
104.17.60.65
104.86.228.140
104.92.252.249
107.154.75.231
12.160.253.2
128.17.230.59
128.245.17.86
128.245.17.87
13.110.30.10
13.110.30.11
13.110.30.13
13.110.30.14
13.110.52.10
13.110.52.11
13.110.52.8
13.110.52.9
13.56.23.27
130.211.6.17
136.147.129.35
15.235.172.162
151.101.130.180
151.101.130.181
151.101.130.187
151.101.194.180
151.101.194.181
151.101.194.187
151.101.2.180
151.101.2.181
```

STEP 8,9-

theHarvester -d target -b bing to collect publicly available information about the domain target.com, this time specifying Bing as the search engine data source. TheHarvester tool initiated the search and parsed through Bing results. As seen in the output, no IP addresses or email addresses were found in this run, but it did successfully identify 3 hostnames associated with the domain: com.target, corporate.target, n.target

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d target -b bing
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
*******************************************************************
*  _  _                                                           *
* | |_| |__   __   __    ^  /\__ _ _ ___   _____  __| |_ __ _ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \ V __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| V /_/ \__,_|_|    \_/ \___||___/\__\___|_|      *
*                                                                 *
* theHarvester 4.6.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: target

Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
        Searching 0 results.
[*] Searching Bing.

[*] No IPs found.

[*] No emails found.

[*] Hosts found: 3
---------------------
com.target
corporate.target
n.target

┌──(kali㉿kali)-[~]
```

Part 7: Collect Information with Maltego

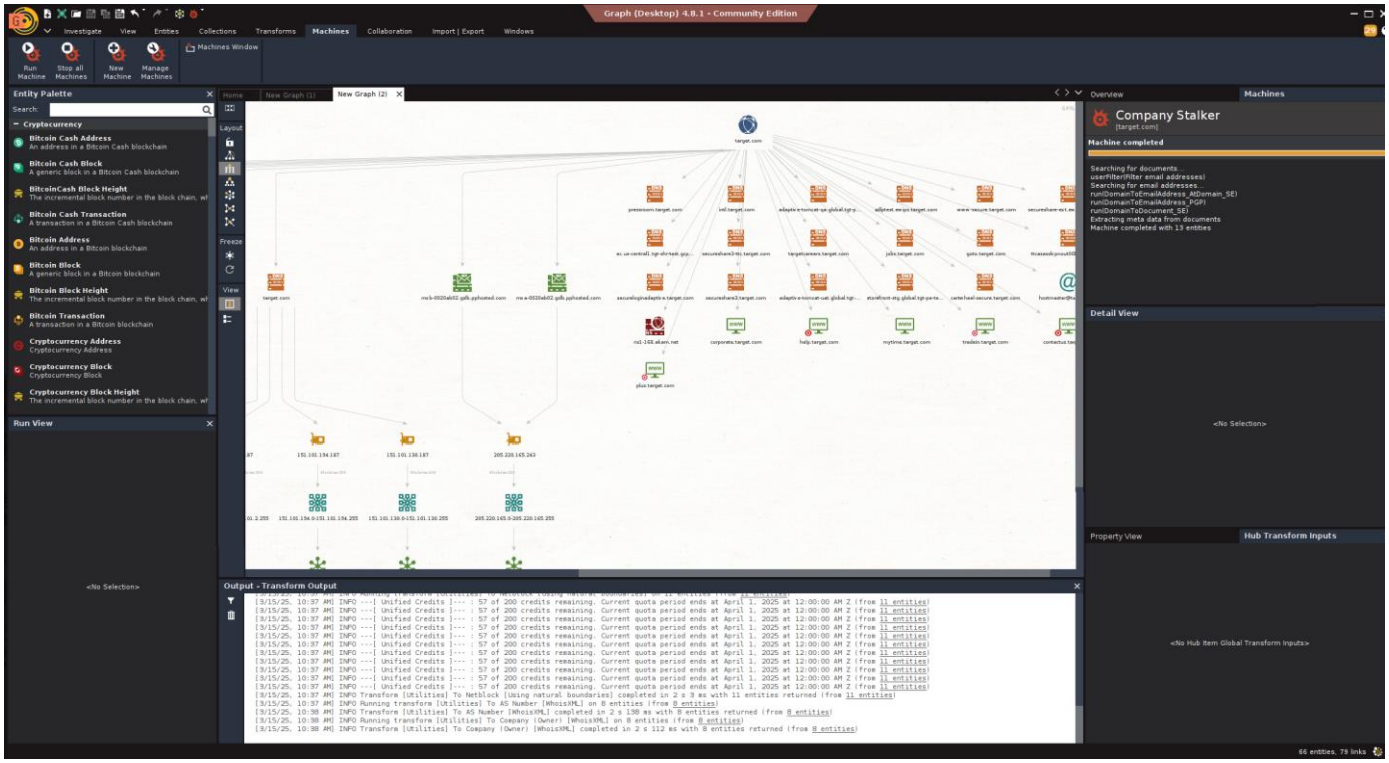
7.1. How to run an email address in Maltego.

