**Phòng thí nghiệm An toàn Thông tin InsecLab**
**Trường Đại học Công nghệ Thông tin (UIT)**

# BÁO CÁO THỰC HÀNH

**Môn học: Bảo mật Web và Ứng dụng**

**Lab 3: Reconnaissance**

*GVHD: Ngô Khánh Khoa*

**Nhóm: 6**

## 1. THÔNG TIN CHUNG:

Lớp: NT213.P11.ANTT.2

| STT | Họ và tên | MSSV | Email |
|---|---|---|---|
| 1 | Lại Quan Thiên | 22521385 | 22521385@gm.uit.edu.vn |
| 2 | Mai Nguyễn Nam Phương | 22521164 | 22521164@gm.uit.edu.vn |
| 3 | Hồ Diệp Huy | 22520541 | 22520541@gm.uit.edu.vn |
| 4 | Nguyễn Phúc Nhi | 22521041 | 22521041@gm.uit.edu.vn |

## 2. NỘI DUNG THỰC HIỆN:[1]

| STT | Nội dung | Tình Trạng | Thực hiện |
|---|---|---|---|
| 1 | Bài 1 | 100% | Quan Thiên |
| 2 | Bài 2 | 100% | Diệp Huy |
| 3 | Bài 3 | 100% | Phúc Nhi |
| 4 | Bài 4 | 100% | Nam Phương |
| 5 | Bài 5 | 100% | Diệp Huy |
| 6 | Bài 6 | 100% | Phúc Nhi |
| 7 | Bài 7 | 100% | Quan Thiên |
| 8 | Bài 8 | 100% | Nam Phương |
| 9 | Bài 9 | 100% | Diệp Huy |
| 10 | Bài 10 | 100% | Phúc Nhi |
| 11 | Bài 11 | 100% | Quan Thiên |
| 12 | Bài 12 | 100% | Phúc Nhi |
| 13 | Bài 13 | 100% | Nam Phương |
| 14 | Bài 14 | 100% | Quan Thiên |

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

| | | | |
|---|---|---|---|
| **15** | Bài 15 | 100% | Diệp Huy |
| **16** | Bài tập Luyện tập 6.1 | 100% | Phúc Nhi |
| **17** | Bài tập Luyện tập Try Hack Me | 100% | Nam Phương |
| **18** | Bài tập Luyện tập Hack The Box | 90% | Thiên, Huy |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

# BÁO CÁO CHI TIẾT

## Bài tập 1: Thực hiện lệnh WHOIS lookup với tên miền indriver.com.

- *Id của IANA của tên miền trên là gì?*
- *Tên miền trên được đăng ký khi nào?*
- *Registar của tên miền trên?*
- *Công ty nào được sử dụng cho dịch vụ name server?*
- *Địa chỉ admin contact email cho tên miền trên?*

**Trả lời:**

```
┌──(kali㉿thinnnlinux)-[~]
└─$ whois indriver.com
   Domain Name: INDRIVER.COM
   Registry Domain ID: 130600645_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.corporatedomains.com
   Registrar URL: http://cscdbs.com
   Updated Date: 2024-08-26T14:18:16Z
   Creation Date: 2004-09-21T21:01:04Z
   Registry Expiry Date: 2025-09-21T21:01:04Z
   Registrar: CSC Corporate Domains, Inc.
   Registrar IANA ID: 299
   Registrar Abuse Contact Email: domainabuse@cscglobal.com
   Registrar Abuse Contact Phone: 8887802723
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS-1336.AWSDNS-39.ORG
   Name Server: NS-1696.AWSDNS-20.CO.UK
   Name Server: NS-294.AWSDNS-36.COM
   Name Server: NS-621.AWSDNS-13.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-11-19T07:32:06Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
```


- Video thực hiện: https://youtu.be/pWiM6hGhuPg

- ID của IANA của tên miền trên là gì? ID IANA của tên miền là: 299

- Tên miền trên được đăng ký khi nào? Ngày đăng ký: 2004-09-21 (21 tháng 9 năm 2004).

- Registrar của tên miền trên? Registrar: CSC Corporate Domains, Inc.

- Công ty nào được sử dụng cho dịch vụ name server? Công ty: Amazon Web Services (AWS), thông qua các name server:

+ ns-294.awsdns-36.com

+ ns-1696.awsdns-20.co.uk

+ ns-1336.awsdns-39.org

+ ns-621.awsdns-13.net

- Địa chỉ admin contact email cho tên miền trên?

=>Admin contact email: domainmaster@indriver.com

**Bài tập 2. 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?**

- Video thực hiện: https://youtu.be/3X8jFgLfMLE

```
hohuy@ubuntu:~$ nslookup -query=mx indriver.com
Server:         127.0.0.53
Address:        127.0.0.53#53

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

Authoritative answers can be found from:

hohuy@ubuntu:~$ dig indriver.com MX

; <<>> DiG 9.18.28-0ubuntu0.20.04.1-Ubuntu <<>> indriver.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35411
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;indriver.com.                  IN      MX

;; ANSWER SECTION:
indriver.com.           0       IN      MX      13 alt3.aspmx.l.google.com.
indriver.com.           0       IN      MX      11 alt1.aspmx.l.google.com.
indriver.com.           0       IN      MX      12 alt2.aspmx.l.google.com.
indriver.com.           0       IN      MX      10 aspmx.l.google.com.
indriver.com.           0       IN      MX      14 alt4.aspmx.l.google.com.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Nov 19 09:39:54 PST 2024
;; MSG SIZE  rcvd: 156

hohuy@ubuntu:~$
```

- Thông tin được cung cấp thêm bởi lệnh DIG:

+ HEADER: giúp biết rằng truy vấn đã được thực hiện thành công, không có lỗi xảy ra, và cho thấy các đặc tính của truy vấn

+ OPT PSEUDOSECTION: Phần này cho biết rằng lệnh dig đã sử dụng tính năng mở rộng của DNS (EDNS), cho phép truyền dữ liệu lớn hơn, cải thiện tốc độ và độ tin cậy của truy vấn DNS

+ QUESTION SECTION: kiểm tra xem truy vấn đã thực hiện đúng như yêu cầu hay chưa

+ ANSWER SECTION: Cho biết kết quả của truy vấn và thông tin MX record có thể được lưu trữ (cached) trong khoảng thời gian TTL

**Bài tập 3: Thực hiện truy vấn IP với tên miền indriver.com? Địa chỉ IP nào map với indriver.com? Tên miền nào trỏ đến địa chỉ 134.209.24.248? Mail server nào liên quan đến tên miền indriver.com?**

**Trả lời:**

- Video thực hiện: https://youtu.be/HFVLM-jaDi8

- Truy vấn IP với tên miền indriver.com bằng câu lệnh *nslookup indriver.com*

```
┌──(kali㉿kali)-[~]
└─$ nslookup indriver.com
Server:         192.168.64.2
Address:        192.168.64.2#53

Non-authoritative answer:
Name:   indriver.com
Address: 108.157.32.99
Name:   indriver.com
Address: 108.157.32.115
Name:   indriver.com
Address: 108.157.32.3
Name:   indriver.com
Address: 108.157.32.21
```

- Địa chỉ IP map với indriver.com là 108.157.32.21

```
┌──(kali㉿kali)-[~]
└─$ host 134.209.24.248
248.24.209.134.in-addr.arpa domain name pointer inlanefreight.com.
```

- Tên miền trỏ đến địa chỉ 134.209.24.248 là inlanefreight.com

```
┌──(kali㉿kali)-[~]
└─$ nslookup -query=mx indriver.com
Server:         192.168.64.2
Address:        192.168.64.2#53

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

Authoritative answers can be found from:
```

- Mail server liên quan đến tên miền indriver.com là:

```
mail exchanger = 13 alt3.aspmx.l.google.com.
mail exchanger = 12 alt2.aspmx.l.google.com.
mail exchanger = 10 aspmx.l.google.com.
mail exchanger = 14 alt4.aspmx.l.google.com.
mail exchanger = 11 alt1.aspmx.l.google.com.
```

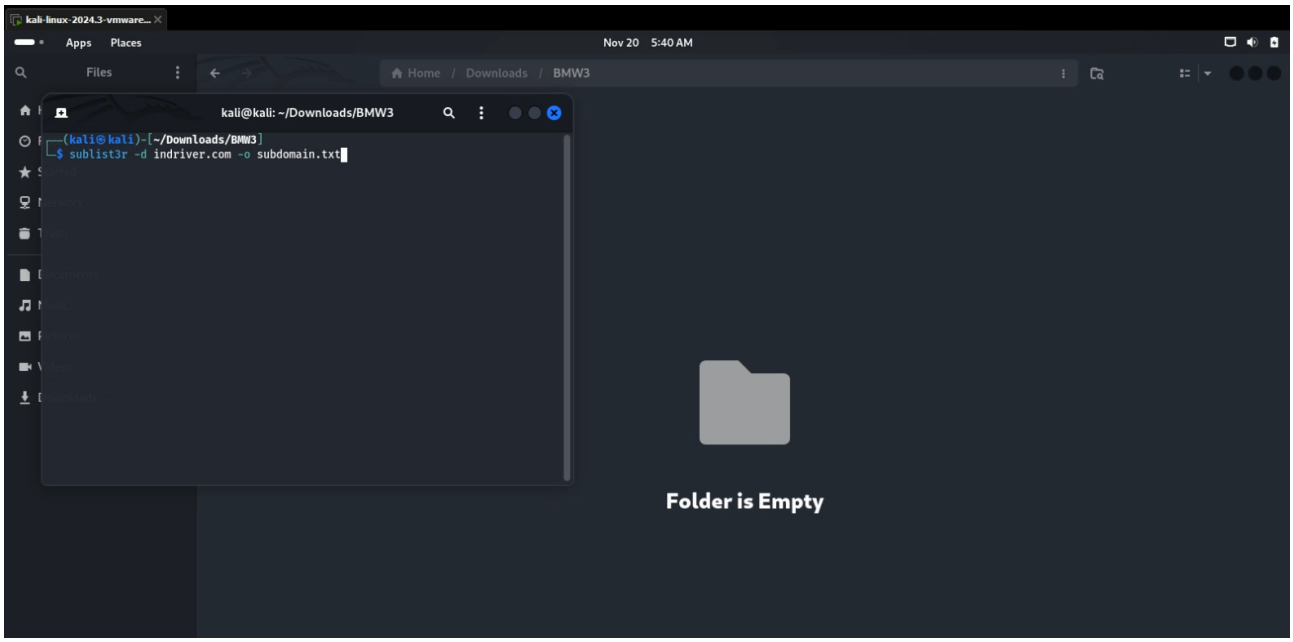
## Bài tập 4: Liệt kê các tên miền phụ của indriver.com, kết quả được lưu trong file csv

- Video thực hiện: https://youtu.be/lo28WLkCu8I

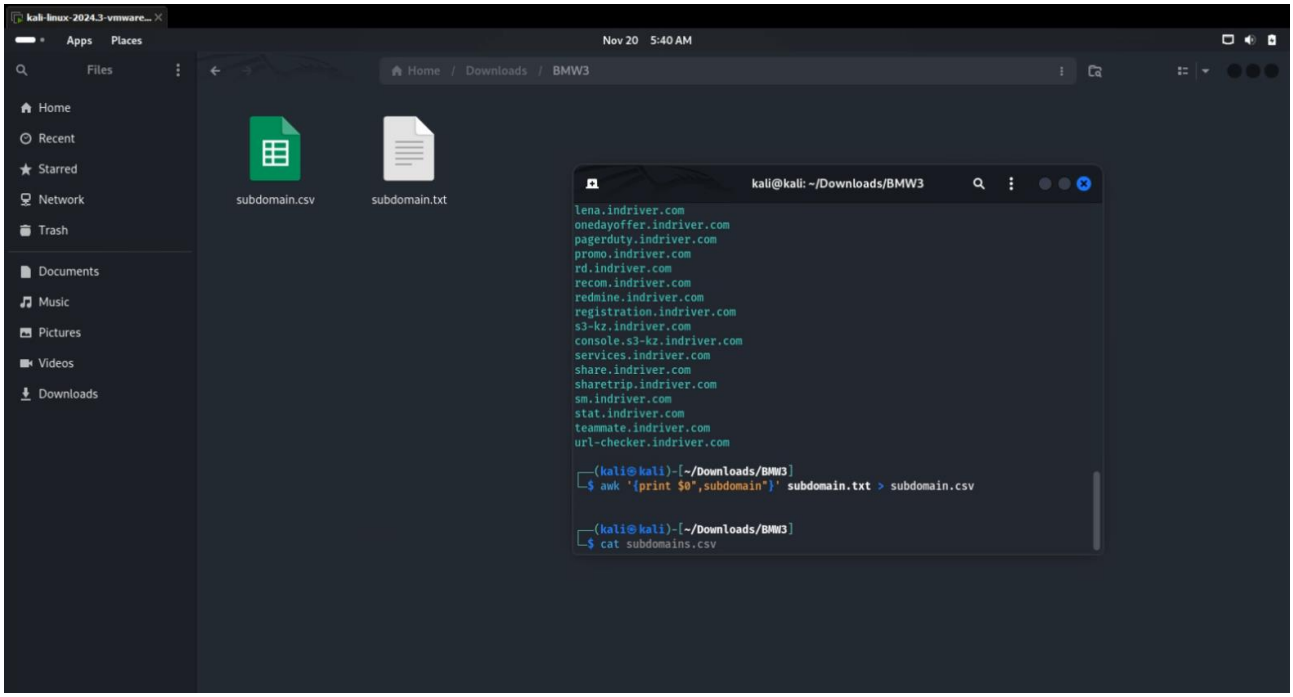
- Sử dụng lệnh "sublist3r -d indriver.com -o subdomain.txt" để sử dụng công cụ sublist3r nhằm liệt kê ra được các miền miền phụ của indriver.com

+ Cờ -d indriver.com chỉ định tên miền đích là indriver.com mà bạn muốn thu thập các subdomain

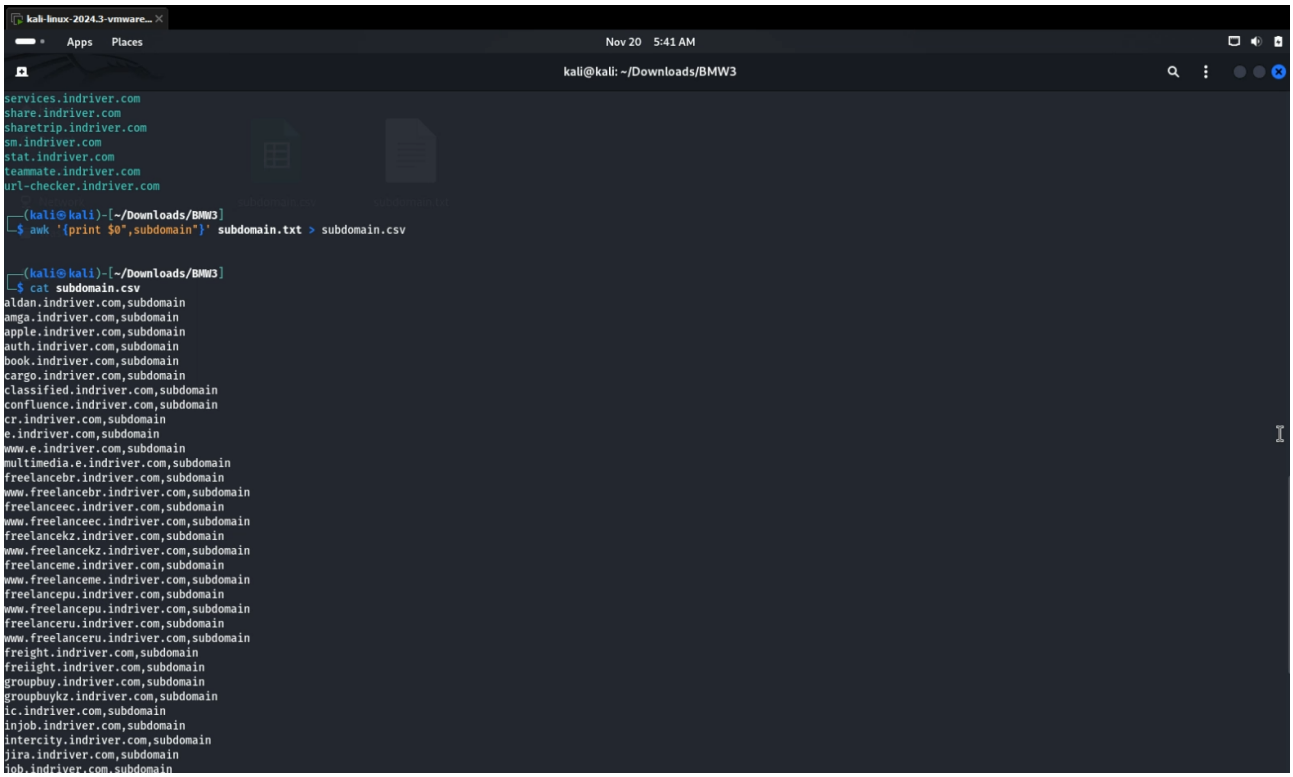
+ Cờ -o subdomain.txt cho biết rằng tất cả các subdomain được tìm thấy sẽ được lưu vào file subdomain.txt




- Sử dụng "awk '{print $0",subdomain"}' subdomain.txt > subdomain.csv" để chuyển kết quả từ file txt sang csv



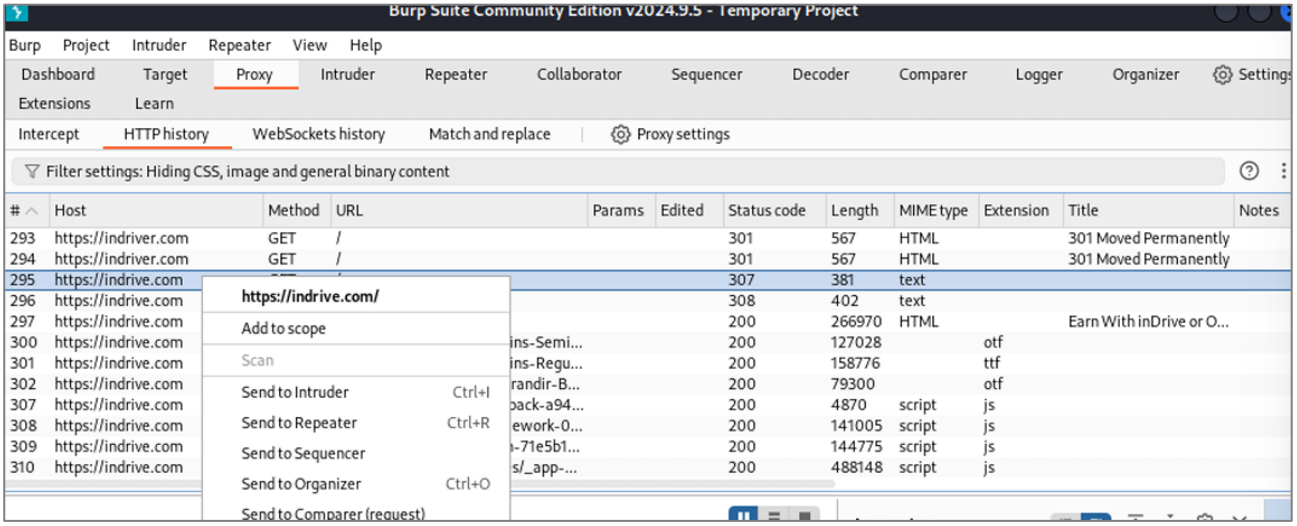
- Kết quả:


kali-linux-2024.3-vmware...
Apps Places
Nov 20 5:41 AM
kali@kali: ~/Downloads/BMW3
services.indriver.com
share.indriver.com
sharetrip.indriver.com
sm.indriver.com
stat.indriver.com
teammate.indriver.com
url-checker.indriver.com
(kali㉿kali)-[~/Downloads/BMW3]
$ awk '{print $0",subdomain"}' subdomain.txt > subdomain.csv
(kali㉿kali)-[~/Downloads/BMW3]
$ cat subdomain.csv
aldan.indriver.com,subdomain
amga.indriver.com,subdomain
apple.indriver.com,subdomain
auth.indriver.com,subdomain
book.indriver.com,subdomain
cargo.indriver.com,subdomain
classified.indriver.com,subdomain
confluence.indriver.com,subdomain
cr.indriver.com,subdomain
e.indriver.com,subdomain
www.e.indriver.com,subdomain
multimedia.e.indriver.com,subdomain
freelancebr.indriver.com,subdomain
www.freelancebr.indriver.com,subdomain
freelanceec.indriver.com,subdomain
www.freelanceec.indriver.com,subdomain
freelancekz.indriver.com,subdomain
www.freelancekz.indriver.com,subdomain
freelanceme.indriver.com,subdomain
www.freelanceme.indriver.com,subdomain
freelancepu.indriver.com,subdomain
www.freelancepu.indriver.com,subdomain
freelanceru.indriver.com,subdomain
www.freelanceru.indriver.com,subdomain
freight.indriver.com,subdomain
freiight.indriver.com,subdomain
groupbuy.indriver.com,subdomain
groupbuykz.indriver.com,subdomain
ic.indriver.com,subdomain
injob.indriver.com,subdomain
intercity.indriver.com,subdomain
jira.indriver.com,subdomain
job.indriver.com,subdomain

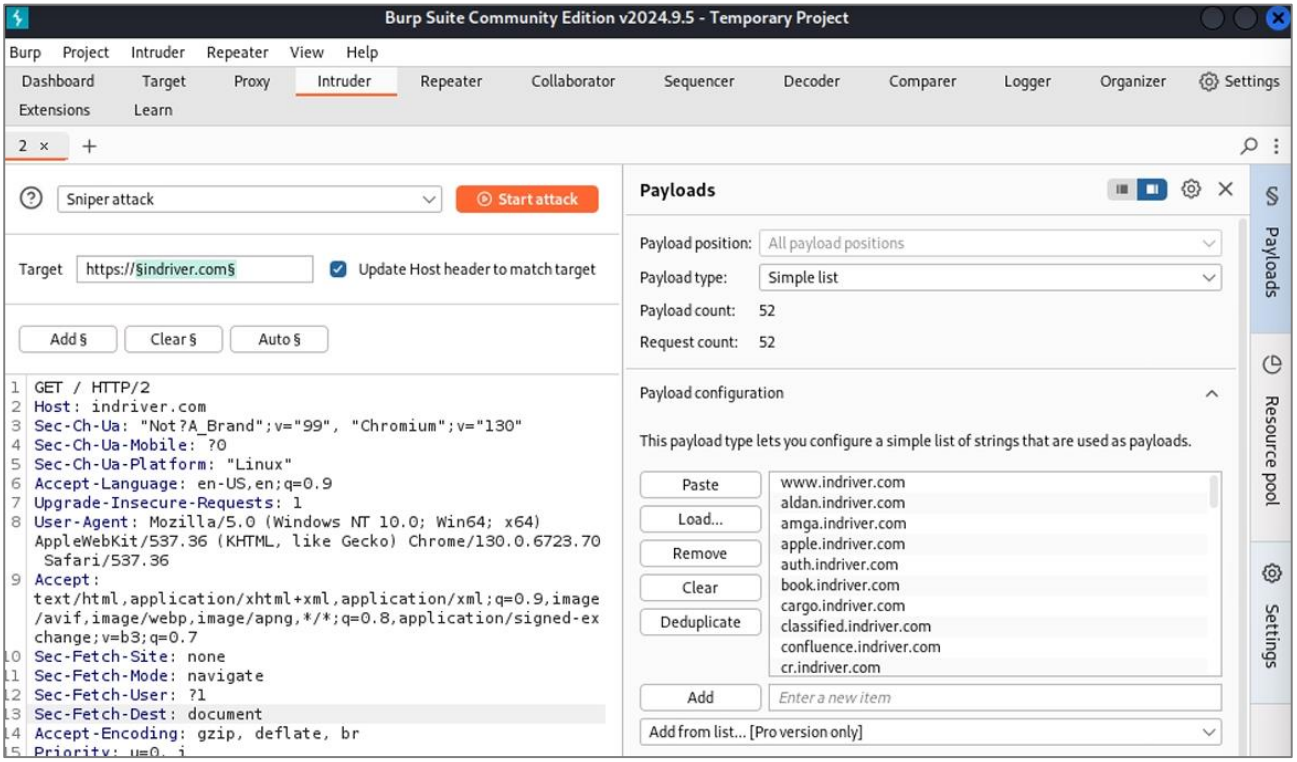
**Bài tập 5. Dựa vào các tên miền phụ đã tìm kiếm được ở bài tập 1 và các tên miền đã bruteforce được thêm bằng burpsuite intruder. Phân loại các tên miền có kết quả trả về status code 200 và các tên miền có kết quả trả về khác**

- Video thực hiện: https://youtu.be/1s8N-57NX7U

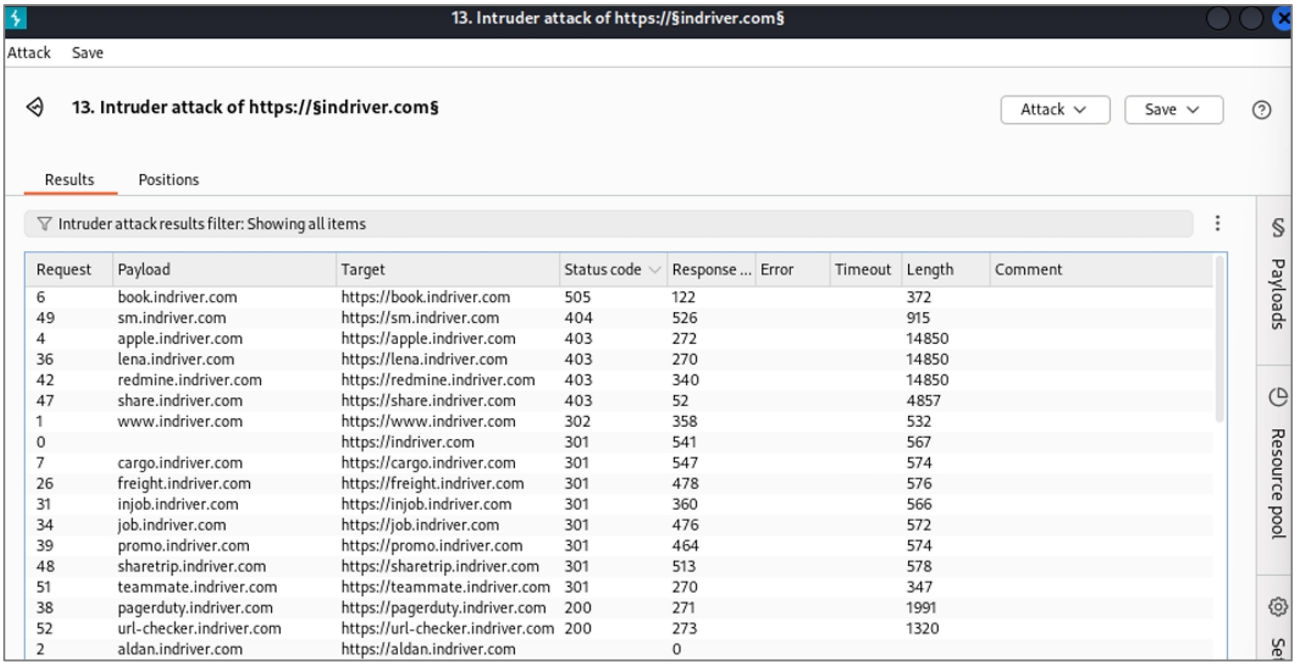
- B1: Dùng Burp Suite bắt gói tin Request từ indriver.com và Send to Intruder




- B2: Chọn vị trí thay thế bởi các payload trong quá trình brute-force là indriver.com và phần payload là các tên miền phụ vừa tìm được ở bài trước



- B3: Nhấn Start Attack và xem kết quả




| Request | Payload | Target | Status code | Response ... | Error | Timeout | Length | Comment |
|---|---|---|---|---|---|---|---|---|
| 6 | book.indriver.com | https://book.indriver.com | 505 | 122 | | | 372 | |
| 49 | sm.indriver.com | https://sm.indriver.com | 404 | 526 | | | 915 | |
| 4 | apple.indriver.com | https://apple.indriver.com | 403 | 272 | | | 14850 | |
| 36 | lena.indriver.com | https://lena.indriver.com | 403 | 270 | | | 14850 | |
| 42 | redmine.indriver.com | https://redmine.indriver.com | 403 | 340 | | | 14850 | |
| 47 | share.indriver.com | https://share.indriver.com | 403 | 52 | | | 4857 | |
| 1 | www.indriver.com | https://www.indriver.com | 302 | 358 | | | 532 | |
| 0 | | https://indriver.com | 301 | 541 | | | 567 | |
| 7 | cargo.indriver.com | https://cargo.indriver.com | 301 | 547 | | | 574 | |
| 26 | freight.indriver.com | https://freight.indriver.com | 301 | 478 | | | 576 | |
| 31 | injob.indriver.com | https://injob.indriver.com | 301 | 360 | | | 566 | |
| 34 | job.indriver.com | https://job.indriver.com | 301 | 476 | | | 572 | |
| 39 | promo.indriver.com | https://promo.indriver.com | 301 | 464 | | | 574 | |
| 48 | sharetrip.indriver.com | https://sharetrip.indriver.com | 301 | 513 | | | 578 | |
| 51 | teammate.indriver.com | https://teammate.indriver.com | 301 | 270 | | | 347 | |
| 38 | pagerduty.indriver.com | https://pagerduty.indriver.com | 200 | 271 | | | 1991 | |
| 52 | url-checker.indriver.com | https://url-checker.indriver.com | 200 | 273 | | | 1320 | |
| 2 | aldan.indriver.com | https://aldan.indriver.com | | 0 | | | | |

