LAB 3 - Reconnaissance

> *GVHD: Ngô Khánh Khoa*
> *Mã môn: NT213.P11.ANTN.1*

Thành viên	MSSV
Vũ Ngọc Quốc Khánh	22520661
Nguyễn Đức Luân	22520825
Đào Hoàng Phúc	22521110

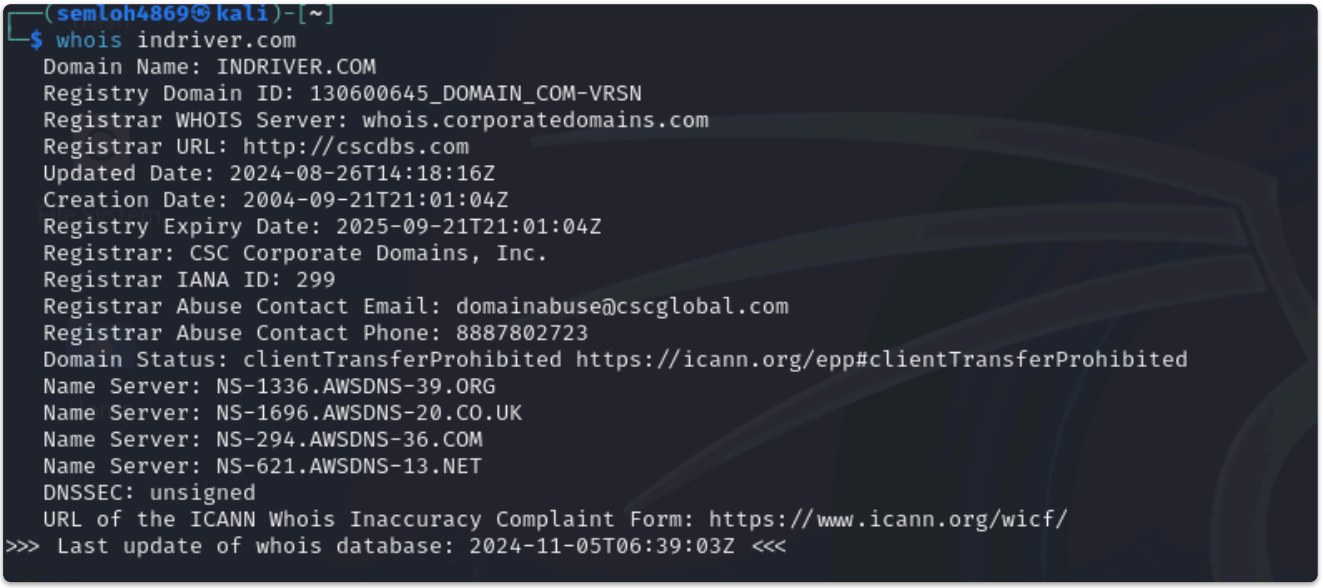
Bài tập 1

Đề bài

Thực hiện lệnh whois lookup với tên miền indriver.com

Các bước thực hiện

Link video: https://youtu.be/lNumU82EMW0



```
Domain Name: indriver.com
Registry Domain ID: 130600645_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2024-08-26T10:18:16Z
Creation Date: 2004-09-21T17:01:04Z
Registrar Registration Expiration Date: 2025-09-21T21:01:04Z
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Manager
Registrant Organization: SUOL INNOVATIONS LTD
Registrant Street: 41 Themistokli Dervi, Hawaii Tower, 1ST Floor, Office 106
Registrant City: Nicosia
Registrant State/Province: Nicosia
Registrant Postal Code: 1066
Registrant Country: CY
Registrant Phone: +357.22667730
Registrant Phone Ext:
Registrant Fax: +357.22667740
Registrant Fax Ext:
Registrant Email: domainmaster@indriver.com
Registry Admin ID:
Admin Name: Domain Manager
Admin Organization: SUOL INNOVATIONS LTD
Admin Street: 41 Themistokli Dervi, Hawaii Tower, 1ST Floor, Office 106
Admin City: Nicosia
Admin State/Province: Nicosia
Admin Postal Code: 1066
Admin Country: CY
Admin Phone: +357.22667730
Admin Phone Ext:
Admin Fax: +357.22667740
Admin Fax Ext:
Admin Email: domainmaster@indriver.com
Registry Tech ID:
Tech Name: Domain Manager
Tech Organization: SUOL INNOVATIONS LTD
Tech Street: 41 Themistokli Dervi, Hawaii Tower, 1ST Floor, Office 106
Tech City: Nicosia
Tech State/Province: Nicosia
Tech Postal Code: 1066
Tech Country: CY
```

+Id của IANA của tên miền trên là gì?
Đáp án: 299
+Tên miền trên được đăng ký khi nào
Đáp án: 21/09/2004
+registar của tên miền trên
Đáp án: CSC Corporate Domains, Inc.
+Công ty nào được sử dụng cho dịch vụ name server
Đáp án: AWS
+Địa chỉ admin contact email cho tên miền trên.
Đáp án: domainmaster@indriver.com

Bài tập 2

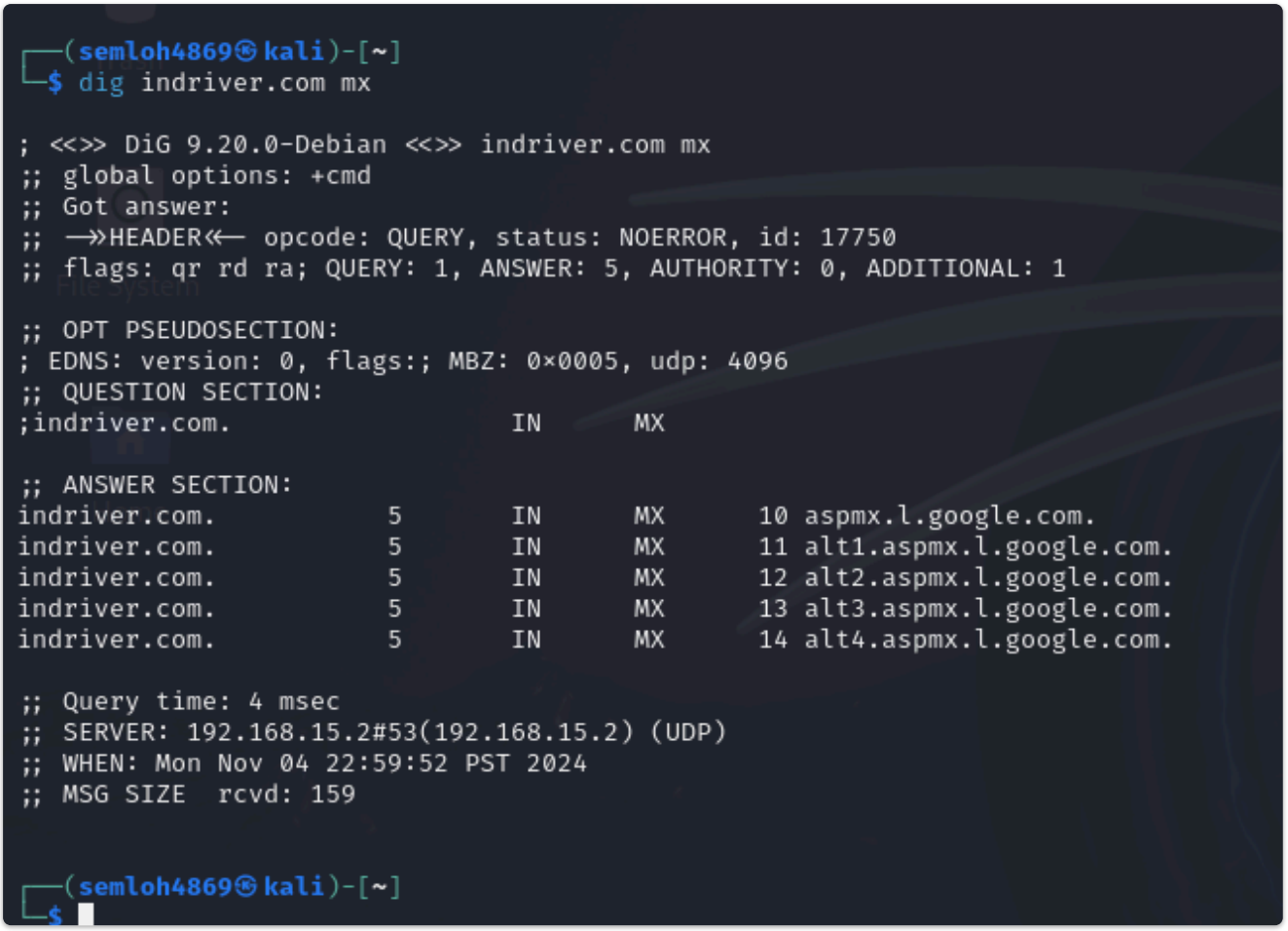
Đề bài

So sánh kết quả khi thực hiện nslookup và dig với loại query là mx với tên miền indriver.com, thông tin nào được cung cấp thêm bởi lệnh DIG, ý nghĩa các thông tin đó như thế nào

Các bước thực hiện

Link video: https://youtu.be/_JapyibzKk8

Kết quả khi dùng lệnh dig với option "mx"



Giải thích:

HEADER Section:

status: NOERROR: Truy vấn thành công, không có lỗi.

flags: qr rd ra: Đánh dấu đây là một truy vấn (qr), với yêu cầu đệ quy (rd) và đã nhận được câu trả lời từ truy vấn đệ quy (ra).

QUESTION SECTION:

Xác nhận rằng truy vấn là cho tên miền indriver.com với loại truy vấn MX.

ANSWER SECTION: Đây là danh sách các bản ghi MX của indriver.com, cùng với độ ưu tiên và tên máy chủ email của Google:

indriver.com. 5 IN MX 10 aspmx.l.google.com.: Bản ghi MX có độ ưu tiên 10, trỏ đến máy chủ aspmx.l.google.com.

indriver.com. 5 IN MX 11 alt1.aspmx.l.google.com.: Độ ưu tiên 11, trỏ đến alt1.aspmx.l.google.com.

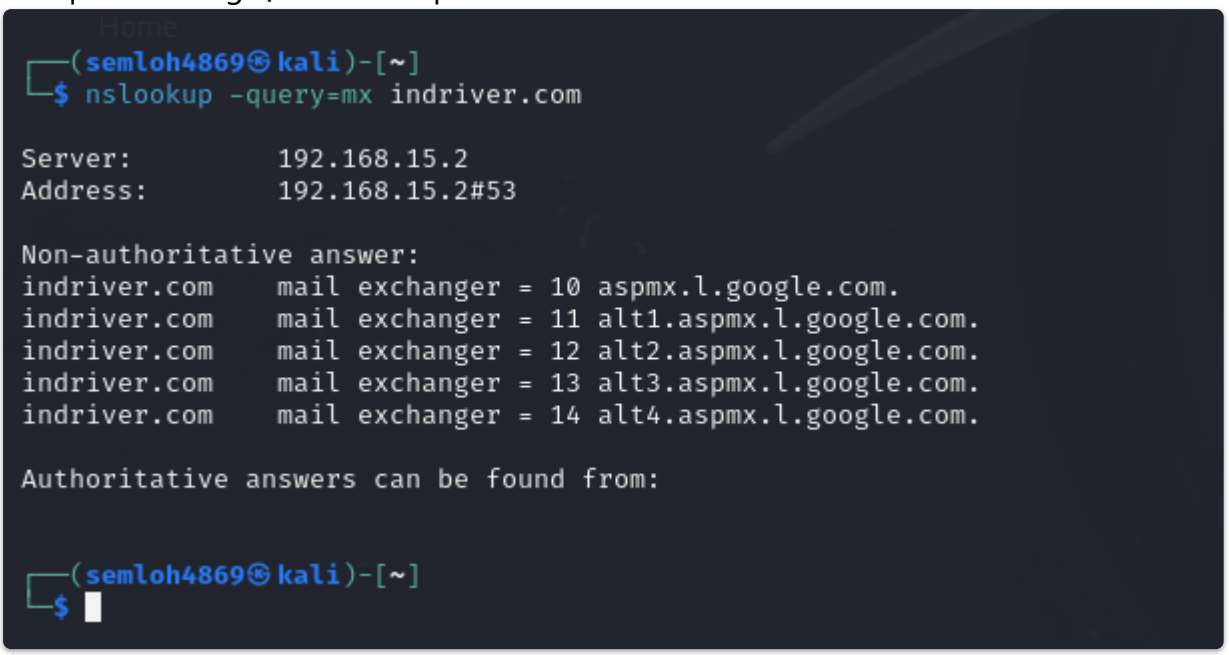
indriver.com. 5 IN MX 12 alt2.aspmx.l.google.com.: Độ ưu tiên 12, trỏ đến alt2.aspmx.l.google.com.

indriver.com. 5 IN MX 13 alt3.aspmx.l.google.com.: Độ ưu tiên 13, trỏ đến alt3.aspmx.l.google.com.
indriver.com. 5 IN MX 14 alt4.aspmx.l.google.com.: Độ ưu tiên 14, trỏ đến alt4.aspmx.l.google.com.
Độ ưu tiên này xác định thứ tự ưu tiên của các máy chủ email, trong đó độ ưu tiên thấp hơn sẽ được thử trước khi đến các máy chủ có độ ưu tiên cao hơn.

Thông tin bổ sung:

Query time: Thời gian để hoàn thành truy vấn là 4 mili giây.
SERVER: Máy chủ DNS thực hiện truy vấn là 192.168.15.2, đây là một địa chỉ IP nội bộ.
WHEN: Thời gian thực hiện truy vấn là Mon Nov 04 22:59:52 PST 2024.
MSG SIZE rcvd: Kích thước thông điệp nhận được là 159 byte.

Kết quả khi dùng lệnh nslookup:



Bài tập 3

Đề bài

Thực hiện truy vấn IP với tên miền indriver.com.