STEP 1,2,3,4,5,6-

I used Maltego to run the Company Stalker machine on the domain target.com. This machine automates the process of discovering publicly available email addresses, documents, and information associated with the domain. I initiated the process by selecting Machines > Run Machine and choosing "Company Stalker" from the available machine options. I entered target.com in the Domain Name box and clicked Finish to begin the process. The graph view displayed the domain node linked to multiple discovered email addresses like Christopher.Osei@target.com, Kyle.Kurtz@target.com

STEP 7,8,9,10,11,12,13-

In this step, I used Maltego's Footprint L1 machine to perform an in-depth reconnaissance of the target domain, target.com. The Footprint L1 machine automates the process of collecting detailed infrastructure-related information such as DNS records, IP addresses, email addresses, and MX records associated with the domain. It generates graphical map visualizing with various interconnected entities. I then switched to the List View, which provided a structured tabular output. The scan identified multiple IPv4 addresses, DNS names, email addresses, and mail servers.



Type	Entity				
maltego.Netblock	13.109.180.0-13.109.180.255	4	1	100
maltego.IPv4Address	13.109.180.6	1	1	100
maltego.IPv4Address	13.109.180.7	1	1	100
maltego.IPv4Address	13.109.180.8	2	1	100
maltego.IPv4Address	13.109.180.9	2	1	100
maltego.Netblock	146.75.30.0-146.75.30.255	1	1	100
maltego.IPv4Address	146.75.30.187	3	1	100
maltego.Netblock	151.101.130.0-151.101.130.255	1	1	100
maltego.IPv4Address	151.101.130.187	1	1	100
maltego.Netblock	151.101.194.0-151.101.194.255	1	1	100
maltego.IPv4Address	151.101.194.187	1	1	100
maltego.Netblock	151.101.2.0-151.101.2.255	1	1	100
maltego.IPv4Address	151.101.2.187	1	1	100
maltego.Netblock	151.101.46.0-151.101.46.255	1	1	100
maltego.IPv4Address	151.101.46.187	2	1	100
maltego.Netblock	151.101.66.0-151.101.66.255	1	1	100
maltego.IPv4Address	151.101.66.187	1	1	100
maltego.Netblock	205.220.165.0-205.220.165.255	1	1	100
maltego.IPv4Address	205.220.165.243	2	1	100
maltego.DNSName	adaptive-tomcat-qa.global.tgt-pe-test.gcp.cloud.target.com	1	0	100
maltego.DNSName	adaptive-tomcat-uat.global.tgt-pe-test.gcp.cloud.target.com	1	0	100
maltego.DNSName	cartwheel-secure.target.com	1	0	100
maltego.DNSName	contactus.target.com	1	3	100
maltego.DNSName	corporate.target.com	1	1	100
maltego.DNSName	ec.us-central1.tgt-shr-test.gcp.cloud.target.com	1	0	100
maltego.DNSName	goto.target.com	1	0	100
maltego.DNSName	help.target.com	1	3	100
maltego.EmailAddr...	hostmaster@target.com.	1	0	100
maltego.DNSName	intl.target.com	1	0	100
maltego.DNSName	investors.target.com	1	1	100
maltego.DNSName	jobs.target.com	1	0	100
maltego.MXRecord	mxa-0020ab02.gslb.pphosted.com	1	1	100
maltego.MXRecord	mxb-0020ab02.gslb.pphosted.com	1	1	100