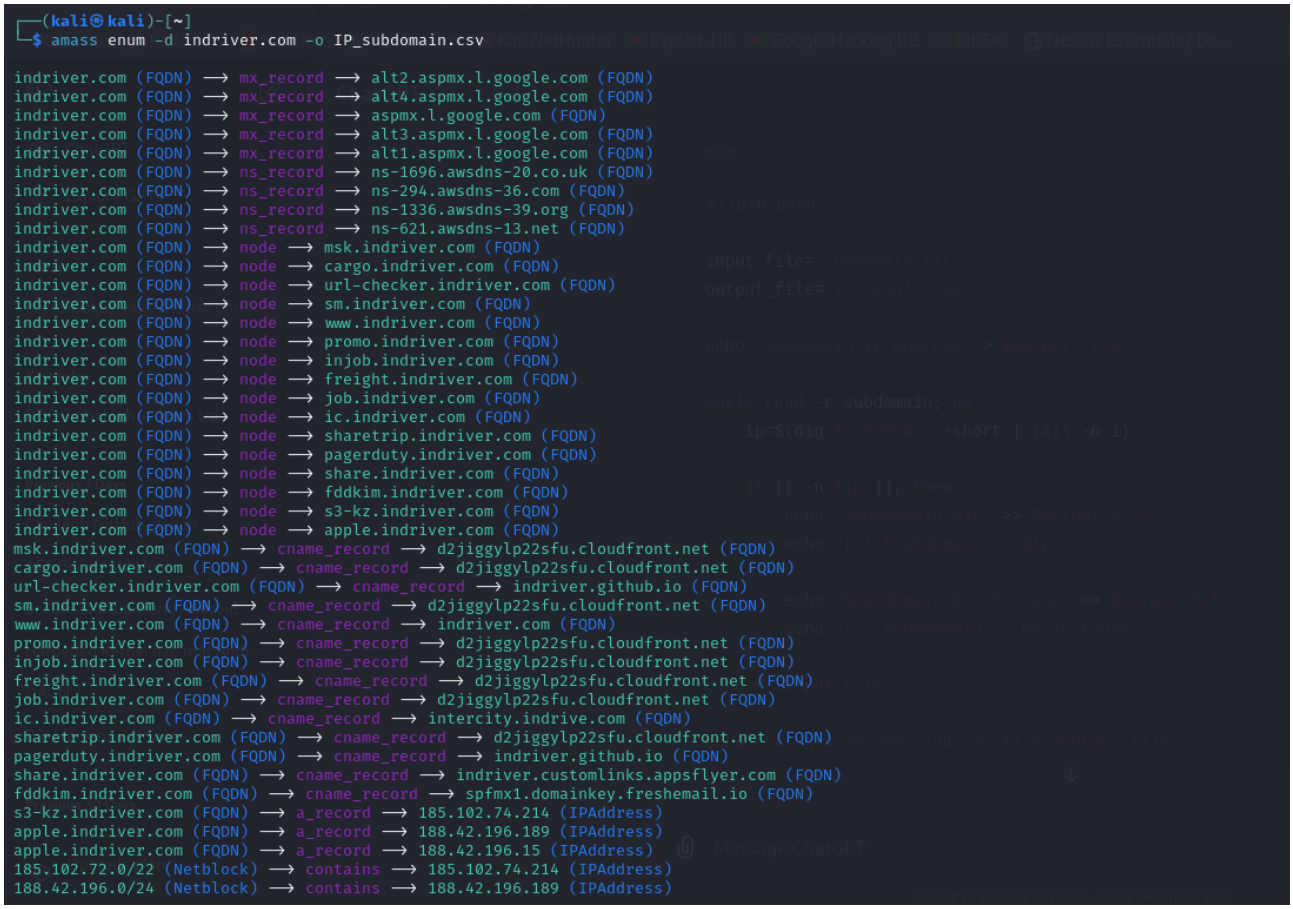
- Status code:
  + 200: Yêu cầu đã thành công và server đã gửi về kết quả mong đợi
  + 301: URL đã được chuyển hướng vĩnh viễn đến một URL mới
  + 302: Tài nguyên được tìm thấy nhưng tại một URL tạm thời
  + 403: Server từ chối cung cấp tài nguyên, dù yêu cầu có hợp lệ
  + 404: Server không tìm thấy tài nguyên được yêu cầu
  + 505: Server không hỗ trợ phiên bản HTTP được sử dụng trong yêu cầu

**Bài tập 6: Ghi nhận lại các địa chỉ IP của tên miền phụ tìm được của *.indriver.com. Kết quả lưu trong file csv.**

**Trả lời:**

- Video thực hiện: https://youtu.be/3rxUURDpgro

- Sử dụng amass để quét các tên miền phụ của *.indriver.com và IP của chúng, sau đó lưu vào file ip_subdomain.csv



- Kiểm tra lại file ip_subdomain.csv

```
┌──(kali㉿kali)-[~]
└─$ cat IP_subdomain.csv
indriver.com (FQDN) ⟶ mx_record ⟶ alt2.aspmx.l.google.com (FQDN)
indriver.com (FQDN) ⟶ mx_record ⟶ alt4.aspmx.l.google.com (FQDN)
indriver.com (FQDN) ⟶ mx_record ⟶ aspmx.l.google.com (FQDN)
indriver.com (FQDN) ⟶ mx_record ⟶ alt3.aspmx.l.google.com (FQDN)
indriver.com (FQDN) ⟶ mx_record ⟶ alt1.aspmx.l.google.com (FQDN)
indriver.com (FQDN) ⟶ ns_record ⟶ ns-1696.awsdns-20.co.uk (FQDN)
indriver.com (FQDN) ⟶ ns_record ⟶ ns-294.awsdns-36.com (FQDN)
indriver.com (FQDN) ⟶ ns_record ⟶ ns-1336.awsdns-39.org (FQDN)
indriver.com (FQDN) ⟶ ns_record ⟶ ns-621.awsdns-13.net (FQDN)
indriver.com (FQDN) ⟶ node ⟶ msk.indriver.com (FQDN)
indriver.com (FQDN) ⟶ node ⟶ cargo.indriver.com (FQDN)
indriver.com (FQDN) ⟶ node ⟶ url-checker.indriver.com (FQDN)
indriver.com (FQDN) ⟶ node ⟶ sm.indriver.com (FQDN)
indriver.com (FQDN) ⟶ node ⟶ www.indriver.com (FQDN)
indriver.com (FQDN) ⟶ node ⟶ promo.indriver.com (FQDN)
indriver.com (FQDN) ⟶ node ⟶ injob.indriver.com (FQDN)
indriver.com (FQDN) ⟶ node ⟶ freight.indriver.com (FQDN)
indriver.com (FQDN) ⟶ node ⟶ job.indriver.com (FQDN)
indriver.com (FQDN) ⟶ node ⟶ ic.indriver.com (FQDN)
indriver.com (FQDN) ⟶ node ⟶ sharetrip.indriver.com (FQDN)
indriver.com (FQDN) ⟶ node ⟶ pagerduty.indriver.com (FQDN)
indriver.com (FQDN) ⟶ node ⟶ share.indriver.com (FQDN)
indriver.com (FQDN) ⟶ node ⟶ fddkim.indriver.com (FQDN)
indriver.com (FQDN) ⟶ node ⟶ s3-kz.indriver.com (FQDN)
indriver.com (FQDN) ⟶ node ⟶ apple.indriver.com (FQDN)
msk.indriver.com (FQDN) ⟶ cname_record ⟶ d2jiggylp22sfu.cloudfront.net (FQDN)
cargo.indriver.com (FQDN) ⟶ cname_record ⟶ d2jiggylp22sfu.cloudfront.net (FQDN)
url-checker.indriver.com (FQDN) ⟶ cname_record ⟶ indriver.github.io (FQDN)
sm.indriver.com (FQDN) ⟶ cname_record ⟶ d2jiggylp22sfu.cloudfront.net (FQDN)
www.indriver.com (FQDN) ⟶ cname_record ⟶ indriver.com (FQDN)
promo.indriver.com (FQDN) ⟶ cname_record ⟶ d2jiggylp22sfu.cloudfront.net (FQDN)
injob.indriver.com (FQDN) ⟶ cname_record ⟶ d2jiggylp22sfu.cloudfront.net (FQDN)
freight.indriver.com (FQDN) ⟶ cname_record ⟶ d2jiggylp22sfu.cloudfront.net (FQDN)
job.indriver.com (FQDN) ⟶ cname_record ⟶ d2jiggylp22sfu.cloudfront.net (FQDN)
ic.indriver.com (FQDN) ⟶ cname_record ⟶ intercity.indrive.com (FQDN)
sharetrip.indriver.com (FQDN) ⟶ cname_record ⟶ d2jiggylp22sfu.cloudfront.net (FQDN)
pagerduty.indriver.com (FQDN) ⟶ cname_record ⟶ indriver.github.io (FQDN)
share.indriver.com (FQDN) ⟶ cname_record ⟶ indriver.customlinks.appsflyer.com (FQDN)
fddkim.indriver.com (FQDN) ⟶ cname_record ⟶ spfmx1.domainkey.freshemail.io (FQDN)
s3-kz.indriver.com (FQDN) ⟶ a_record ⟶ 185.102.74.214 (IPAddress)
apple.indriver.com (FQDN) ⟶ a_record ⟶ 188.42.196.189 (IPAddress)
apple.indriver.com (FQDN) ⟶ a_record ⟶ 188.42.196.15 (IPAddress)
185.102.72.0/22 (Netblock) ⟶ contains ⟶ 185.102.74.214 (IPAddress)
```

**Bài tập 7: Brute-force các vhosts với trang web indriver.com, có tên miền nào trả về status-code 200 không?**

**Trả lời:**

- Video thực hiện: https://youtu.be/hl7o1p7TQ4Q

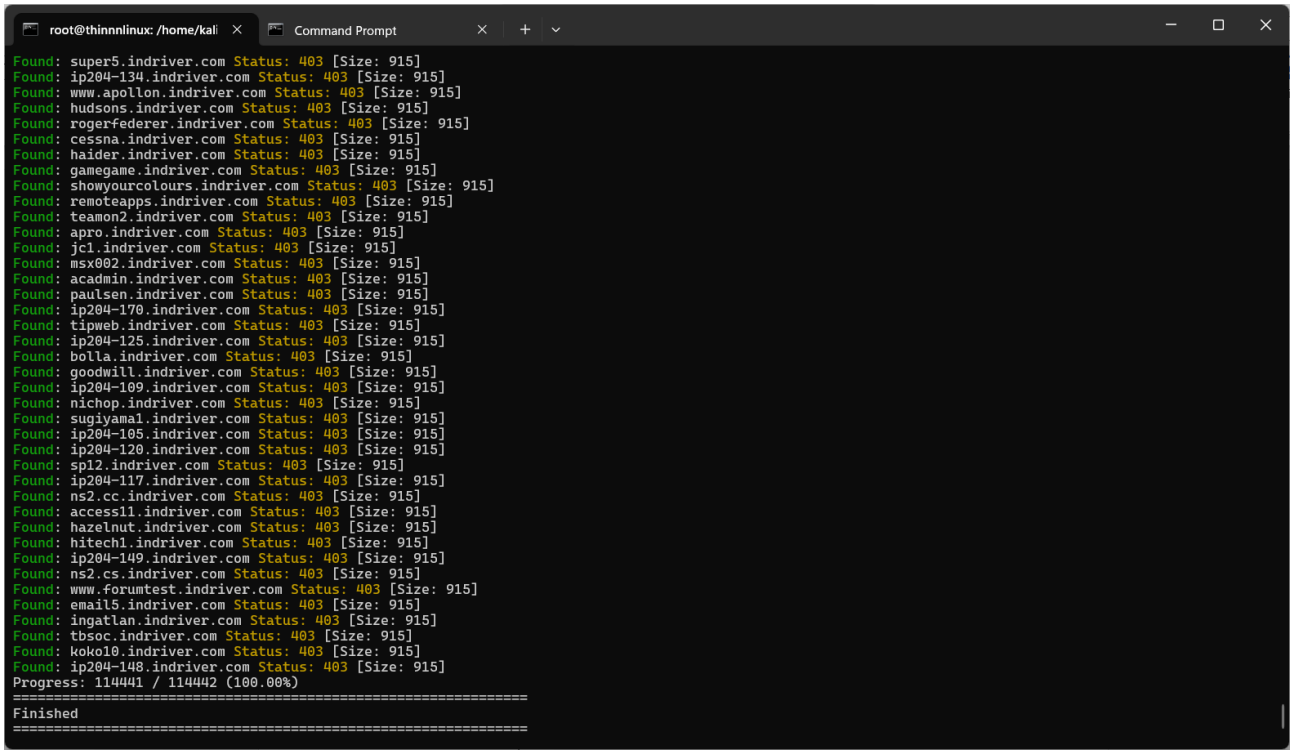
- Bước 1: sử dụng **Gobuster** để brute-force tìm các **virtual hosts (vhosts)** của trang web https://indriver.com, trong đó:

```
┌──(root㉿thinnnlinux)-[/home/kali/Documents/NT213/Lab_3]
└─# gobuster vhost -u http://indriver.com -w subdomains-top1million-110000.txt --append-domain --output gobuster_output.txt
```

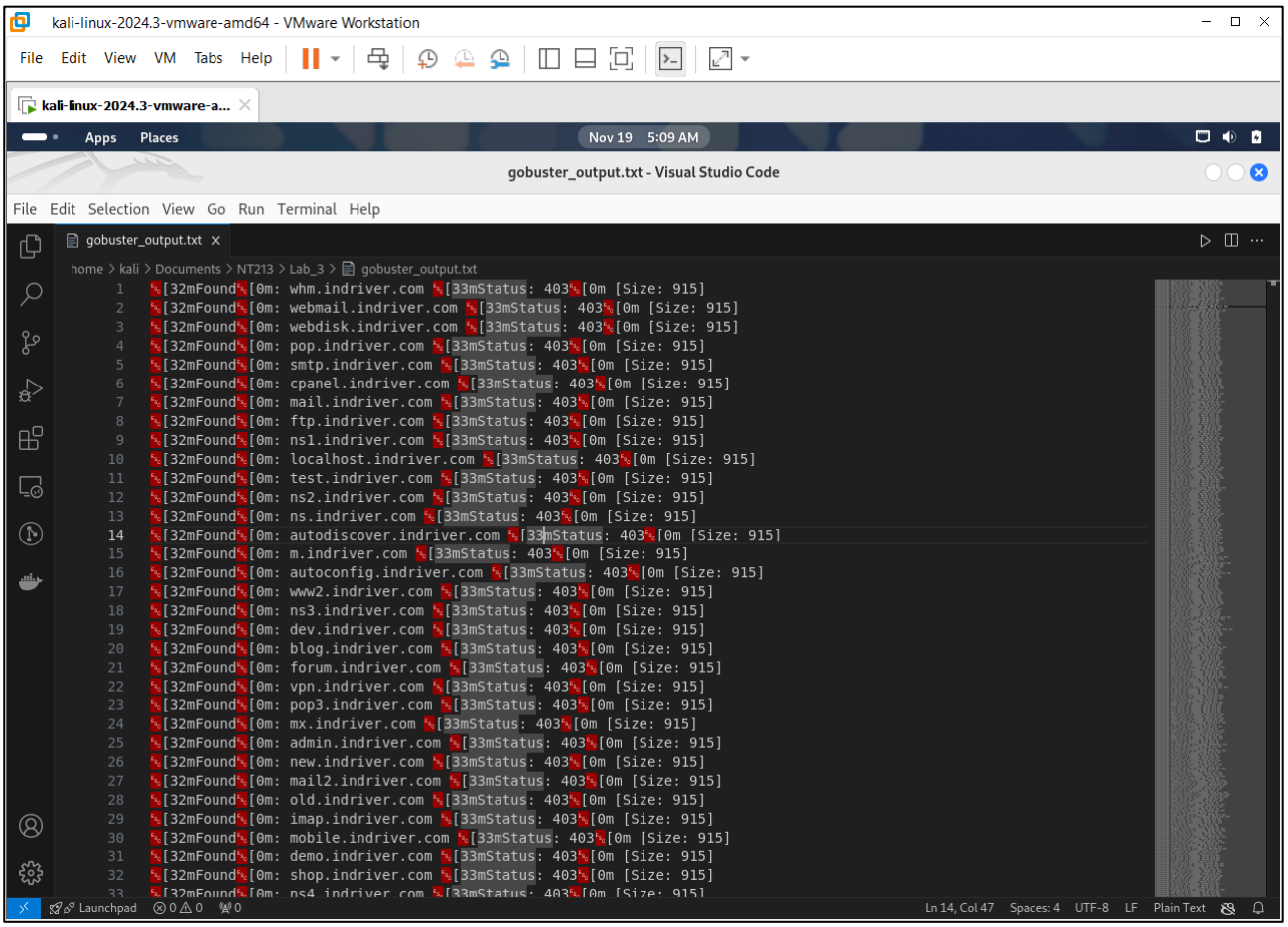
+ Giải thích từng phần lệnh

1. gobuster vhost:
   - Chế độ **vhost** trong Gobuster dùng để brute-force các virtual hosts trên một domain.
   - Virtual hosts là các subdomains hoặc domain được định danh bằng cách sử dụng Host header trong HTTP request.
2. -u http://indriver.com:
   - Chỉ định URL của trang web cần kiểm tra. Ở đây là http://indriver.com.
   - Gobuster sẽ gửi các yêu cầu HTTP đến địa chỉ này.
3. -w subdomains-top1million-110000.txt:
   - Sử dụng file wordlist chứa các tên miền con (subdomains) để brute-force.
   - File subdomains-top1million-110000.txt có danh sách khoảng 110.000 từ thường được sử dụng làm subdomains (VD: admin, login, api).
4. --append-domain: Tự động thêm domain chính indriver.com vào sau mỗi từ trong wordlist. Ví dụ:
   - Từ wordlist: admin
   - Kết quả brute-force: admin.indriver.com
5. --output gobuster_output.txt: Ghi kết quả brute-force vào file gobuster_output.txt. File này sẽ chứa các subdomains được tìm thấy cùng với mã trạng thái (status code) trả về từ server.

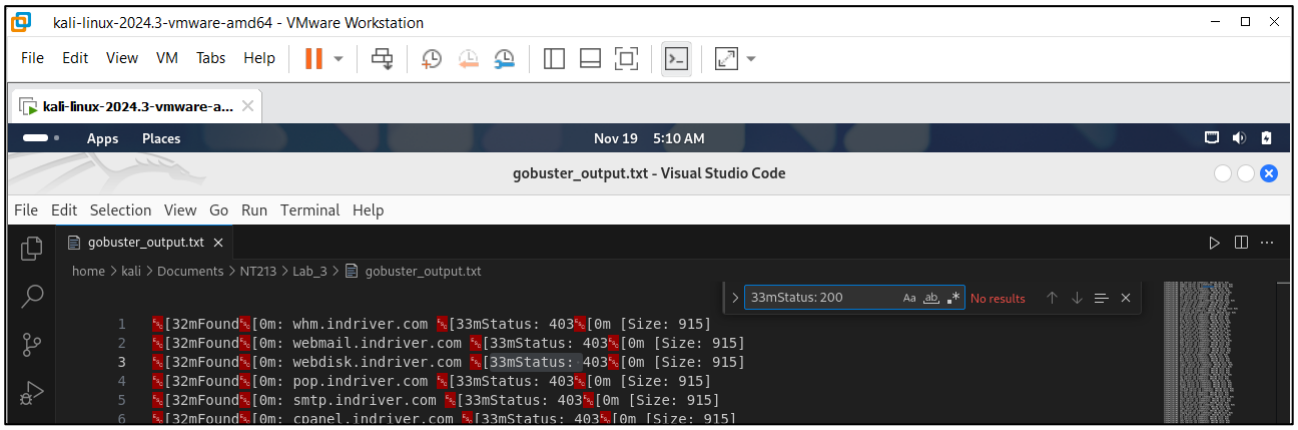
+ Sau khi brute force xong:




- Bước 2: Kiểm tra kết quả:



- Bước 3: Tìm xem mã code 200 trong file output:




- Kết quả cuối cùng ta có thể thấy là không có tên miền nào trả về status-code 200, có thể do:

+ **Vhost không tồn tại**: Các subdomains hoặc virtual hosts trong wordlist có thể không tồn tại thực sự trên máy chủ indriver.com. Trong trường hợp này, server sẽ trả về mã lỗi 404 (Not Found) hoặc 403 (Forbidden) nếu server tồn tại nhưng không cho phép truy cập.

+ **Trang web yêu cầu xác thực**: Nếu một trang web yêu cầu xác thực người dùng (như đăng nhập), Gobuster có thể nhận được mã lỗi 403 (Forbidden) vì không có thông tin xác thực trong yêu cầu.

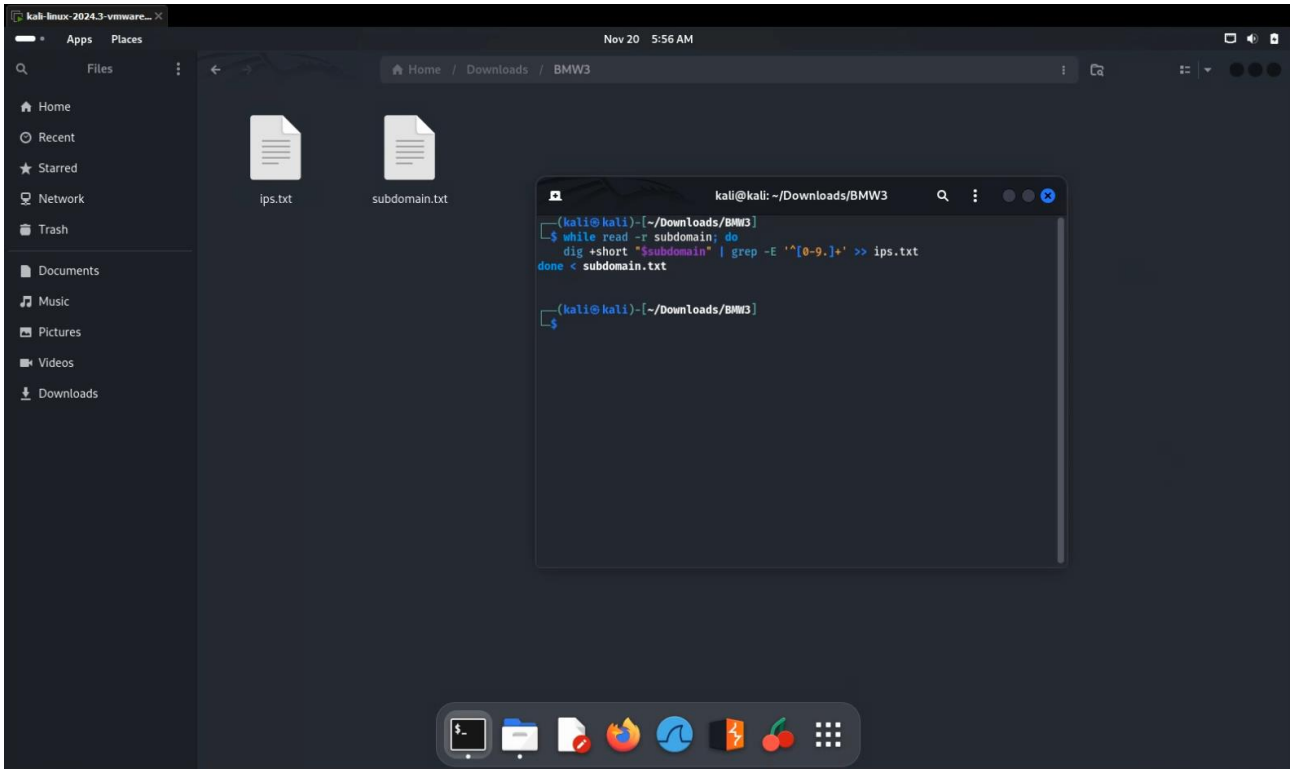
+ **Cấu hình server chặn brute-force**: Server có thể sử dụng các biện pháp bảo mật (như rate limiting, firewall, hoặc các phương pháp bảo vệ khác) để chặn các yêu cầu từ các công cụ như Gobuster, khiến tất cả các yêu cầu trả về mã 403 hoặc các mã trạng thái khác.

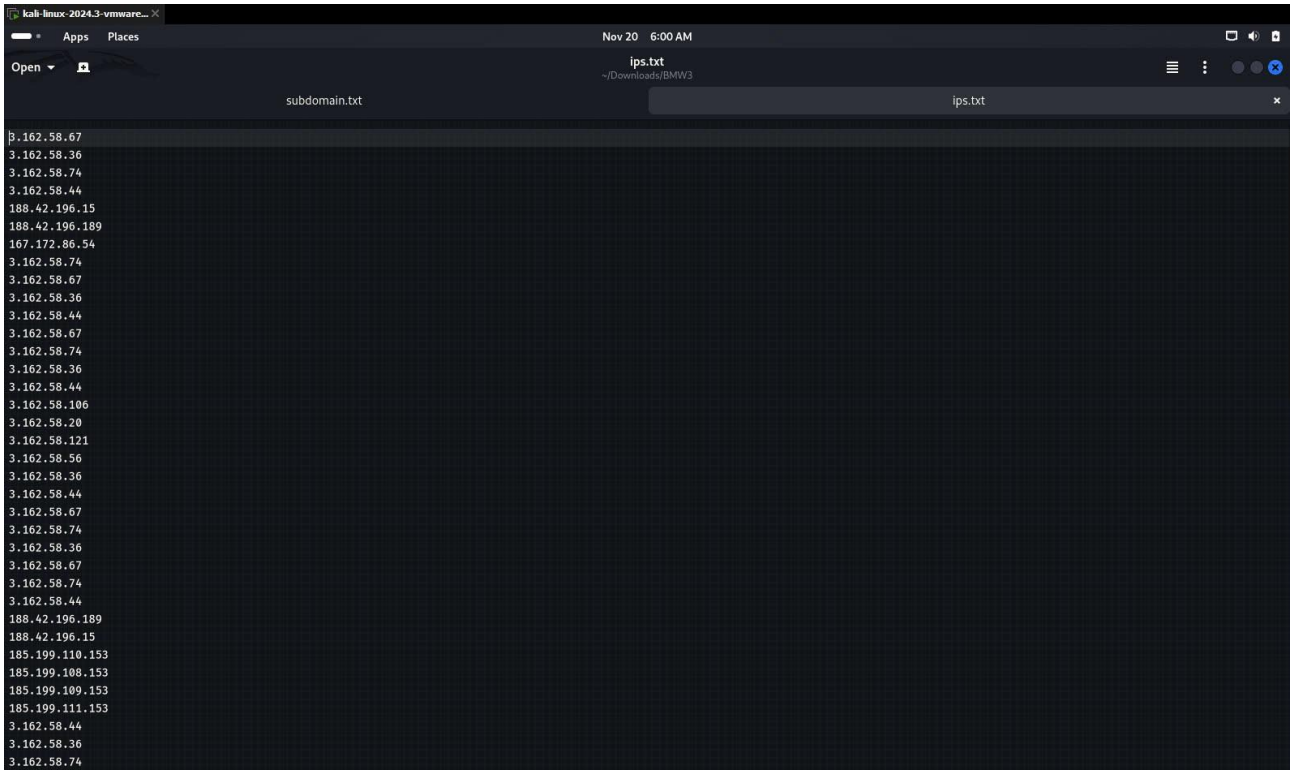
+ **Tên miền bị ẩn hoặc không cấu hình**: Một số subdomains có thể đã được cấu hình nhưng bị ẩn hoặc không được phép truy cập công khai (có thể đã bị tắt hoặc bị chặn trong cấu hình của máy chủ).

**Bài tập 8: Brute-force các vhosts với trang web indriver.com, có tên miền nào trả về status-code 200 không?**

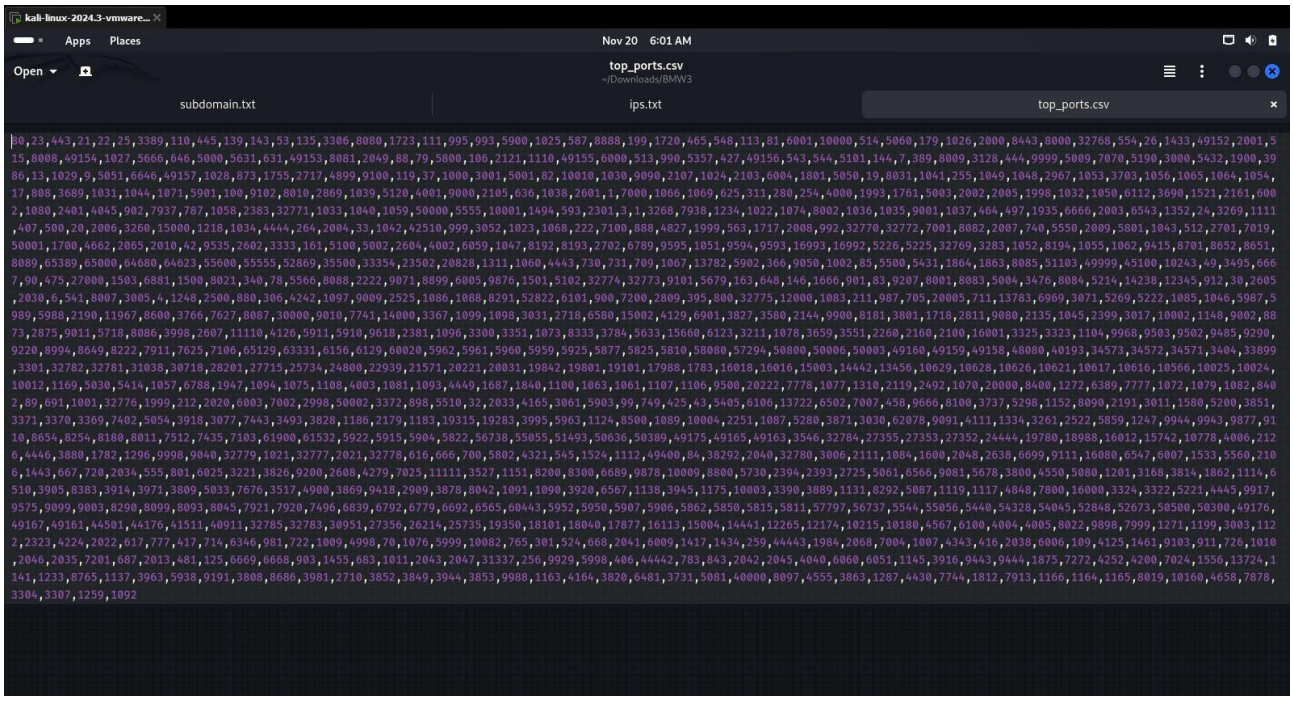
**Trả lời:**

- Video thực hiện: https://youtu.be/R6b0RqCLl1I
- Ta sẽ sử dụng lại danh sách subdomain submain.txt đã lấy được ở các task trước
- Sử dụng lệnh dig để lấy địa chỉ IP từ các subdomain trong danh sách vào file ips.txt