Các bước thực hiện

Link video: https://youtu.be/fSI7PYC2SGQ
+Địa chỉ IP nào map với indriver.com

```
┌──(semloh4869㉿kali)-[~]
└─$ nslookup indriver.com
Server:         192.168.15.2
Address:        192.168.15.2#53

Non-authoritative answer:
Name:   indriver.com
Address: 3.165.82.24
Name:   indriver.com
Address: 3.165.82.80
Name:   indriver.com
Address: 3.165.82.101
Name:   indriver.com
Address: 3.165.82.90
```

+Tên miền nào trỏ đến địa chỉ 134.209.24.248

```
┌──(semloh4869㉿kali)-[~]
└─$ nslookup 134.209.24.248

248.24.209.134.in-addr.arpa     name = inlanefreight.com.

Authoritative answers can be found from:
```

+Mail server nào liên quan đến tên miền indriver.com

```
┌──(semloh4869㉿kali)-[~]
└─$ nslookup -query=mx indriver.com

Server:         192.168.15.2
Address:        192.168.15.2#53

Non-authoritative answer:
indriver.com    mail exchanger = 10 aspmx.l.google.com.
indriver.com    mail exchanger = 11 alt1.aspmx.l.google.com.
indriver.com    mail exchanger = 12 alt2.aspmx.l.google.com.
indriver.com    mail exchanger = 13 alt3.aspmx.l.google.com.
indriver.com    mail exchanger = 14 alt4.aspmx.l.google.com.

Authoritative answers can be found from:
```

aspmx.l.google.com với độ ưu tiên 10
alt1.aspmx.l.google.com với độ ưu tiên 11
alt2.aspmx.l.google.com với độ ưu tiên 12
alt3.aspmx.l.google.com với độ ưu tiên 13
alt4.aspmx.l.google.com với độ ưu tiên 14

Bài tập 4

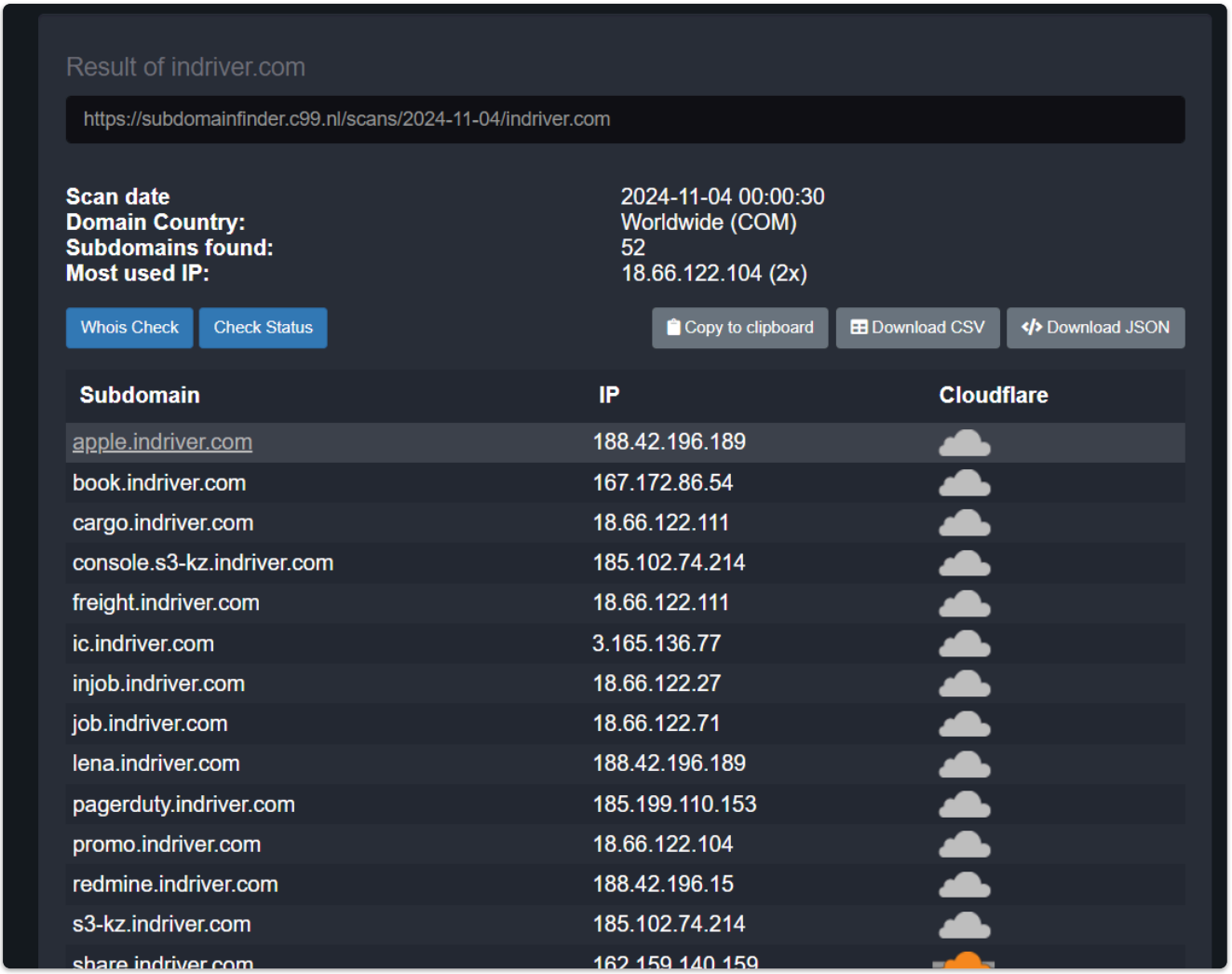
Đề bài

Liệt kê các tên miền phụ của indriver.com, kết quả lưu trong file csv.

Các bước thực hiện

Link video: https://youtu.be/VSCBqLJZ9_M

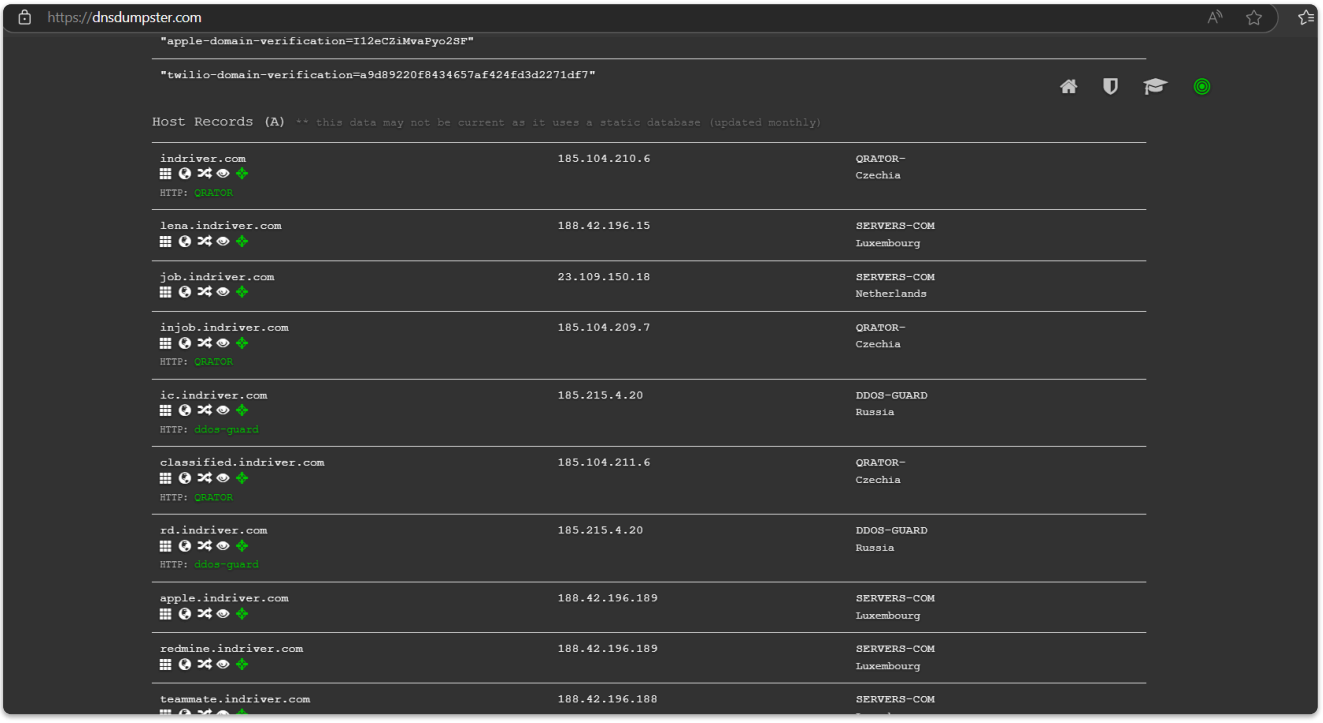
Sử dụng Subdomainfinder : https://subdomainfinder.c99.nl/ nhập domain cần tìm:



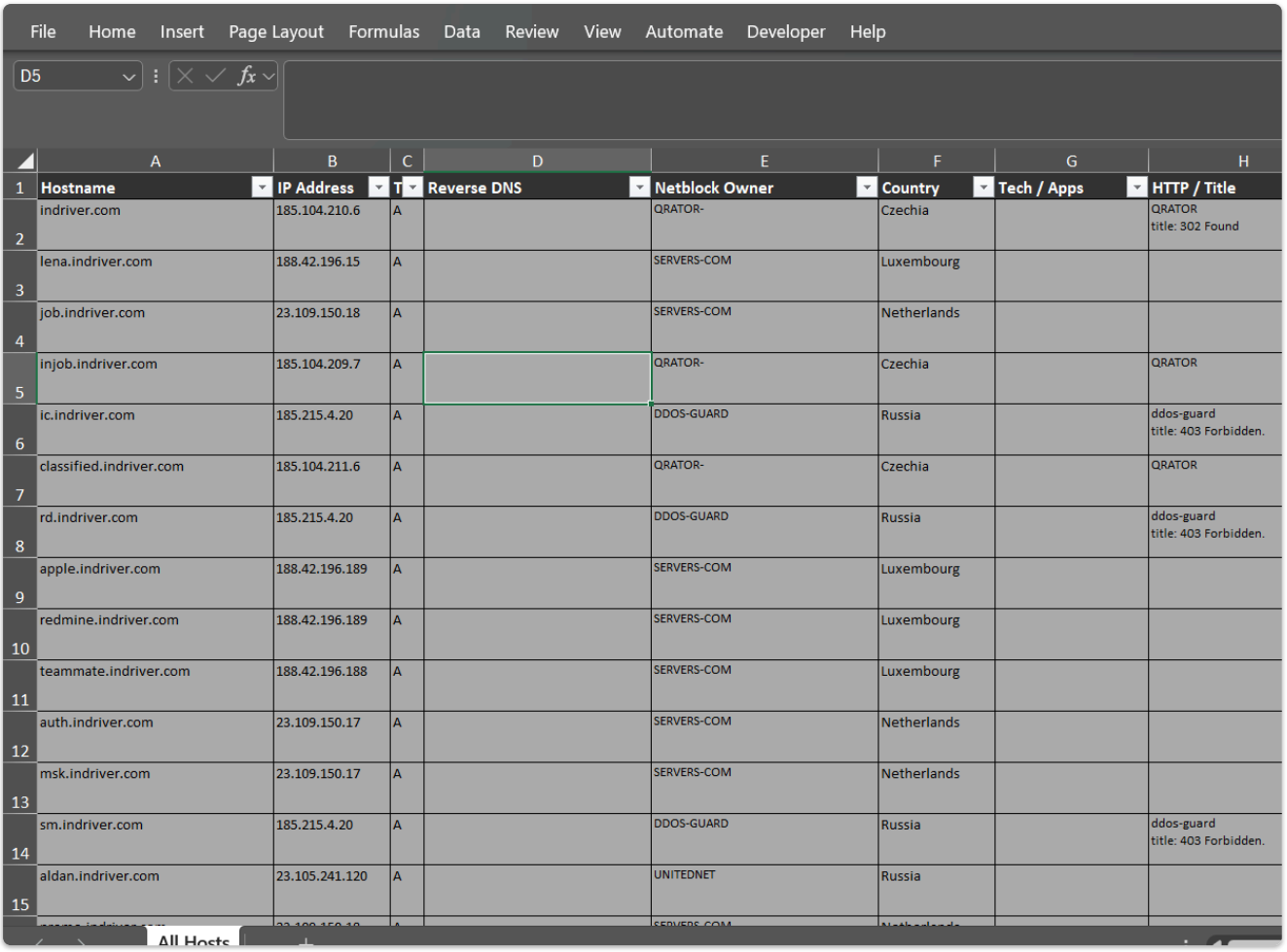
Kết quả lưu file csv:

	A	B	C	D	E	F
1	Subdomain	IP	Cloudflare			
2	apple.indriver.com	188.42.196.189	FALSE			
3	book.indriver.com	167.172.86.54	FALSE			
4	cargo.indriver.com	18.66.122.111	FALSE			
5	console.s3-kz.indriver.com	185.102.74.214	FALSE			
6	freight.indriver.com	18.66.122.111	FALSE			
7	ic.indriver.com	3.165.136.77	FALSE			
8	injob.indriver.com	18.66.122.27	FALSE			
9	job.indriver.com	18.66.122.71	FALSE			
10	lena.indriver.com	188.42.196.189	FALSE			
11	pagerduty.indriver.com	185.199.110.153	FALSE			
12	promo.indriver.com	18.66.122.104	FALSE			
13	redmine.indriver.com	188.42.196.15	FALSE			
14	s3-kz.indriver.com	185.102.74.214	FALSE			
15	share.indriver.com	162.159.140.159	TRUE			
16	sharetrip.indriver.com	18.66.122.71	FALSE			
17	sm.indriver.com	18.66.122.104	FALSE			
18	teammate.indriver.com	188.42.196.188	FALSE			
19	url-checker.indriver.com	185.199.108.153	FALSE			
20	www.indriver.com	3.165.136.76	FALSE			
21						
22						
23						

Sử dụng công cụ khác là https://dnsdumpster.com/ và nhập domain cần tìm.



Kết quả lưu file csv:



	A	B	C	D	E	F	G	H
1	Hostname	IP Address	T	Reverse DNS	Netblock Owner	Country	Tech / Apps	HTTP / Title
2	indriver.com	185.104.210.6	A		QRATOR-	Czechia		QRATOR title: 302 Found
3	lena.indriver.com	188.42.196.15	A		SERVERS-COM	Luxembourg		
4	job.indriver.com	23.109.150.18	A		SERVERS-COM	Netherlands		
5	injob.indriver.com	185.104.209.7	A		QRATOR-	Czechia		QRATOR
6	ic.indriver.com	185.215.4.20	A		DDOS-GUARD	Russia		ddos-guard title: 403 Forbidden.
7	classified.indriver.com	185.104.211.6	A		QRATOR-	Czechia		QRATOR
8	rd.indriver.com	185.215.4.20	A		DDOS-GUARD	Russia		ddos-guard title: 403 Forbidden.
9	apple.indriver.com	188.42.196.189	A		SERVERS-COM	Luxembourg		
10	redmine.indriver.com	188.42.196.189	A		SERVERS-COM	Luxembourg		
11	teammate.indriver.com	188.42.196.188	A		SERVERS-COM	Luxembourg		
12	auth.indriver.com	23.109.150.17	A		SERVERS-COM	Netherlands		
13	msk.indriver.com	23.109.150.17	A		SERVERS-COM	Netherlands		
14	sm.indriver.com	185.215.4.20	A		DDOS-GUARD	Russia		ddos-guard title: 403 Forbidden.
15	aldan.indriver.com	23.105.241.120	A		UNITEDNET	Russia		

Bài tập 5

Đề bài

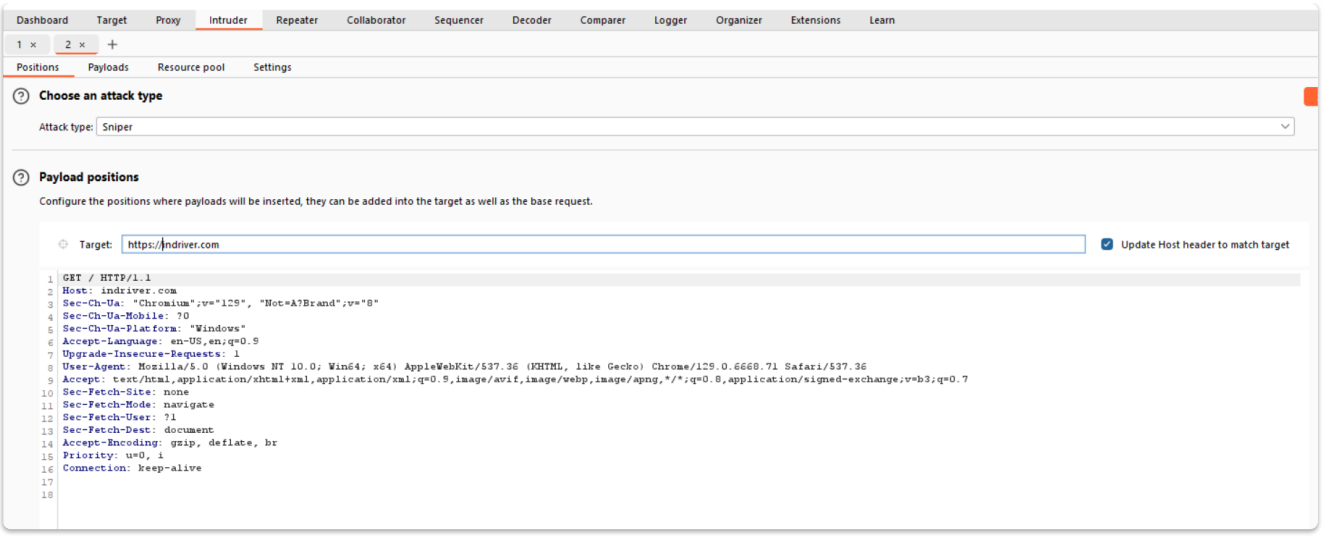
Dựa vào các tên miền phụ đã tìm kiếm được ở bài tập 1 và các tên miền đã bruteforce được thêm bằng burpsuite intruder. Phân loại các tên miền có kết quả trả về status code 200 và các tên miền có kết quả trả về khác.