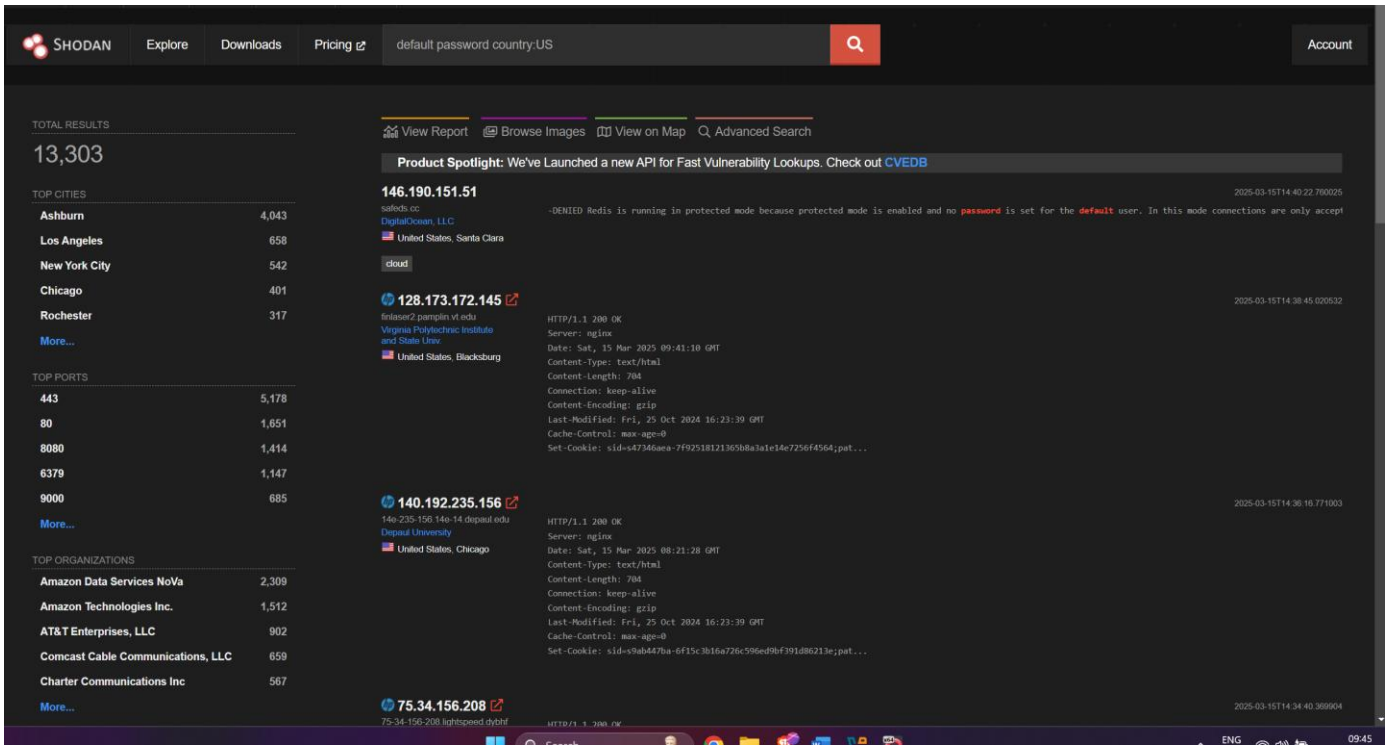
Output - Transform Output

```
[3/15/25, 10:37 AM] INFO ---[ Unified Credits ]--- : 57 of 200 credits remaining. Current quota period ends at April 1, 2025 at 12:00:00 AM Z (from 11 entities)
[3/15/25, 10:37 AM] INFO ---[ Unified Credits ]--- : 57 of 200 credits remaining. Current quota period ends at April 1, 2025 at 12:00:00 AM Z (from 11 entities)
[3/15/25, 10:37 AM] INFO ---[ Unified Credits ]--- : 57 of 200 credits remaining. Current quota period ends at April 1, 2025 at 12:00:00 AM Z (from 11 entities)
[3/15/25, 10:37 AM] INFO ---[ Unified Credits ]--- : 57 of 200 credits remaining. Current quota period ends at April 1, 2025 at 12:00:00 AM Z (from 11 entities)
[3/15/25, 10:37 AM] INFO ---[ Unified Credits ]--- : 57 of 200 credits remaining. Current quota period ends at April 1, 2025 at 12:00:00 AM Z (from 11 entities)
[3/15/25, 10:37 AM] INFO ---[ Unified Credits ]--- : 57 of 200 credits remaining. Current quota period ends at April 1, 2025 at 12:00:00 AM Z (from 11 entities)
[3/15/25, 10:37 AM] INFO ---[ Unified Credits ]--- : 57 of 200 credits remaining. Current quota period ends at April 1, 2025 at 12:00:00 AM Z (from 11 entities)
[3/15/25, 10:37 AM] INFO ---[ Unified Credits ]--- : 57 of 200 credits remaining. Current quota period ends at April 1, 2025 at 12:00:00 AM Z (from 11 entities)
[3/15/25, 10:37 AM] INFO ---[ Unified Credits ]--- : 57 of 200 credits remaining. Current quota period ends at April 1, 2025 at 12:00:00 AM Z (from 11 entities)
[3/15/25, 10:37 AM] INFO ---[ Unified Credits ]--- : 57 of 200 credits remaining. Current quota period ends at April 1, 2025 at 12:00:00 AM Z (from 11 entities)
[3/15/25, 10:37 AM] INFO ---[ Unified Credits ]--- : 57 of 200 credits remaining. Current quota period ends at April 1, 2025 at 12:00:00 AM Z (from 11 entities)
[3/15/25, 10:37 AM] INFO Transform [Utilities] To Netblock [Using natural boundaries] completed in 2 s 3 ms with 11 entities returned (from 11 entities)
[3/15/25, 10:37 AM] INFO Running transform [Utilities] To AS Number [WhoisXML] on 8 entities (from 8 entities)
[3/15/25, 10:38 AM] INFO Transform [Utilities] To AS Number [WhoisXML] completed in 2 s 138 ms with 8 entities returned (from 8 entities)
[3/15/25, 10:38 AM] INFO Running transform [Utilities] To Company (Owner) [WhoisXML] on 8 entities (from 8 entities)
[3/15/25, 10:38 AM] INFO Transform [Utilities] To Company (Owner) [WhoisXML] completed in 2 s 112 ms with 8 entities returned (from 8 entities)
```