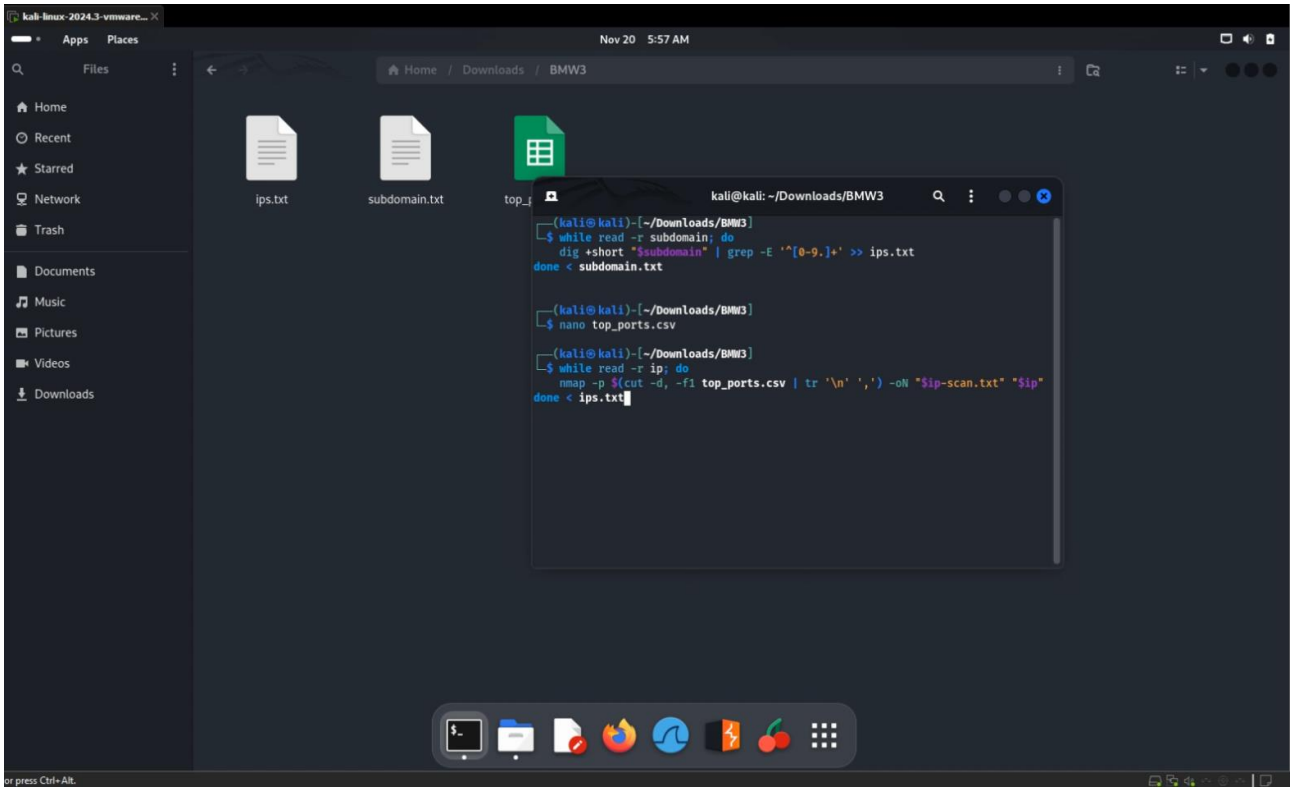


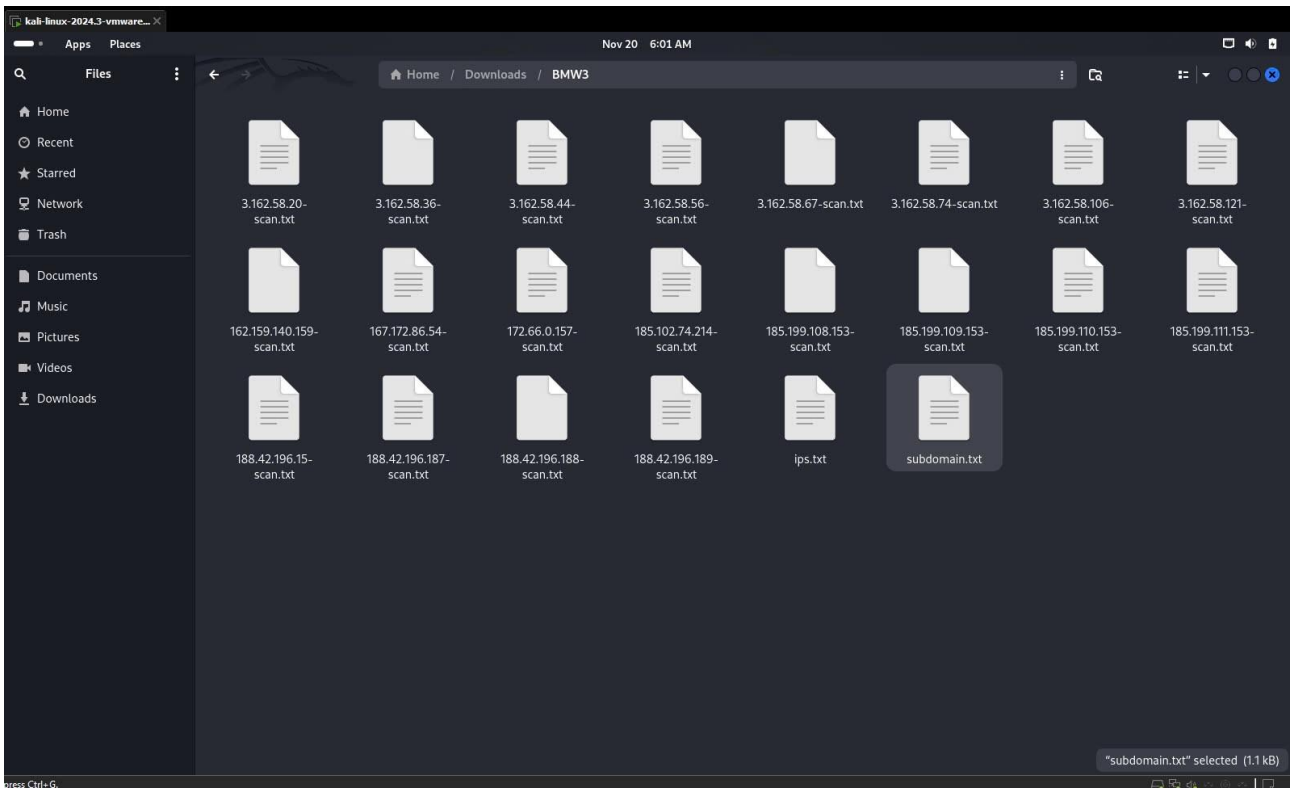



- Thực hiện lấy danh sách 1000 port phổ biến về file top_ports.csv

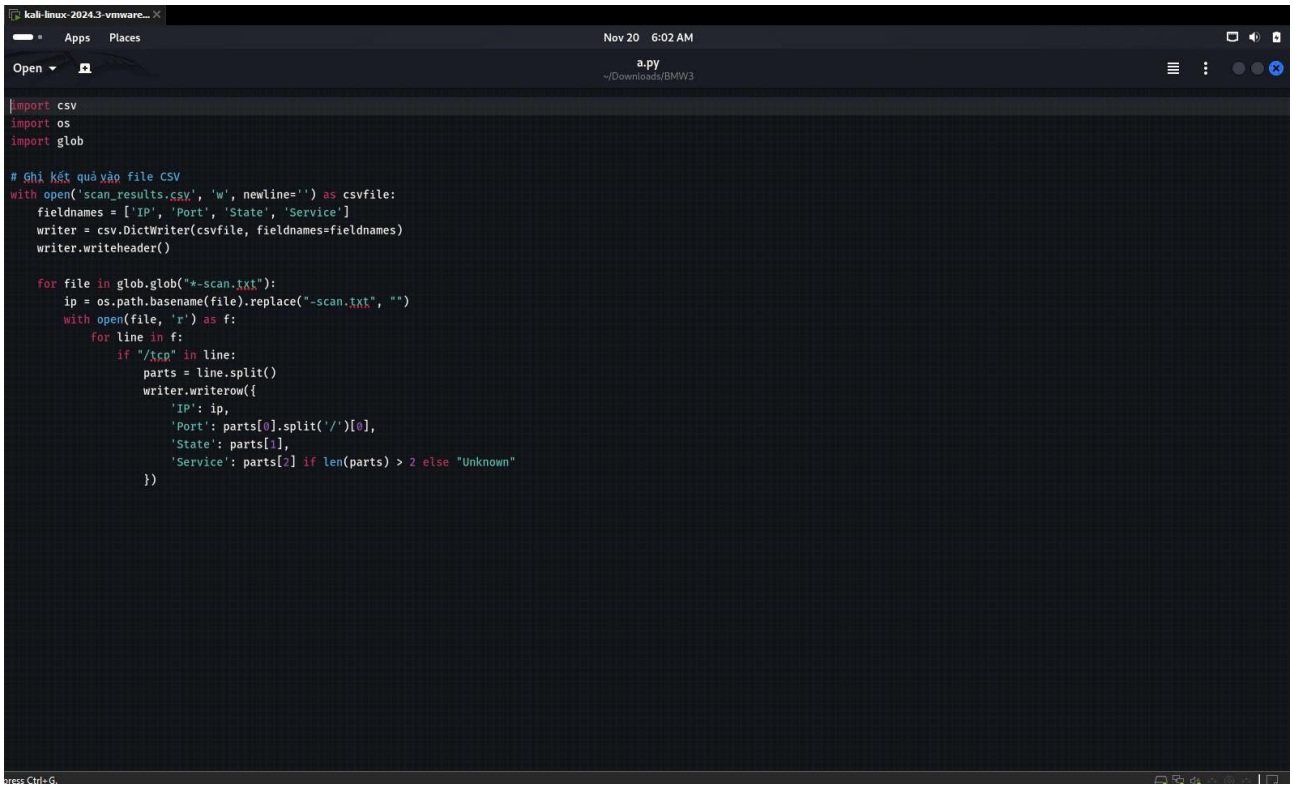



- Sử dụng nmap để scan 1000 port phổ biến trên các IP tìm được

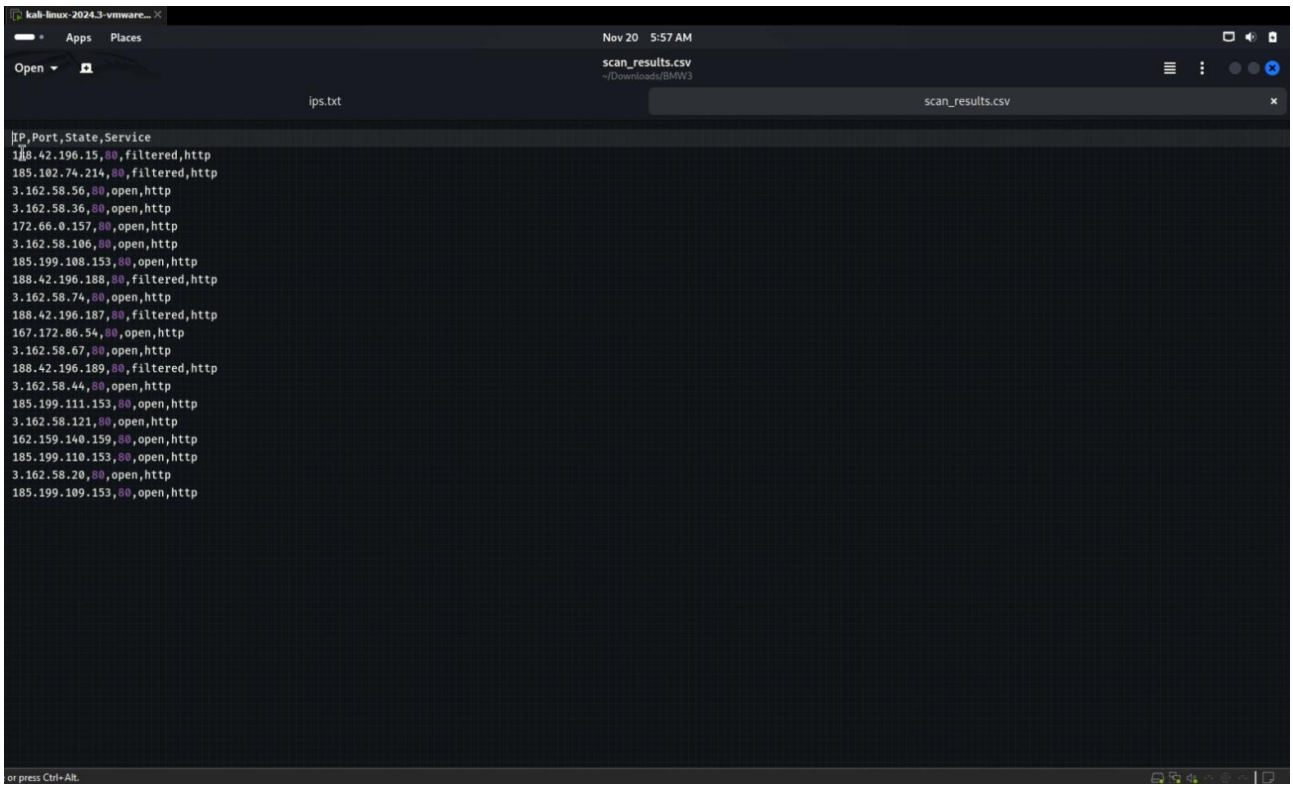





- Sau đó dùng 1 file python với tác dụng tổng hợp két quả từ các file .txt của nmap thành csv




- Ta được file kết quả như sau:

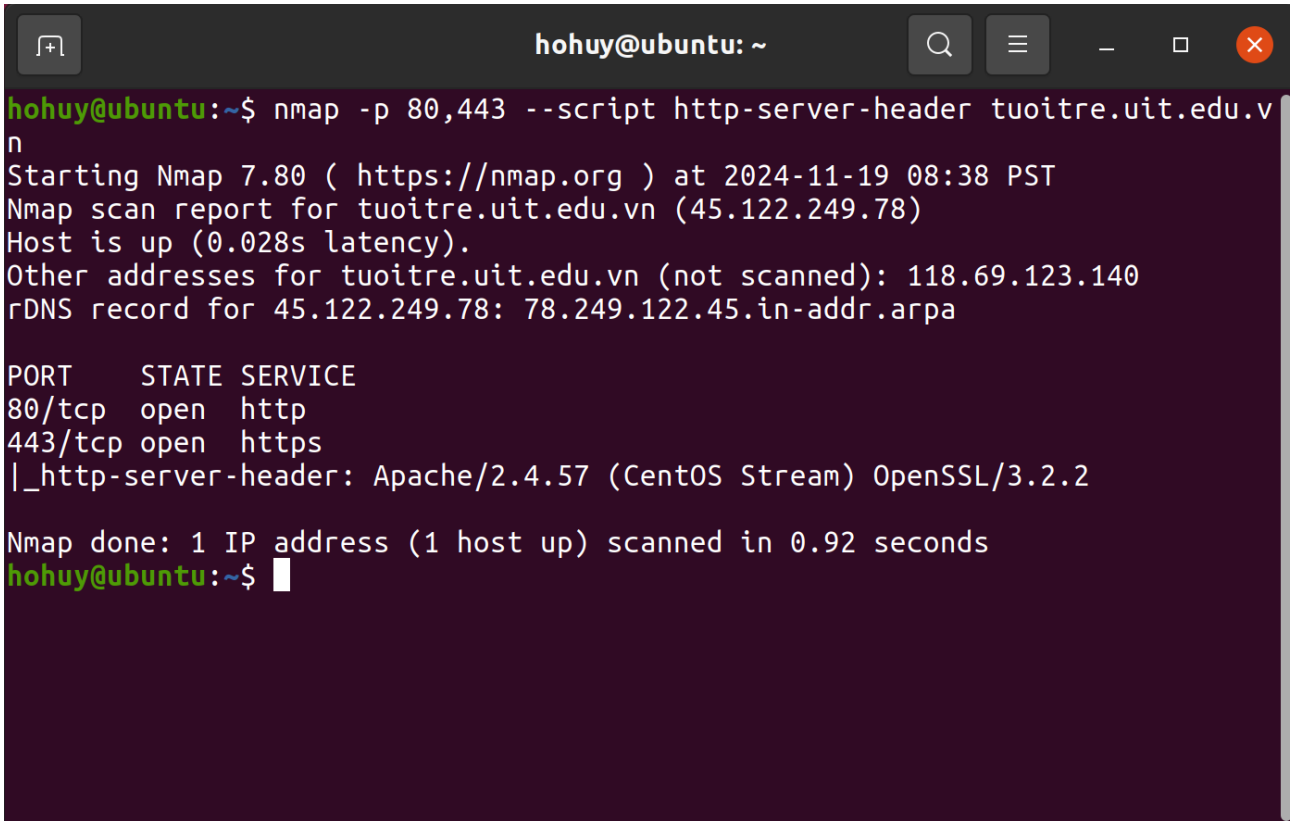

kali-linux-2024.3-vmware...
Apps Places
Nov 20 5:57 AM
Open
scan_results.csv
~/Downloads/BMW3
ips.txt
scan_results.csv
IP,Port,State,Service
188.42.196.15,80,filtered,http
185.102.74.214,80,filtered,http
3.162.58.56,80,open,http
3.162.58.36,80,open,http
172.66.0.157,80,open,http
3.162.58.106,80,open,http
185.199.108.153,80,open,http
188.42.196.188,80,filtered,http
3.162.58.74,80,open,http
188.42.196.187,80,filtered,http
167.172.86.54,80,open,http
3.162.58.67,80,open,http
188.42.196.189,80,filtered,http
3.162.58.44,80,open,http
185.199.111.153,80,open,http
3.162.58.121,80,open,http
162.159.140.159,80,open,http
185.199.110.153,80,open,http
3.162.58.20,80,open,http
185.199.109.153,80,open,http
or press Ctrl+Alt.

**Bài tập 9. Xác định phiên bản Apache được sử dụng của web tuoitre.uit.edu.vn.**

- Video thực hiện: https://youtu.be/Sv9SQxOT8ug

- Sử dụng nmap để thực hiện quét, lệnh này sẽ quét các cổng 80 và 443 (HTTP và HTTPS) và kiểm tra các thông tin phiên bản từ tiêu đề HTTP Server.

nmap -p 80,443 --script http-server-header tuoitre.uit.edu.vn



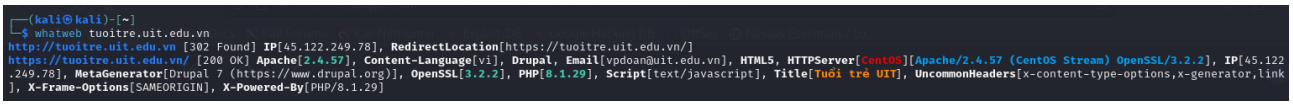

- Kết quả: Apache/2.4.57

**Bài tập 10: CMS nào được sử dụng của trang web tuoitre.uit.edu.vn.**

**Trả lời:**

- Video thực hiện: https://youtu.be/vEOiJD637yo

- Sử dụng công cụ whatweb để quét trang tuoitre.uit.edu.vn



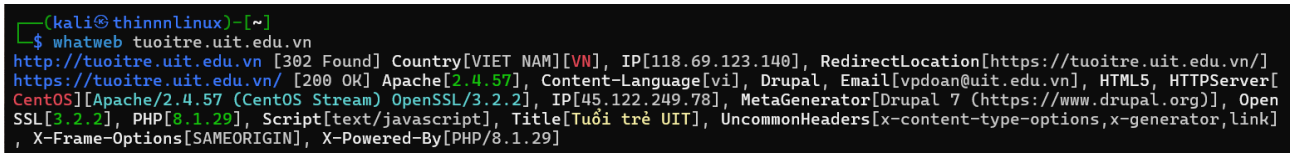

- Ta biết được rằng trang này sử dụng CMS Drupal 7 qua trường thông tin MetaGenerator

**Bài tập 11: Hệ điều hành và webserver nào được sử dụng của trang web tuoitre.uit.edu.vn.**

**Trả lời:**

- Video thực hiện: https://youtu.be/ncjIVS1peDE

- Ta sử dụng WhatWeb - 1 công cụ giúp xác định các công nghệ đang được sử dụng trên một trang web.




- Dựa trên kết quả từ công cụ WhatWeb, trang web **tuoitre.uit.edu.vn** sử dụng các công nghệ sau:

+ Webserver: Apache 2.4.57 (CentOS Stream)

+ Hệ điều hành: CentOS Stream

+ CMS: Drupal 7

+ Phiên bản PHP: 8.1.29

+ OpenSSL: 3.2.2

+ Header HTTP: X-Frame-Options: SAMEORIGIN, X-Powered-By: PHP/8.1.29

- Trang web sử dụng:

+ Hệ điều hành: **CentOS Stream**

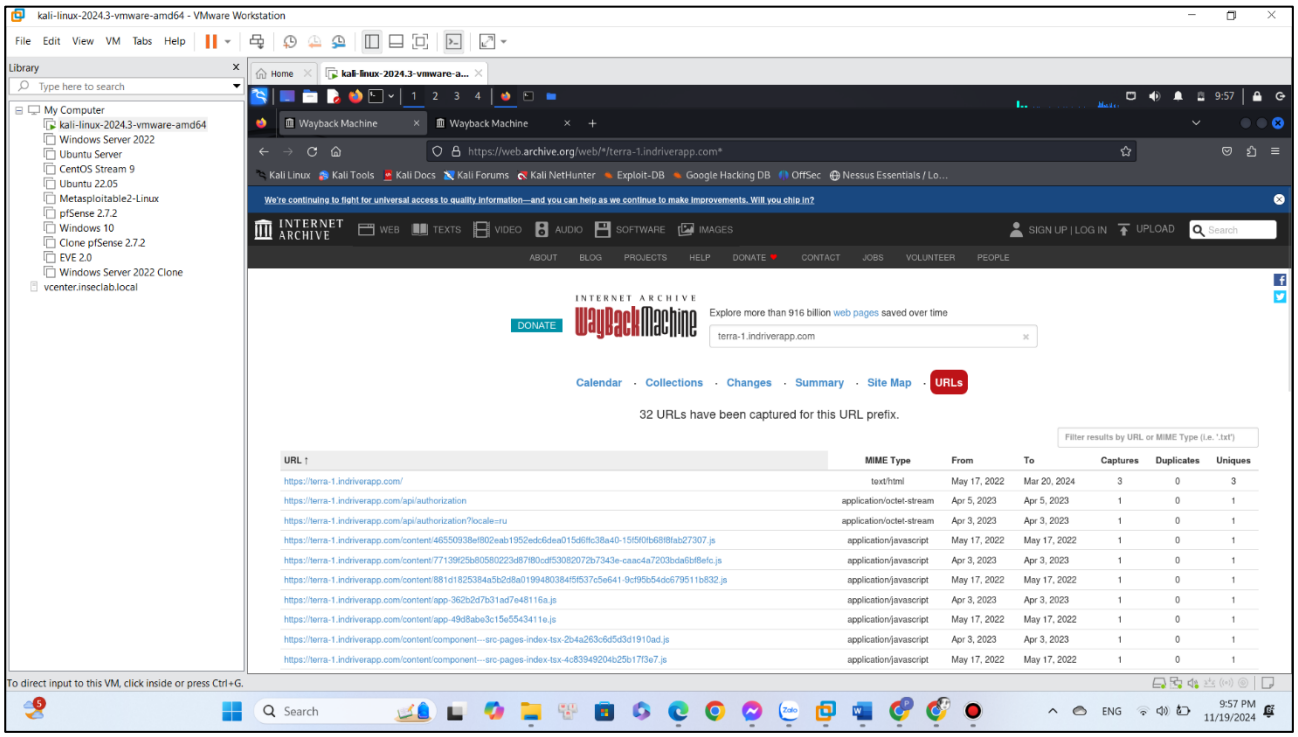
+ Webserver: **Apache/2.4.57 (CentOS Stream)**

**Bài tập 12: 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?**

**Trả lời:**

- Video thực hiện: https://youtu.be/AEP3oXgUhIo

- 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




- Ta tìm thấy file https://terra-1.indriverapp.com/robots.txt

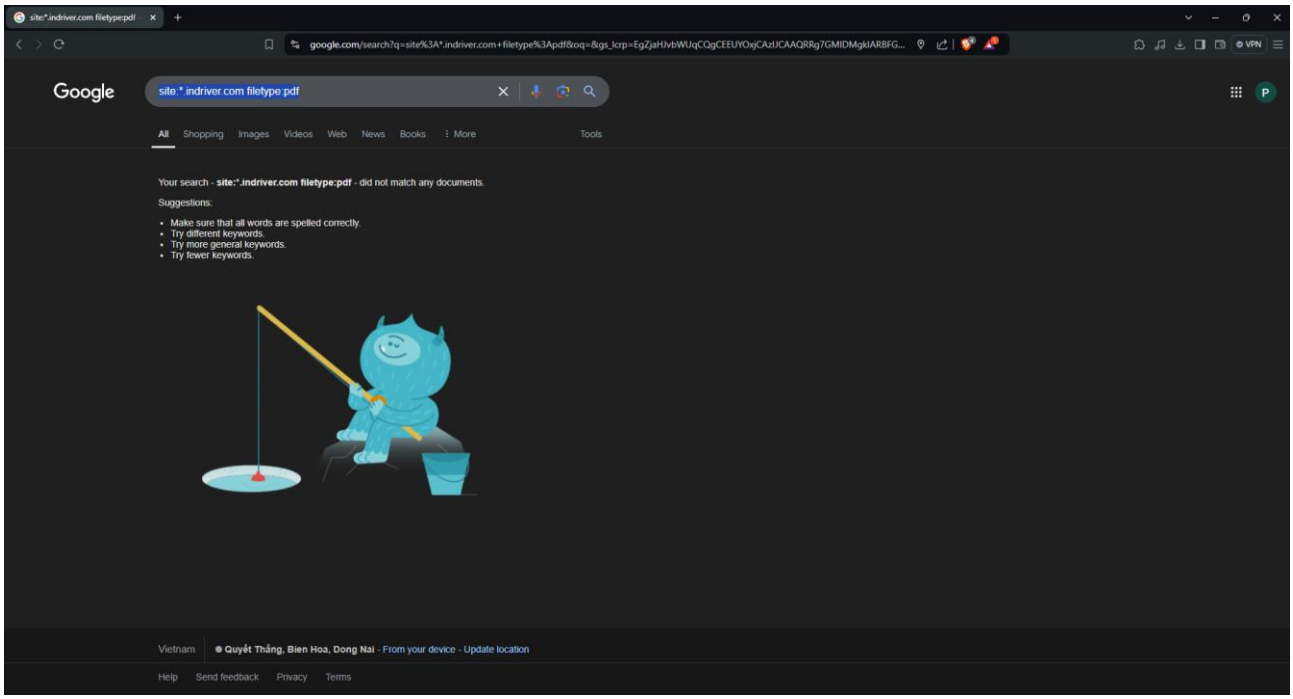

- Theo kết quả tìm kiếm trên Internet, file robots.txt là tệp văn bản trong thư mục gốc của trang web, dùng để hướng dẫn bot công cụ tìm kiếm (web crawler) về các khu vực được phép hoặc không được phép thu thập dữ liệu. Nó chứa các chỉ thị như User agent (bot áp dụng), Disallow (chặn truy cập), và Sitemap (đường dẫn sơ đồ trang web). Tuy nhiên, robots.txt không bảo mật và chỉ là một hướng dẫn cho bot.

**Bài tập 13: Tìm kiếm các tập tin pdf, excel, word, trên *.indriver.com.**

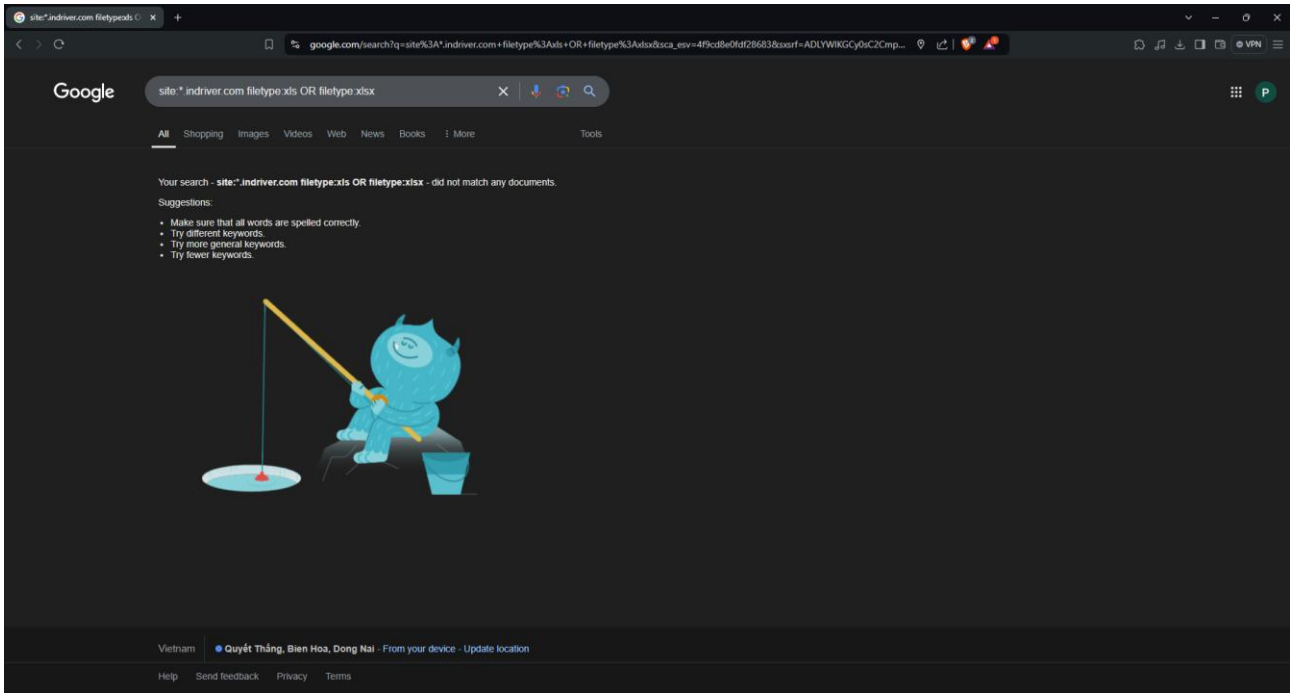
**Trả lời:**

- Video thực hiện: https://youtu.be/7QuJ3VYoqiU
- Lần lượt thực hiện các tìm kiếm trên google như sau:

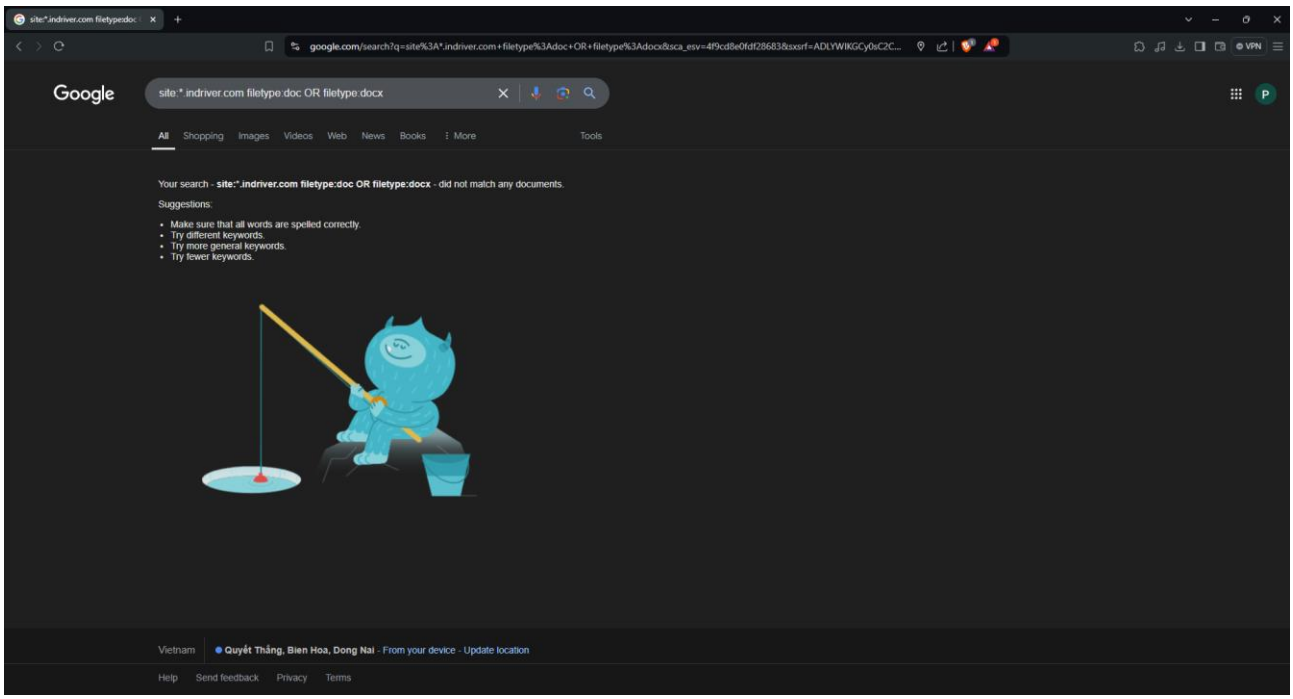
+ Tìm kiếm các tập tin pdf: site:*.indriver.com filetype:pdf