Các bước thực hiện

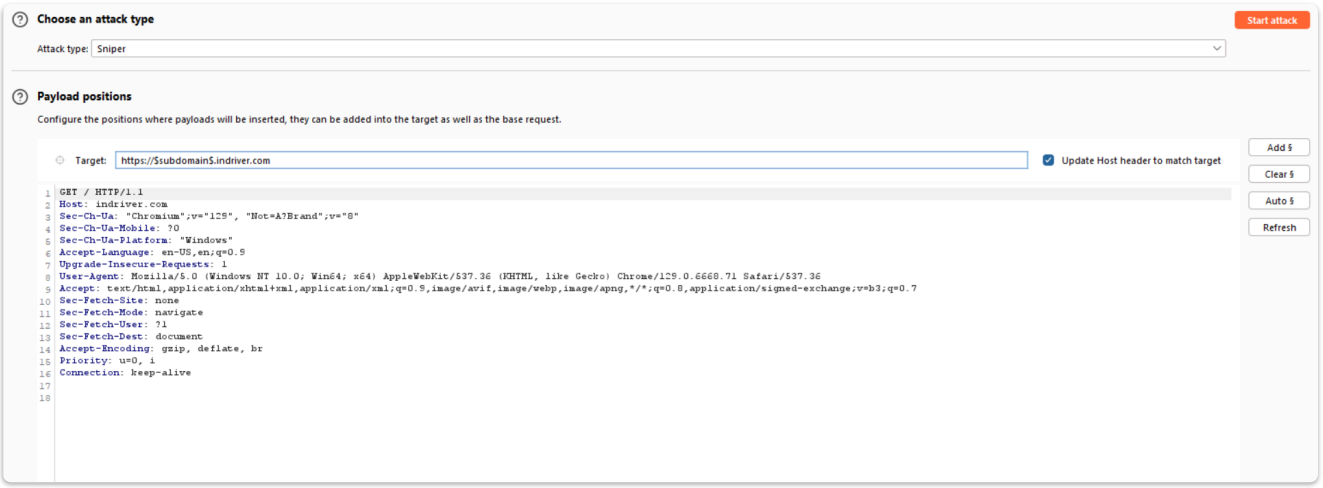
Link video: https://youtu.be/hogIdhkKJEo

+Sử dụng công cụ Burp Suite:

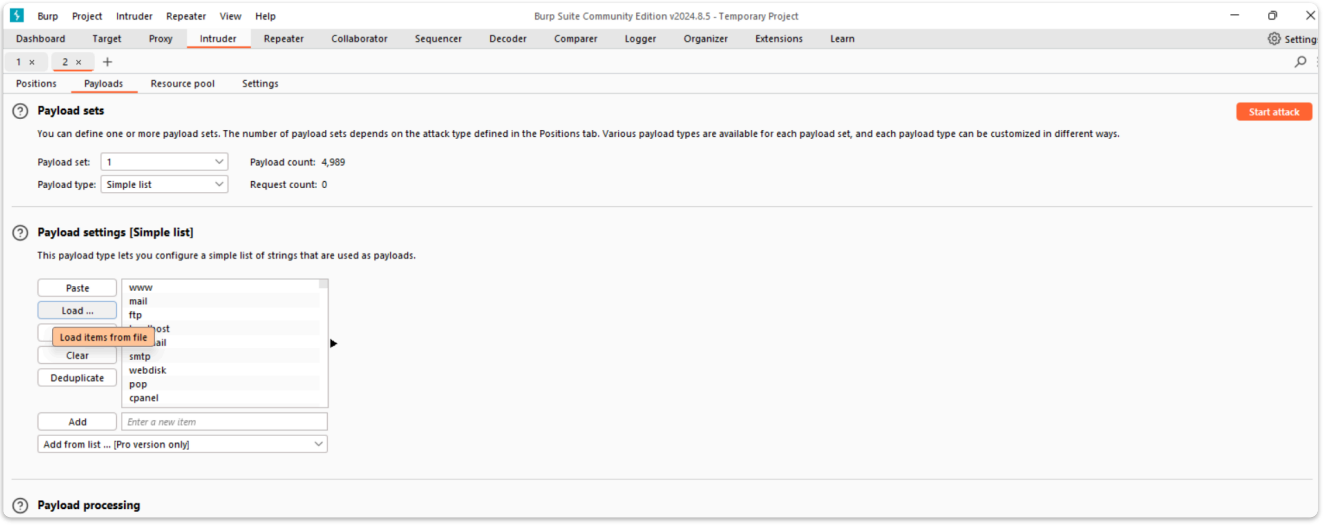
Bước 1: mở Browser và truy cập tên miền indriver.com và chọn một gói tin đem vào Intruder:



Bước 2: Thêm subdomain vào url để tìm kiếm, sử dụng nút Add "$"

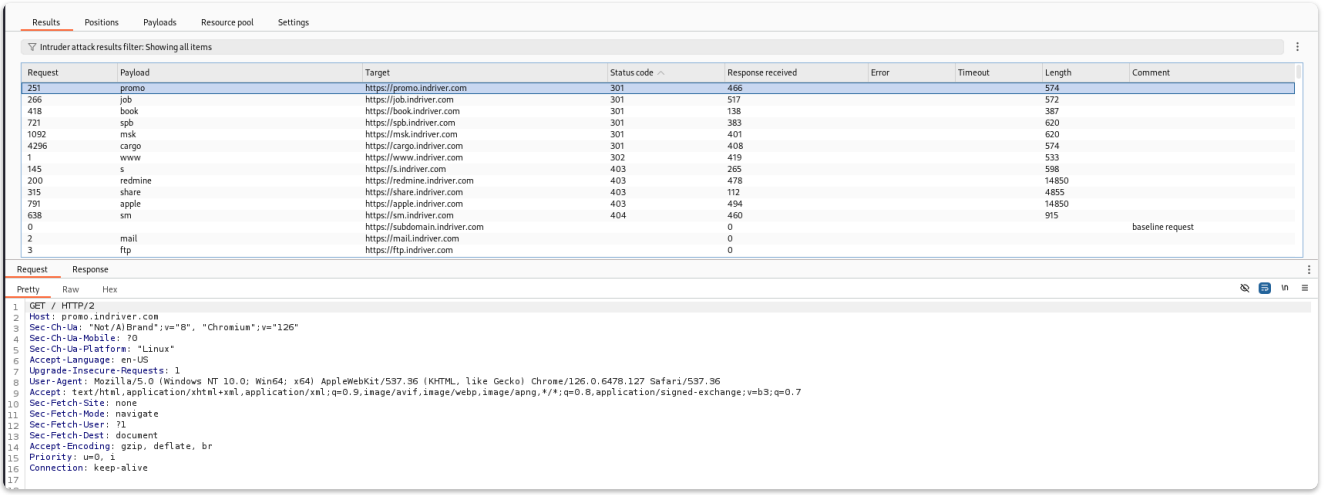


Bước 3: Qua tab payload, tiến hành load list subdomain vào



Bước 4: Start attack và kiểm tra kết quả trả về, có thể tuỳ chỉnh thời gian giữa 2 câu request tại Resource pool để phù hợp với tốc độ trả về của trang web cần tìm kiếm, tránh việc trang

web bị ddos.



Từ kết quả thu được cho thấy không có tên miền nào có phản hồi là 200. Các tên miền có phản hồi khác bao gồm:
promo.indriver.com
job.indriver.com
book.indriver.com
spb.indriver.com
msk.indriver.com
cargo.indriver.com
www.indriver.com
s.indriver.com
redmine.indriver.com
share.indriver.com
apple.indriver.com
sm.indriver.com
Các tên miền này có các phản hồi trạng thái khác nhau như 301, 302, 403, hoặc 404.

Bài tập 6

Link youtube: https://www.youtube.com/watch?v=Kmun3AuTYyA

Đề bài

Ghi nhận lại các địa chỉ IP của tên miền phụ tìm được của *.indriver.com. Kết quả lưu trong file csv.

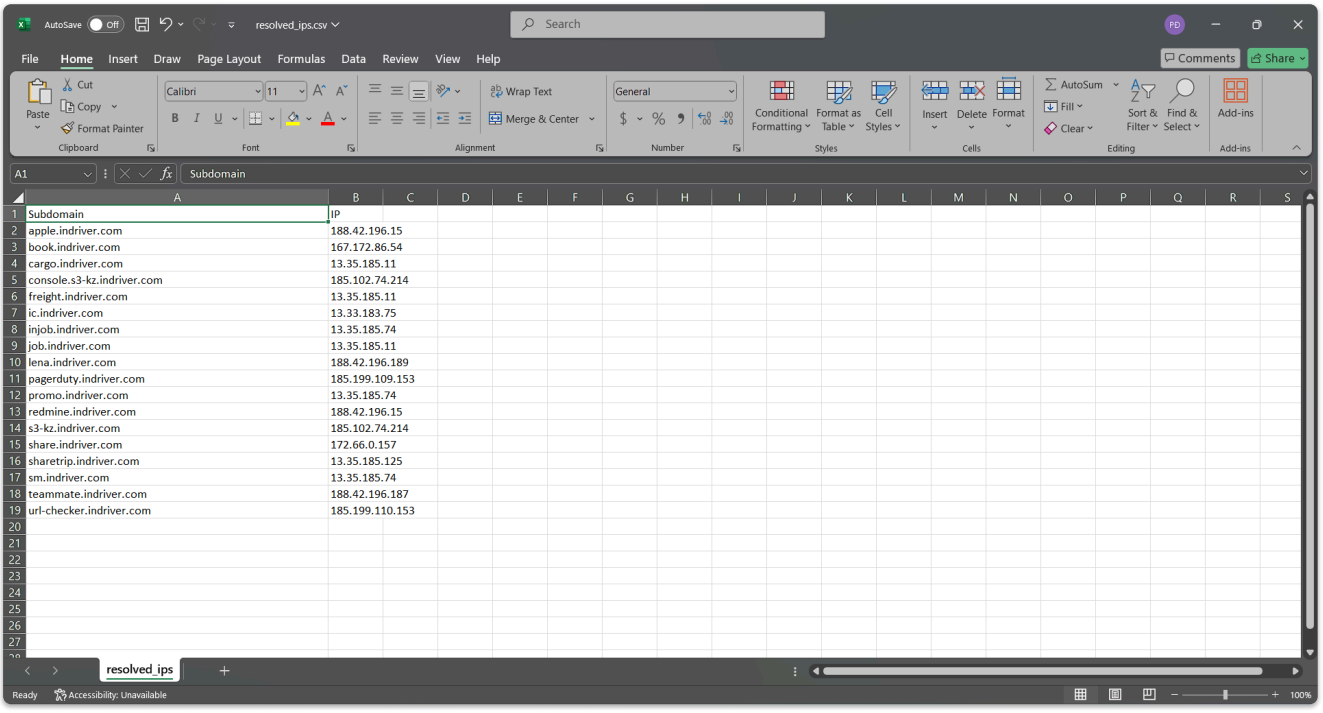
Các bước thực hiện

Thực hiện chạy bash script duyệt qua các subdomain kiếm được trong file csv từ câu trên và thực hiện nslookup từng subdomain

```
#!/bin/bash

# Define input and output files
```

```
input_file="domains.csv"  # Change this to the path of your domain list
file
output_file="resolved_ips.csv"

# Initialize CSV file with header
echo "Subdomain,IP" > "$output_file"

# Loop through each line in the input file, skipping the header
tail -n +2 "$input_file" | while IFS=, read -r subdomain _ ; do
    # Skip empty lines
    if [[ -z "$subdomain" ]]; then
        continue
    fi

    # Perform nslookup and extract the IP address
    resolved_ip=$(nslookup "$subdomain" 2>/dev/null | awk '/^Address: / {
print $2; exit }')

    # If IP is found, append to the CSV file
    if [[ -n "$resolved_ip" ]]; then
        echo "$subdomain,$resolved_ip,$cloudflare" >> "$output_file"
    else
        echo "$subdomain,No IP found,$cloudflare" >> "$output_file"
    fi
done

echo "IP resolution completed. Results saved in $output_file."
```

Kết quả chạy lệnh



Subdomain	IP
apple.indriver.com	188.42.196.15
book.indriver.com	167.172.86.54
cargo.indriver.com	13.35.185.11
console.s3-kz.indriver.com	185.102.74.214
freight.indriver.com	13.35.185.11
ic.indriver.com	13.33.183.75
injob.indriver.com	13.35.185.74
job.indriver.com	13.35.185.11
lena.indriver.com	188.42.196.189
pagerduty.indriver.com	185.199.109.153
promo.indriver.com	13.35.185.74
redmine.indriver.com	188.42.196.15
s3-kz.indriver.com	185.102.74.214
share.indriver.com	172.66.0.157
sharetrip.indriver.com	13.35.185.125
sm.indriver.com	13.35.185.74
teammate.indriver.com	188.42.196.187
url-checker.indriver.com	185.199.110.153

Bài tập 7

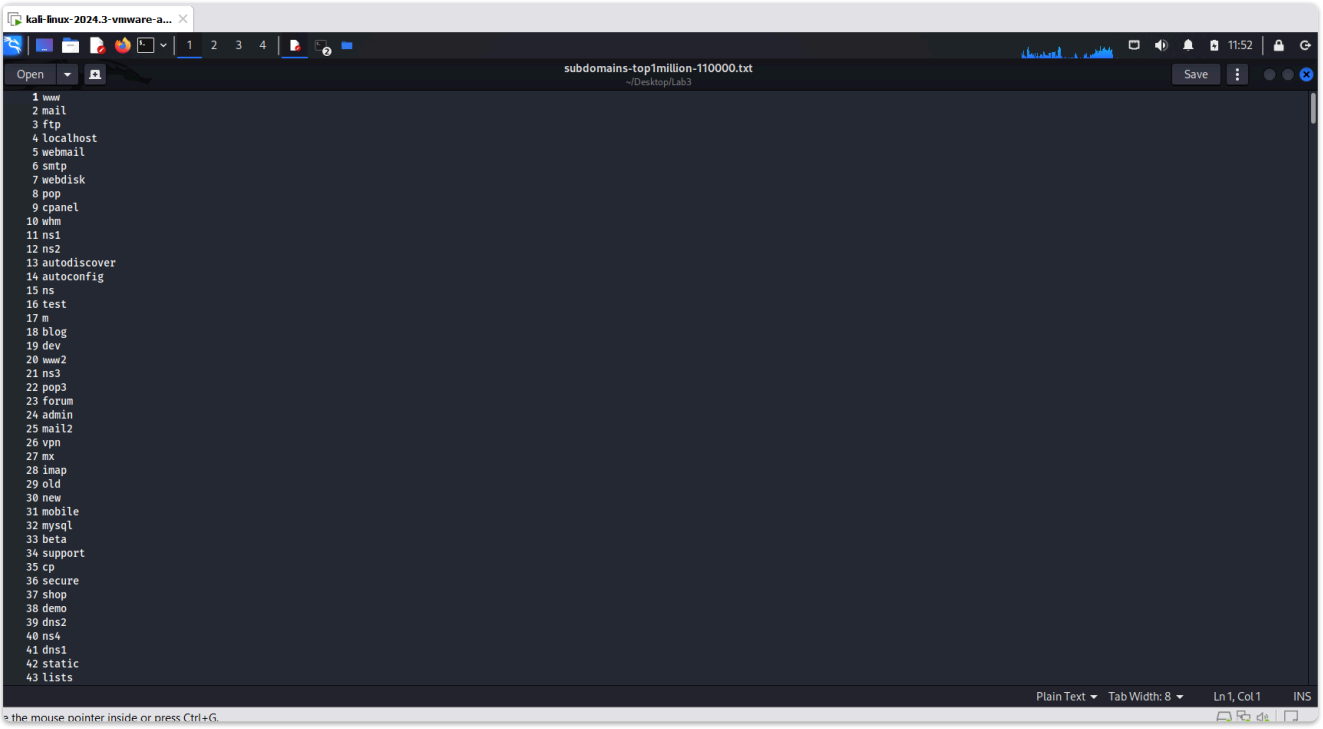
Link video: https://www.youtube.com/watch?v=k9jDkE8jlW4

Đề bài

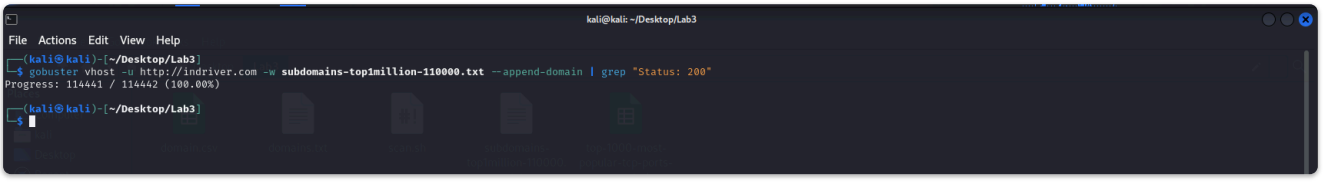
Brute-force các vhosts với trang web indriver.com, có tên miền nào trả về status-code 200 không?