8. Shodan

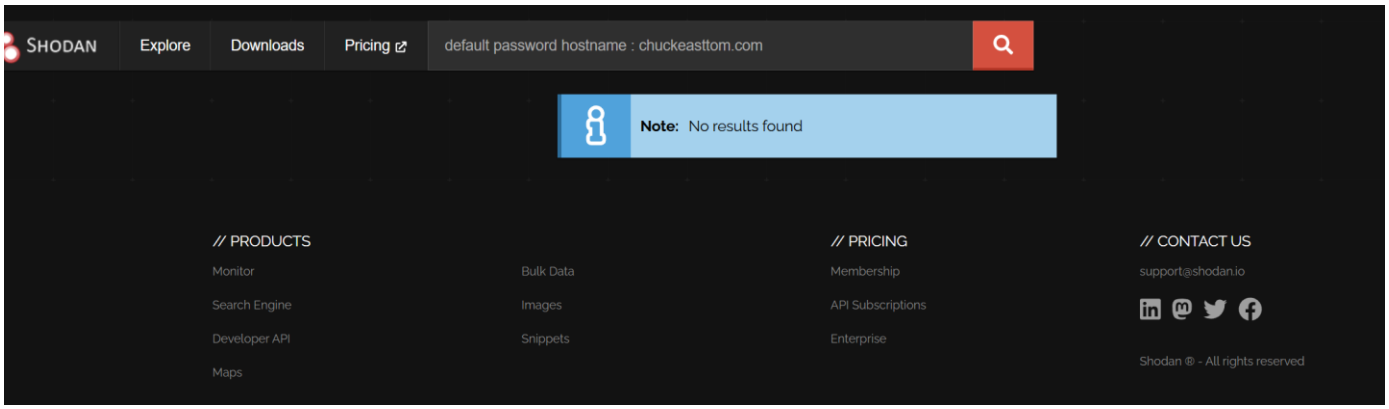
default password country : US

Shodan returned 13,303 results, displaying devices that may have weak or default credentials from various organizations like DigitalOcean, Virginia Polytechnic Institute, and DePaul University. It also identified open ports, with 443 (HTTPS), 80 (HTTP), and 8080 being the most common. One of the concerning results shows a Redis instance with no password set for the default user, indicating a potential security risk.