+ Tìm kiếm các tập tin excel: site:*.indriver.com filetype:xls OR filetype:xlsx




+ Tìm kiếm các tập tin Word: site:*.indriver.com filetype:doc OR filetype:docx

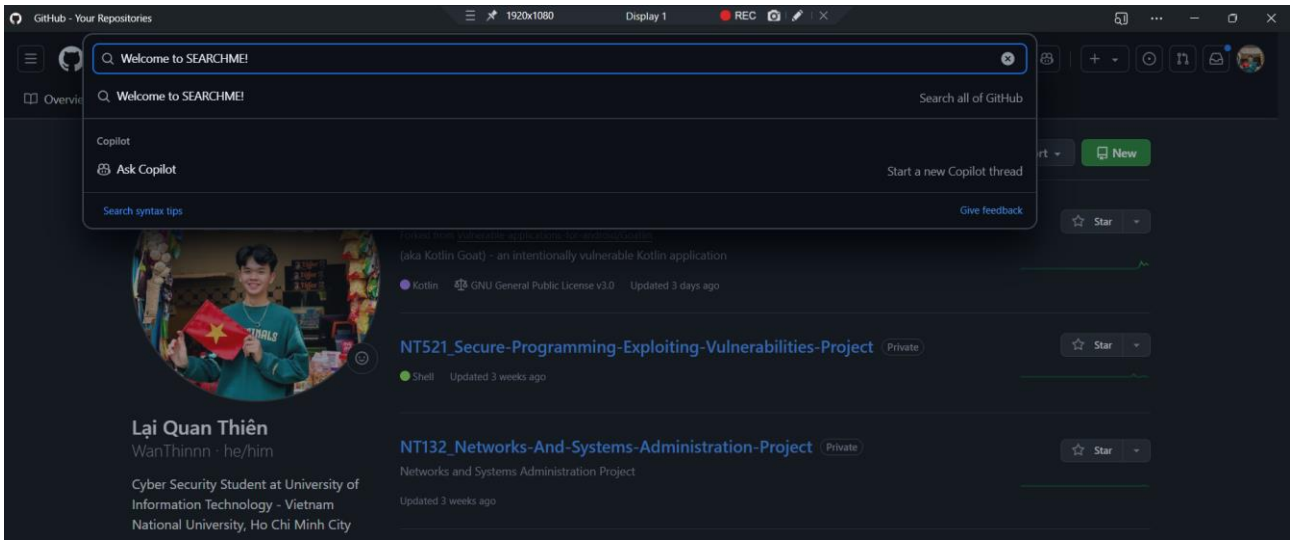

site:*.indriver.com filetype:doc
google.com/search?q=site%3A*.indriver.com+filetype%3Adoc+OR+filetype%3Adocx&sca_esv=4f9cd8e0fdf28683&sxsrf=ADLYWIKGCy0sC2C...
Google
site:*.indriver.com filetype:doc OR filetype:docx
All Shopping Images Videos Web News Books More Tools
Your search - site:*.indriver.com filetype:doc OR filetype:docx - did not match any documents.
Suggestions:
Make sure that all words are spelled correctly.
Try different keywords.
Try more general keywords.
Try fewer keywords.
Vietnam
Quyết Thắng, Bien Hoa, Dong Nai - From your device - Update location
Help Send feedback Privacy Terms

**Bài tập 14: 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.**

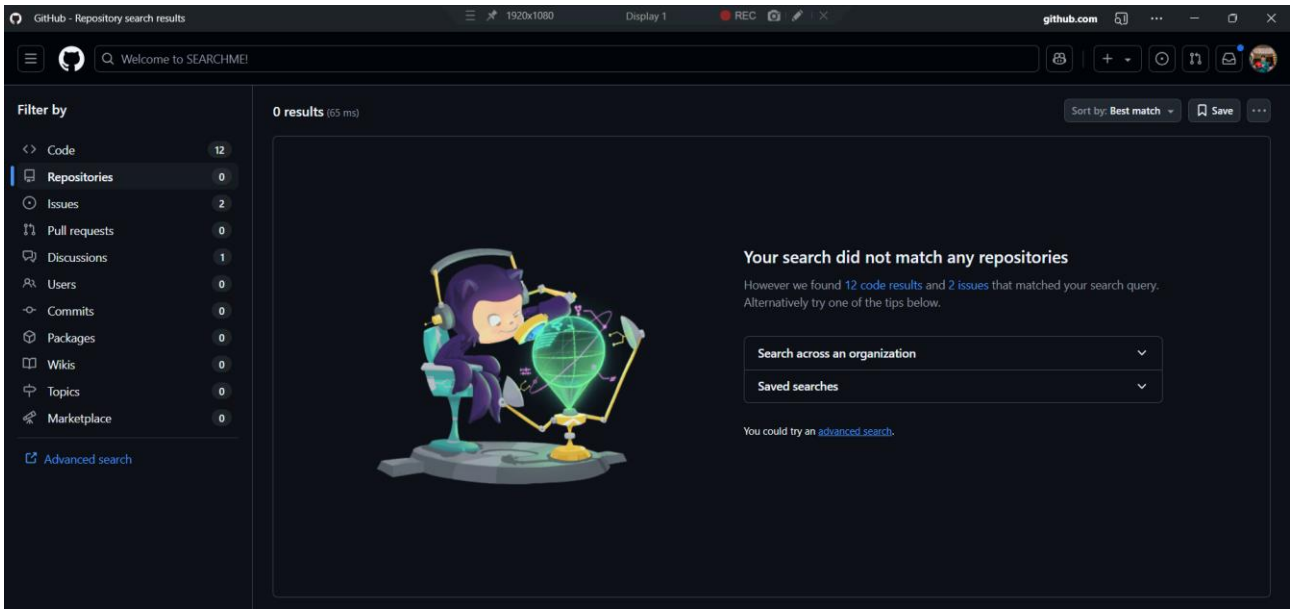
**Trả lời:**

- Video thực hiện: https://youtu.be/jS2w4ziKww0

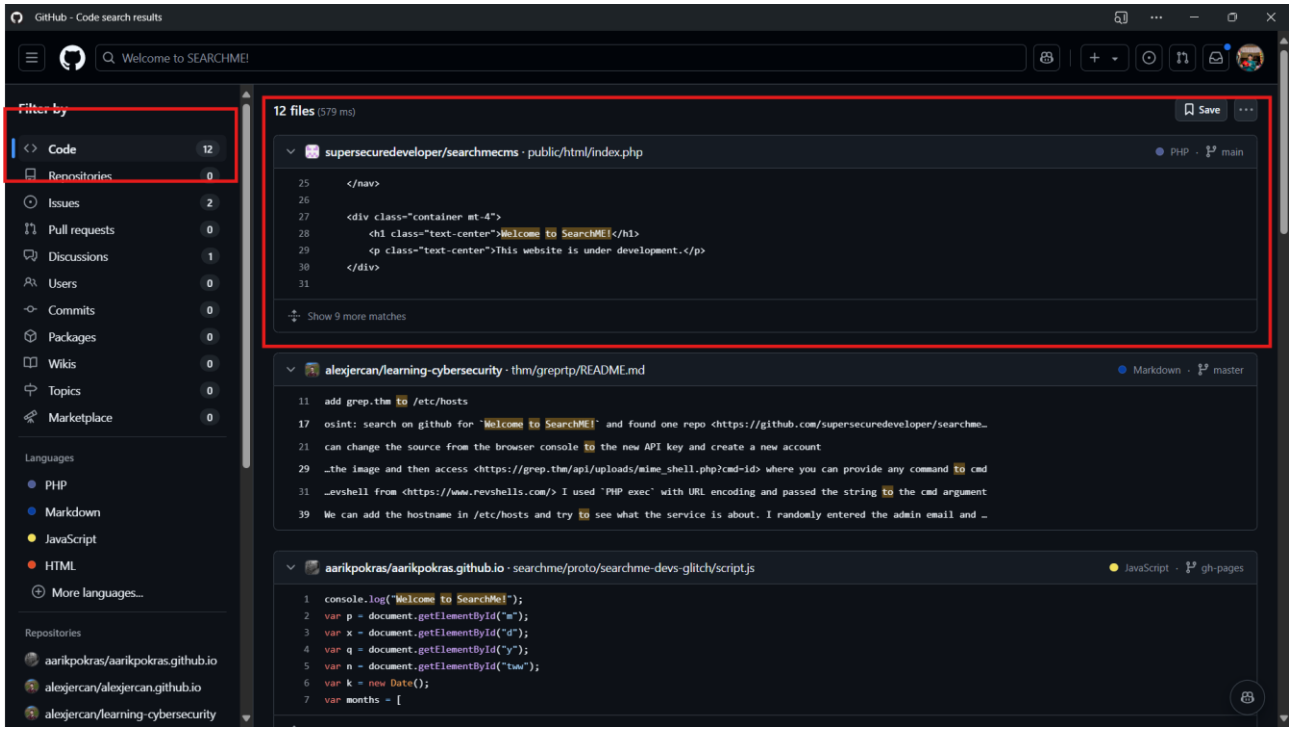
- Trước tiên, ta cần tìm kiếm trong github với cụm từ được gợi ý trên trang bài tập: "Welcome to SEARCHME!"



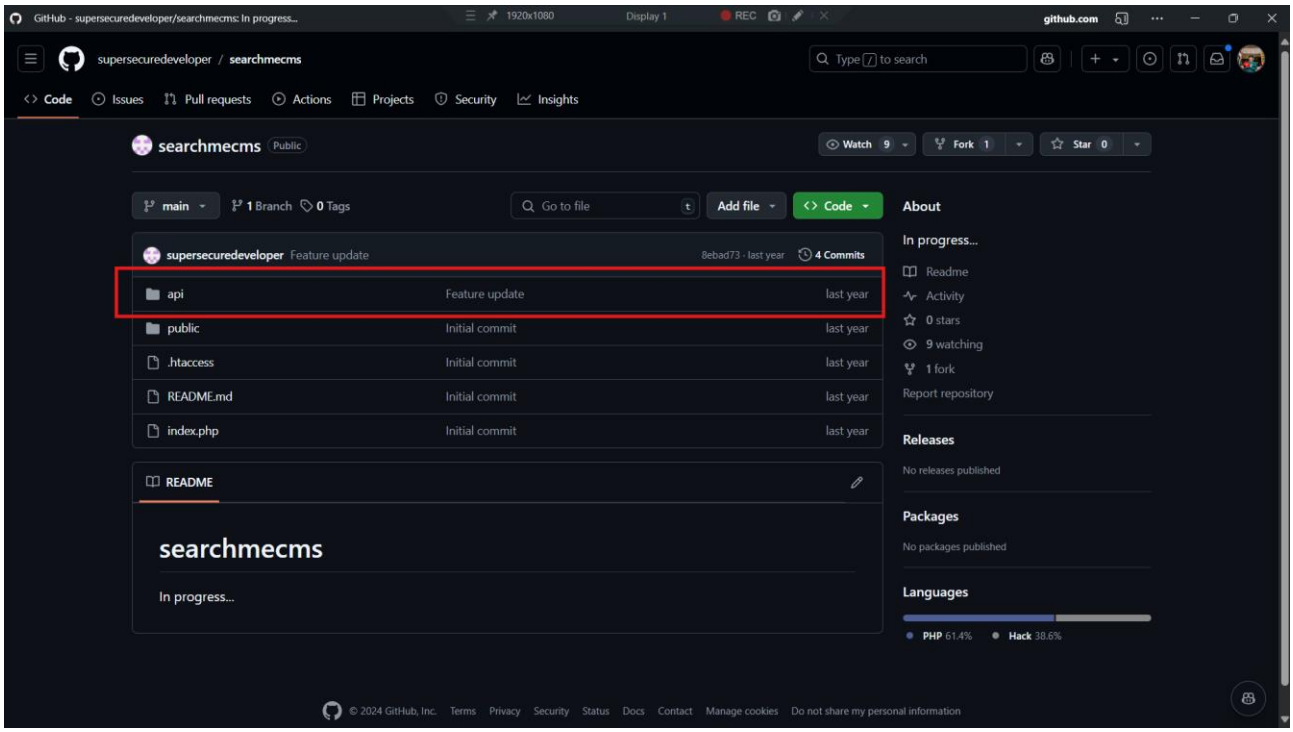

- Có thể thấy ta tìm được 12 code results và 2 issues trên github:



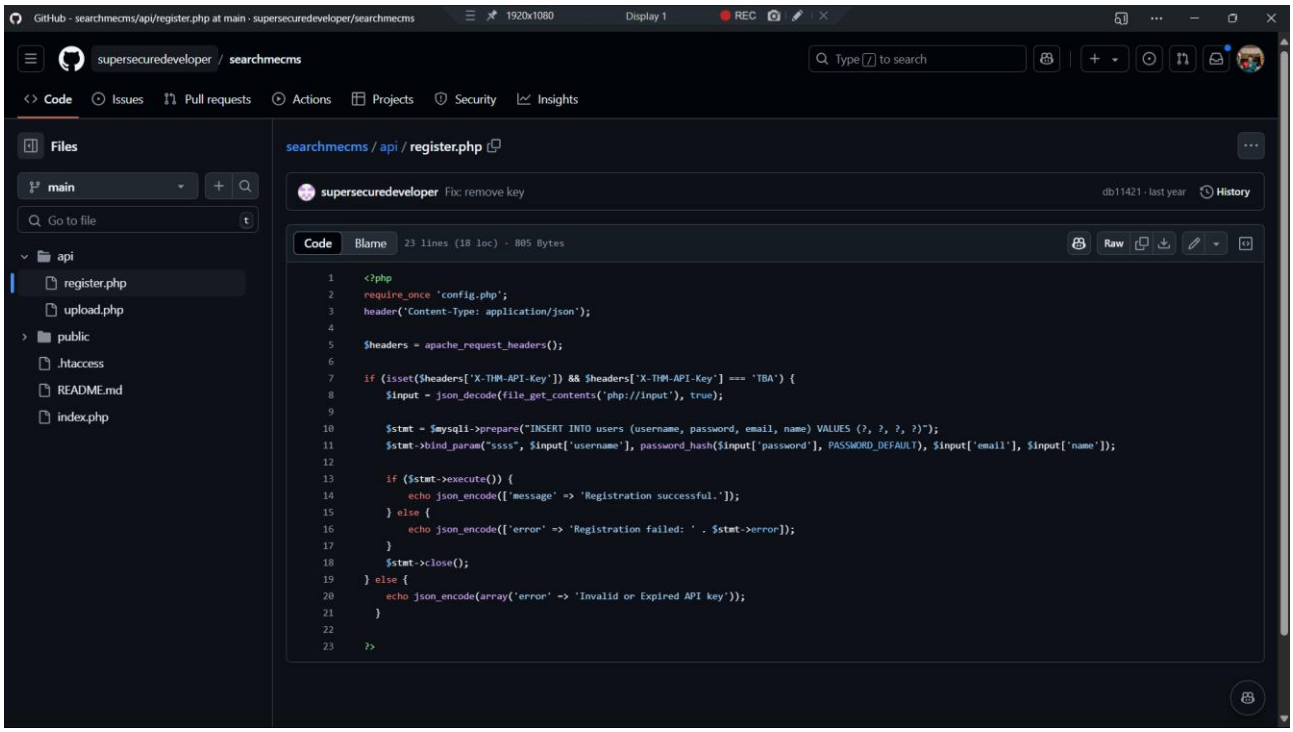
- Ta truy cập vào mục "Code" và tìm được đoạn code khá tương đồng với giao diện được gợi ý trong bài lab.




- Truy cập vào Repo -> API



- Vậy là ta đã tìm thấy API key cho phép user tạo tài khoản:




- Nhận định: Trong đoạn mã PHP trên, **API key** được sử dụng để bảo vệ và xác thực các yêu cầu đăng ký tài khoản từ người dùng. Cụ thể, khi một yêu cầu được gửi tới máy chủ, API key sẽ được kiểm tra trong phần **header** của yêu cầu. Cụ thể:

+ **Kiểm tra API key**: Đoạn mã sẽ kiểm tra xem yêu cầu có chứa header X-THM-API-Key hay không và nếu có, nó sẽ so sánh giá trị của API key với giá trị 'TBA'. Nếu API key khớp, yêu cầu sẽ được tiếp tục xử lý; nếu không, hệ thống sẽ trả về thông báo lỗi.

+ **Xử lý dữ liệu đăng ký**: Nếu API key hợp lệ, mã sẽ đọc dữ liệu JSON từ thân yêu cầu (sử dụng php://input) và thực hiện thao tác thêm người dùng vào cơ sở dữ liệu. Cụ thể, nó sẽ chuẩn bị một câu lệnh SQL để thêm thông tin người dùng mới vào bảng users, bao gồm tên đăng nhập, mật khẩu (được mã hóa), email và tên.

+ **Thông báo kết quả**: Sau khi thực hiện thao tác thêm người dùng vào cơ sở dữ liệu, hệ thống trả về thông báo thành công hoặc lỗi dưới dạng JSON, giúp hệ thống phía client xử lý tiếp.

+ **Nếu API key không hợp lệ**: Nếu API key không hợp lệ hoặc không có trong header, mã sẽ trả về thông báo lỗi rằng API key không hợp lệ hoặc đã hết hạn.

- Tóm tắt API key trong đoạn mã này:

+ **Mục đích**: Xác thực và bảo mật yêu cầu trước khi cho phép thực hiện các thao tác tạo tài khoản.

+ **Kiểm tra**: API key phải được gửi trong header của yêu cầu dưới tên X-THM-API-Key, và giá trị phải khớp với 'TBA' để yêu cầu tiếp tục.

+ **Nếu không hợp lệ**: Trả về thông báo lỗi "Invalid or Expired API key".

=> Đoạn mã này cho phép tạo tài khoản người dùng qua một API được bảo vệ bằng API key, giúp ngăn chặn các truy cập không hợp lệ từ những người dùng không có quyền.

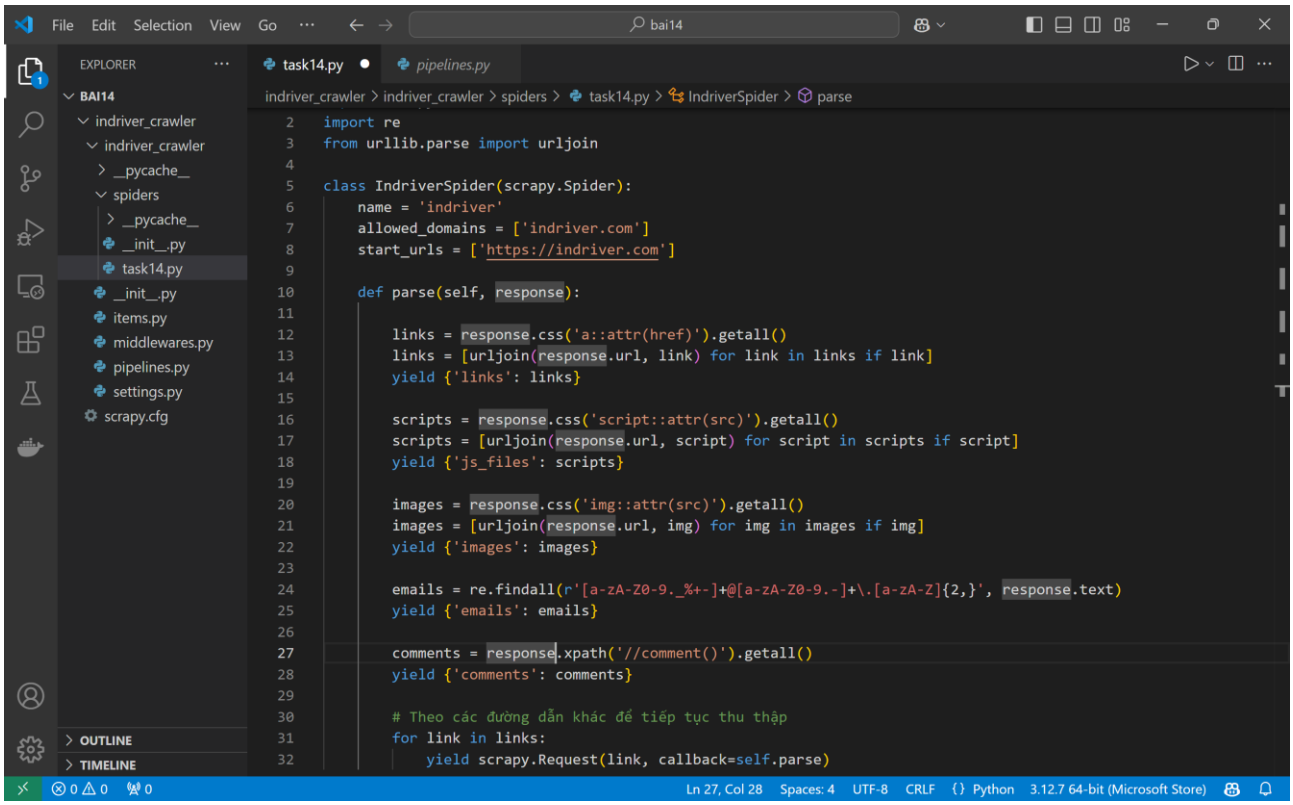
**Bài tập 15: Viết code crawling trang web https://indriver.com để lấy các thông tin liên quan như list email, các đường dẫn liên kết (links), danh sách js, images, comment. Gợi ý: có thể dùng thư viện scrapy của python.**

- Video thực hiện: https://youtu.be/U4caBbkQzFk

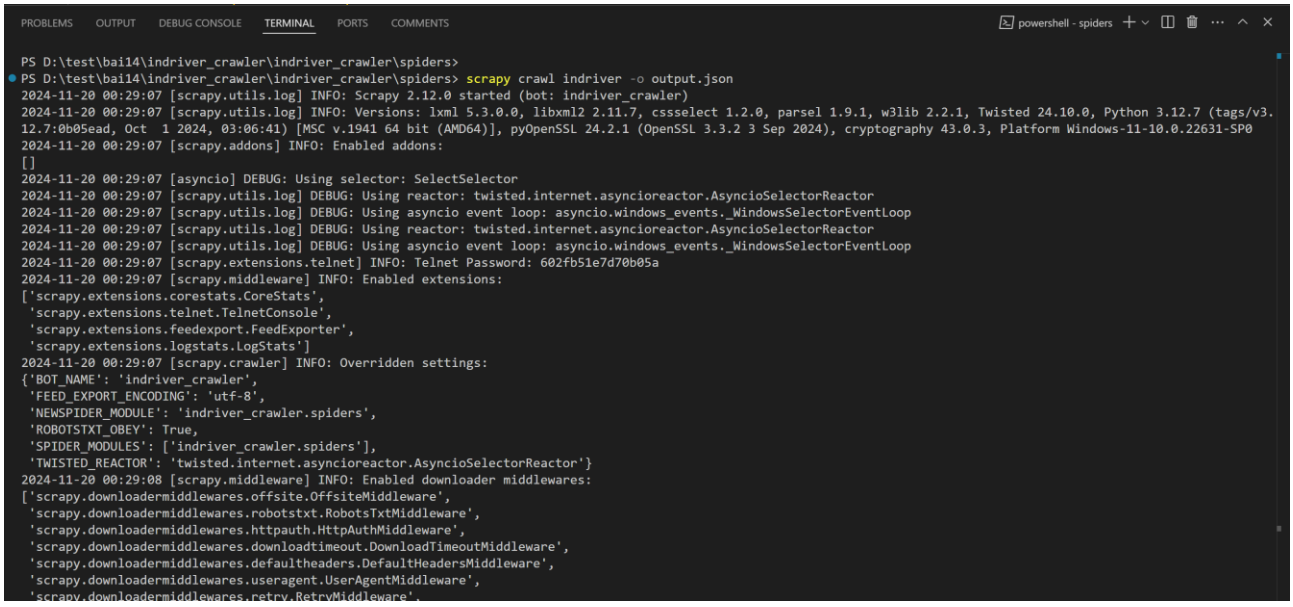
- Tạo dự án scrapy bằng lệnh:

**scrapy startproject indriver_crawler**

- Thêm file code crawling vào indriver_crawler/spiders ta được dự án như hình:




- Chạy Spider scrapy crawl indriver -o output.json:



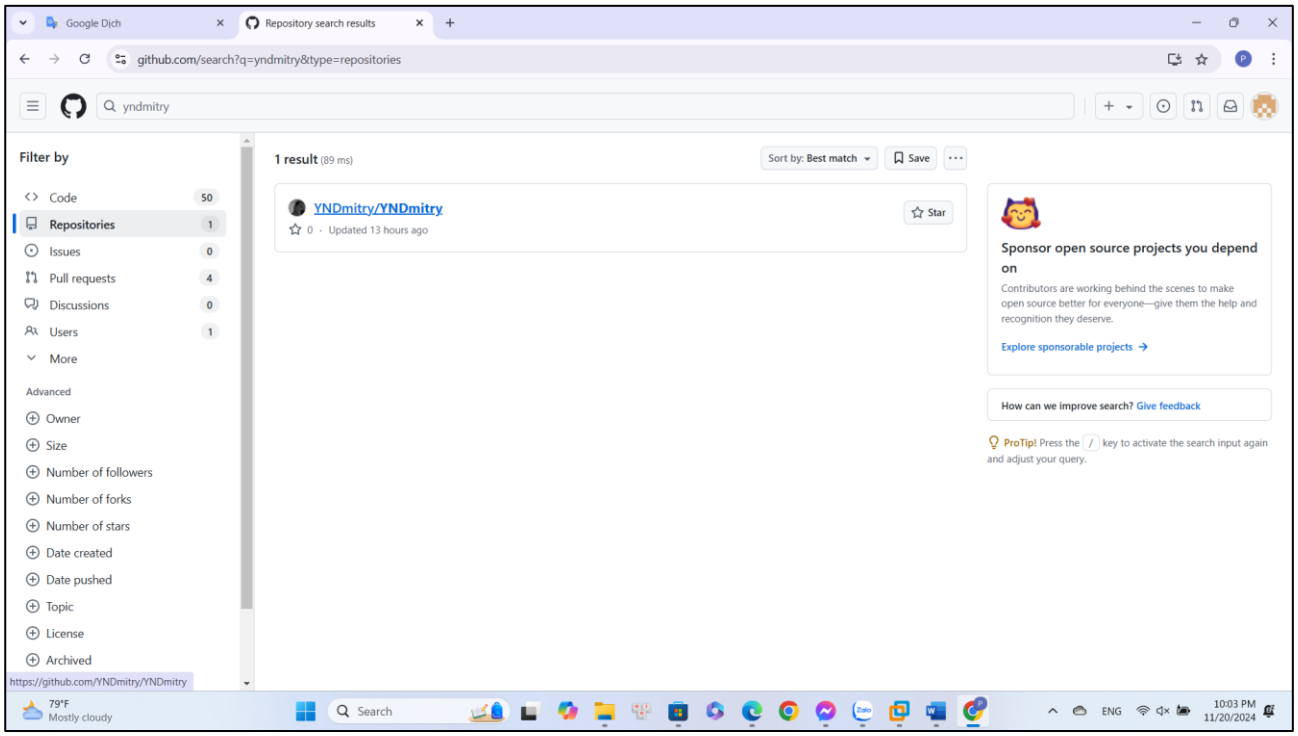
- output.json:

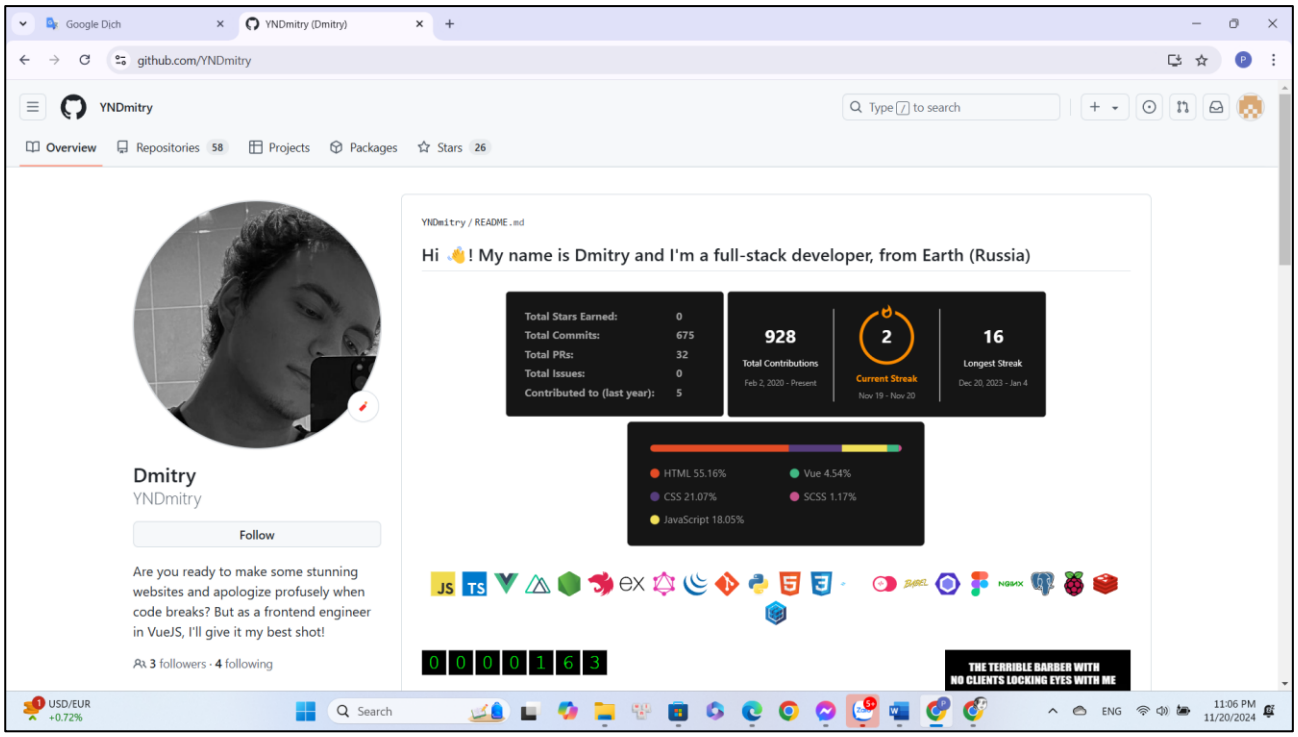

indriver_crawler > indriver_crawler > spiders > {} output.json > ...
[
{"links": ["https://indrive.com/en-vn", "https://indrive.com/en-vn/fair-services", "https://indrive.com/en-vn/city-rides", "https://indrive.com/en-vn/intercity-ride
{"js_files": ["https://indrive.com/_next/static/chunks/polyfills-42372ed130431b0a.js", "https://indrive.com/_next/static/chunks/webpack-4ae7d6faa12f89f1.js", "https
{"images": ["https://indrive.com/images/logo/logo--white.svg", "https://indrive.com/images/logo/logo--dark.svg", "https://indstatic.io/indstatic-main/flags/VN.svg",
{"emails": ["support@indrive.com", "support@indrive.com", "support@indriver.com", "support@indrive.com", "u003esupport@indrive.com", "gr@indrive.com", "u003egr@indr
{"comments": ["<!-- -->", "<!-- -->", "<!-- -->", "<!-- -->"]}
]