Các bước thực hiện

Tải file subdomains-top1million-110000.txt từ repository https://github.com/danielmiessler/SecLists



Chạy lệnh `gobuster vhost -u http://indriver.com -w subdomains-top1million-110000.txt --append-domain | grep "Status: 200"` không cho kết quả nào trả về status 200



Bài tập 8

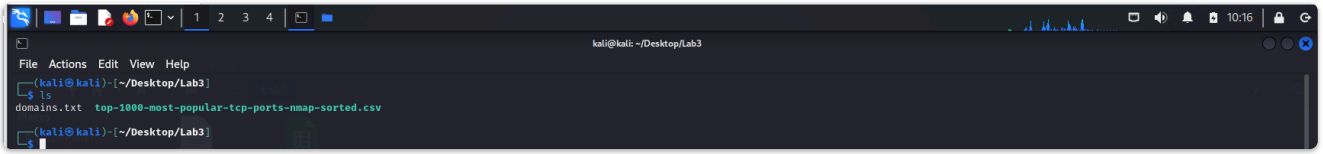
Link video: https://www.youtube.com/watch?v=amPMcHa_1Xg

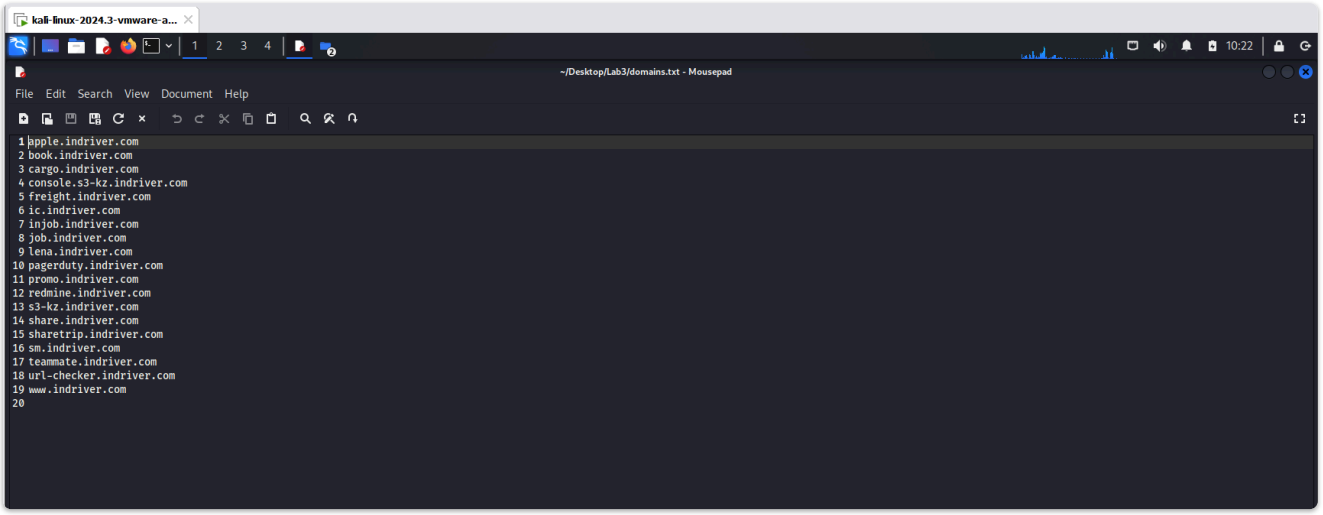
Đề bài

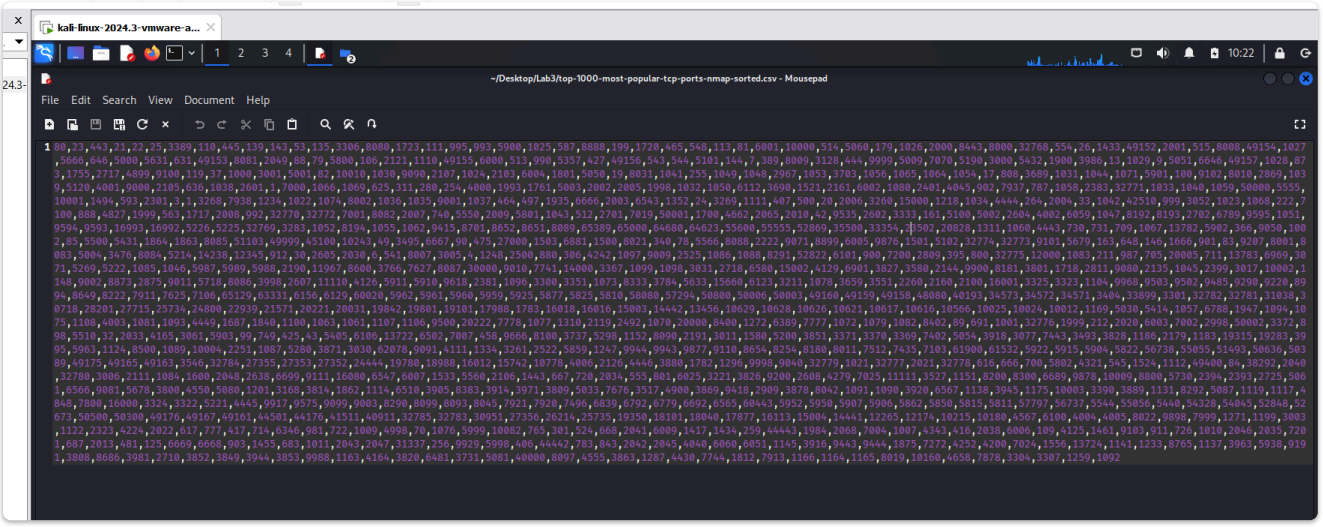
Thực hiện scan 1000 port phổ biến trên các danh sách IP tìm được của *.indriver.com. Báo cáo kết quả tìm được trong file csv.

Các bước thực hiện

Ta thực hiện tải file `top-1000-most-popular-tcp-ports-nmap-sorted.csv` từ link github và tạo file domains.txt chỉ có subdomains từ file domains.csv ở câu 6





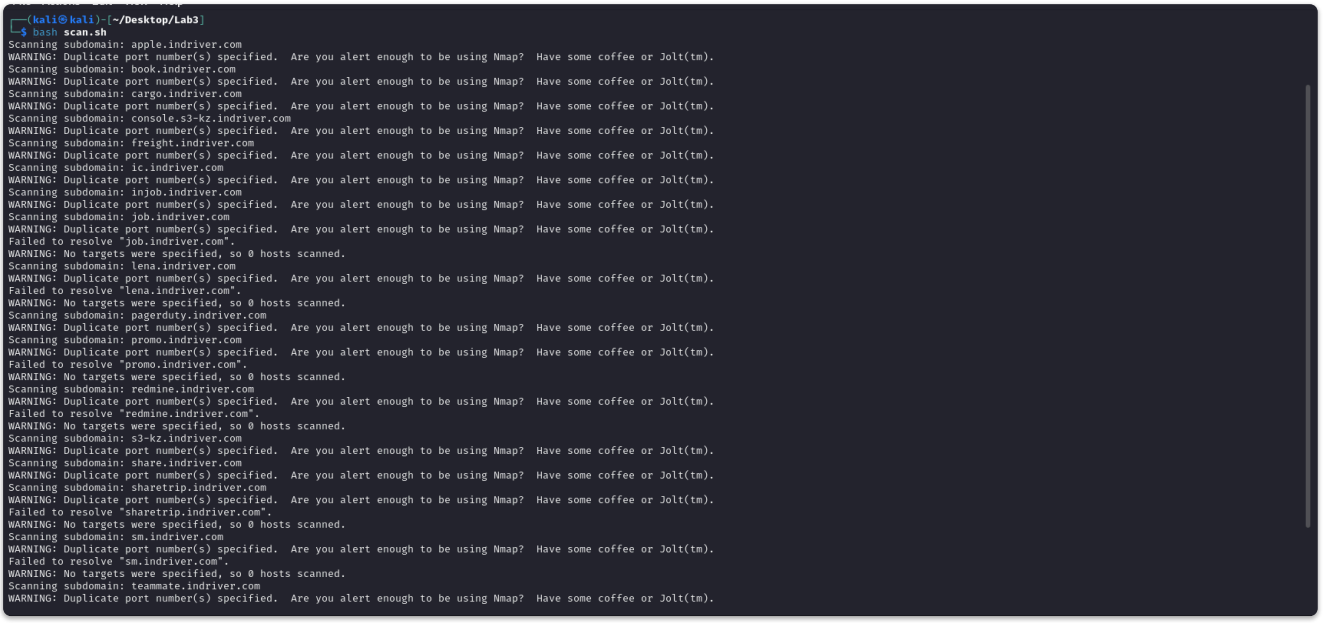


Chạy script sau để scan port của các subdomains:

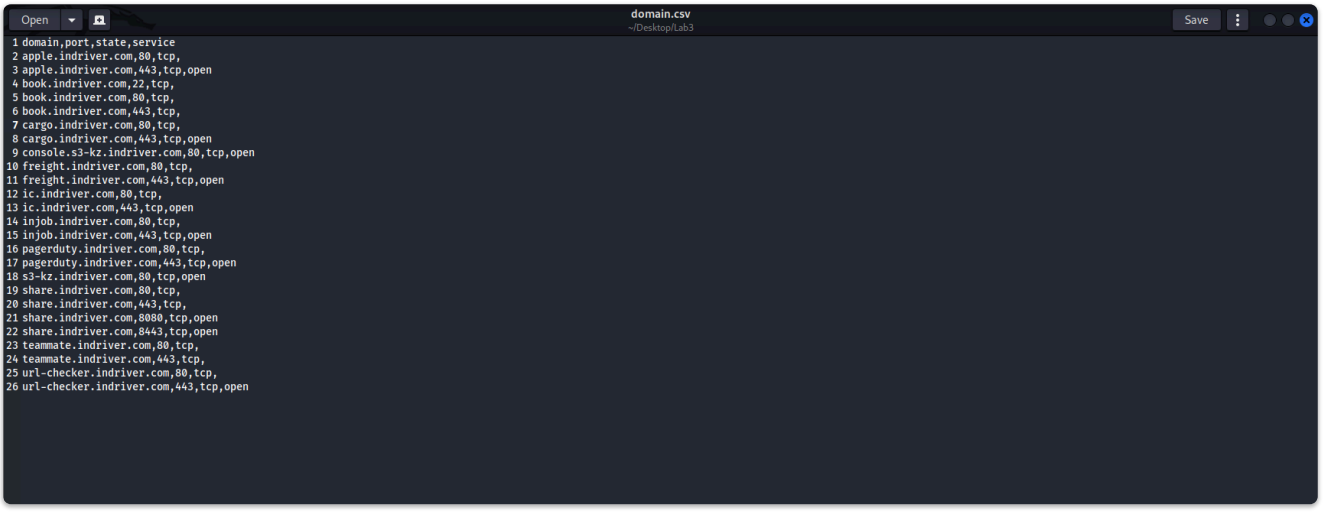
```
!/bin/bash

# Đọc cổng từ tệp CSV và chuyển đổi chúng thành chuỗi cổng phân tách bằng dấu phẩy
port=$(tr '\n' ',' < top-1000-most-popular-tcp-ports-nmap-sorted.csv | sed 's/,$//')

# Xuất header vào file CSV
if [ ! -f domain.csv ]; then
    echo "domain,port,state,service" > domain.csv
fi

# Đọc từng subdomain từ file domains.txt và quét từng subdomain với các port đã chỉ định
```

```
while IFS= read -r domain; do
    # Kiểm tra nếu dòng trong file không rỗng
    if [[ -n "$domain" ]]; then
        # Quét domain với nmap và xuất kết quả vào file CSV
        echo "Scanning subdomain: $domain"
        # Sử dụng lệnh nmap và định dạng lại kết quả để ghi vào CSV
        nmap -sS -T4 -p "$port" "$domain" | awk -v domain="$domain" '
        BEGIN {
            FS="[: /]";
            OFS=","
        }
        /open/ {
            print domain, $1, $2, $3
        }' >> domain.csv
    fi
done < domains.txt
```

Chạy script



File kết quả domain.csv



Bài tập 9

Link video: https://www.youtube.com/watch?v=xh_6kf-LtcY

Đề bài

Xác định phiên bản Apache được sử dụng của web tuoitre.uit.edu.vn

Các bước thực hiện

Sử dụng công cụ wappalyzer ta lấy được version của Apache là 2.4.57

Bài tập 10

Link video: https://www.youtube.com/watch?v=xh_6kf-LtcY

Đề bài

CMS nào được sử dụng của trang web tuoitre.uit.edu.vn

Các bước thực hiện

Sử dụng công cụ wappalyzer ta thấy rằng CMS là Drupal 7

Bài tập 11

Link video: https://www.youtube.com/watch?v=xh_6kf-LtcY

Đề bài

Hệ điều hành và webserver nào được sử dụng của trang web tuoitre.uit.edu.vn

Các bước thực hiện

Sử dụng công cụ wappalyzer ta thấy rằng OS là CentOS và webserver là Apache HTTP Server

Bài tập 12

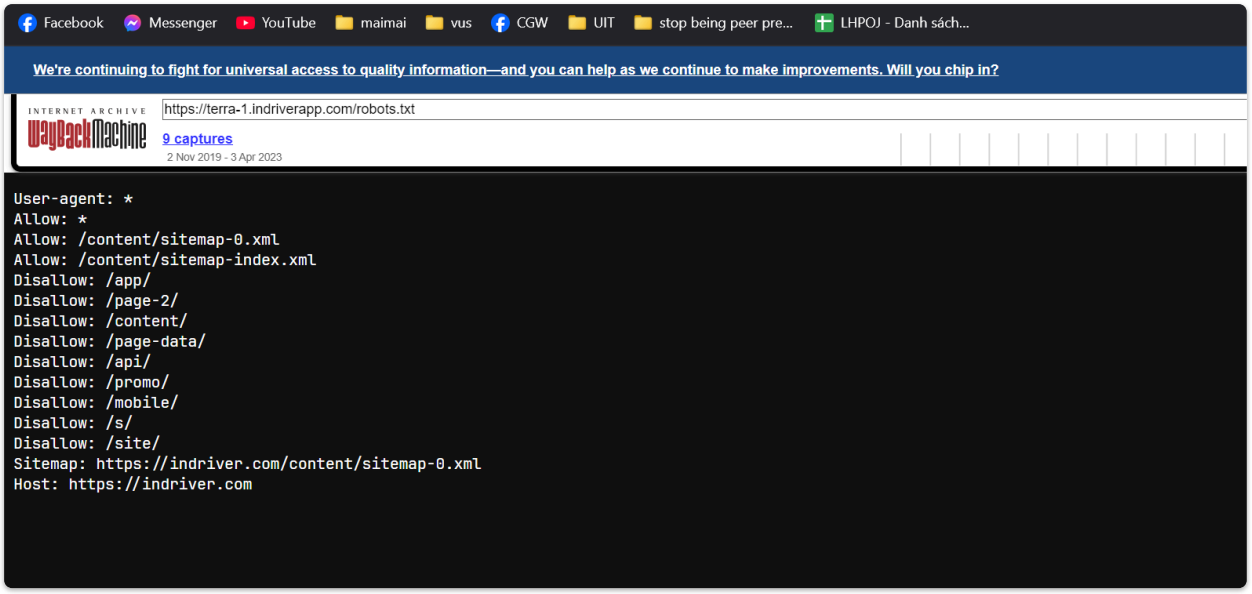
Link video: link

Đề bài

Sử dụng https://web.archive.org/ tìm kiếm và ghi nhận lại dữ liệu quá khứ các tên miền phụ không còn tồn tại hiện nay của terra-1.indriverapp.com. File https://terra-1.indriverapp.com/robots.txt có chứa nội dung gì