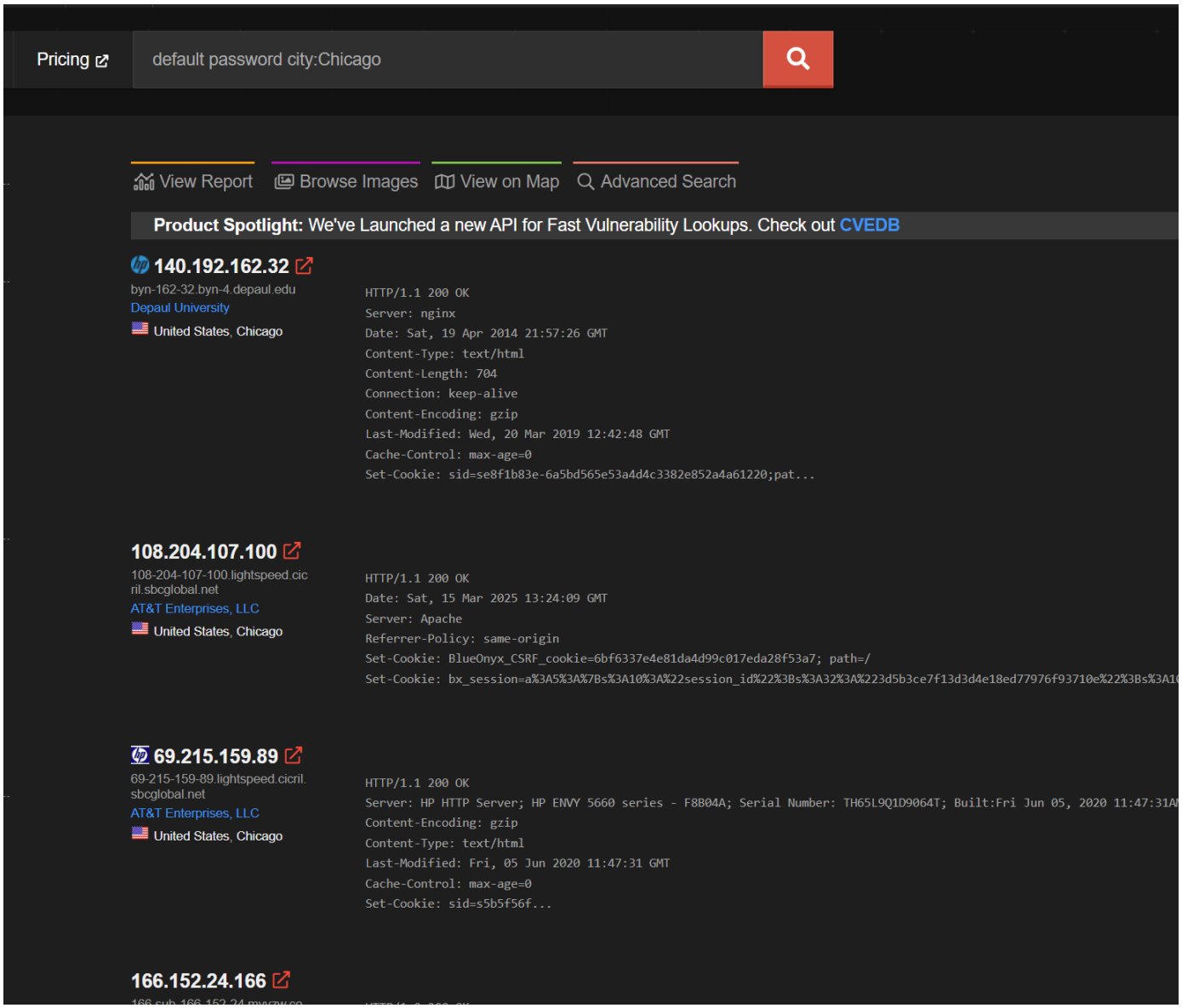
default password hostname : chuckeasttom . com

Shodan did not detect any devices under the hostname chuckeasttom.com that are using default passwords. This could mean either there are no publicly exposed devices linked to this hostname with default credentials, or the devices are properly secured,