**Bài tập luyện tập: Which sites did YNDmitry develop on inDrive.com?**

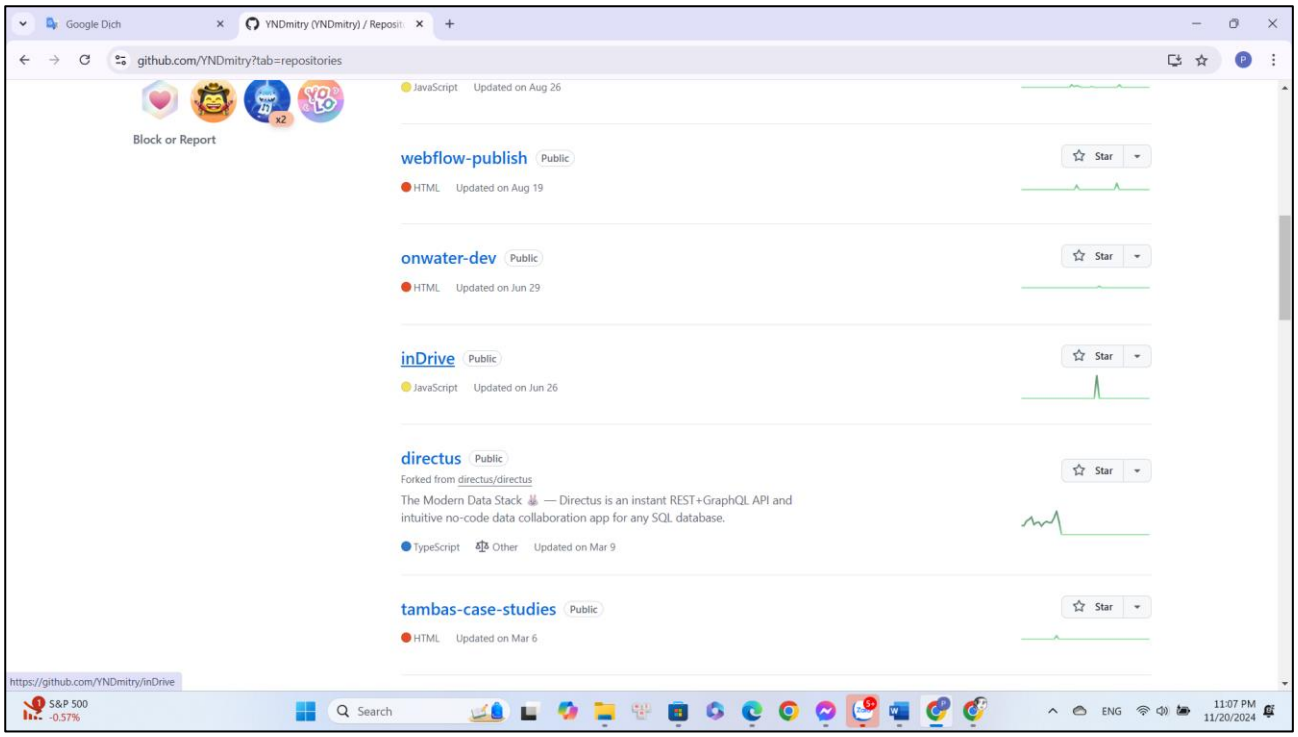
**Trả lời:**

- Video thực hiện: https://youtu.be/15eylePVNLg
- Ta tìm kiếm thông tin về YNDmitry trên git

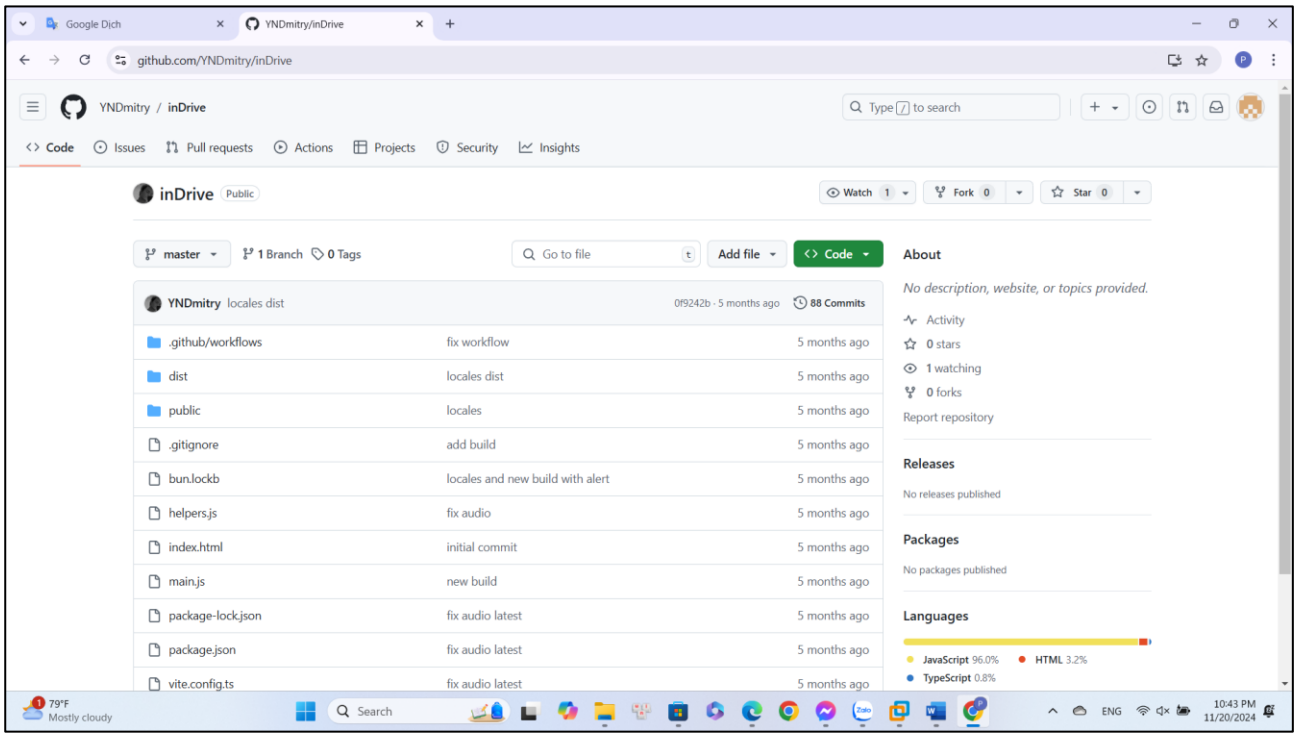



- Ta thấy được Repository inDrive như sau



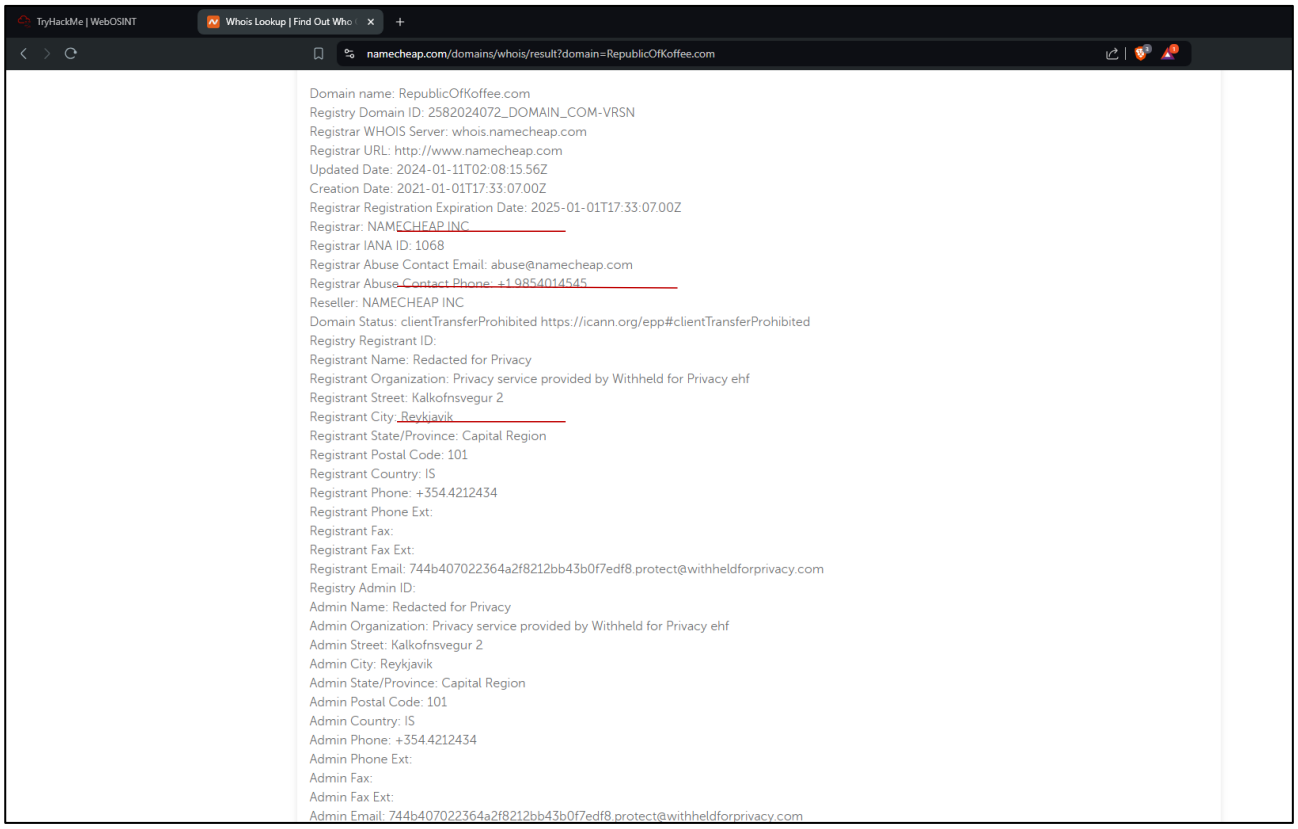

- Ta thấy sites mà YNDmitry đã phát triển trên inDrive.com ở đây

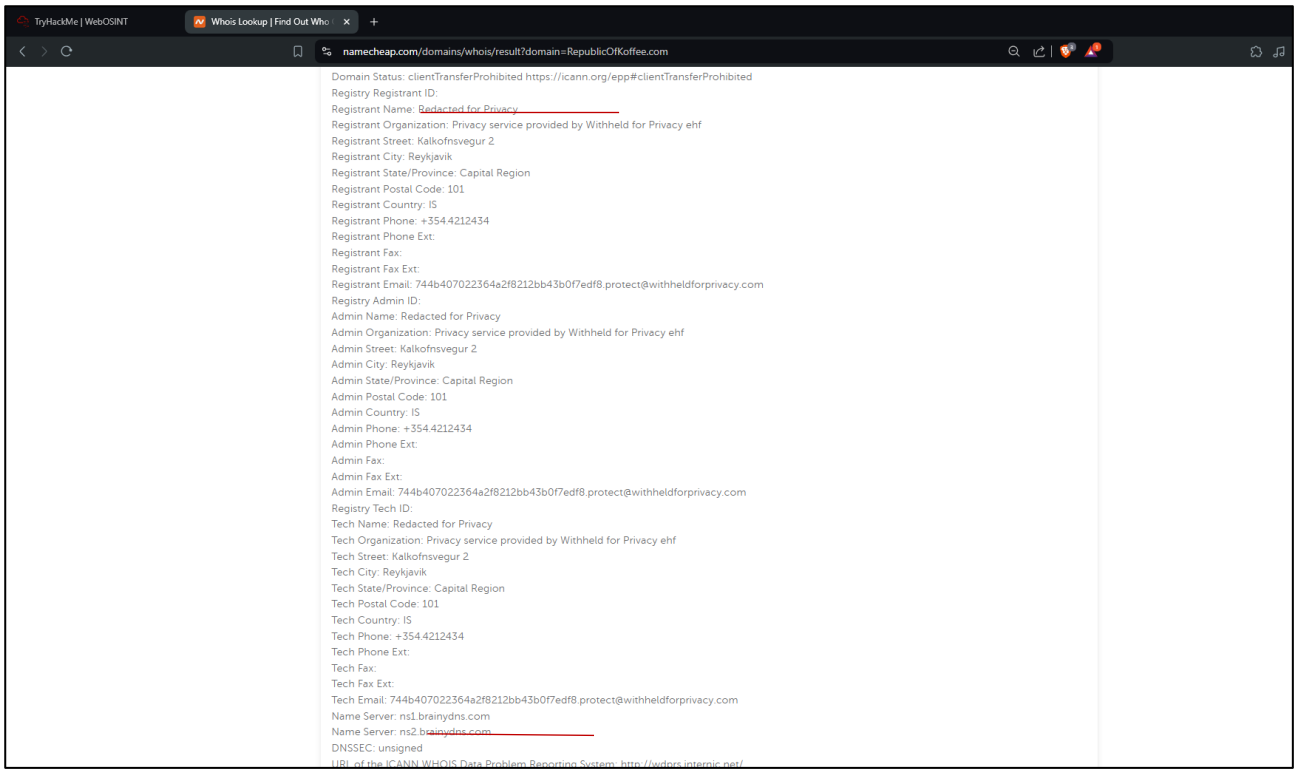


**Bài tập luyện tập:TryHackMe**

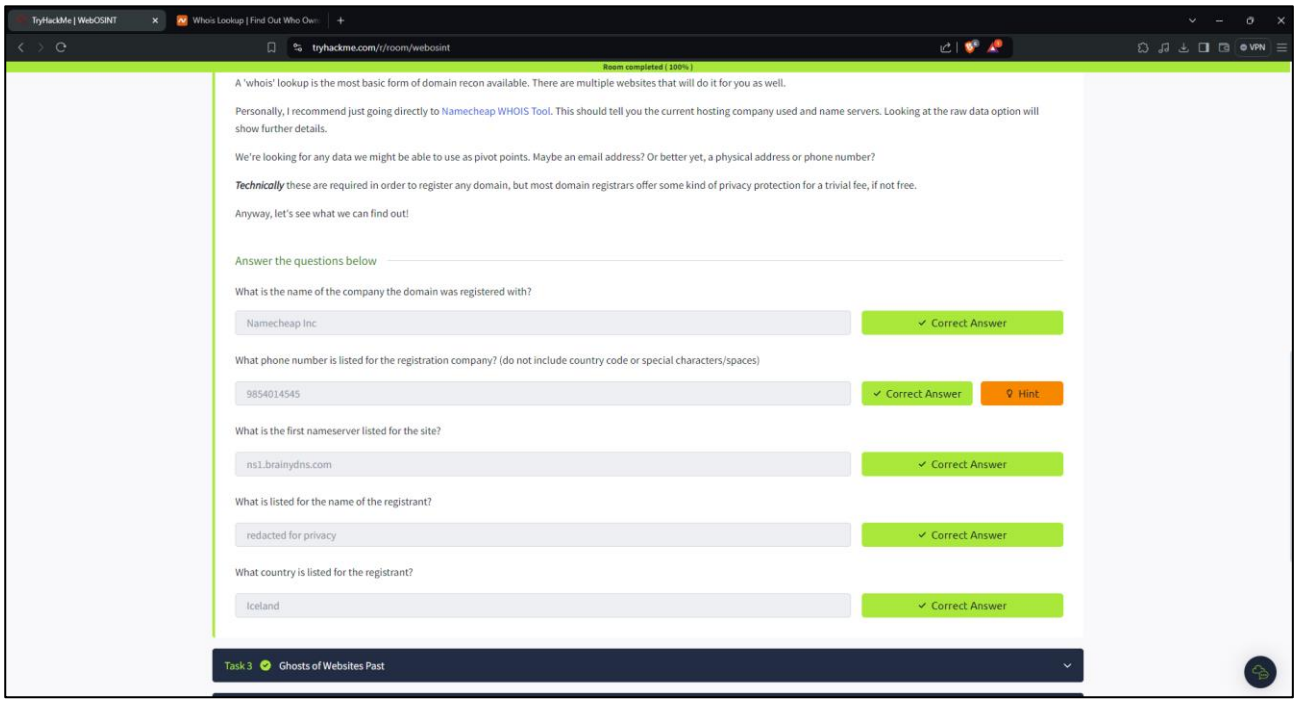
**Trả lời:**

- Video thực hiện: https://youtu.be/DXHwy1pj1PE
- Task 1: Không cần câu trả lời
- Task 2: Dựa vào các thông tin trong Whois ta trả lời được các câu hỏi trong lab

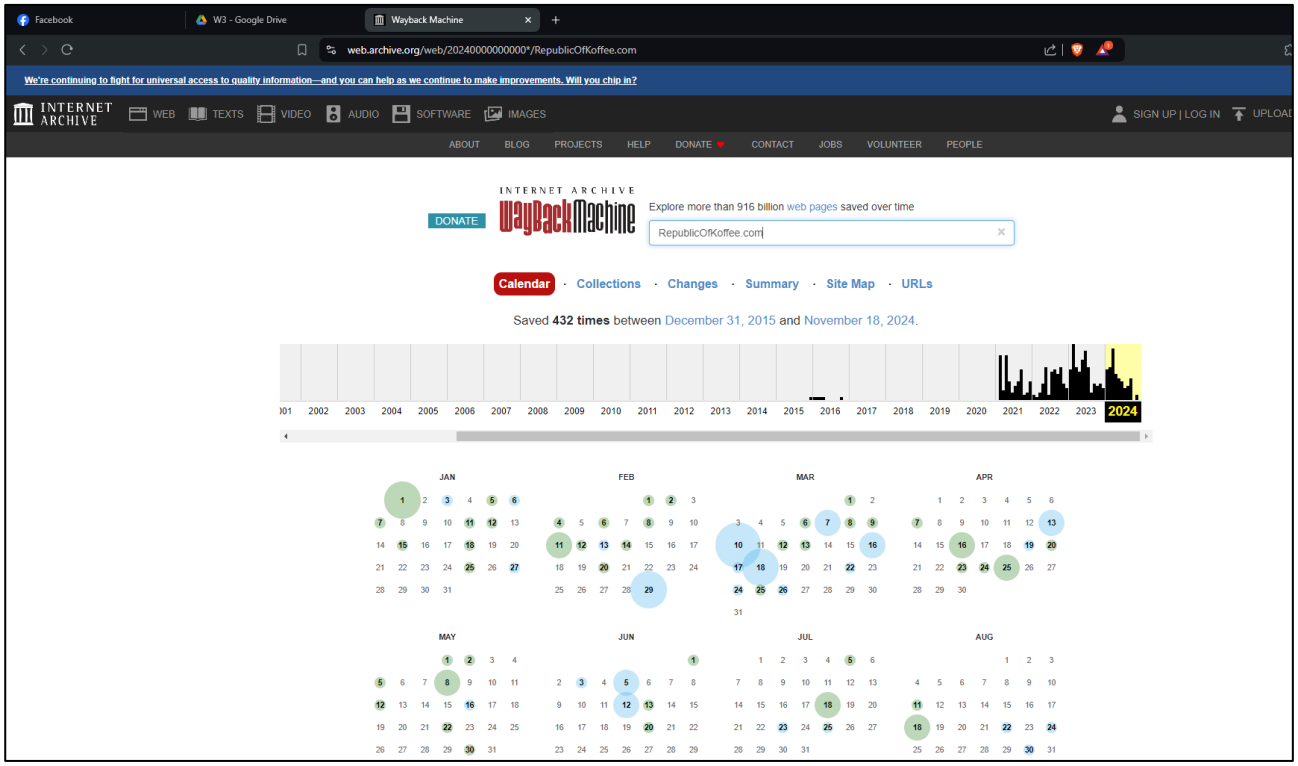


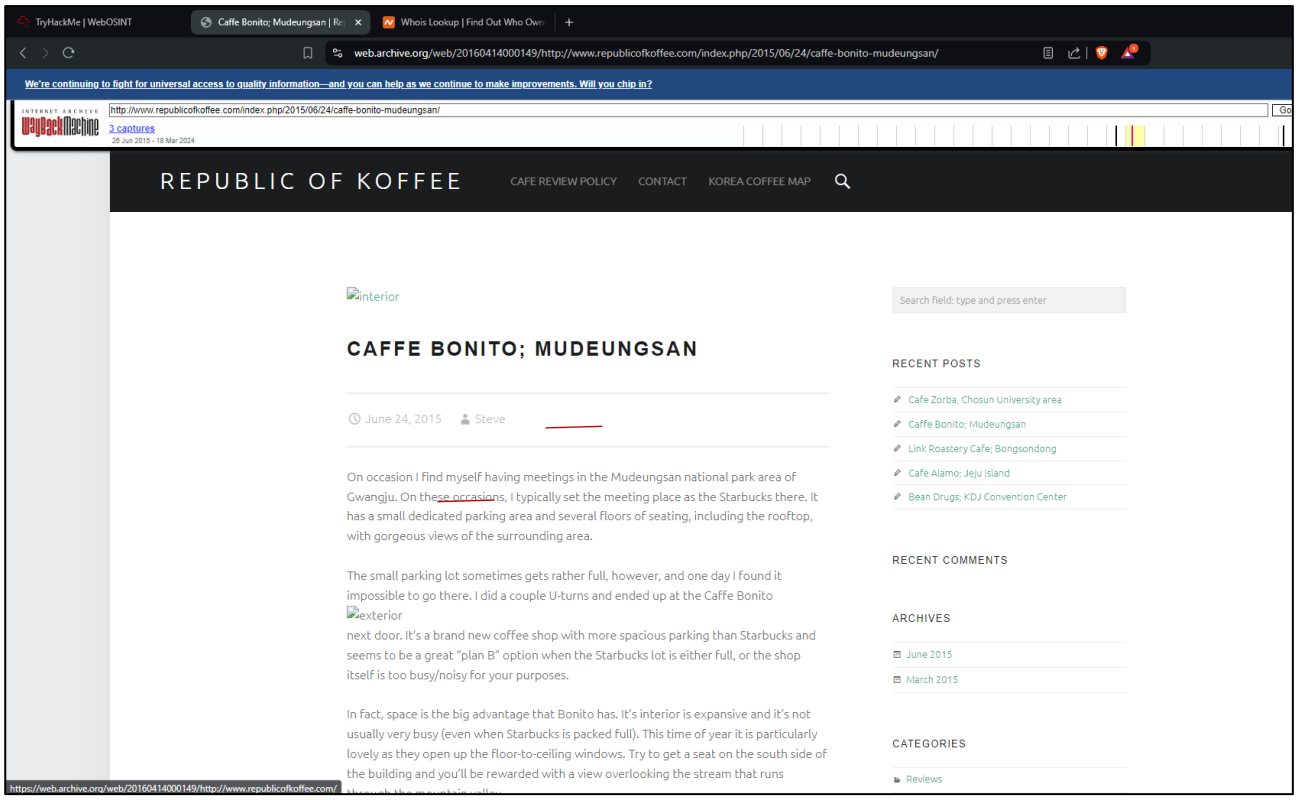

TryHackMe | WebOSINT
Whois Lookup | Find Out Who
namecheap.com/domains/whois/result?domain=RepublicOfKoffee.com
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Redacted for Privacy
Registrant Organization: Privacy service 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 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

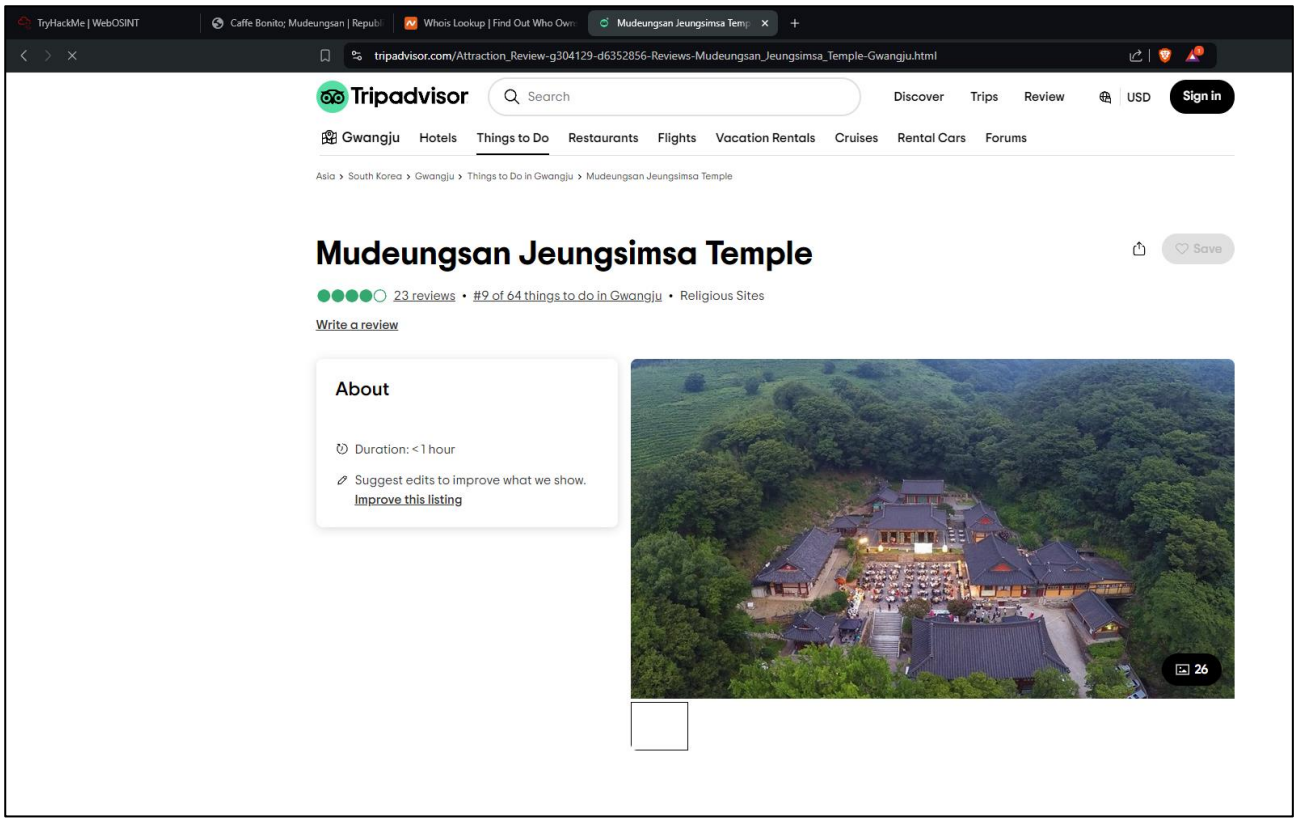
+ Kết quả:

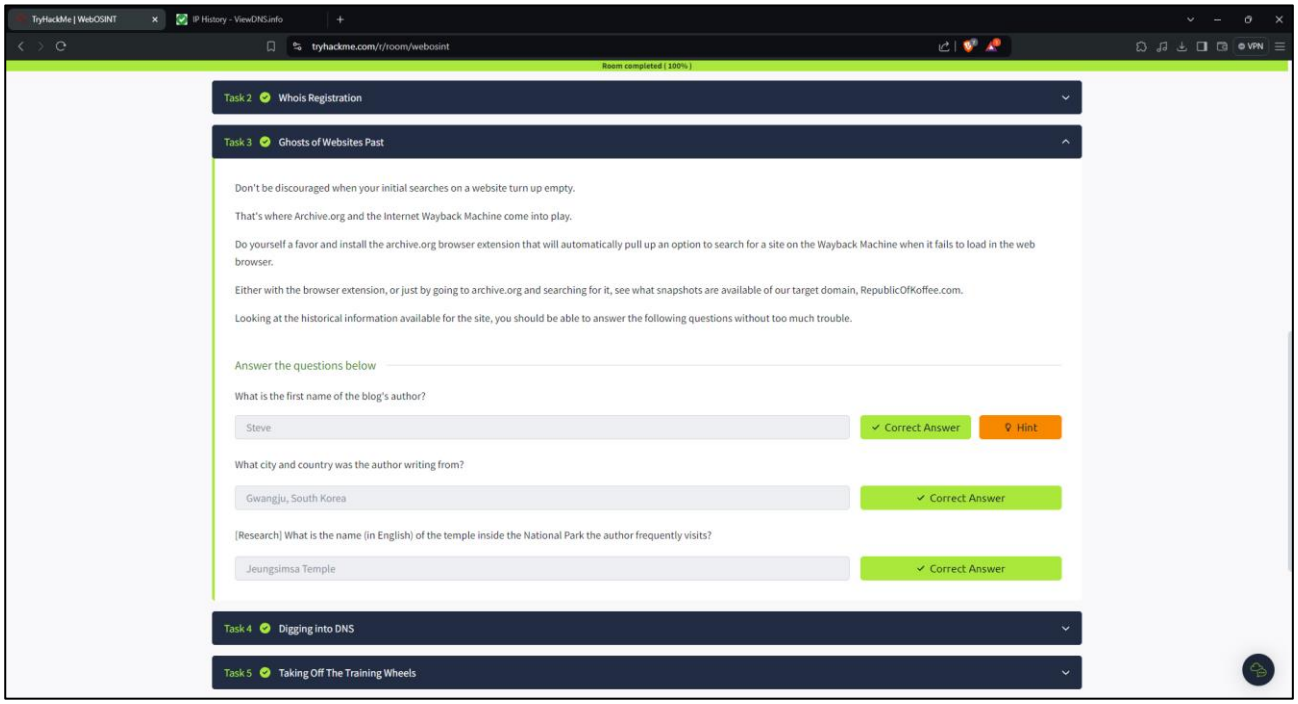

TryHackMe | WebOSINT
Whois Lookup | Find Out Who Own
tryhackme.com/r/room/webosint
Room completed ( 100% )
A 'whois' lookup is the most basic form of domain recon available. There are multiple websites that will do it for you as well.
Personally, I recommend just going directly to Namecheap WHOIS Tool. This should tell you the current hosting company used and name servers. Looking at the raw data option will show further details.
We're looking for any data we might be able to use as pivot points. Maybe an email address? Or better yet, a physical address or phone number?
Technically these are required in order to register any domain, but most domain registrars offer some kind of privacy protection for a trivial fee, if not free.
Anyway, let's see what we can find out!
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
Ghosts of Websites Past

- Task 3: Sử dụng trang web Archive.org và truy cập vào 1 blog bất kì ta sẽ thấy tên tác giả là Steve, địa chỉ của tác giả ở Gwangju là 1 thành phố của Hàn Quốc ( South Korea ). Ngoài ra ta có thể tìm thấy thông tin của ngôi chùa thông qua tìm kiếm google