Các bước thực hiện

- Có thể tìm thấy các tên miền không còn tồn tại của trang web terra-1.indriverapp.com bằng Internet Archiver và chọn vào tab URLs.
- Có thể tìm thấy file https://terra-1.indriverapp.com/robots.txt bằng cách nhấn vào URL trong tab URLs



Bài tập 13

Link video: link

Đề bài

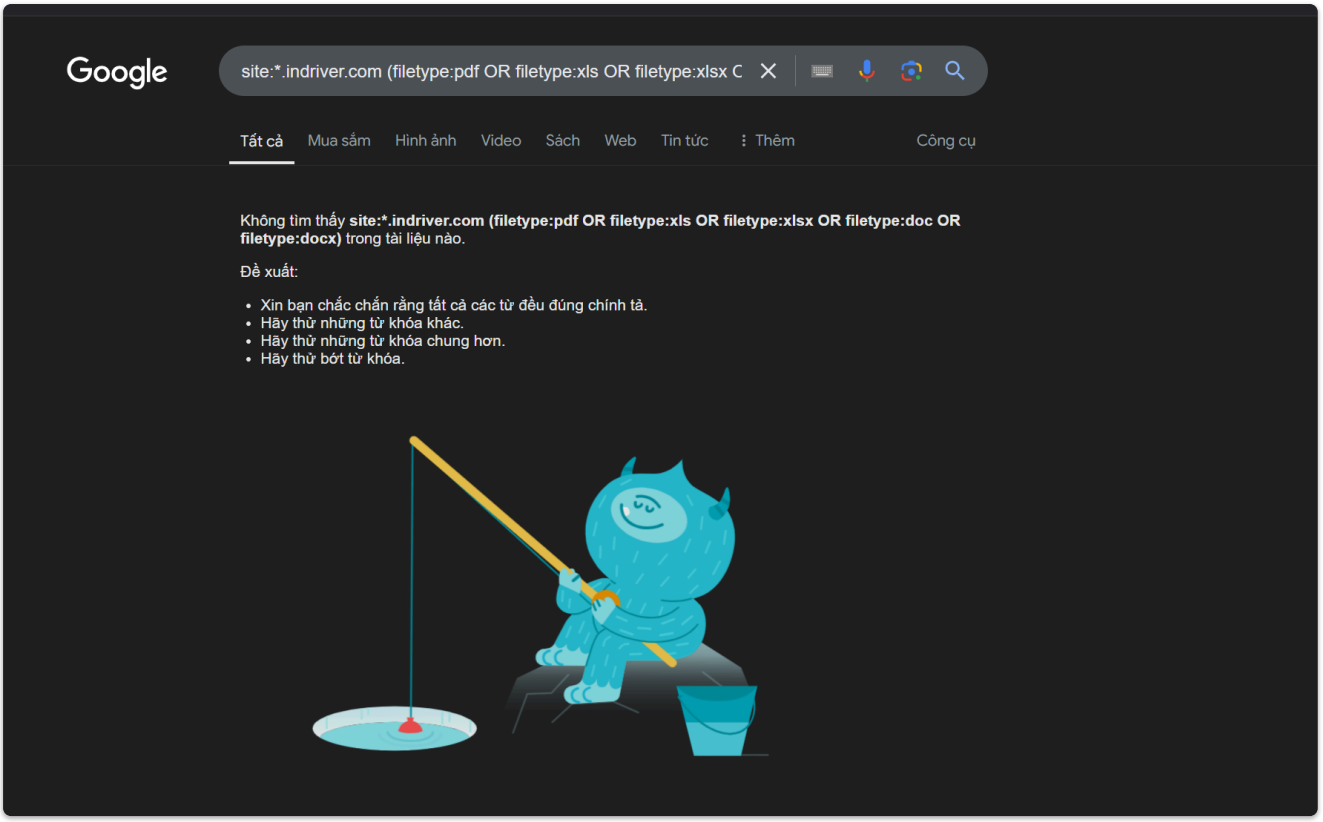
Tìm kiếm các tập tin pdf, excel, word, trên *.indriver.com.

Các bước thực hiện

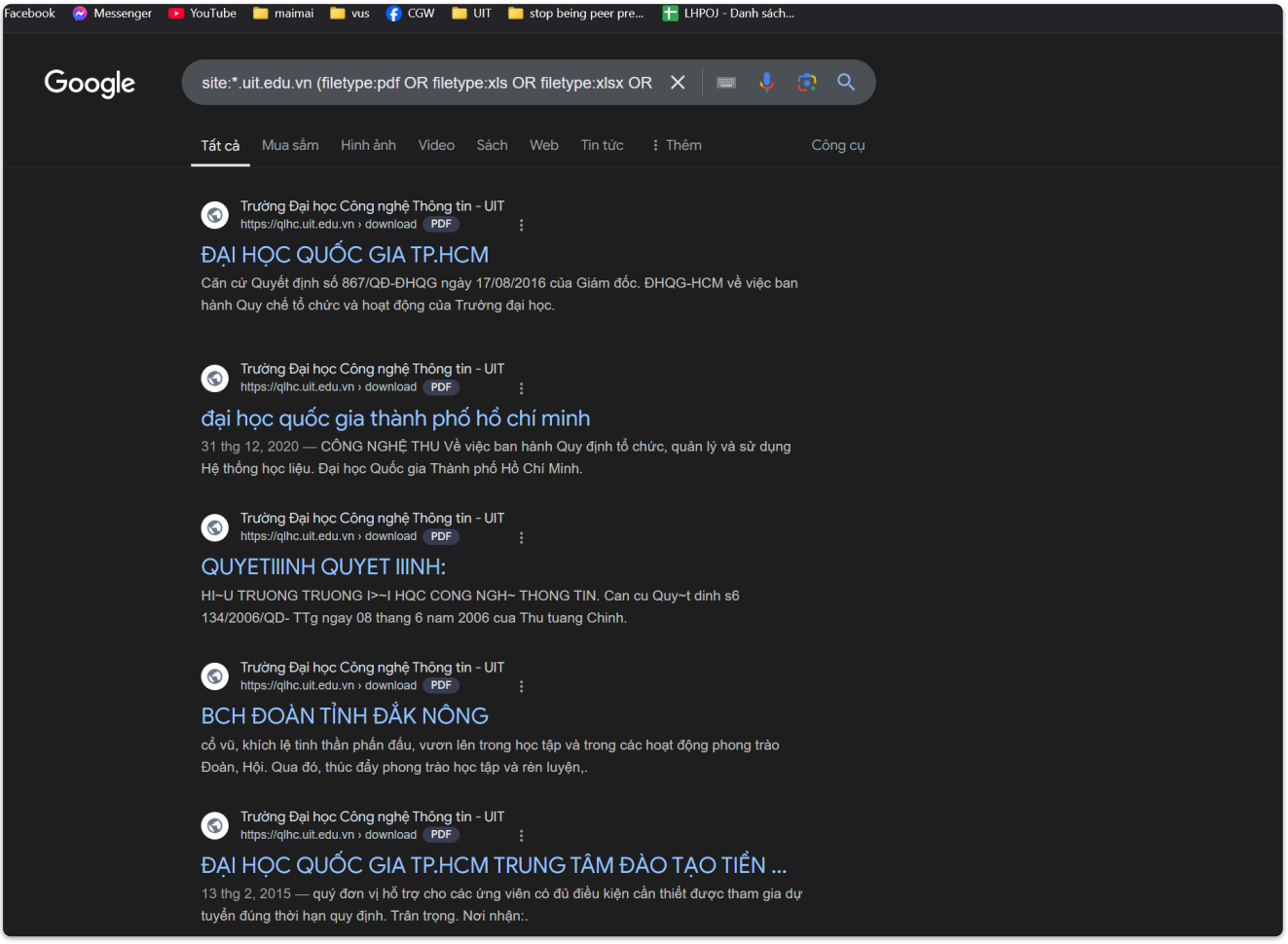
Ta có thể dùng đoạn text sau để tìm kiếm

```
site:*.indriver.com filetype:pdf
site:*.indriver.com filetype:doc
site:*.indriver.com filetype:docx
site:*.indriver.com filetype:xls
site:*.indriver.com filetype:xlsx
```

Kết quả trả về



Thử tìm kiếm với domain *.uit.edu.vn



Bài tập 14

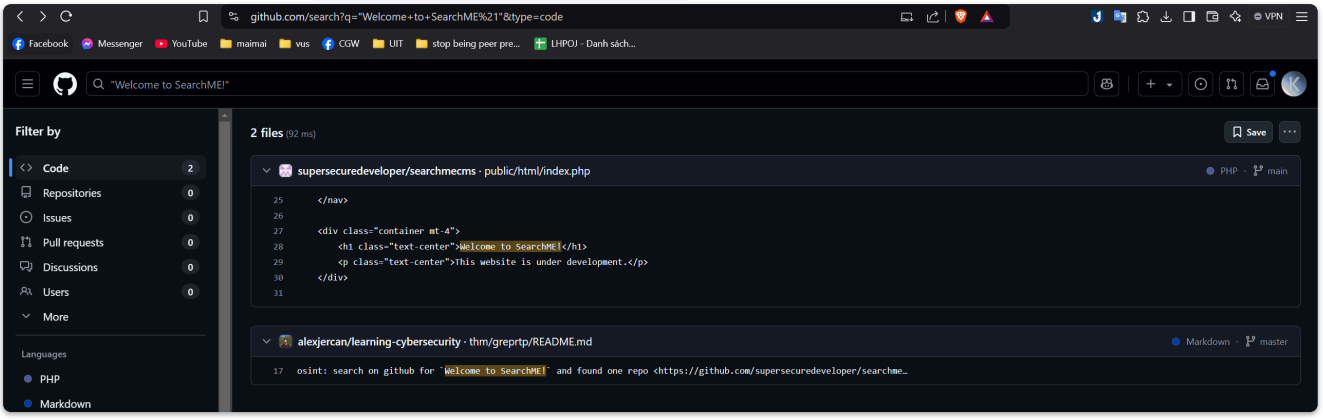
Link video link

Đề bài

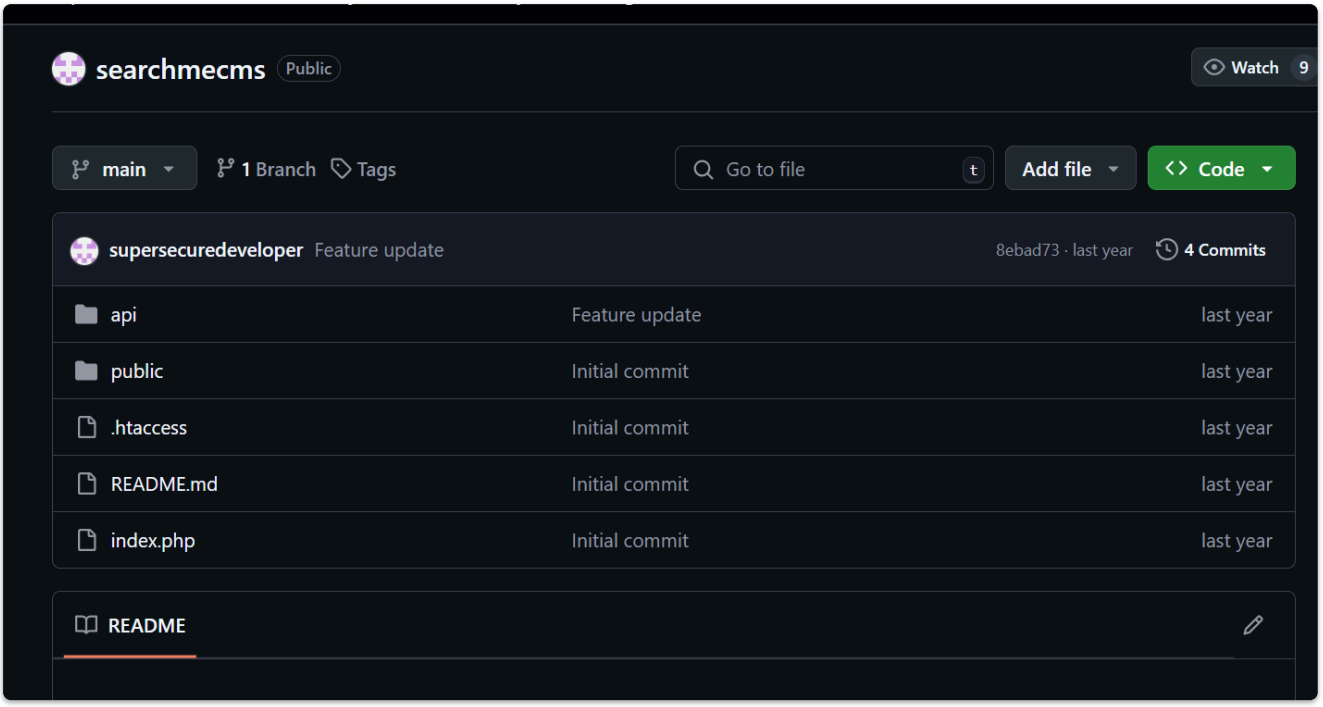
Chúng tôi có 1 trang web đang trong quá trình phát triển, hày tìm thử API key cho phép user tạo tài khoản trên website này

Các bước thực hiện

Tìm kiếm với từ khóa `"Welcome to SearchME!"`, ta có kết quả là mã nguồn của web



Vào trong trang GitHub, ta thấy được folder gọi là api



Vào folder apu vào xem mã nguồn của register.php

```php
<?php
require_once 'config.php';
header('Content-Type: application/json');

$headers = apache_request_headers();

if (isset($headers['X-THM-API-Key']) && $headers['X-THM-API-Key'] ===
'TBA') {
    $input = json_decode(file_get_contents('php://input'), true);

    $stmt = $mysqli->prepare("INSERT INTO users (username, password,
```

```
email, name) VALUES (?, ?, ?, ?)");
    $stmt->bind_param("ssss", $input['username'],
password_hash($input['password'], PASSWORD_DEFAULT), $input['email'],
$input['name']);

    if ($stmt->execute()) {
        echo json_encode(['message' => 'Registration successful.']);
    } else {
        echo json_encode(['error' => 'Registration failed: ' . $stmt-
>error]);
    }
    $stmt->close();
} else {
    echo json_encode(array('error' => 'Invalid or Expired API key'));
  }

?>
```

Ta thấy có dòng

```
if (isset($headers['X-THM-API-Key']) && $headers['X-THM-API-Key'] ===
'TBA')
```

Vậy api key là `TBA`

Bài tập 15

Link video: link

Đề bài

Viết code crawling trang web https://indriver.com để lấy các thông tin liên quan như list email, các đường dẫn liên kết (links), danh sách js, images, comment.
Gợi ý: có thể dùng thư viện scrapy của python.