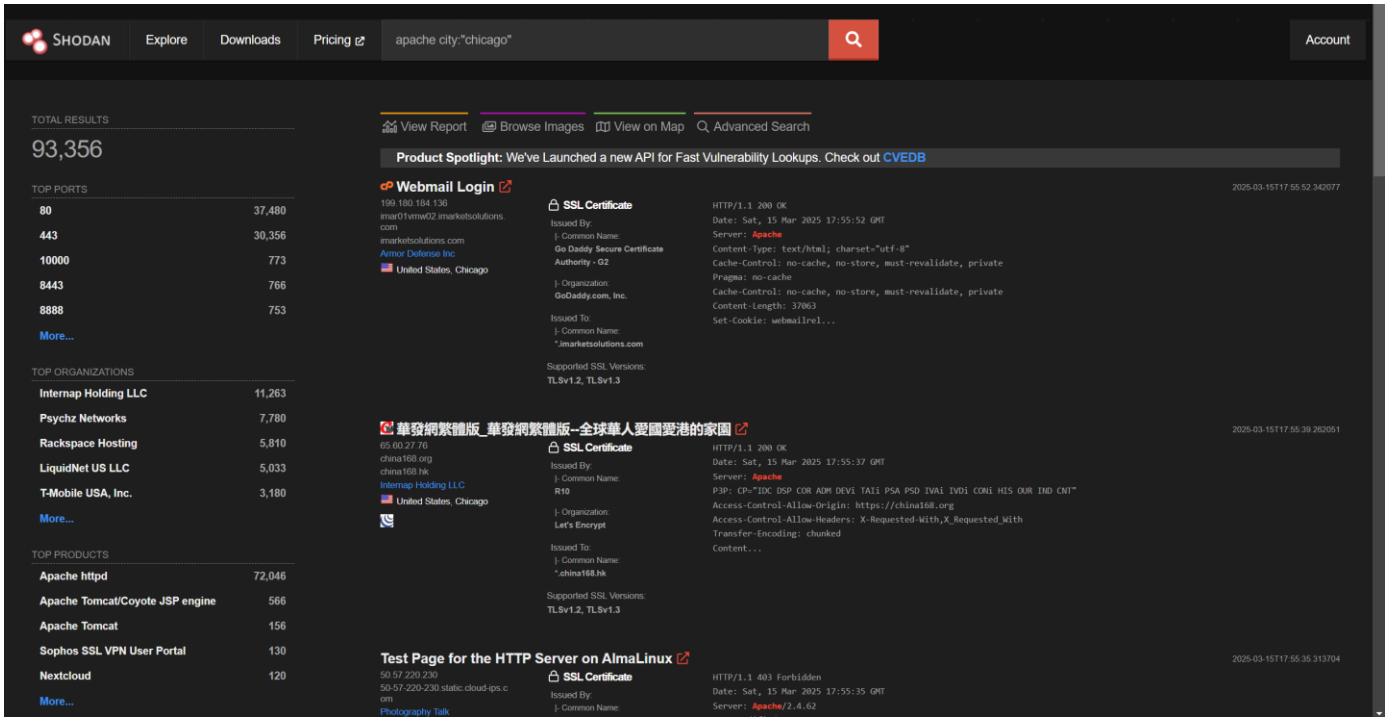
default password city : Chicago

This search filtered Shodan results to identify devices located in the city of Chicago that may still be using default passwords, which is a common security misconfiguration. The results revealed multiple IP addresses including those associated with DePaul University and AT&T Enterprises, showing web servers running nginx and Apache, and even a printer interface (HP ENVY 5660 series) with HTTP headers visible.



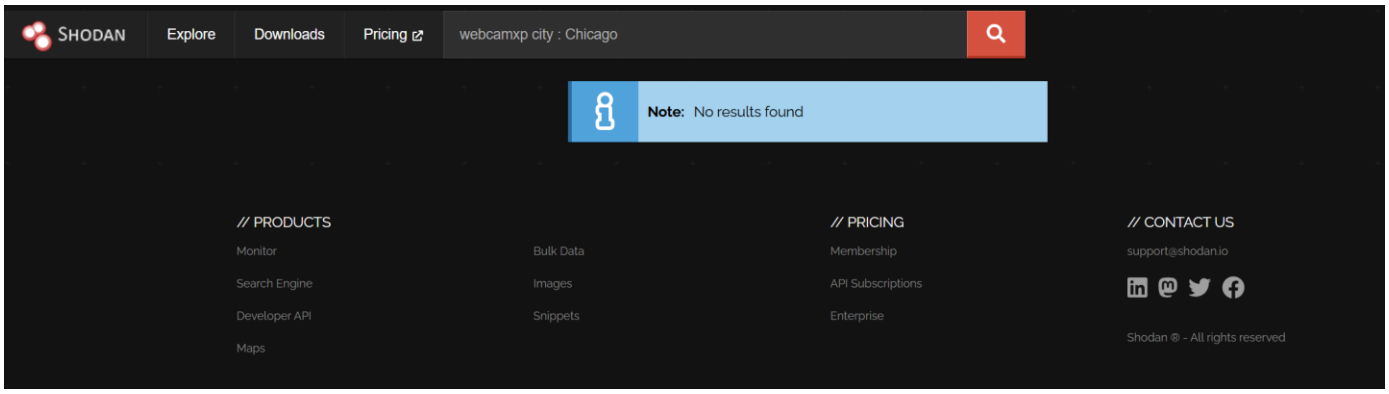
apache city :" chicago "