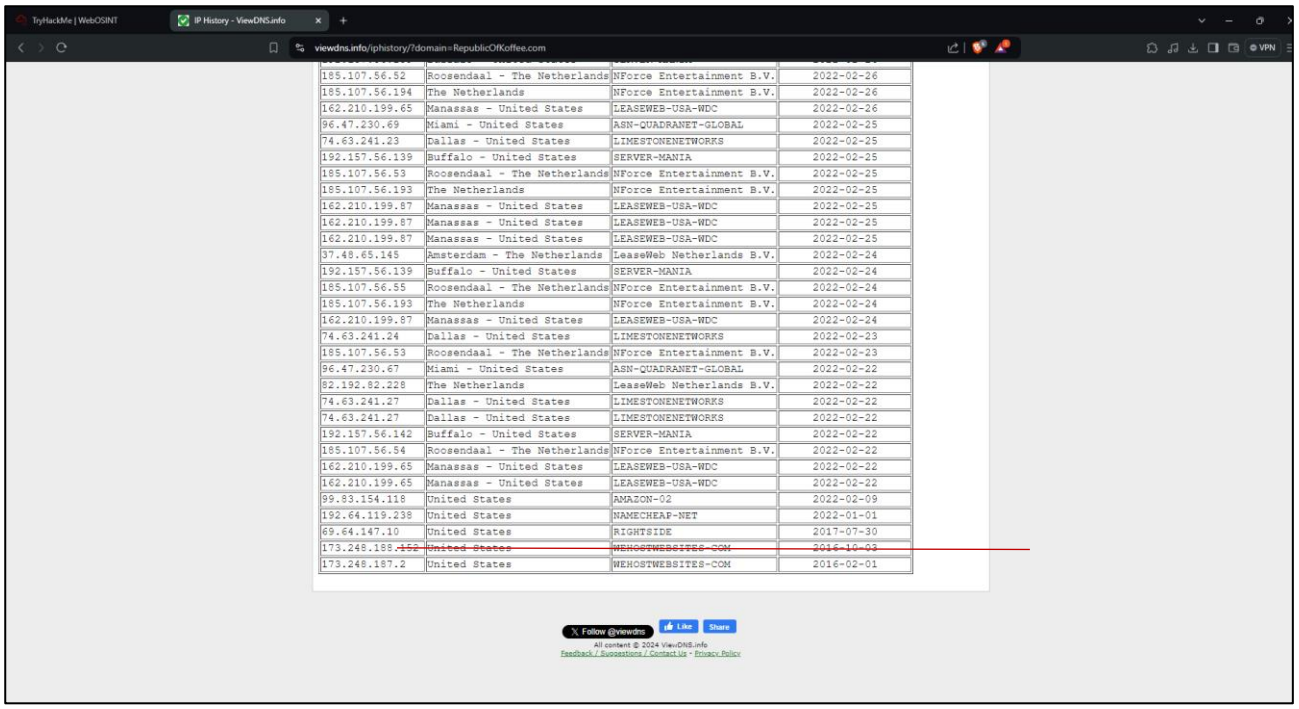





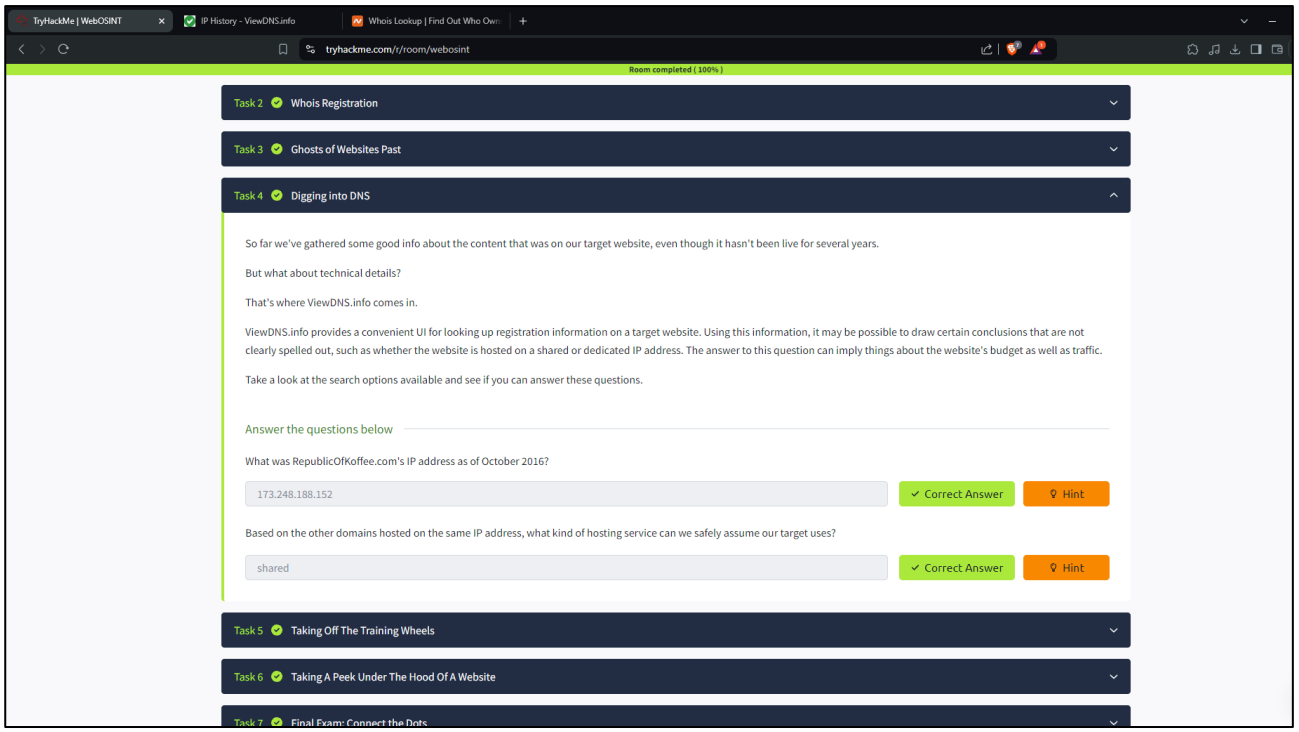

- Task 4: Thực hiện truy cập vào trang web https://viewdns.info/

+ Dựa vào tiện ích IP History của trang web, ta sẽ check được lịch sử IP sử dụng của domain mà ta muốn tìm kiếm ( cụ thể ở đây là RepublicOfKoffee.com )



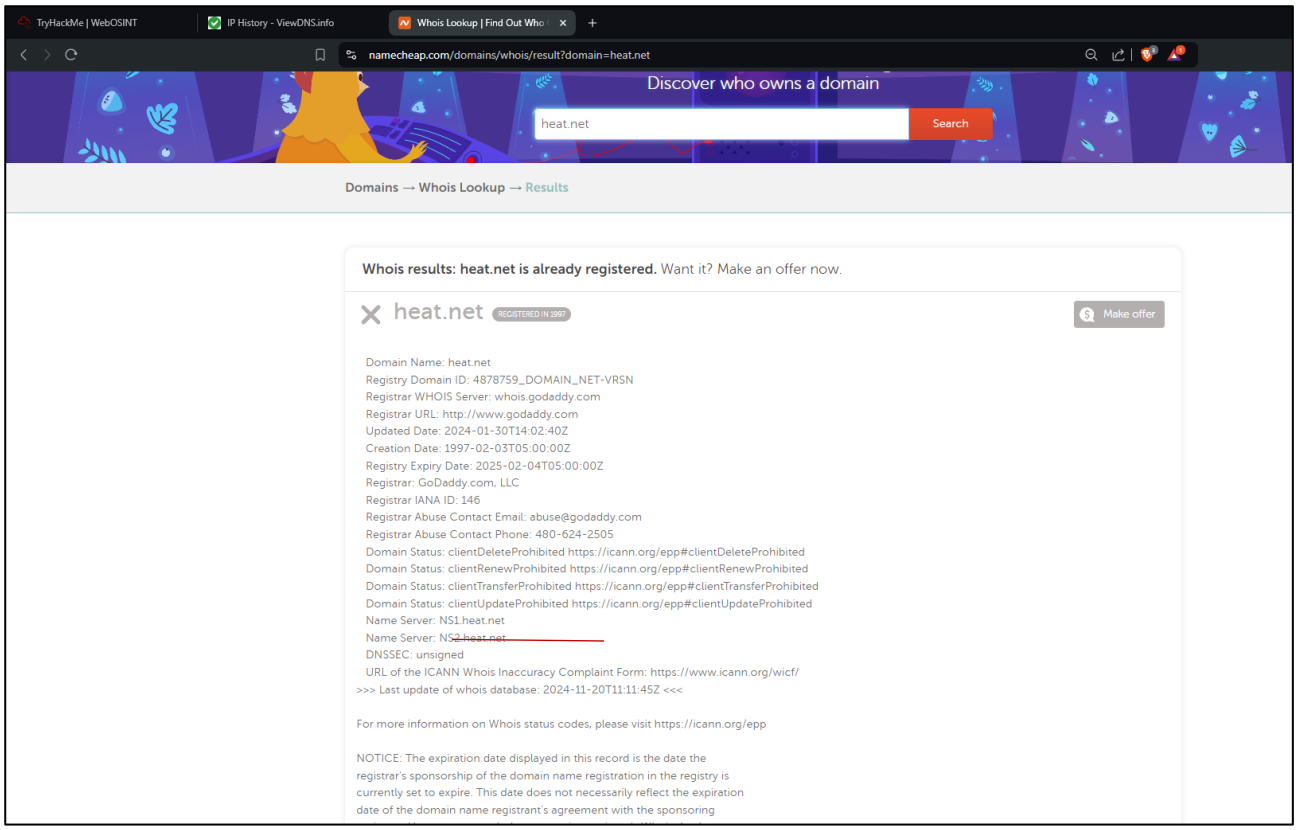
| | | | |
|---|---|---|---|
| 185.107.56.52 | Roosendaal - The Netherlands | NForce Entertainment B.V. | 2022-02-26 |
| 185.107.56.194 | The Netherlands | NForce Entertainment B.V. | 2022-02-26 |
| 162.210.199.65 | Manassas - United States | LEASEWEB-USA-WDC | 2022-02-26 |
| 96.47.230.69 | Miami - United States | ASN-QUADRANET-GLOBAL | 2022-02-25 |
| 74.63.241.23 | Dallas - United States | LIMESTONENETWORKS | 2022-02-25 |
| 192.157.56.139 | Buffalo - United States | SERVER-MANIA | 2022-02-25 |
| 185.107.56.53 | Roosendaal - The Netherlands | NForce Entertainment B.V. | 2022-02-25 |
| 185.107.56.193 | The Netherlands | NForce Entertainment B.V. | 2022-02-25 |
| 162.210.199.87 | Manassas - United States | LEASEWEB-USA-WDC | 2022-02-25 |
| 162.210.199.87 | Manassas - United States | LEASEWEB-USA-WDC | 2022-02-25 |
| 162.210.199.87 | Manassas - United States | LEASEWEB-USA-WDC | 2022-02-25 |
| 37.48.65.145 | Amsterdam - The Netherlands | LeaseWeb Netherlands B.V. | 2022-02-24 |
| 192.157.56.139 | Buffalo - United States | SERVER-MANIA | 2022-02-24 |
| 185.107.56.55 | Roosendaal - The Netherlands | NForce Entertainment B.V. | 2022-02-24 |
| 185.107.56.193 | The Netherlands | NForce Entertainment B.V. | 2022-02-24 |
| 162.210.199.87 | Manassas - United States | LEASEWEB-USA-WDC | 2022-02-24 |
| 74.63.241.24 | Dallas - United States | LIMESTONENETWORKS | 2022-02-23 |
| 185.107.56.53 | Roosendaal - The Netherlands | NForce Entertainment B.V. | 2022-02-23 |
| 96.47.230.67 | Miami - United States | ASN-QUADRANET-GLOBAL | 2022-02-22 |
| 82.192.82.228 | The Netherlands | LeaseWeb Netherlands B.V. | 2022-02-22 |
| 74.63.241.27 | Dallas - United States | LIMESTONENETWORKS | 2022-02-22 |
| 74.63.241.27 | Dallas - United States | LIMESTONENETWORKS | 2022-02-22 |
| 192.157.56.142 | Buffalo - United States | SERVER-MANIA | 2022-02-22 |
| 185.107.56.54 | Roosendaal - The Netherlands | NForce Entertainment B.V. | 2022-02-22 |
| 162.210.199.65 | Manassas - United States | LEASEWEB-USA-WDC | 2022-02-22 |
| 162.210.199.65 | Manassas - United States | LEASEWEB-USA-WDC | 2022-02-22 |
| 99.83.154.118 | United States | AMAZON-02 | 2022-02-09 |
| 192.64.119.238 | United States | NAMECHEAP-NET | 2022-01-01 |
| 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 |

+ Dựa trên các tên miền khác được lưu trữ trên cùng một địa chỉ IP ta có thể nhận ra đây là Shared web hosting – một dịch vụ lưu trữ web cho phpes nhiều website cùng chia sẻ tài nguyên của một máy chủ vật lí duy nhất



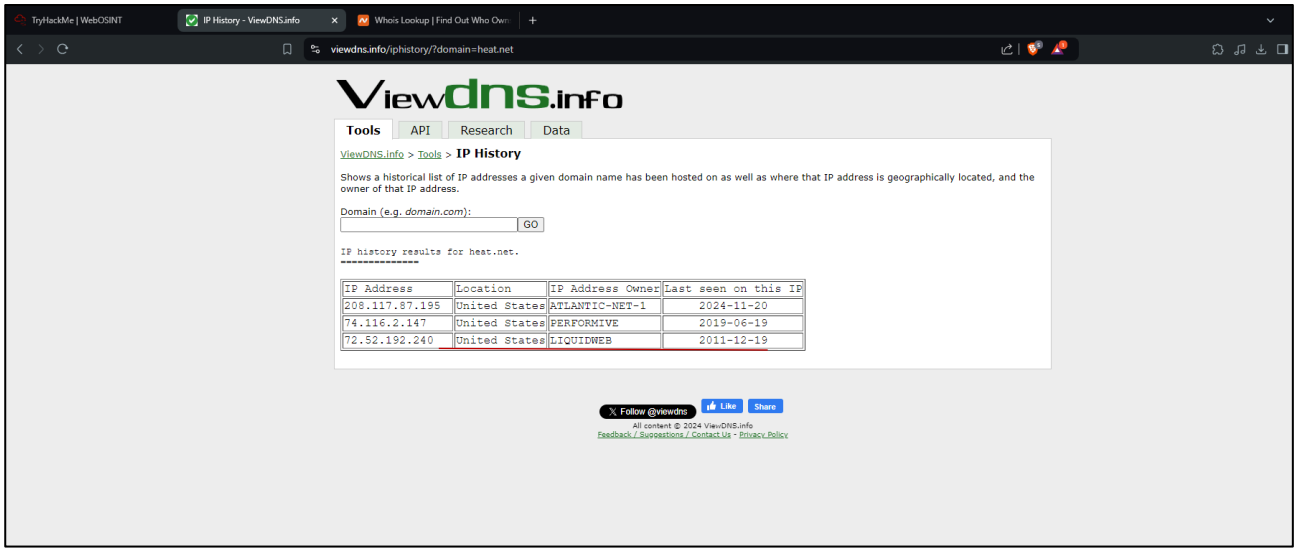

- Task 5: Tương tự như ở Task 2, ta sẽ tiếp tục sử dụng các trang web ở các task trước để khai thác nhưng bây giờ mục tiêu của ta sẽ là domain heat.net

+ What is the second nameserver listed for the domain?

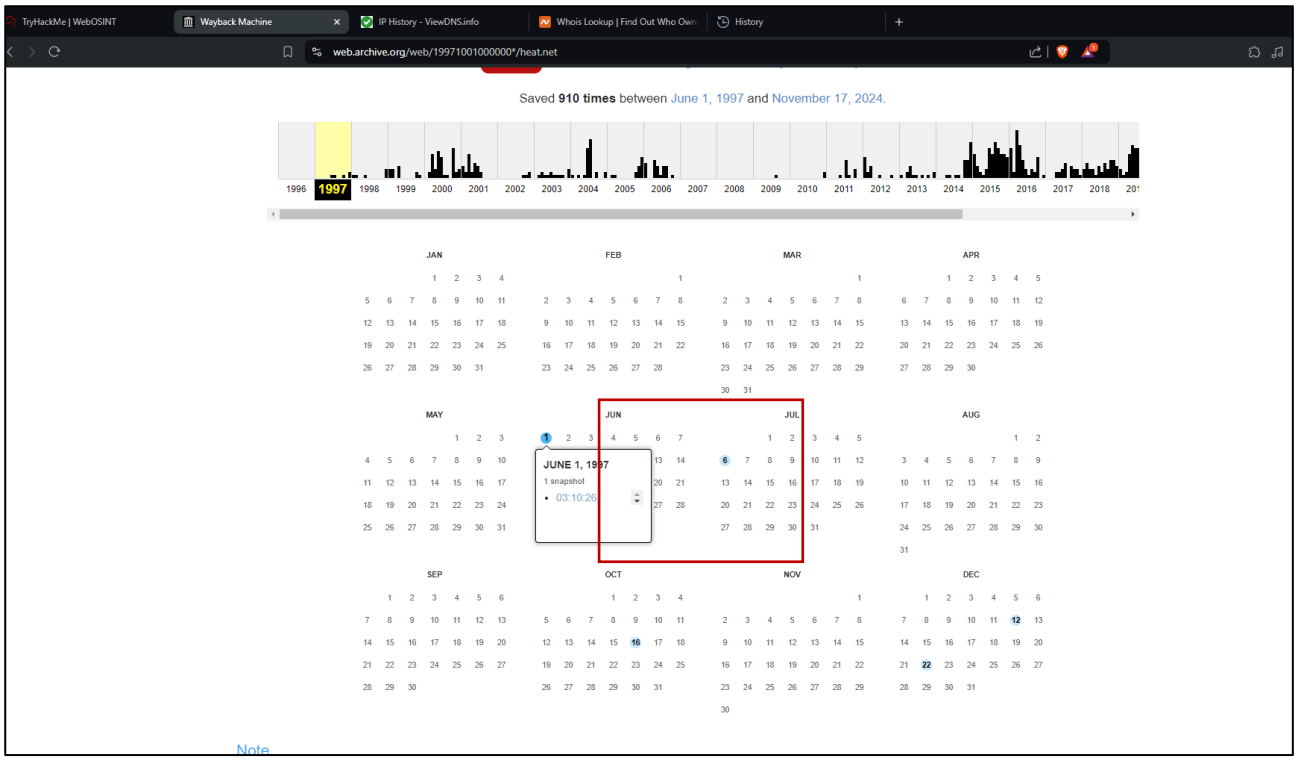



+ What IP address was the domain listed on as of December 2011?

+ Based on domains that share the same IP, what kind of hosting service is the domain owner using?

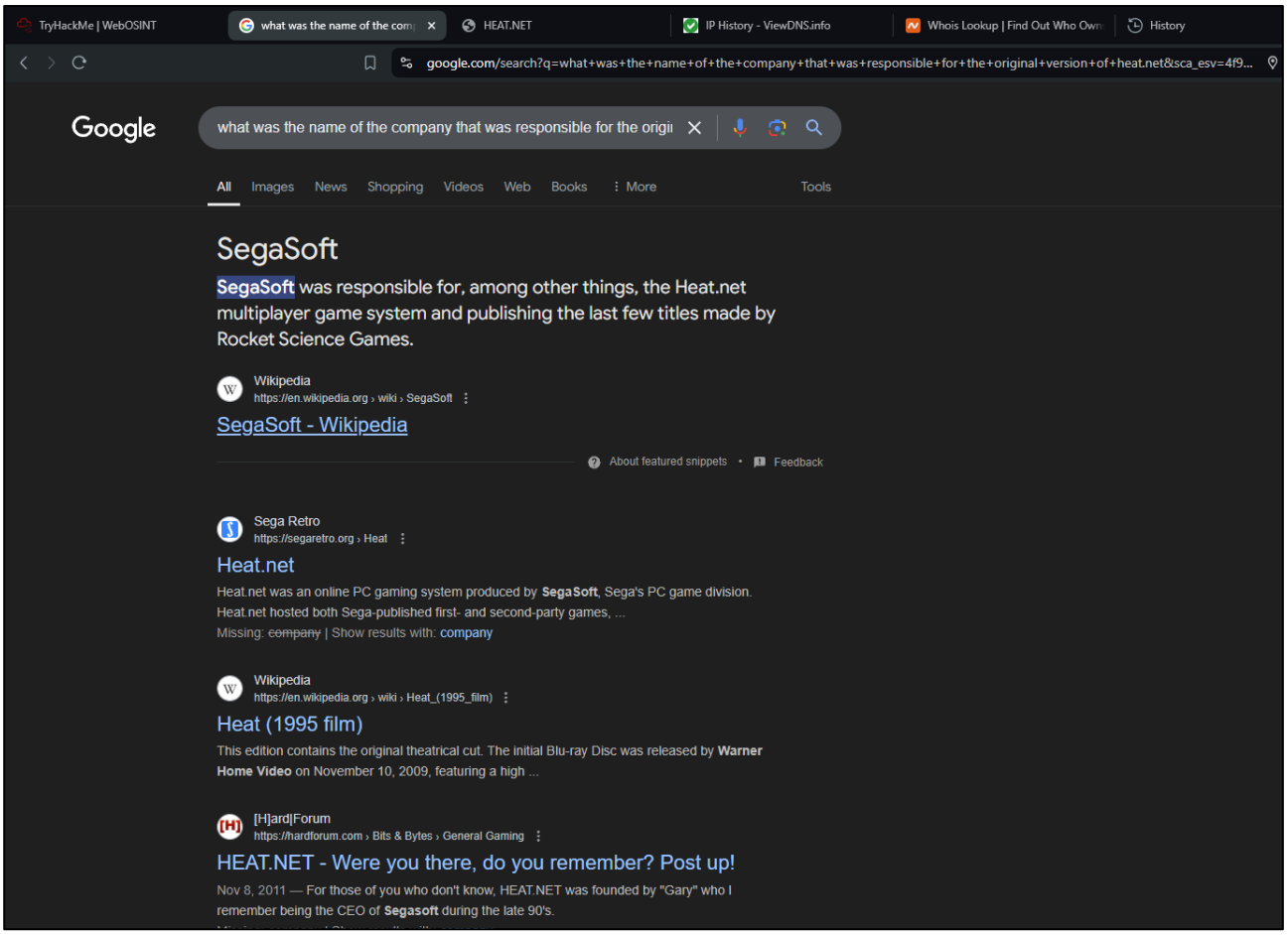



+ On what date did was the site first captured by the internet archive? (MM/DD/YY format)

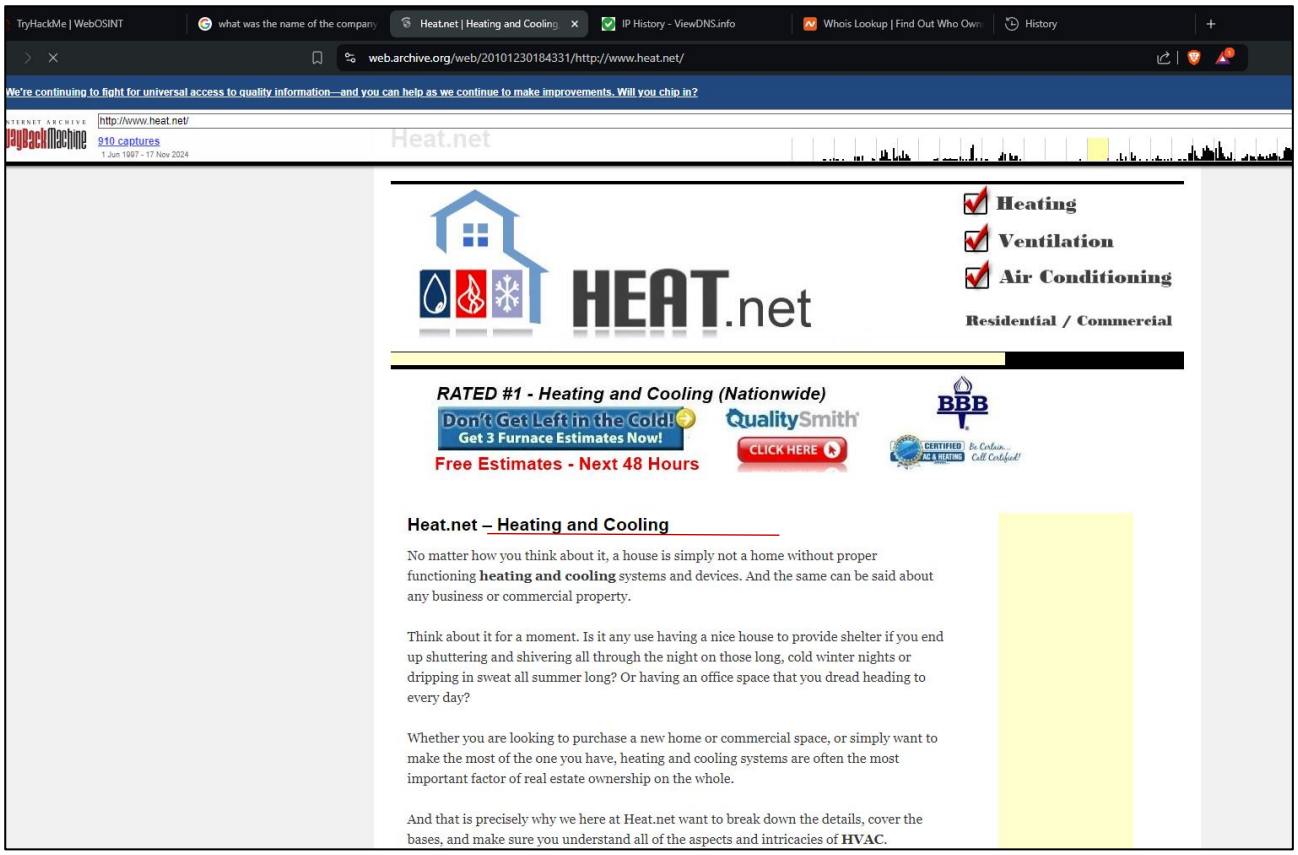


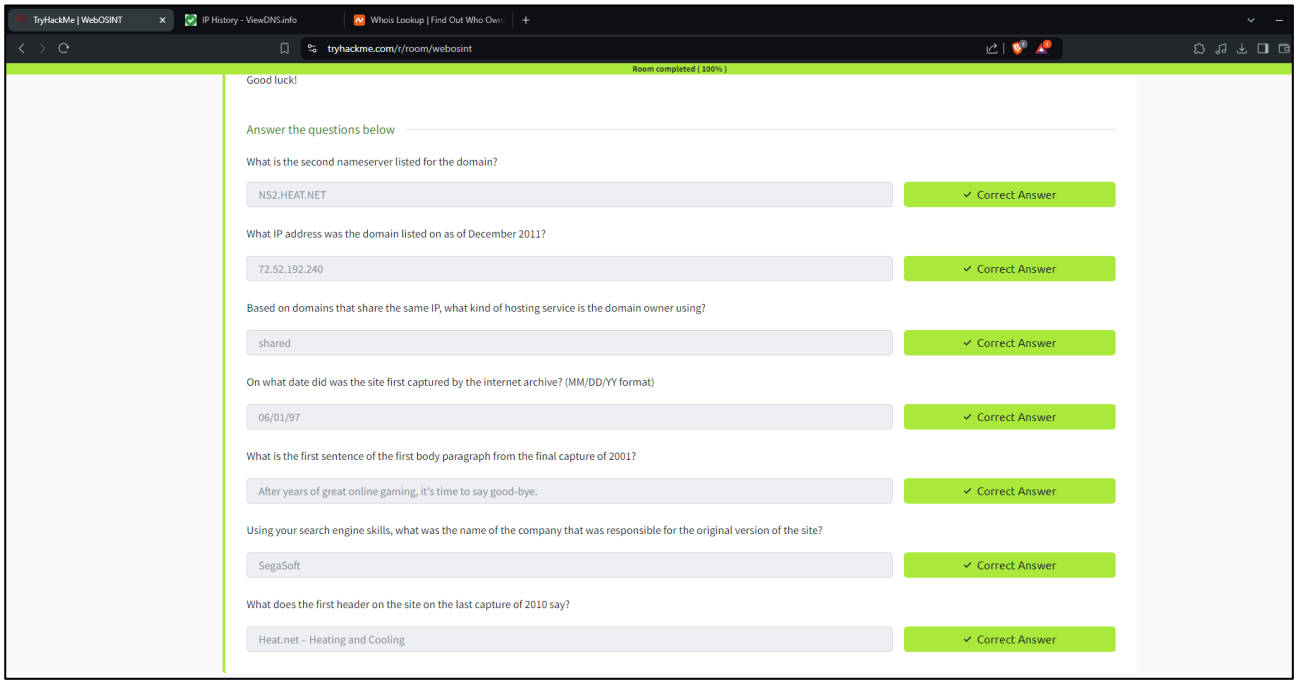

+ What is the first sentence of the first body paragraph from the final capture of 2001?

+ Using your search engine skills, what was the name of the company that was responsible for the original version of the site?



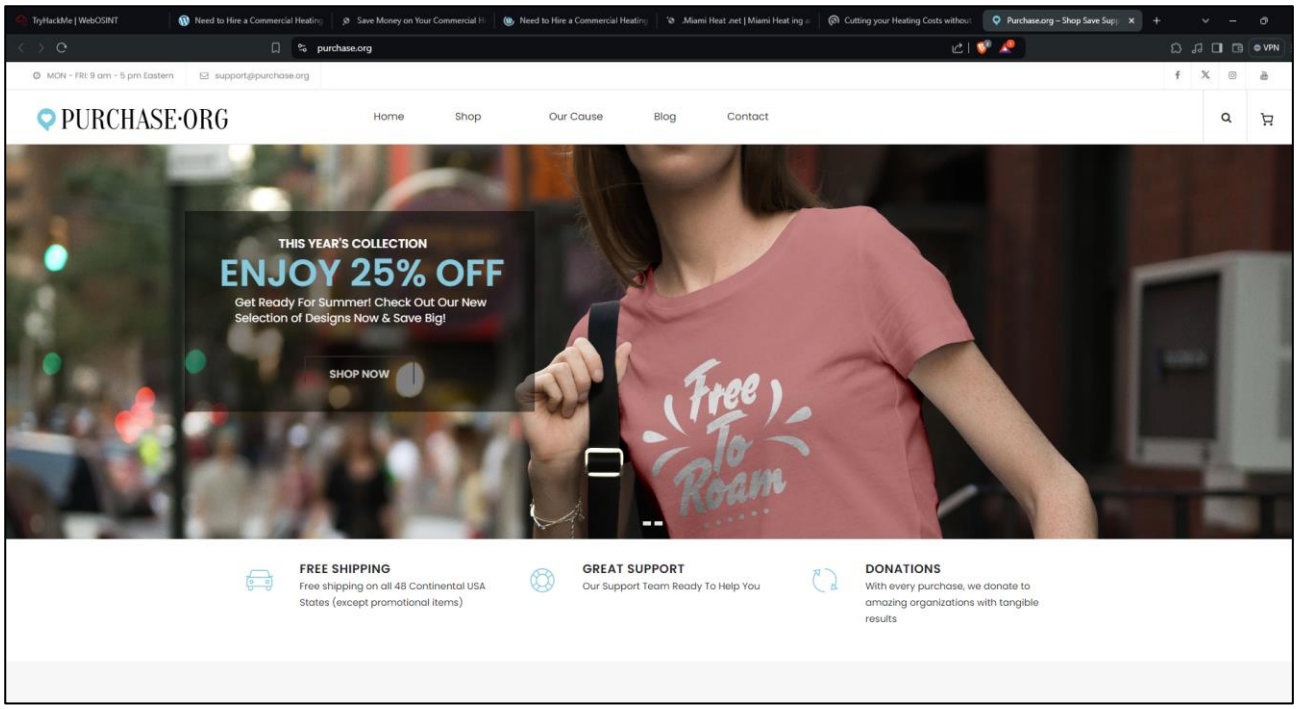

+ What does the first header on the site on the last capture of 2010 say?