Các bước thực hiện

Sử dụng `beautifulsoup` để tìm kiếm

```
import requests
from bs4 import BeautifulSoup, Comment
import re
from urllib.parse import urljoin
import json

url = 'https://indriver.com'

response = requests.get(url)
```

```
response.raise_for_status()

soup = BeautifulSoup(response.text, 'lxml')

emails = set(re.findall(r'[a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,}',
response.text))

links = set()
for link in soup.find_all('a', href=True):
    full_url = urljoin(url, link['href'])
    links.add(full_url)

js_files = set()
for script in soup.find_all('script', src=True):
    js_url = urljoin(url, script['src'])
    js_files.add(js_url)

images = set()
for img in soup.find_all('img', src=True):
    img_url = urljoin(url, img['src'])
    images.add(img_url)

comments = [str(comment) for comment in soup.find_all(string=lambda text:
isinstance(text, Comment))]

data = {
    "emails": list(emails),
    "links": list(links),
    "js_files": list(js_files),
    "images": list(images),
    "comments": comments
}

with open("output.json", "w", encoding="utf-8") as f:
    json.dump(data, f, ensure_ascii=False, indent=4)

print("Data has been saved to output.json")
```

```
{
    "emails": [
        "u003emarketing@indrive.com",
        "support@indriver.com",
        "marketing@indrive.com",
        "gr@indrive.com",
        "support@indrive.com",
        "u003egr@indrive.com",
        "u003esupport@indrive.com"
    ],
```

```
    "links": [
        "https://indriver.com/vi-vn/blog",
        "https://indriver.com/vi-vn/legal",
        "https://indriver.com/vi-vn/driver",
        "https://indriver.com/vi-vn/book",
        "https://en.wikipedia.org/wiki/InDrive",
        "https://services.indrive.com/",
        "https://x.com/indrive",
        "https://indriver.com/vi-vn/company",
        "https://www.auroratechaward.com/",
        "https://indriver.com/vi-vn/fair-services",
        "https://alternativa.film/",
        "https://indriver.com/vi-vn/newsroom",
        "https://indriver.com/vi-vn/contacts",
        "https://www.facebook.com/indrive/",
        "https://indriver.com/vi-vn/sustainability",
        "https://underdogtechaward.com/",
        "https://movie.indrive.com/",
        "https://supernovas.indrive.com/en/home",
        "https://indriver.com/vi-vn/earn-courier",
        "https://couriers.indrive.com/",
        "https://beginit.indrive.com/",
        "https://indriver.com/vi-vn/delete-account",
        "https://indriver.com/vi-vn/offer",
        "https://indriver.com/vi-vn/intercity-rides",
        "https://indriver.com/vi-vn/safety",
        "https://indriver.com/vi-vn/intercity-driver",
        "https://indriver.com/vi-vn",
        "https://indriver.com/vi-vn/city-rides",
        "https://indriver.com/vi-vn/business",
        "https://indriver.com/vi-vn/earn-services",
        "https://ventures.indrive.com/",
        "https://www.instagram.com/indrive/",
        "https://indriver.com/vi-vn/invision",
        "https://indriver.com/vi-vn/freight-delivery",
        "https://careers.indrive.com/"
    ],
    "js_files": [
        "https://indriver.com/_next/static/chunks/124-
753c43ebf799764c.js",
        "https://indriver.com/_next/static/chunks/pages/index-
fd7485b58dcb7f26.js",
        "https://indriver.com/_next/static/chunks/polyfills-
42372ed130431b0a.js",
        "https://indriver.com/_next/static/chunks/822-
2b3dc504816a838f.js",

"https://indriver.com/_next/static/05MgPxEu9Xdm6RQ2TY2yh/_ssgManifest.js",
        "https://indriver.com/_next/static/chunks/pages/_app-
9a022731aa7a7917.js",
```

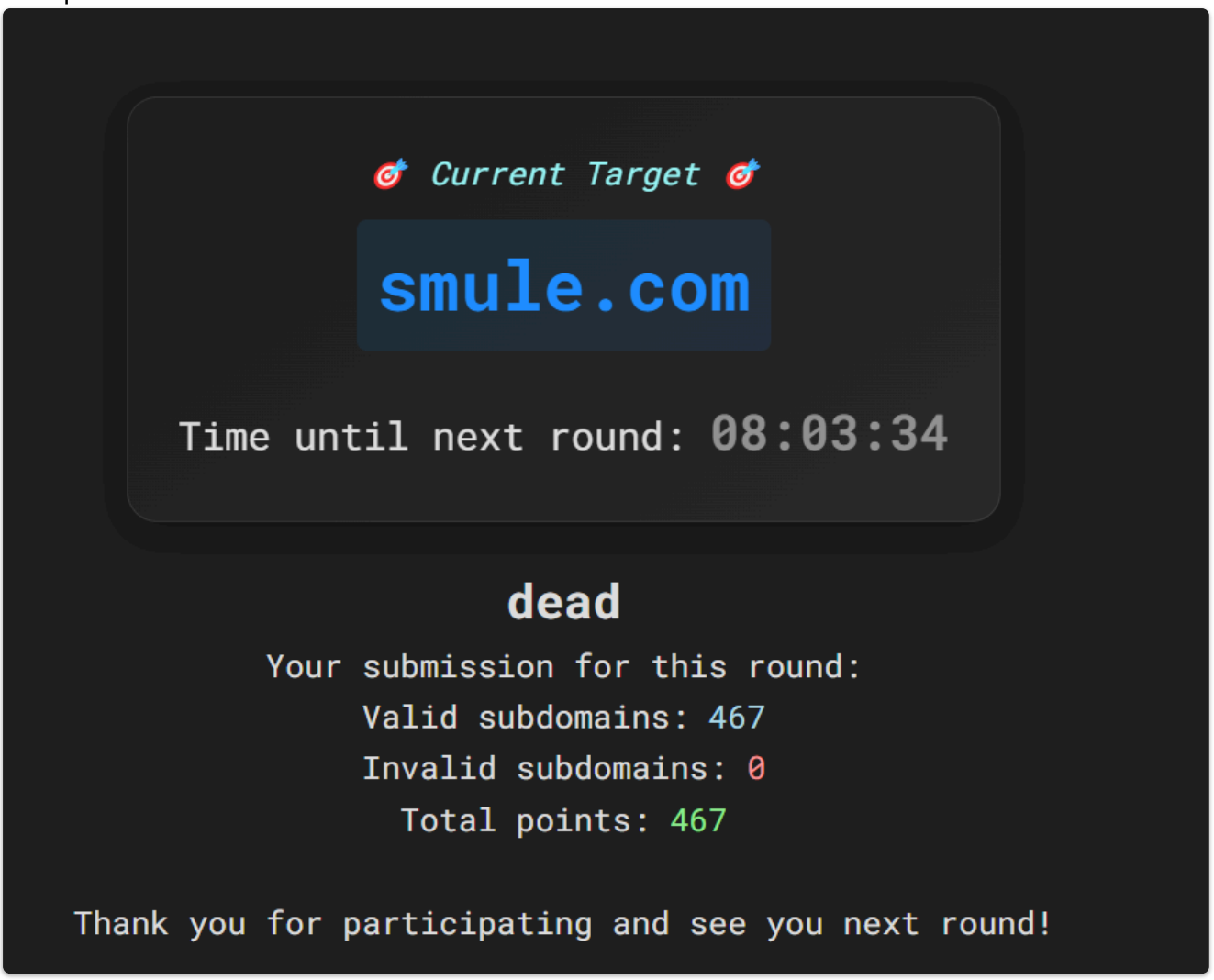
```
"https://indriver.com/_next/static/05MgPxEu9Xdm6RQ2TY2yh/_buildManifest.js
",
        "https://indriver.com/_next/static/chunks/webpack-
4ae7d6faa12f89f1.js",
        "https://indriver.com/_next/static/chunks/229-
62d87702c5ca71d9.js",
        "https://indriver.com/_next/static/chunks/framework-
0e6d174fa0a17919.js",
        "https://indriver.com/_next/static/chunks/main-
3f064f40dfca4a05.js"
    ],
    "images": [
        "https://indriver.com/_next/image?
url=%2Fimages%2Fpeople%2F1.png&w=3840&q=75",
        "https://indriver.com/_next/image?url=%2Fimages%2Fsafety-
section%2Fus%2Fl%2Fperson.png&w=3840&q=75",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fimpact%2Fus%2Fl%2F1.png&w=3840&q=75",
        "https://indriver.com/images/header/earn-with-indrive.svg",
        "https://indriver.com/images/icons/next.svg",
        "https://indriver.com/images/header/impact.svg",
        "https://indriver.com/images/icons/wiki.svg",
        "https://indriver.com/images/icons/app-store.svg",
        "https://indriver.com/images/header/cube.svg",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fslides%2Fus%2Fl%2Fslide_1.jpg&w=3840&q=75",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fslides%2Fus%2Fl%2Fslide_2.jpg&w=3840&q=75",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fimpact%2Fus%2Fl%2F2.png&w=3840&q=75",
        "https://indriver.com/images/icons/instagram.svg",
        "https://indriver.com/_next/image?url=%2Fimages%2Fbook-
section%2Fbook-bg.jpg&w=3840&q=75",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fpeople%2F2.png&w=3840&q=75",
        "https://indriver.com/images/layers/layer.svg",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fslides%2Fus%2Fl%2Fslide_0.jpg&w=3840&q=75",
        "https://indriver.com/images/icons/outerpath-arrow.svg",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fservices%2Fcourier.jpg&w=828&q=75",
        "https://indriver.com/images/icons/x.svg",
        "https://indriver.com/images/icons/google-play.svg",
        "https://indstatic.io/indstatic-main/flags/VN.svg",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fpeople%2F3.png&w=3840&q=75",
        "https://indriver.com/images/icons/circle.svg",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fimpact%2Fus%2Fl%2F6.png&w=3840&q=75",
```

```
        "https://indriver.com/_next/image?
url=%2Fimages%2Fpeople%2F4.png&w=3840&q=75",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fservices%2Fservices.jpg&w=828&q=75",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fvalues%2Fperformance.jpeg&w=3840&q=75",
        "https://indriver.com/images/icons/arrow-right.svg",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fvalues%2Fpeople.jpeg&w=3840&q=75",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fimpact%2Fus%2Fl%2F5.png&w=3840&q=75",
        "https://indriver.com/images/icons/close.svg",
        "https://indriver.com/images/header/about-us.svg",
        "https://indriver.com/images/book-section/layer.svg",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fimpact%2Fus%2Fl%2F7.png&w=3840&q=75",
        "https://indriver.com/images/icons/fb.svg",
        "https://indriver.com/images/logo/logo--white.svg",
        "https://indriver.com/images/icons/app-gallery.svg",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fvalues%2Fpurpose.png&w=3840&q=75",
        "https://indriver.com/images/logo/logo--dark.svg",
        "https://indriver.com/images/icons/arrow.svg",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fservices%2Fintercity.jpg&w=828&q=75",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fservices%2Fcity.jpg&w=828&q=75",
        "https://indriver.com/images/icons/circle-close.svg",
        "https://indriver.com/images/header/fair-services.svg",
        "https://indriver.com/_next/image?url=%2Fimages%2Fbook-
section%2Fbook-bg-mobile.jpg&w=750&q=75",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fimpact%2Fus%2Fl%2F4.png&w=3840&q=75",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fimpact%2Fus%2Fl%2F3.png&w=3840&q=75",
        "https://indriver.com/images/safety-section/safety.svg",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fslides%2Fus%2Fl%2Fslide_3.jpg&w=3840&q=75",
        "https://indriver.com/_next/image?
url=%2Fimages%2Fservices%2Ffreight.jpg&w=828&q=75"
    ],
    "comments": [
        " ",
        " ",
        " ",
        " "
    ]
}
```

Bài tập thực hành

Recon Royale

Kết quả



Các bước thực hiện

Sử dụng SecurityTrails

Tryhackme - WebOSINT

Link video: link

Task 2

Sau khi tra whois của trang web, ta có các thông tin mình cần

republicofkoffee.com PREMIUM

Domain name: RepublicOfKoffee.com
Registry Domain ID: 2582024072_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2024-01-11T02:08:15.56Z
Creation Date: 2021-01-01T17:33:07.00Z
Registrar Registration Expiration Date: 2025-01-01T17:33:07.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.9854014545
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Redacted for Privacy
Registrant Organization: Privacy service provided by Withheld for Privacy ehf
Registrant Street: Kalkofnsvegur 2
Registrant City: Reykjavik
Registrant State/Province: Capital Region
Registrant Postal Code: 101
Registrant Country: IS
Registrant Phone: +354.4212434
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: 744b407022364a2f8212bb43b0f7edf8.protect@withheldforprivacy.com
Registry Admin ID:
Admin Name: Redacted for Privacy
Admin Organization: Privacy service provided by Withheld for Privacy ehf
Admin Street: Kalkofnsvegur 2
Admin City: Reykjavik
Admin State/Province: Capital Region
Admin Postal Code: 101

Admin Postal Code: 101
Admin Country: IS
Admin Phone: +354.4212434
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: 744b407022364a2f8212bb43b0f7edf8.protect@withheldforprivacy.com
Registry Tech ID:
Tech Name: Redacted for Privacy
Tech Organization: Privacy service provided by Withheld for Privacy ehf
Tech Street: Kalkofnsvegur 2
Tech City: Reykjavik
Tech State/Province: Capital Region
Tech Postal Code: 101
Tech Country: IS
Tech Phone: +354.4212434
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: 744b407022364a2f8212bb43b0f7edf8.protect@withheldforprivacy.com
Name Server: ns1.brainydns.com
Name Server: ns2.brainydns.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-11-17T22:17:55.05Z <<<
For more information on Whois status codes, please visit https://icann.org/epp

Answer the questions below

What is the name of the company the domain was registered with?

Namecheap Inc — ✓ Correct Answer

What phone number is listed for the registration company? (do not include country code or special characters/spaces)

9854014545 — ✓ Correct Answer — Hint

What is the first nameserver listed for the site?

ns1.brainydns.com — ✓ Correct Answer

What is listed for the name of the registrant?

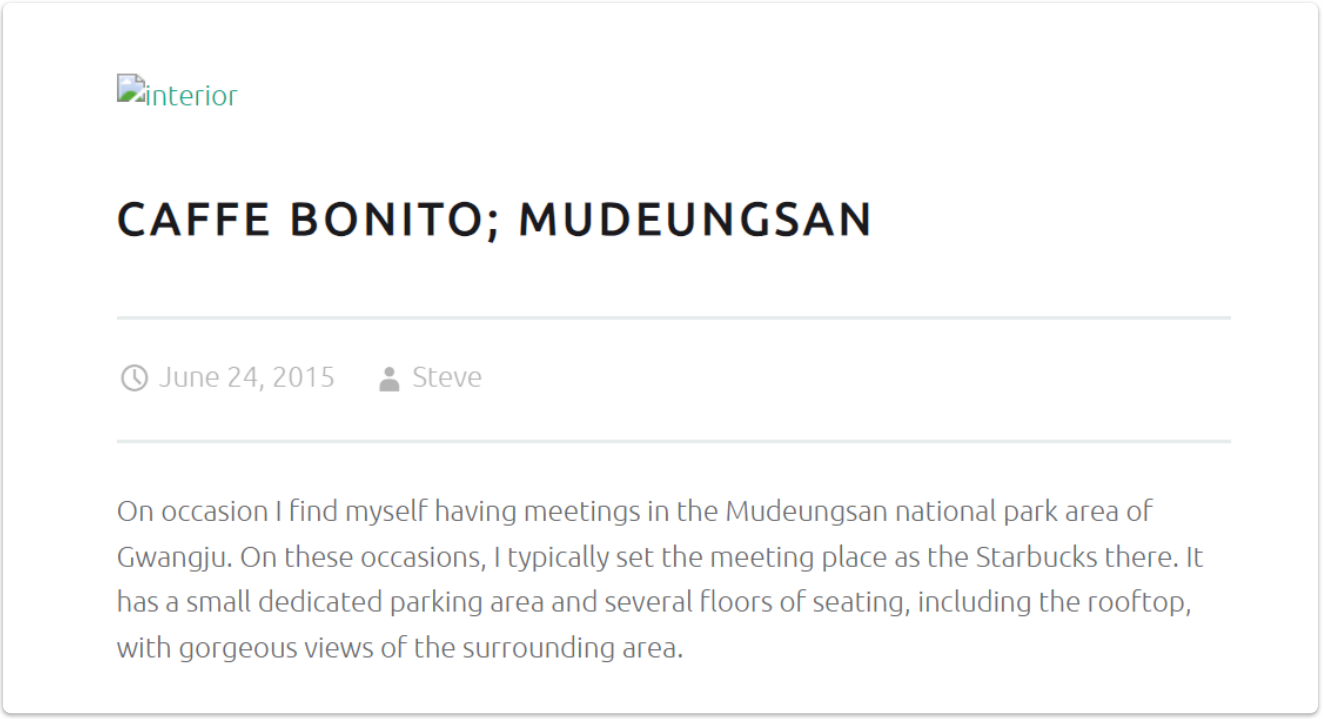
redacted for privacy — ✓ Correct Answer

What country is listed for the registrant?