This search revealed a large number of exposed devices and servers running the Apache HTTP server, along with detailed information about their configurations, SSL certificates, server responses, and host organizations. The results included entities such as Armor Defense Inc., Internap Holding LLC, and others, showcasing Apache-powered login portals, webmail interfaces, and default server pages.



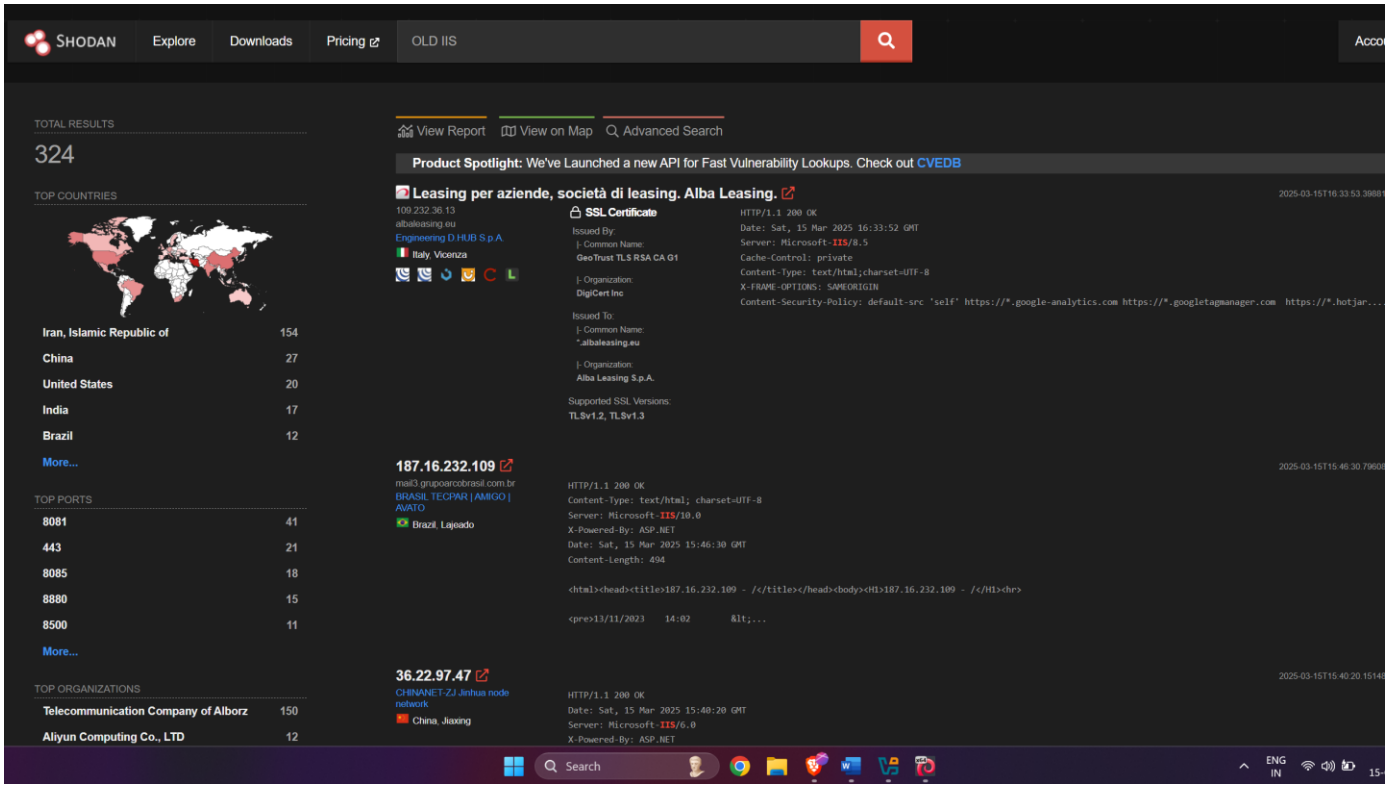
webcamxp city : Chicago

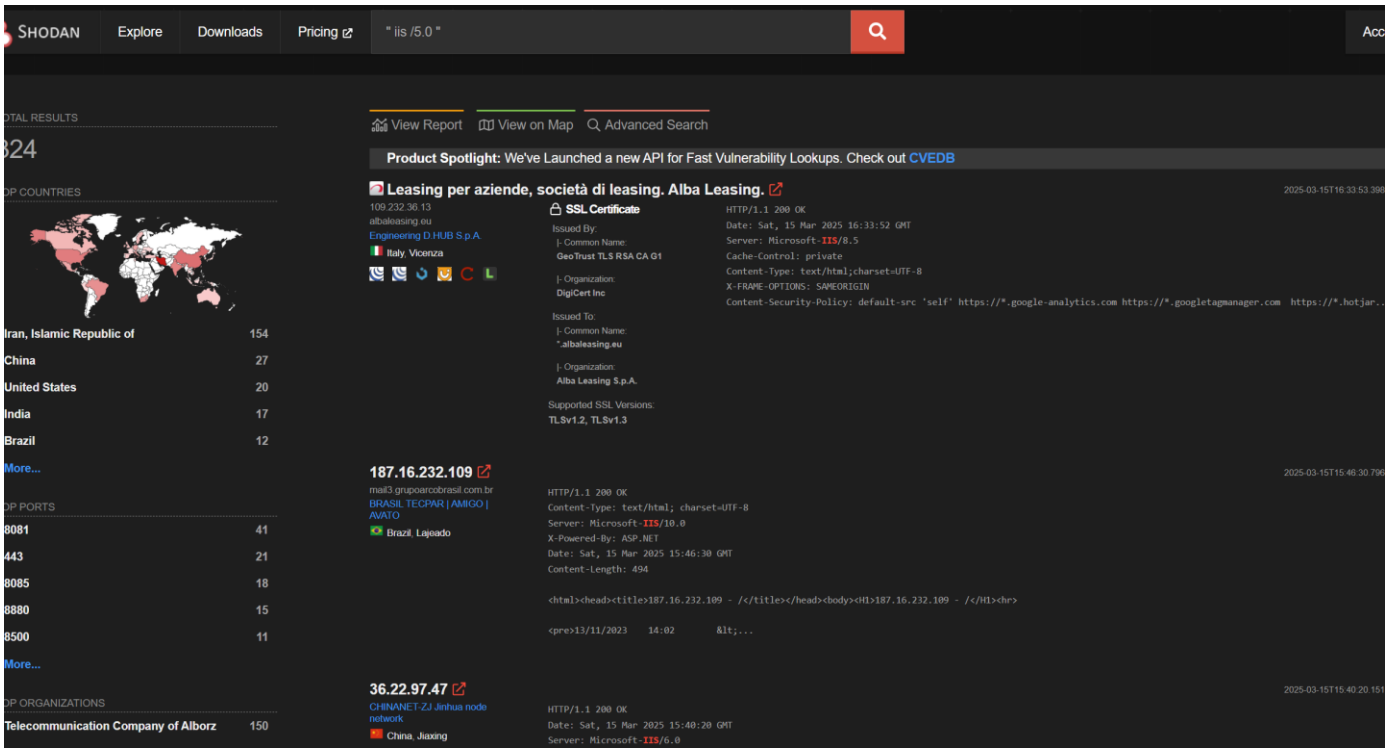
no results were found, indicating that no publicly exposed webcamxp devices were detected in this region. This could either mean that such devices are not in use, are properly secured, or are not indexed by Shodan due to lack of response on scanned ports.



OLD IIS

The search results successfully revealed multiple internet-facing servers running outdated Microsoft IIS versions, such as IIS/5.0 and IIS/6.0. These older server versions are considered vulnerable, as they are no longer supported by Microsoft and may contain several known security flaws.



" iis /5.0 "

several servers across various countries like Brazil, China, and the United States, are still running IIS/5.0 which are highly vulnerable to multiple exploits.