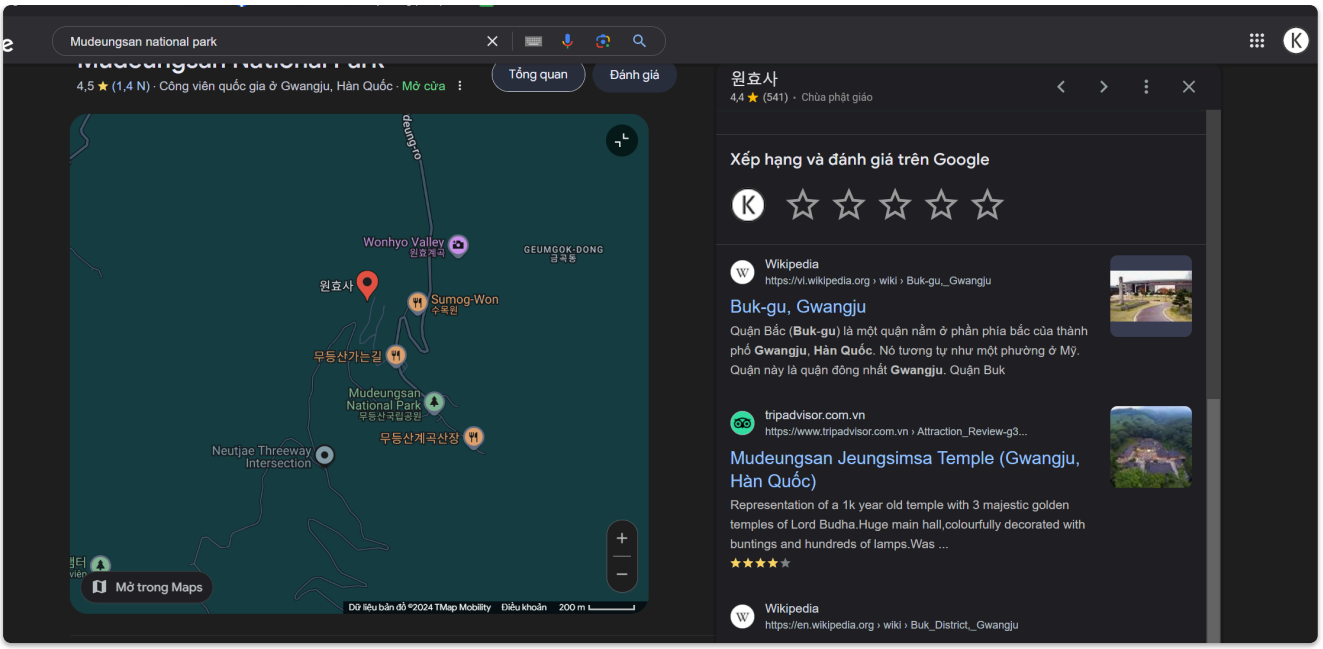
Iceland — ✓ Correct Answer

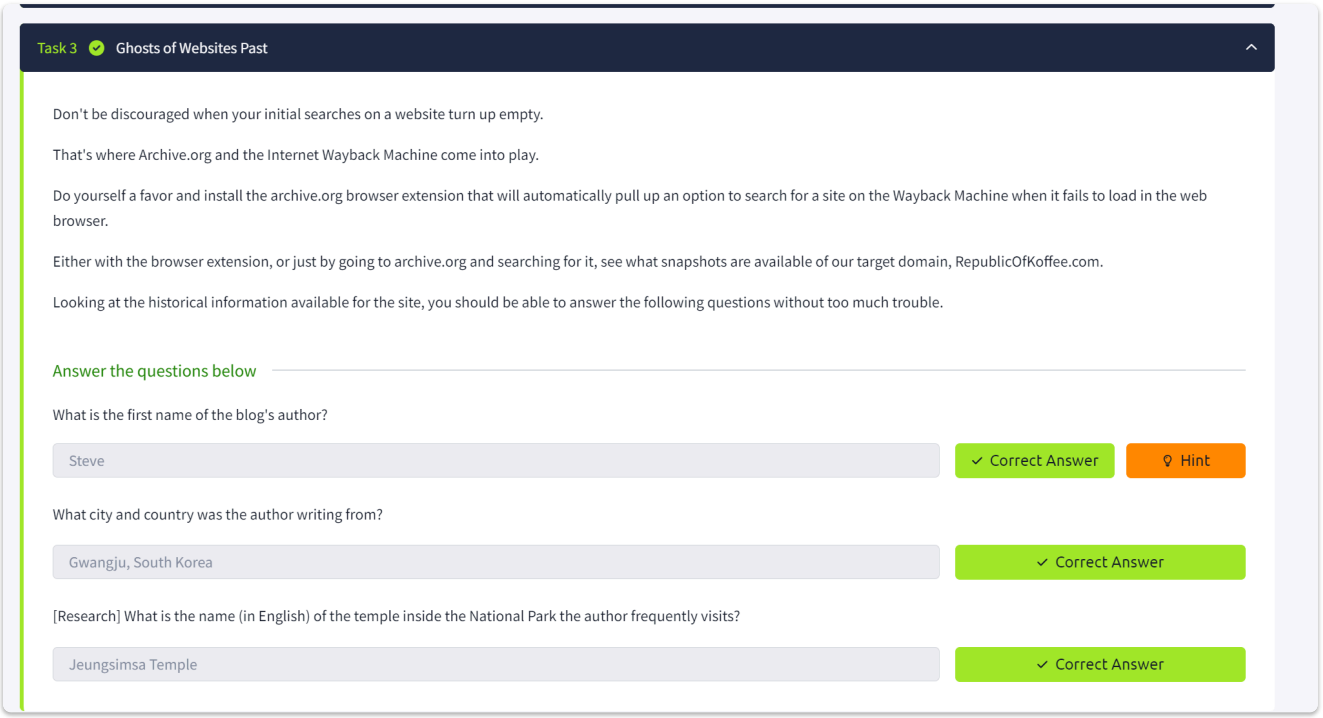
Task 3

Vào trong Web Archiver của RepulicOfKoffee và vào bài viết này ta sẽ có thông tin mình cần



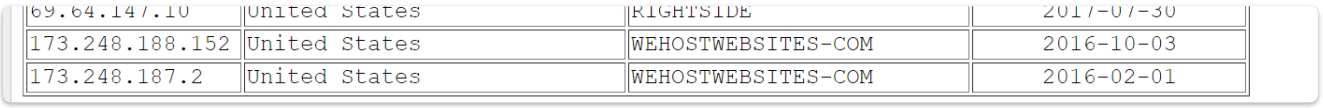
Đền thờ trong công viên khi tim trên Google





Task 4

Vào viewDNS để tìm



69.64.147.10	United States	RIGHTSIDE	2017-07-30
173.248.188.152	United States	WEHOSTWEBSITES-COM	2016-10-03
173.248.187.2	United States	WEHOSTWEBSITES-COM	2016-02-01

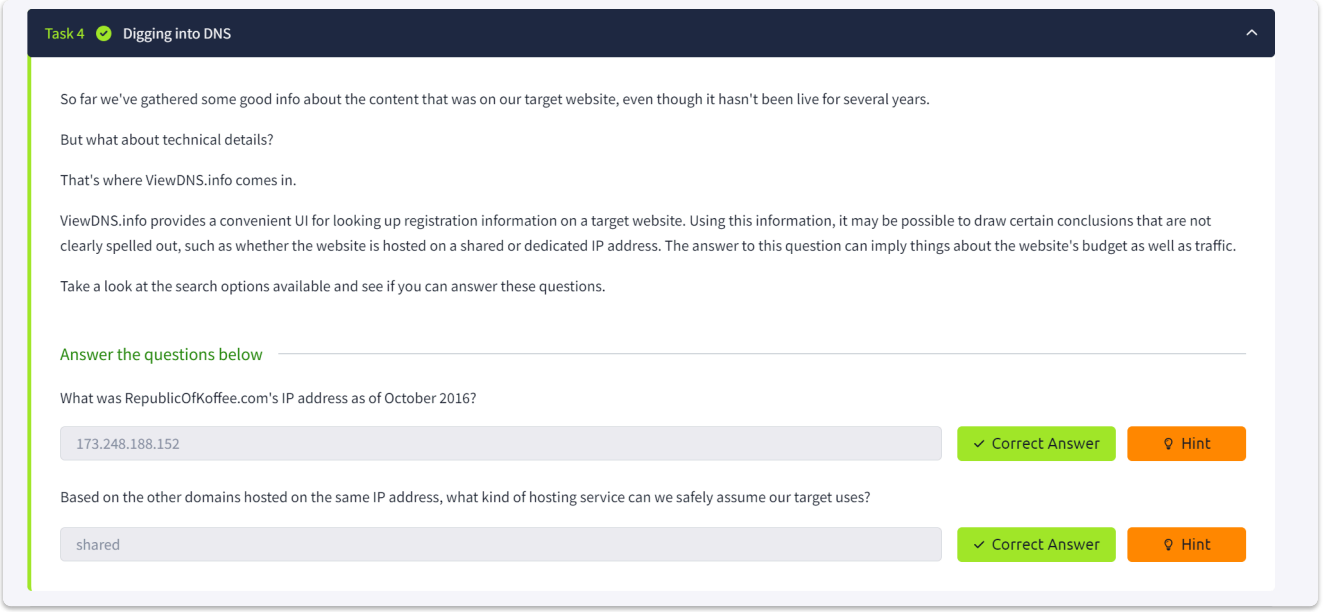
Dùng tool Reverse IP Lookup để tìm hiểu IP này đang host các website nào

Reverse IP results for 173.248.188.152
==========

There are 72 domains hosted on this server.
The complete listing of these is below:

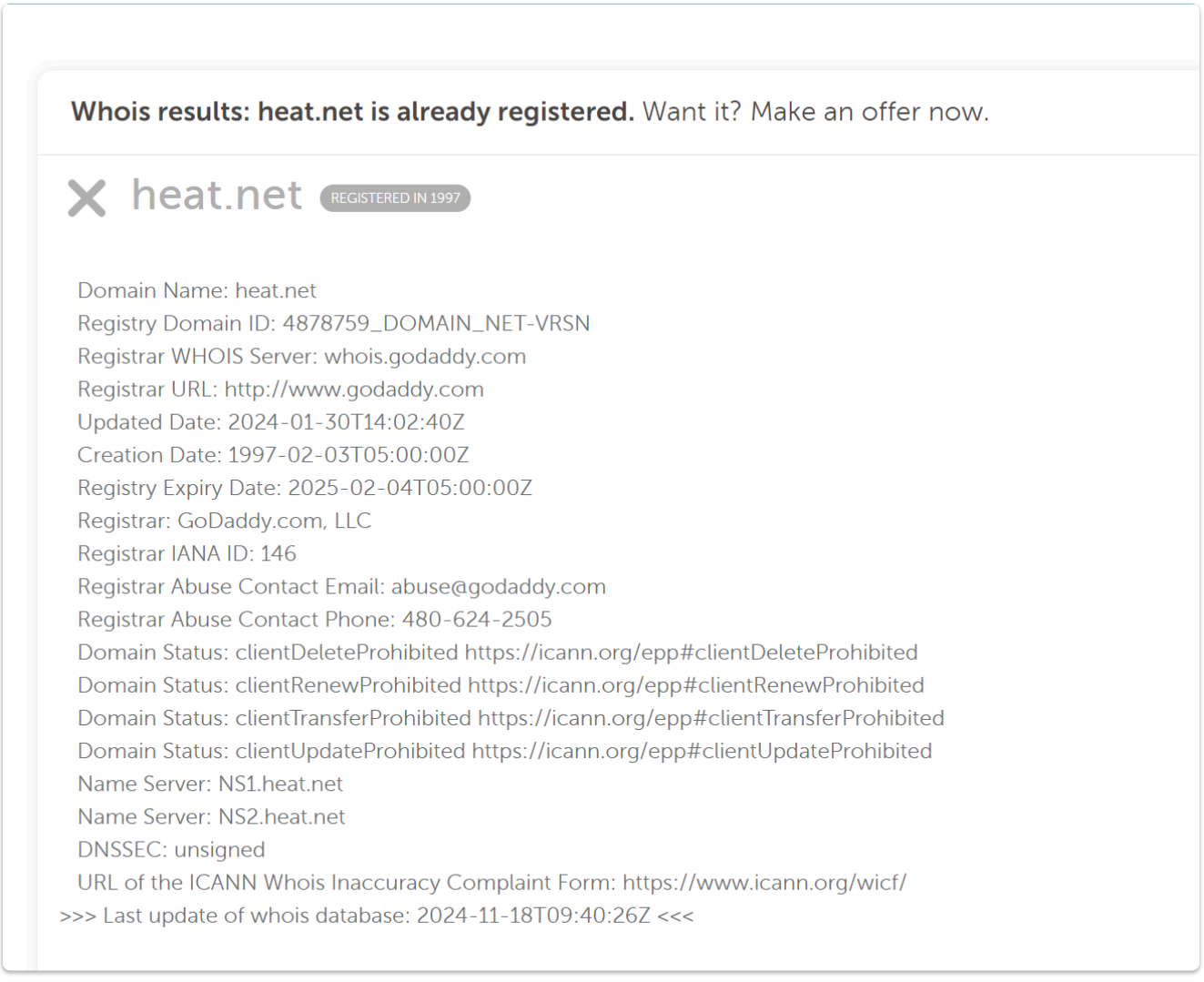
Domain	Last Resolved Date
acmx.com	2018-04-02
adventuratransport.com	2017-05-17
advisicon.com.mx	2017-11-01
animaenglish.org	2018-07-06
assaggiogourmet.com	2017-10-02
assistant-andrew.com	2017-05-31
assistat-daniel.com	2017-06-12
aztecaaceros.com	2017-06-17
bjj-tech.com	2024-11-17
bnbspacemanagement.com	2017-05-12
carrpropertymgmtnc.com	2017-06-01
coursesinlondon.org	2017-06-09
desayunovirtual.com	2017-01-02
drillcodemexico.mx	2017-08-09
drillcodemexico.net	2017-10-09
dumogtutors.com	2018-04-02
enphasesunshinecoast.com.au	2018-07-15
epix.mobi	2017-06-15
esgytsa.com	2018-06-01
farmmap.com.au	2016-10-16
fishingkayakreviews.co	2018-03-31
florackcolo.com	2017-05-17
freskosalon.com.mx	2017-10-11
gumaexpresscleaners.com	2017-06-01
hangitstraight.co.nz	2017-11-25
healthychanges.life	2017-10-24
hitchedwebservices.com	2017-05-04
homelabel.info	2017-10-10
hufhas.life	2017-10-24
hungrylizard.com.au	2018-07-01
iamliv.be	2017-10-10

Vậy là họ đang `shared`



Task 5

Kiểm tra Whois



Kiểm tra IP history

ViewDNS.info

Tools | API | Research | Data

ViewDNS.info > Tools > **IP History**

Shows a historical list of IP addresses a given domain name has been hosted on as well as where that IP address is geographically located, and the owner of that IP address.

Domain (e.g. *domain.com*):
GO

IP history results for heat.net.
==========

IP Address	Location	IP Address Owner	Last seen on this IP
208.117.87.195	United States	ATLANTIC-NET-1	2024-11-17
74.116.2.147	United States	PERFORMIVE	2019-06-19
72.52.192.240	United States	LIQUIDWEB	2011-12-19

Kiểm tra reverse IP

ViewDNS.info

Tools | API | Research | Data

ViewDNS.info > Tools > **IP History**

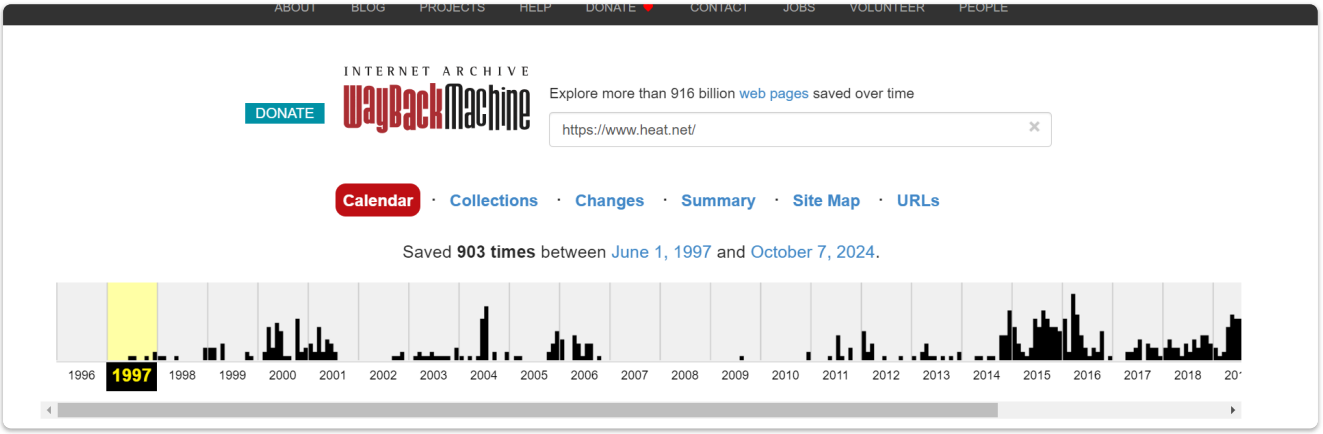
Shows a historical list of IP addresses a given domain name has been hosted on as well as where that IP address is geographically located, and the owner of that IP address.

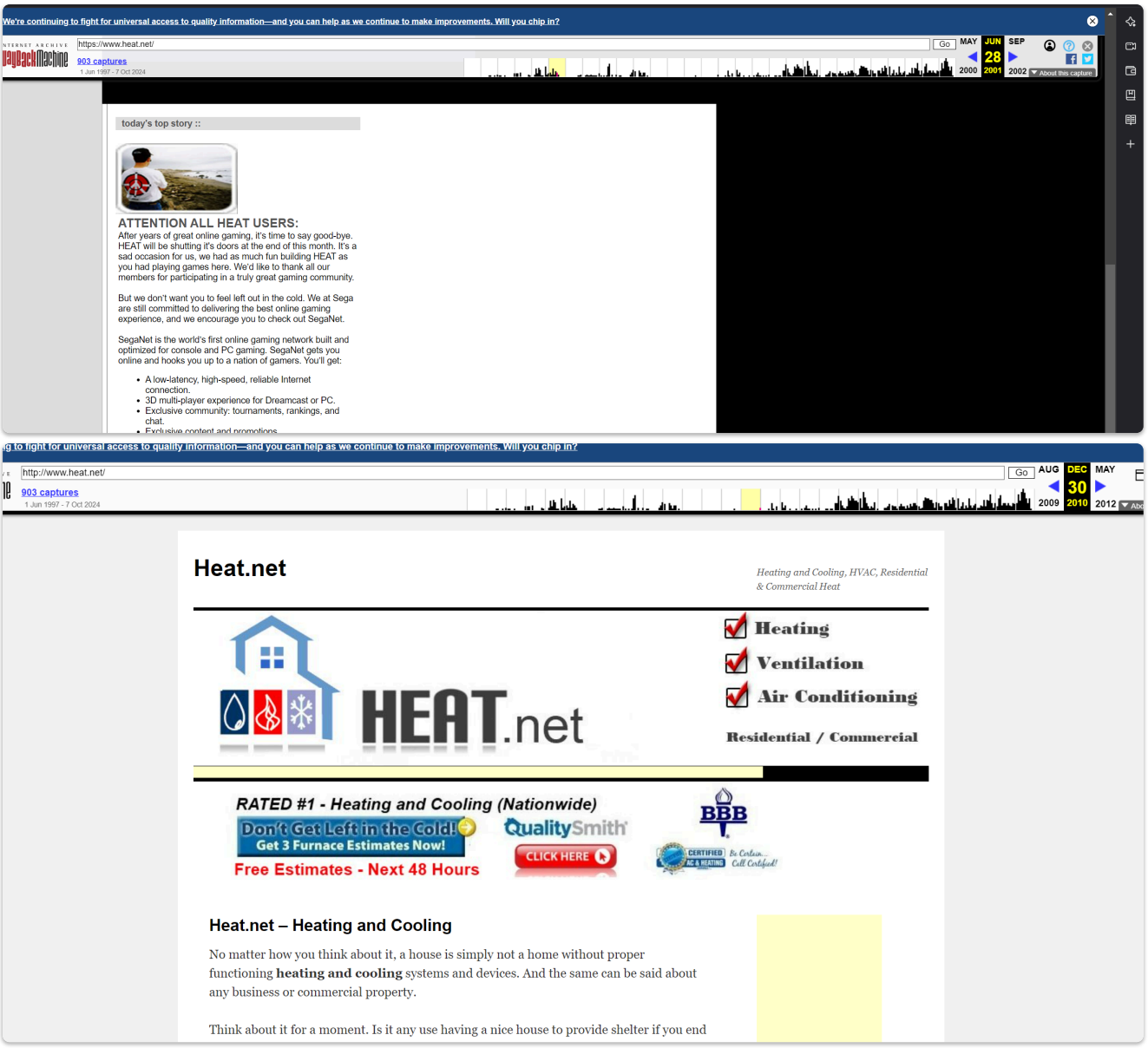
Domain (e.g. *domain.com*):
GO

IP history results for heat.net.
==========

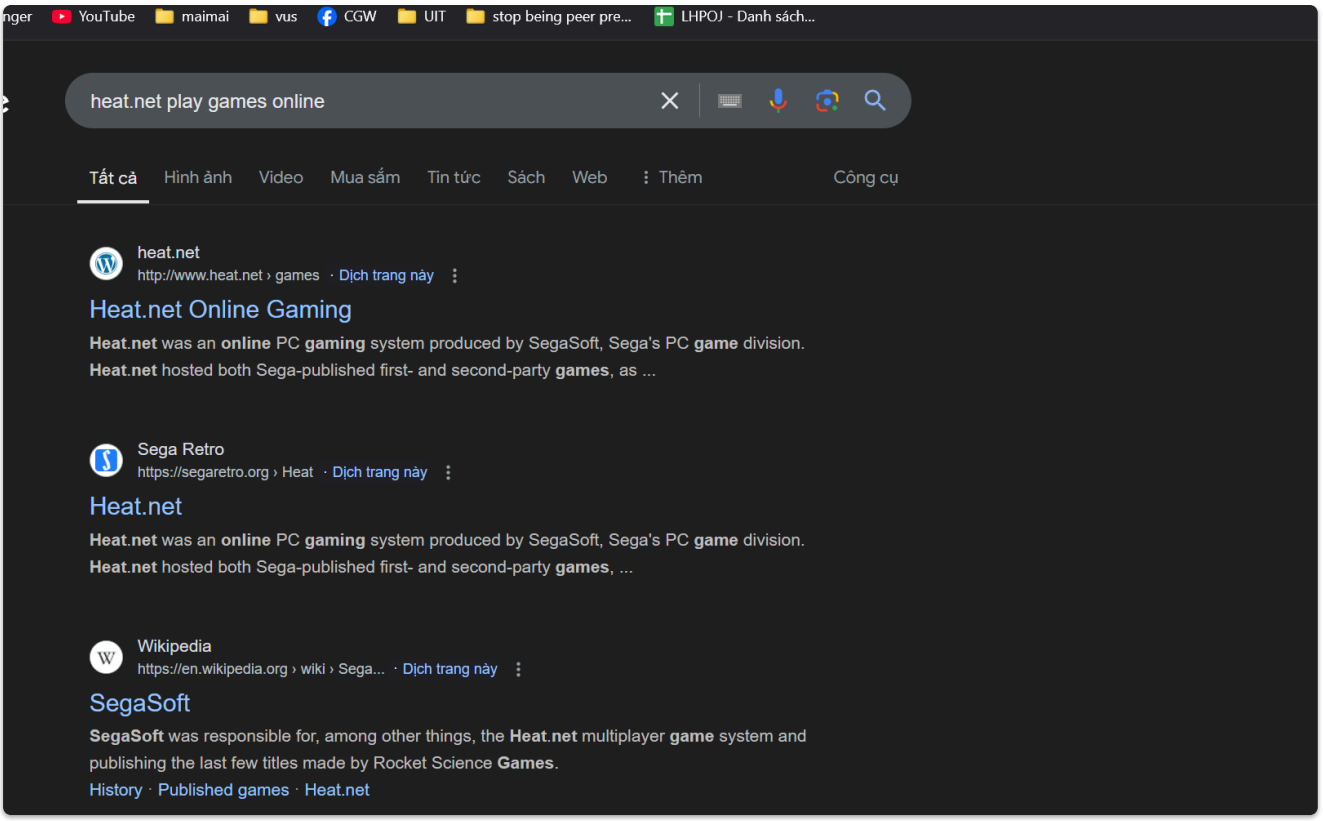
IP Address	Location	IP Address Owner	Last seen on this IP
208.117.87.195	United States	ATLANTIC-NET-1	2024-11-17
74.116.2.147	United States	PERFORMIVE	2019-06-19
72.52.192.240	United States	LIQUIDWEB	2011-12-19

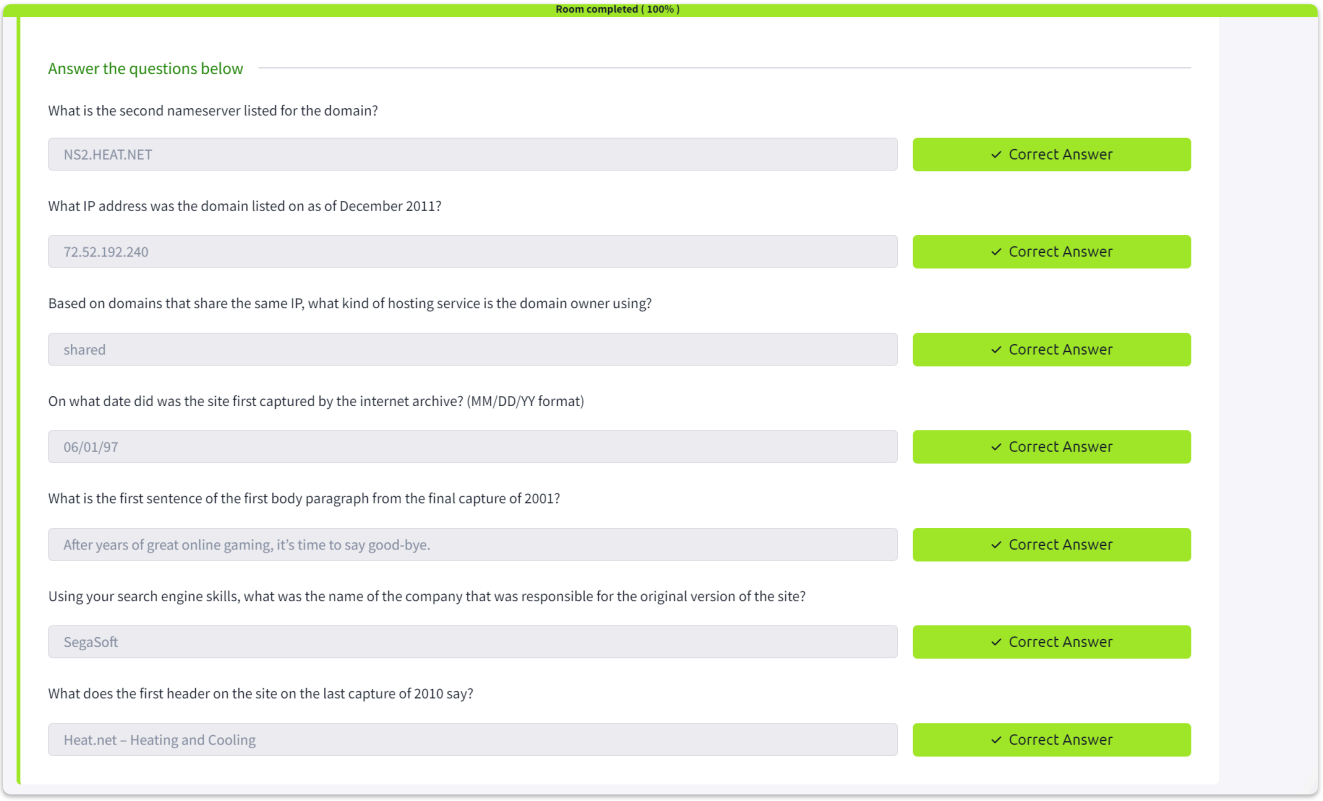
Kiểm tra trên Internet Archive





Tìm kiếm trên Google



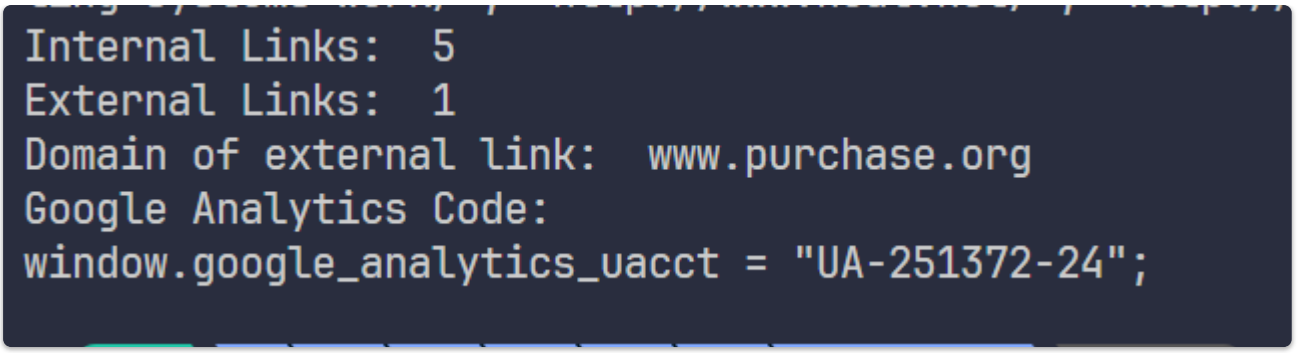


Task 6

Sử dụng đoạn code python để tìm

```
from bs4 import BeautifulSoup
import re
url = "http://www.heat.net/36/need-to-hire-a-commercial-heating-
contractor/"
def check(link):
    if link.startswith("http://www.heat.net") and link != url and not
```

```
link.endswith('.php')  and not link.endswith('uncategorized/'):
        return True
    return False
with open("task6.html", "r") as f:
    data = f.read()
soup = BeautifulSoup(data, 'html.parser')
#Google analytics code
ga_code = soup.find_all(string=re.compile("UA-"))
article = soup.find_all(id="post-36")
#find internal links
internal_links = []
for link in article[0].find_all('a', href=True):
    if check(link['href']) and link['href'] not in internal_links:
        internal_links.append(link['href'])

#find external links
external_links = []
for link in article[0].find_all('a', href=True):
    if not link['href'].startswith("http://www.heat.net"):
        external_links.append(link['href'])

print("Internal Links: ", len(internal_links))
print("External Links: ", len(external_links))
print("Domain of external link: ", external_links[0].split('/')[2])
print("Google Analytics Code: ", ga_code[0])
```



Have at it!

Answer the questions below

How many internal links are in the text of the article?

5 ✓ Correct Answer Hint

How many external links are in the text of the article?

1 ✓ Correct Answer Hint

Website in the article's only external link (that isn't an ad)

purchase.org ✓ Correct Answer

Try to find the Google Analytics code linked to the site

UA-251372-24 ✓ Correct Answer

Is the the Google Analytics code in use on another website? Yay or nay

nay ✓ Correct Answer Hint

Does the link to this website have any obvious affiliate codes embedded with it? Yay or Nay

Nay ✓ Correct Answer Hint

Task 7

IP history của purchase.org

172.67.197.177	Unknown	Cloudflare, Inc	2022-02-03
104.21.92.201	Unknown	Cloudflare, Inc	2022-02-03
104.27.185.115	Unknown	Cloudflare, Inc	2021-01-14
104.27.184.115	Unknown	Cloudflare, Inc	2021-01-14
206.196.110.108	United States	CDM	2017-11-03
67.43.1.187	United States	LIQUIDWEB	2013-04-19
72.52.193.127	United States	LIQUIDWEB	2012-11-16

IP history của heat.net

ViewDNS.info

Tools | API | Research | Data

ViewDNS.info > Tools > **IP History**

Shows a historical list of IP addresses a given domain name has been hosted on as well as where that IP address is geographically loc
owner of that IP address.

Domain (e.g. *domain.com*):
GO

IP history results for heat.net.
==========

IP Address	Location	IP Address Owner	Last seen on this IP
208.117.87.195	United States	ATLANTIC-NET-1	2024-11-18
74.116.2.147	United States	PERFORMIVE	2019-06-19
72.52.192.240	United States	LIQUIDWEB	2011-12-19

Like Share

Đều có LIQUIDWEB

Vào trang của LIQUIDWEB và nhìn vào tên công ty