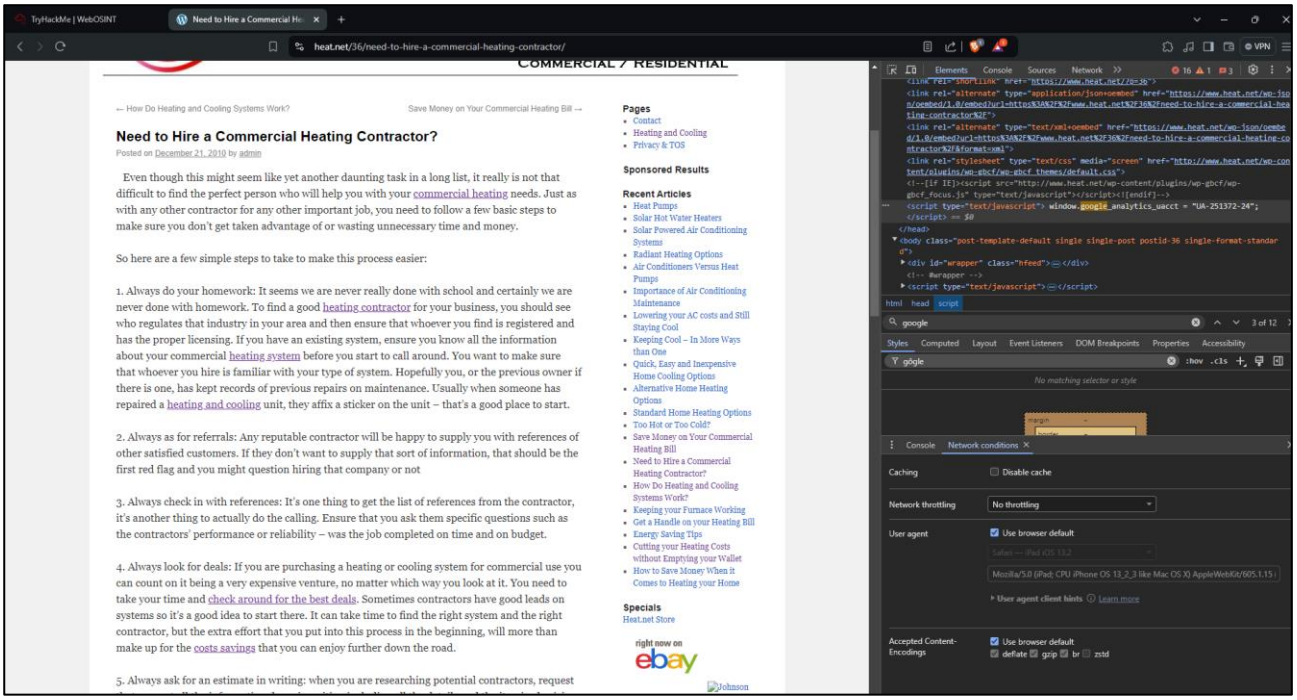




- Task 6: Truy cập vào đường dẫn yêu cầu đưa ra là heat.net/36/need-to-hire-a-commercial-heating-contractor/

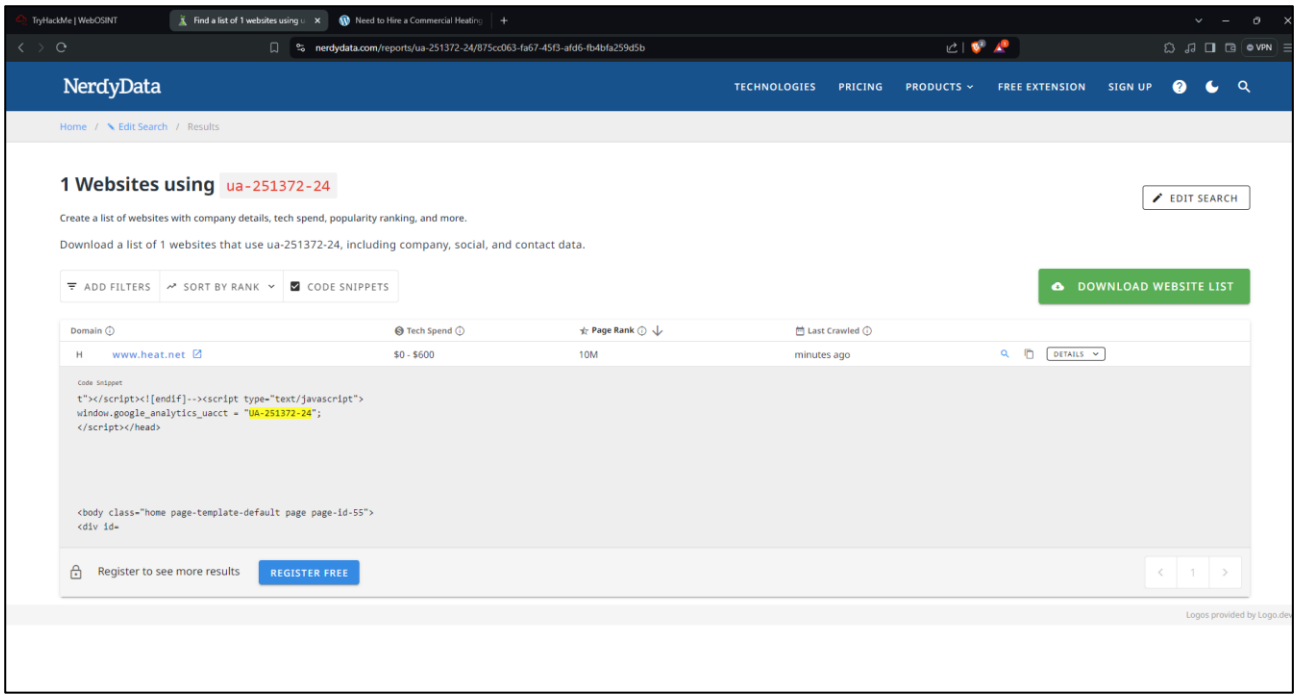
+ Đầu tiên ta thấy được có 6 link ta có thể hover vào, truy cập từng link một ta sẽ thấy có 5 link thuộc heat.net và 1 link là đường dẫn đến purchase.org



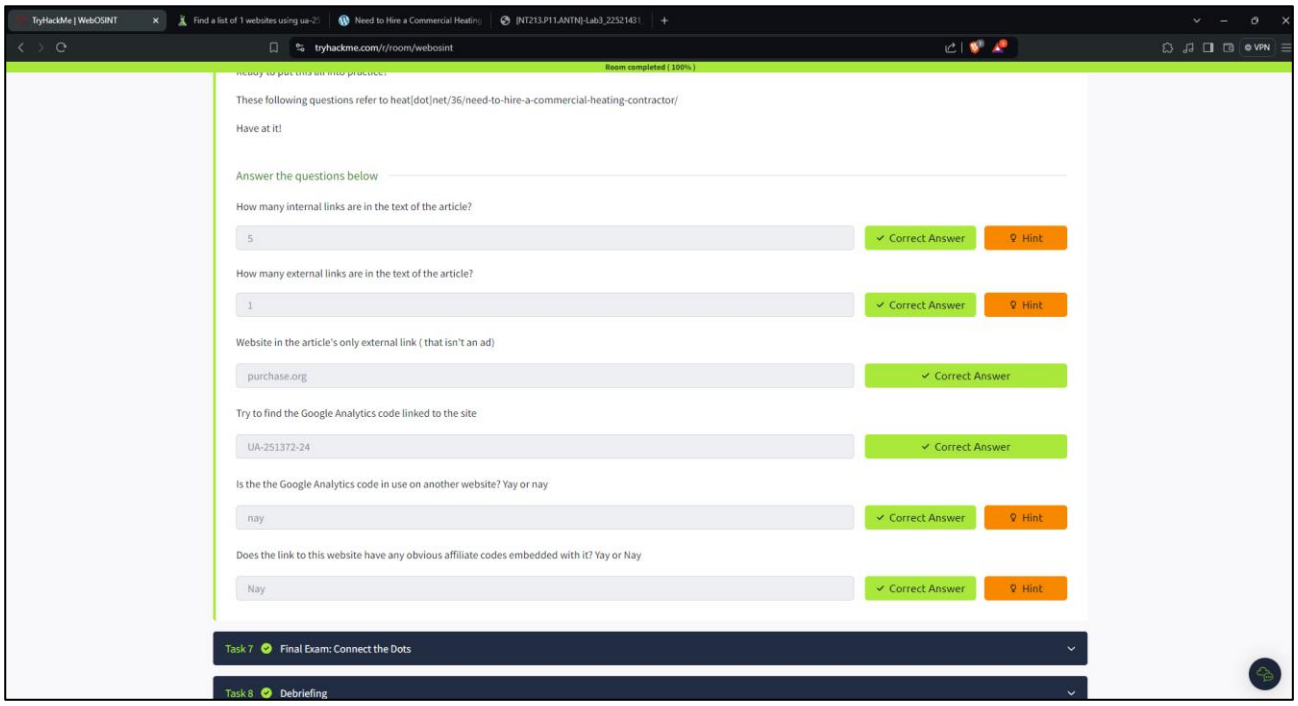

+ Tiếp theo ở trang web chính, thực hiện F12 -> ở tab Element ta Ctrl F rồi điền vào chữ google => tìm kiếm lần lượt để tìm Google Analytics code




+ Truy cập https://www.nerdydata.com/ và tìm kiếm những trang web có sử dụng mã code này sẽ thấy chỉ có duy nhất 1 trang web là heat.net sử dụng nó nên câu trả lời sẽ là nay

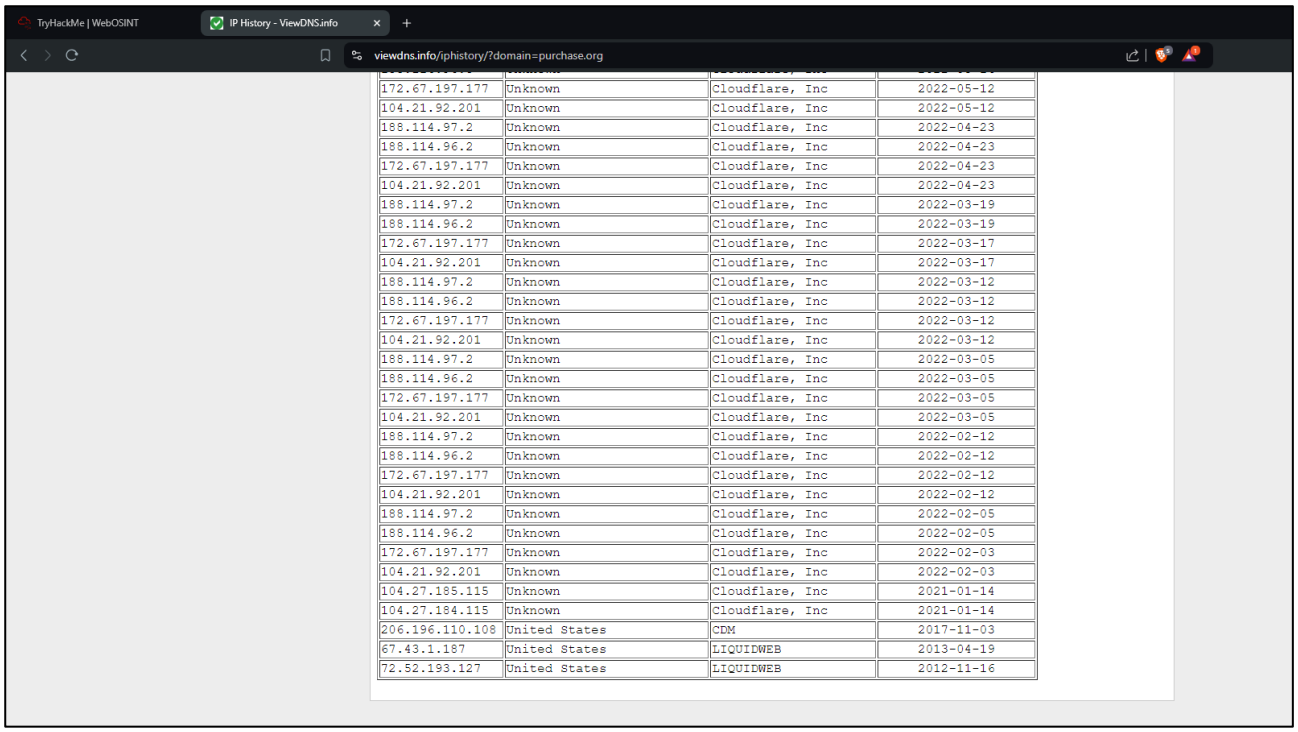



+ Ngoài ra khi truy cập vào purchase.org thì không có mã liên kết nào được đính kèm vào đó nên câu trả lời là Nay



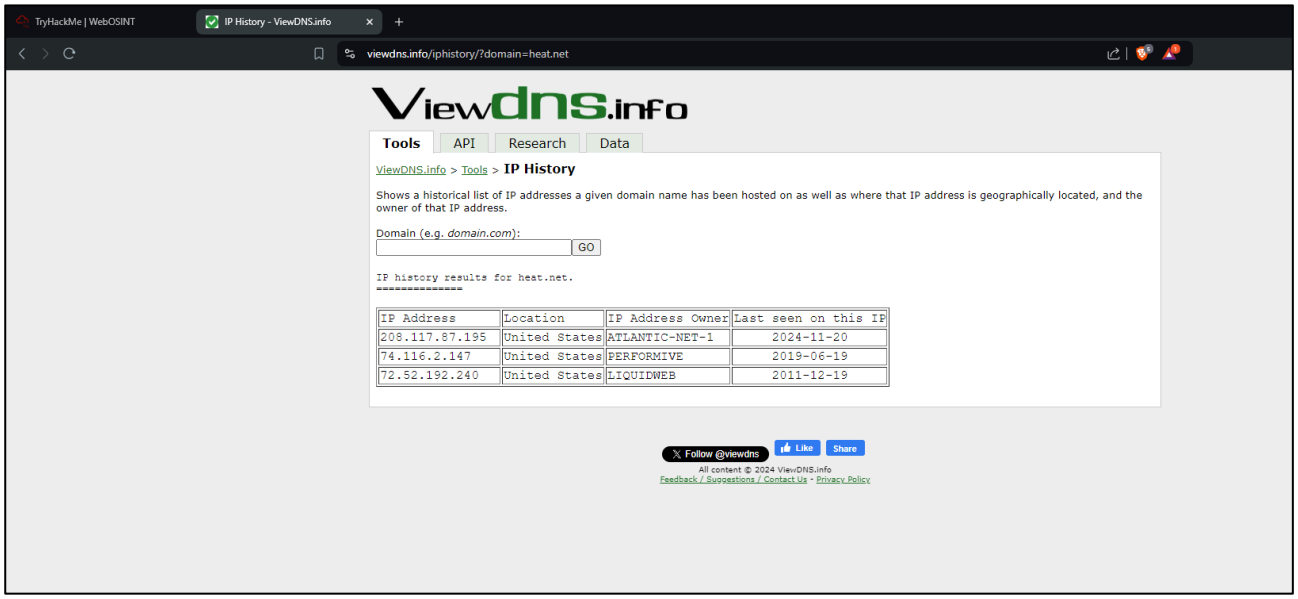

- Task 7: Sử dụng IP History để tìm điểm chung của heat.net và purchase.org

+ Purchase.org



| | | | |
|---|---|---|---|
| 172.67.197.177 | Unknown | Cloudflare, Inc | 2022-05-12 |
| 104.21.92.201 | Unknown | Cloudflare, Inc | 2022-05-12 |
| 188.114.97.2 | Unknown | Cloudflare, Inc | 2022-04-23 |
| 188.114.96.2 | Unknown | Cloudflare, Inc | 2022-04-23 |
| 172.67.197.177 | Unknown | Cloudflare, Inc | 2022-04-23 |
| 104.21.92.201 | Unknown | Cloudflare, Inc | 2022-04-23 |
| 188.114.97.2 | Unknown | Cloudflare, Inc | 2022-03-19 |
| 188.114.96.2 | Unknown | Cloudflare, Inc | 2022-03-19 |
| 172.67.197.177 | Unknown | Cloudflare, Inc | 2022-03-17 |
| 104.21.92.201 | Unknown | Cloudflare, Inc | 2022-03-17 |
| 188.114.97.2 | Unknown | Cloudflare, Inc | 2022-03-12 |
| 188.114.96.2 | Unknown | Cloudflare, Inc | 2022-03-12 |
| 172.67.197.177 | Unknown | Cloudflare, Inc | 2022-03-12 |
| 104.21.92.201 | Unknown | Cloudflare, Inc | 2022-03-12 |
| 188.114.97.2 | Unknown | Cloudflare, Inc | 2022-03-05 |
| 188.114.96.2 | Unknown | Cloudflare, Inc | 2022-03-05 |
| 172.67.197.177 | Unknown | Cloudflare, Inc | 2022-03-05 |
| 104.21.92.201 | Unknown | Cloudflare, Inc | 2022-03-05 |
| 188.114.97.2 | Unknown | Cloudflare, Inc | 2022-02-12 |
| 188.114.96.2 | Unknown | Cloudflare, Inc | 2022-02-12 |
| 172.67.197.177 | Unknown | Cloudflare, Inc | 2022-02-12 |
| 104.21.92.201 | Unknown | Cloudflare, Inc | 2022-02-12 |
| 188.114.97.2 | Unknown | Cloudflare, Inc | 2022-02-05 |
| 188.114.96.2 | Unknown | Cloudflare, Inc | 2022-02-05 |
| 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 |

+ heat.net



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 | 2024-11-20 |
| 74.116.2.147 | United States | PERFORMIVE | 2019-06-19 |
| 72.52.192.240 | United States | LIQUIDWEB | 2011-12-19 |

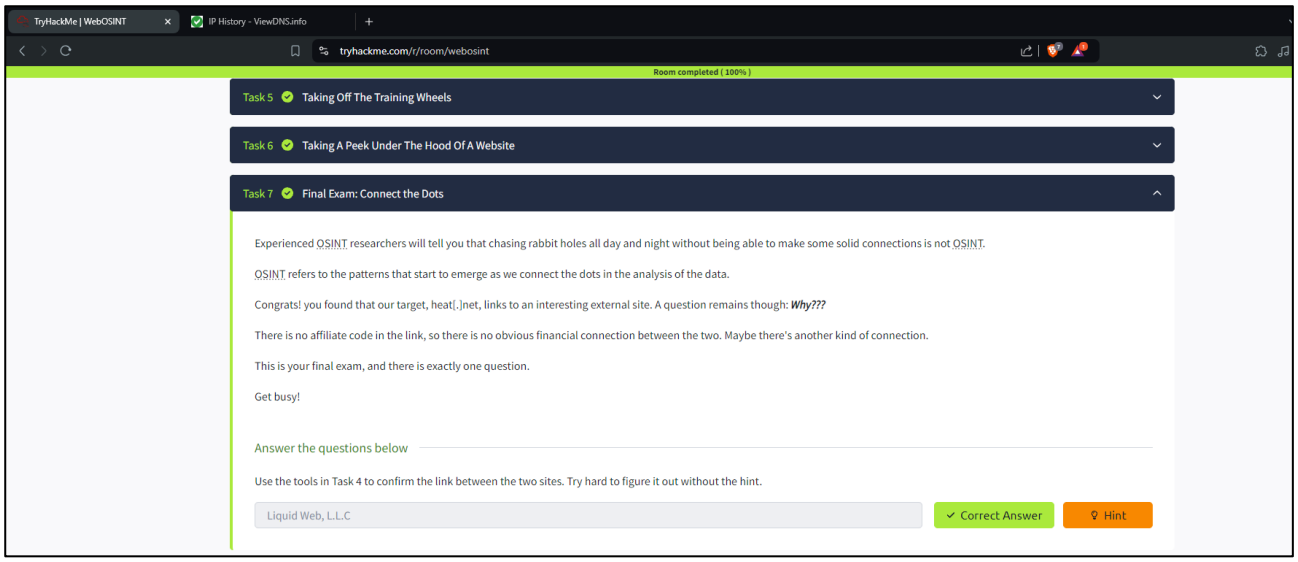
Follow @viewdns Like Share

All content © 2024 ViewDNS.info

Feedback / Suggestions / Contact Us - Privacy Policy

,

⇨ Có thể thấy cả hai đều có chung chủ sở hữu là LIQUIDWEB

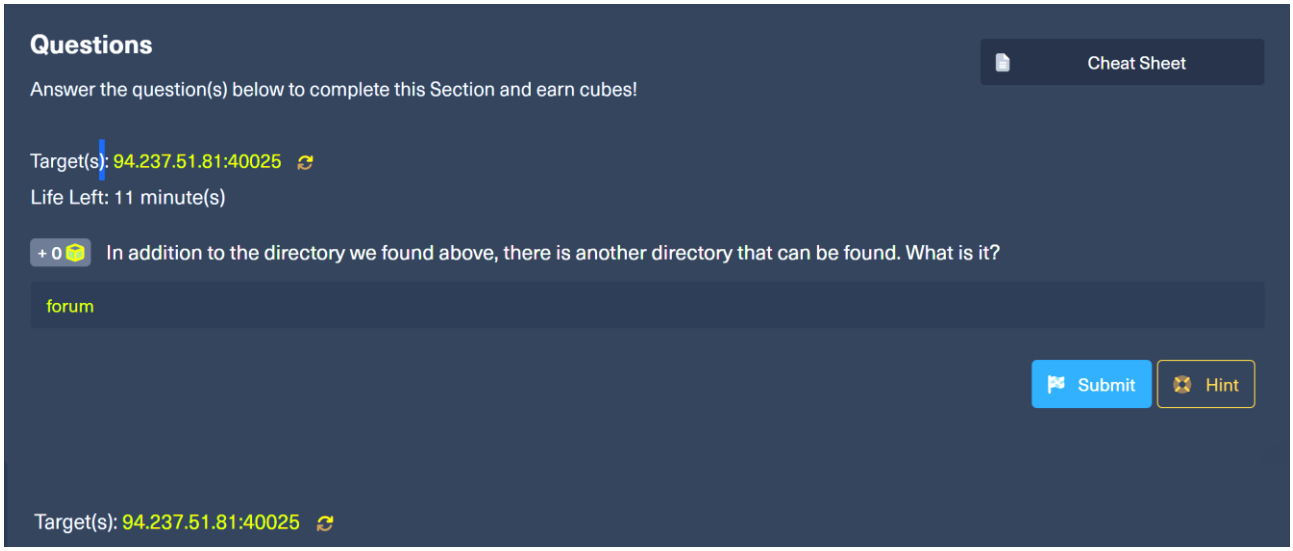



- Task 8 và Task 9: hai task này cho ta biết thêm các thông tin hữu ích về OSINT, vì vậy chỉ cần submit trống là được

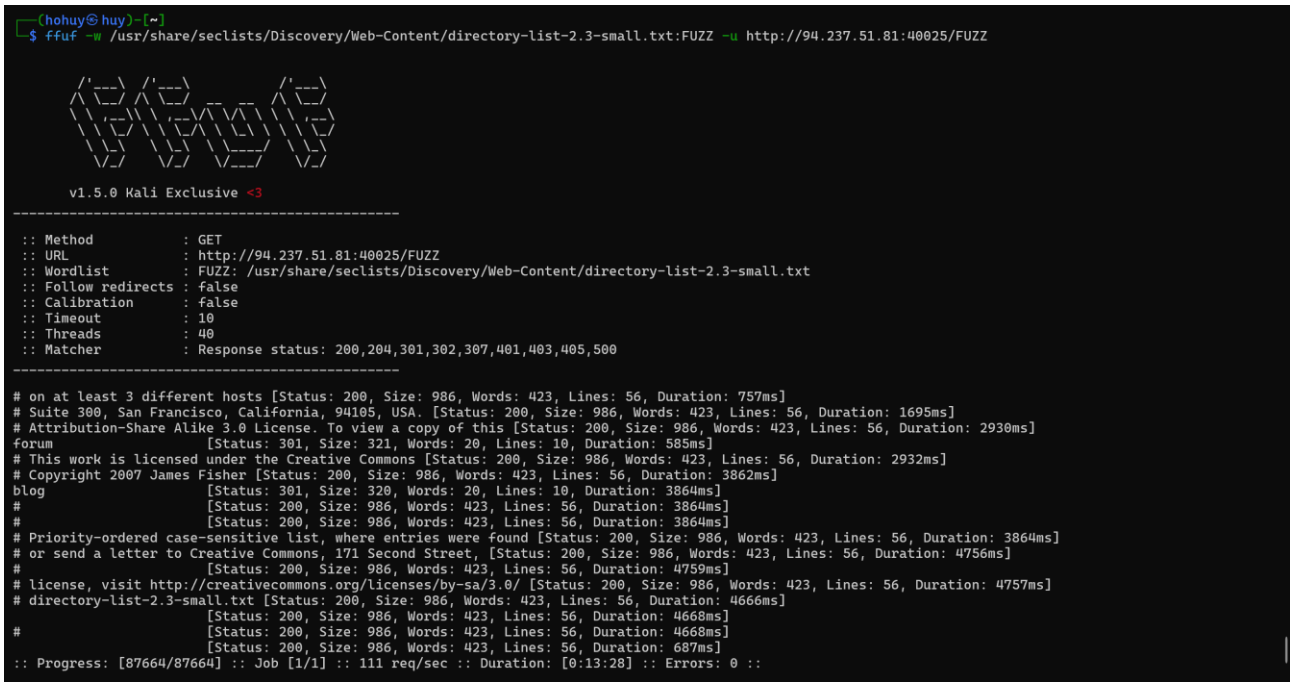
**Bài Tập Làm Thêm HackTheBox:** https://academy.hackthebox.com/module/details/54

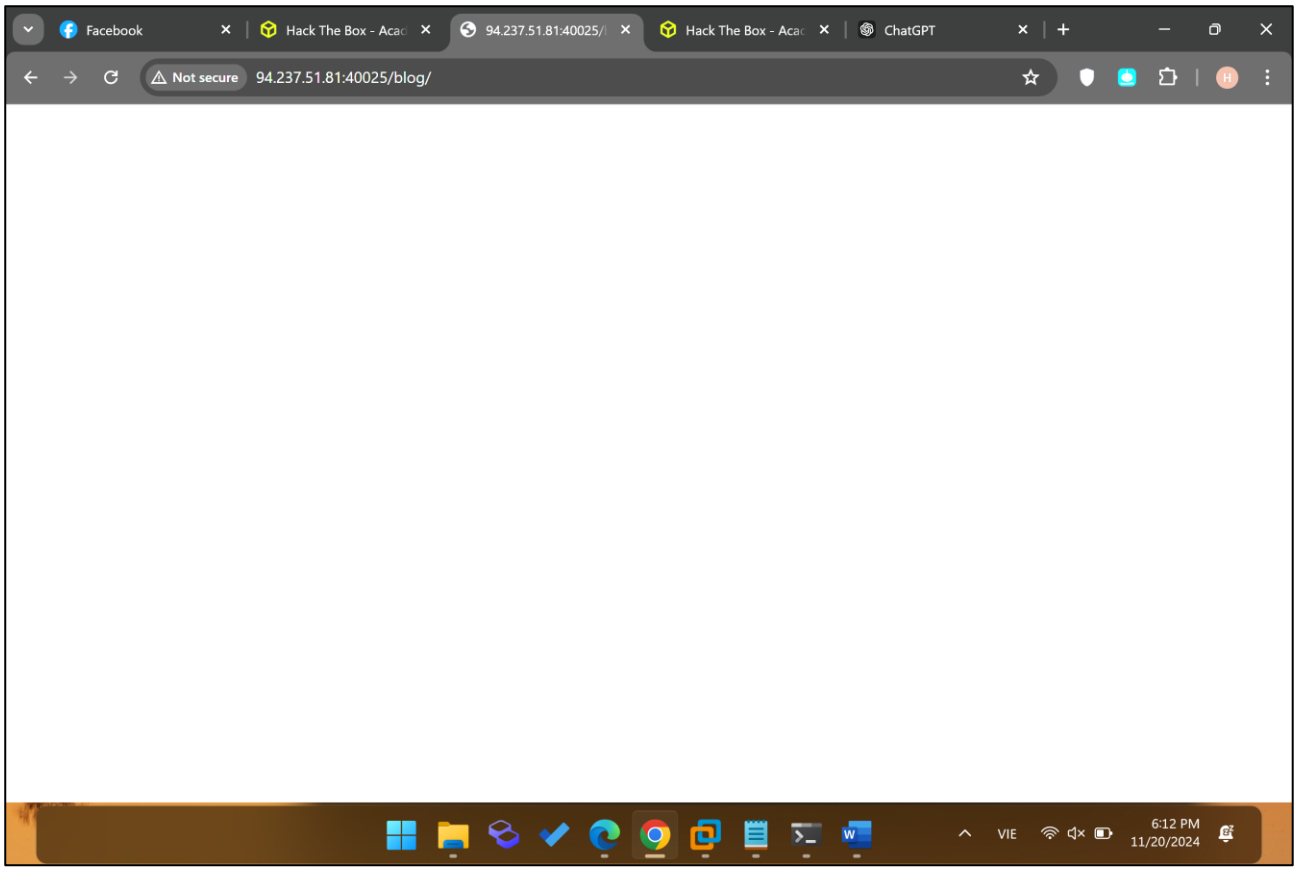
**Task: Directory Fuzzing**

- Video thực hiện: https://youtu.be/ATXu4l0yzUo
- Target IP:



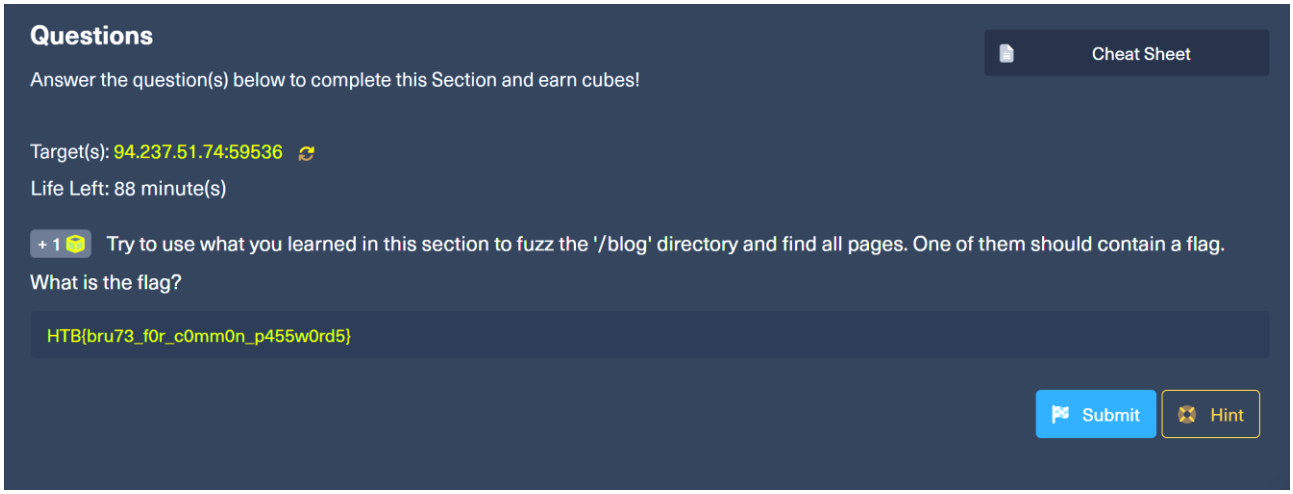

- Thực hiện theo hướng dẫn bài Lab



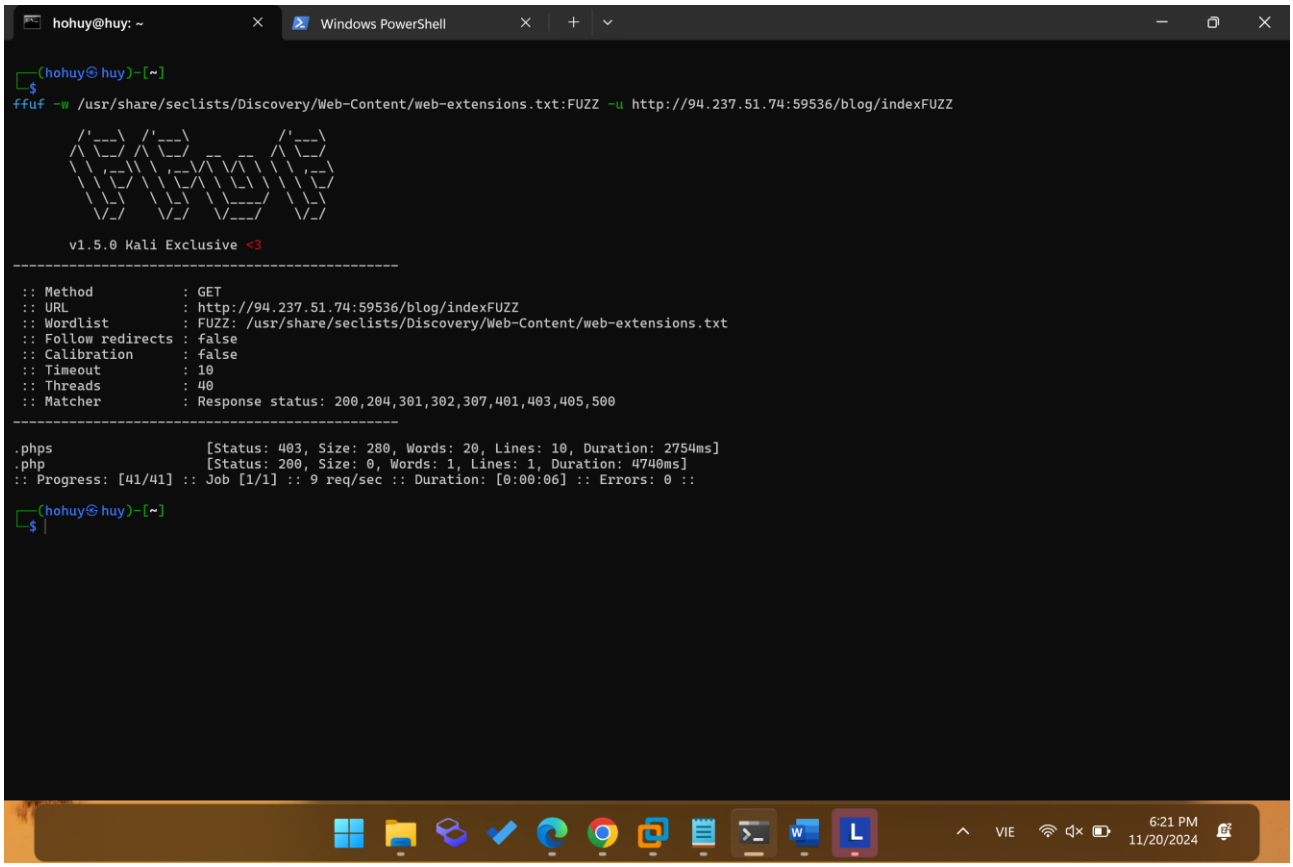



## Task: Page Fuzzing

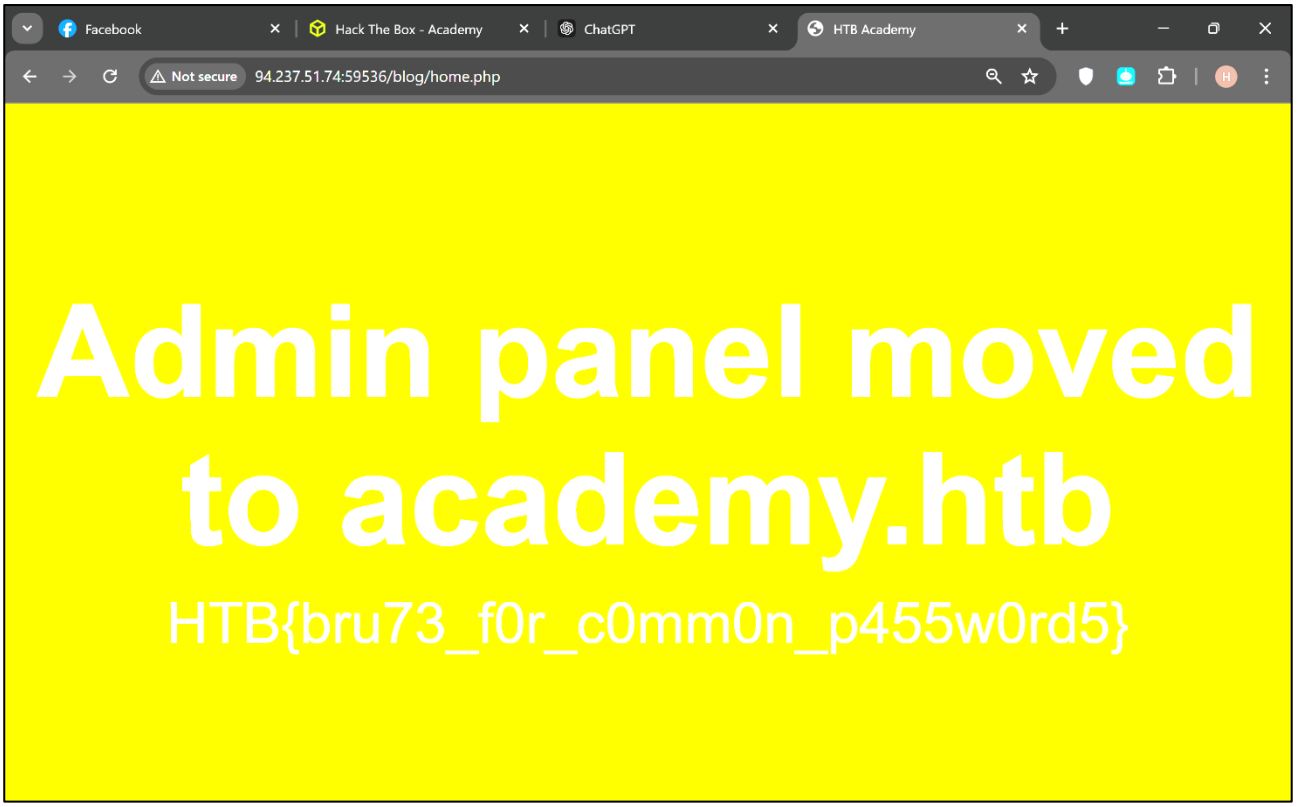
- Video thực hiện: https://youtu.be/Zb-TPK92c8c
- Server IP:



- Thực hiện:

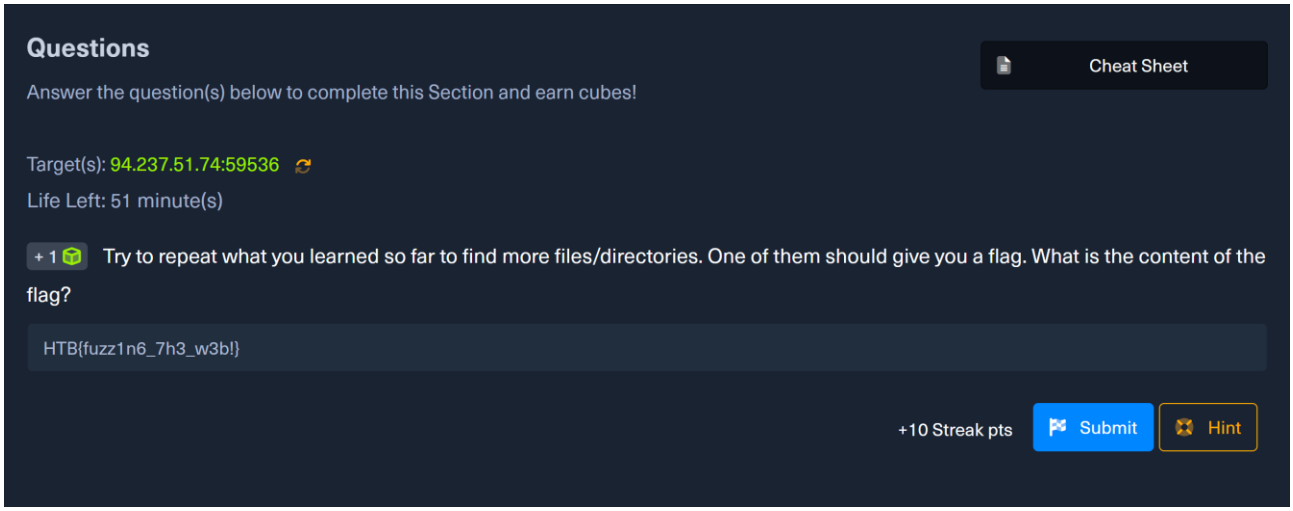



- Kết quả:

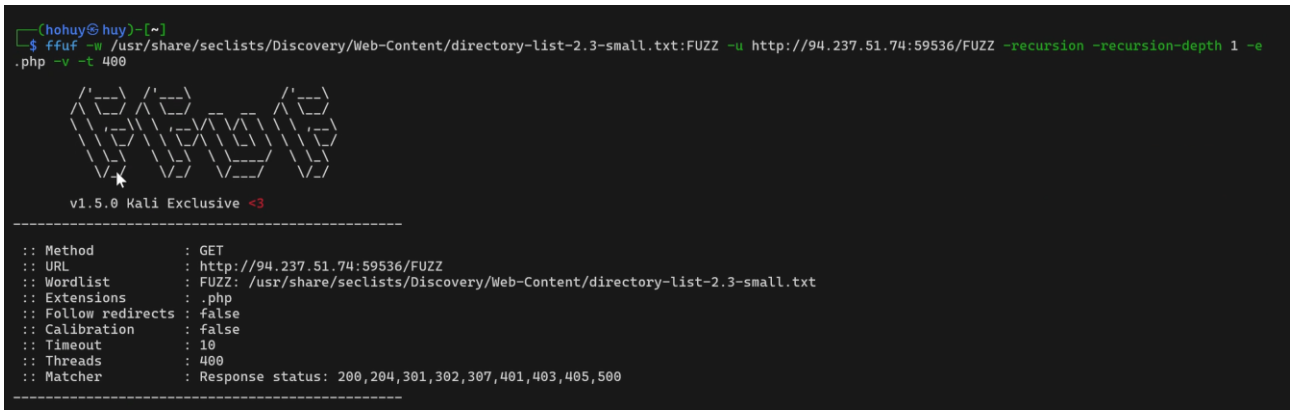


## Task: Recursive Fuzzing

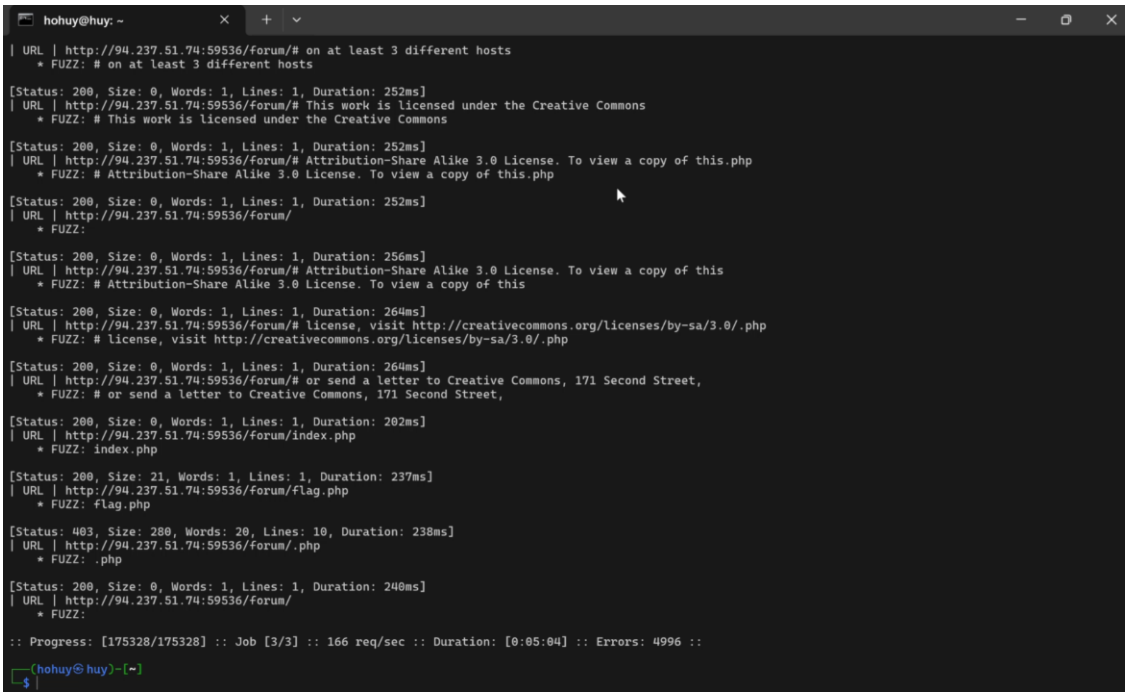
- Video thực hiện: https://youtu.be/MX1w-BnmnsM
- Target IP:

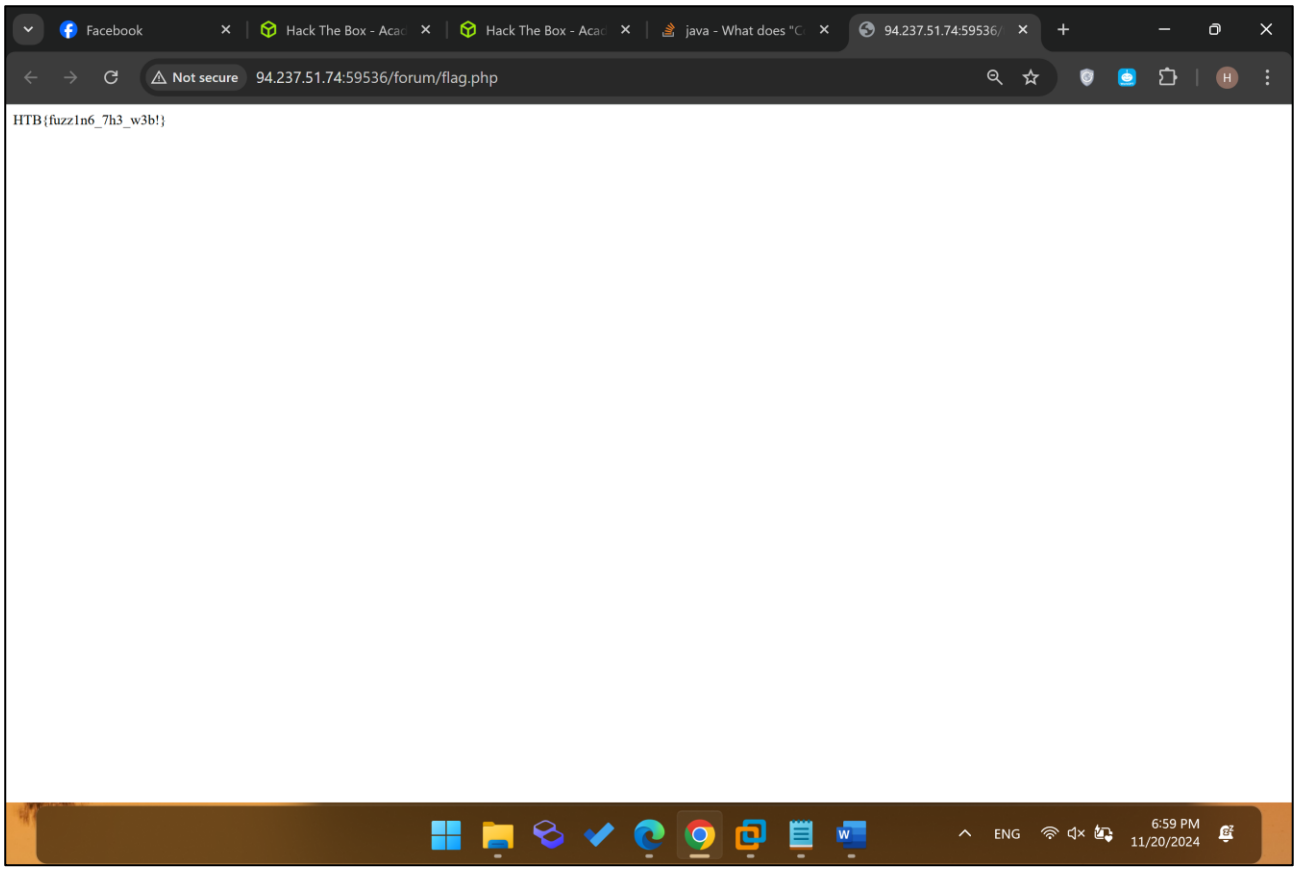



- Thực hiện:




- Kết quả:

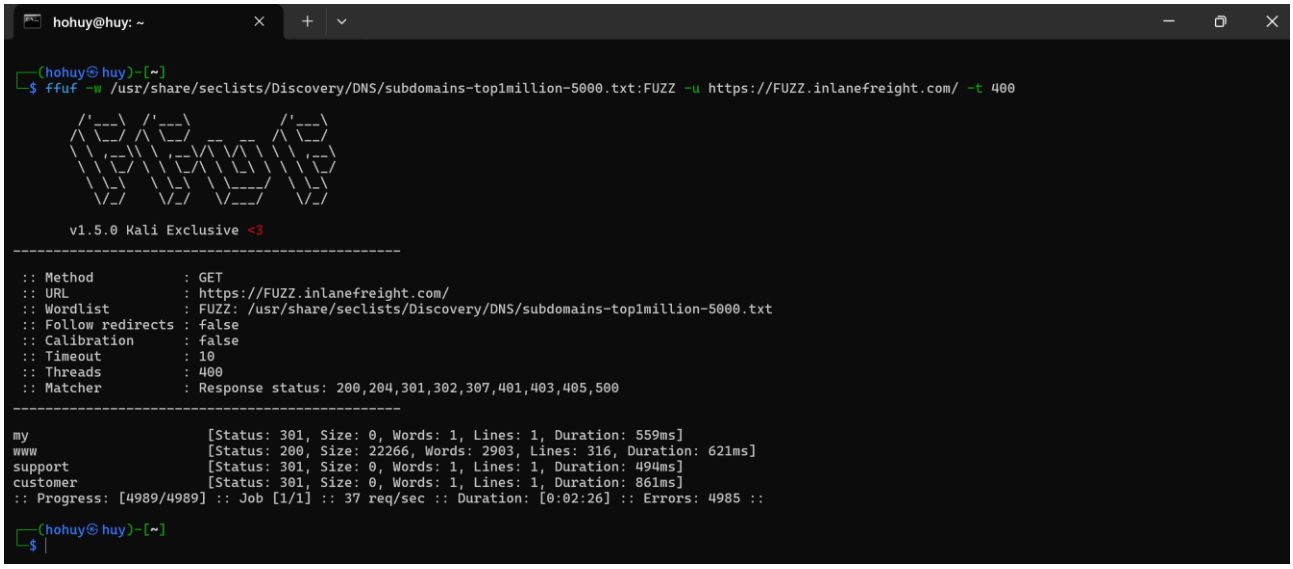



Facebook
Hack The Box - Aca
Hack The Box - Aca
java - What does "C
94.237.51.74:59536/
Not secure
94.237.51.74:59536/forum/flag.php
HTB{fuzz1n6_7h3_w3b!}
ENG
6:59 PM
11/20/2024

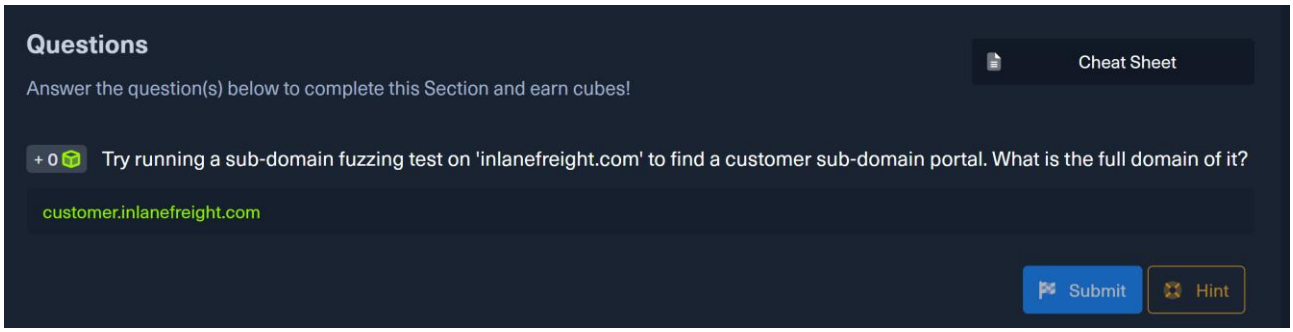
## Task: Sub-domain Fuzzing

- Video thực hiện: https://youtu.be/MdWl69ig_M0

- Thực hiện:

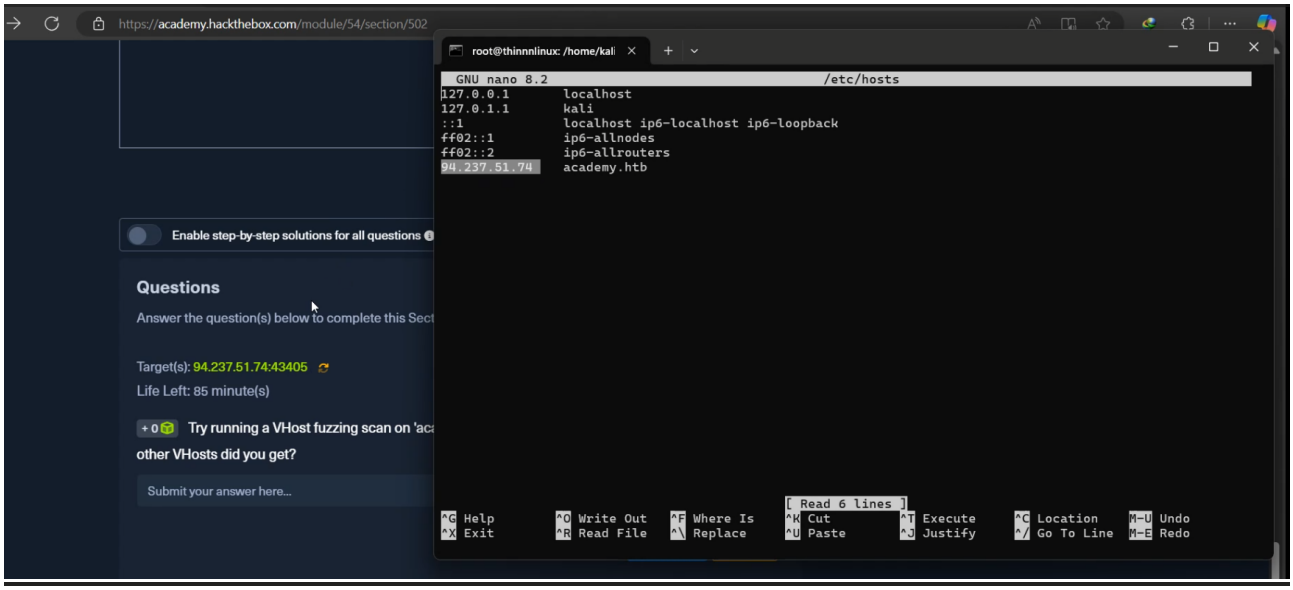



- Kết quả:

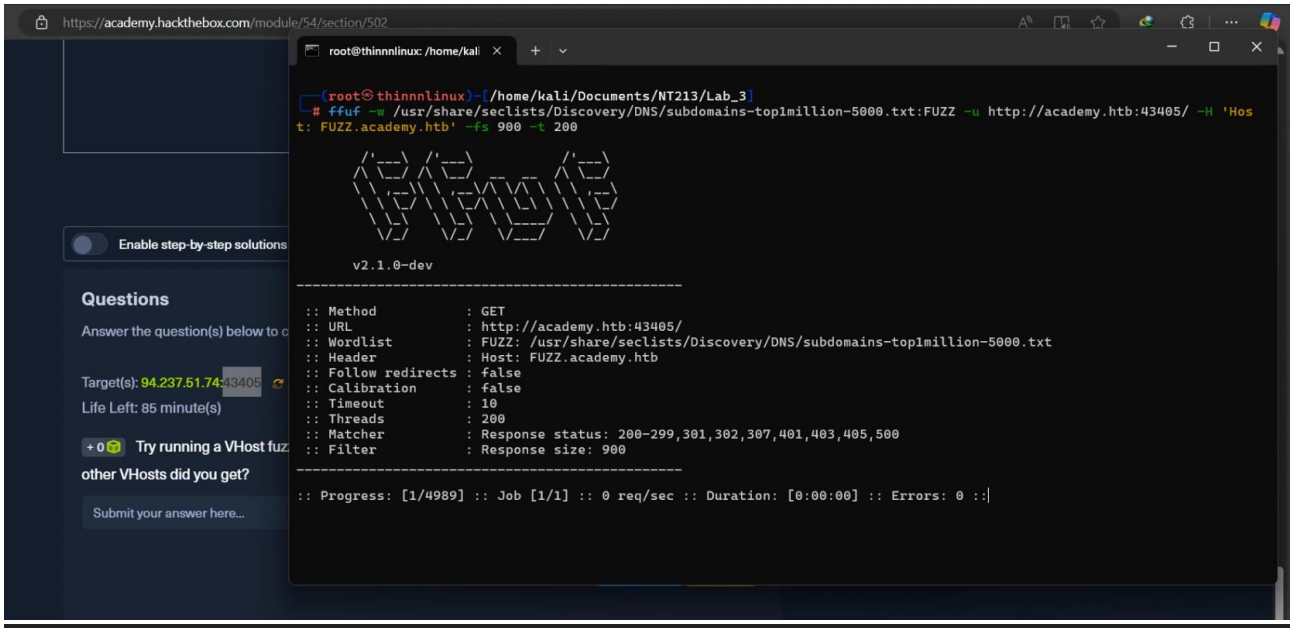


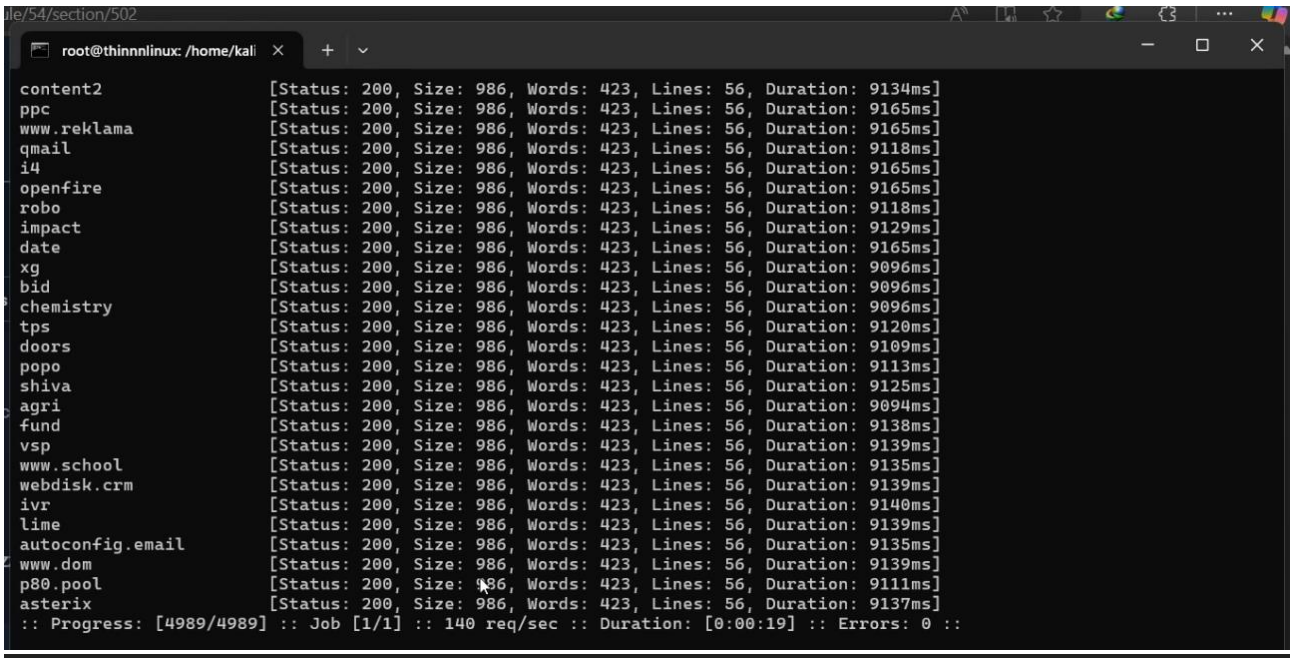
## Task: Filtering Results

- Video thực hiện: https://youtu.be/kxeTYCckg8c
- Cấu hình hosts:

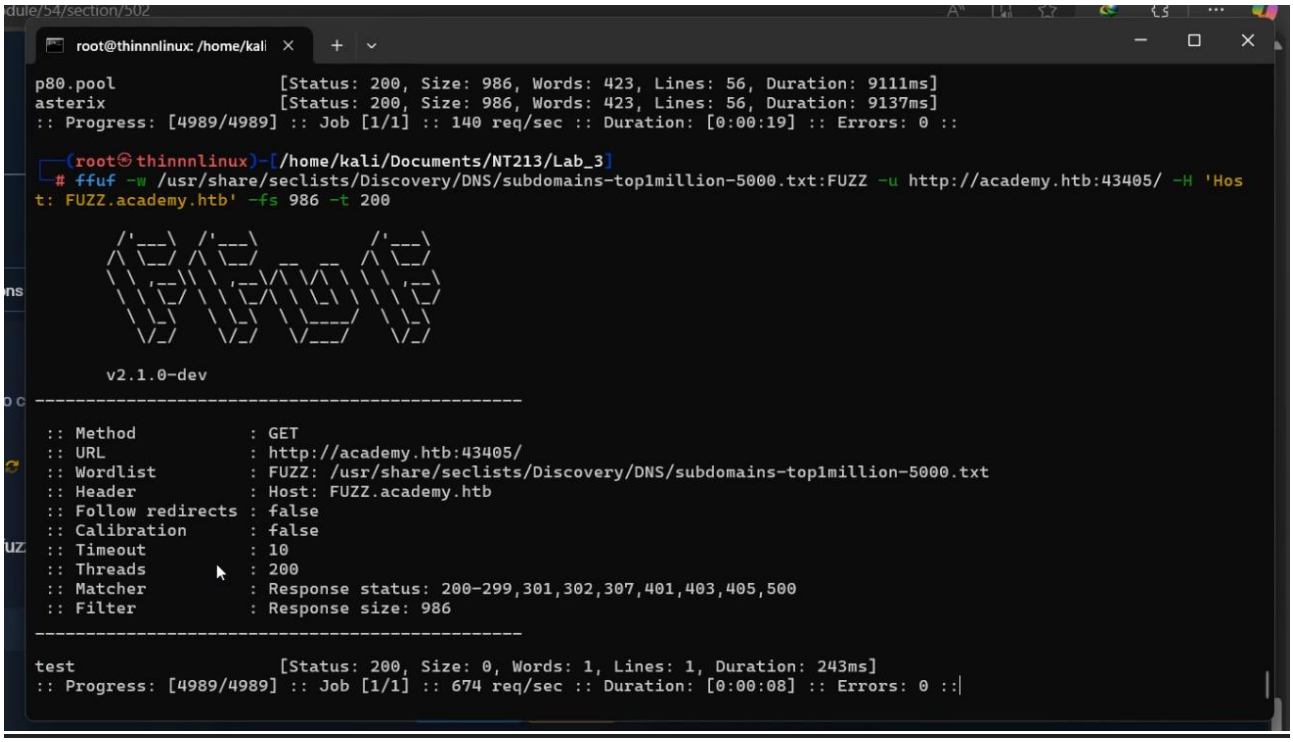



- Chạy lệnh như hình dưới, ở đây ta lấy thông số -fs là 900

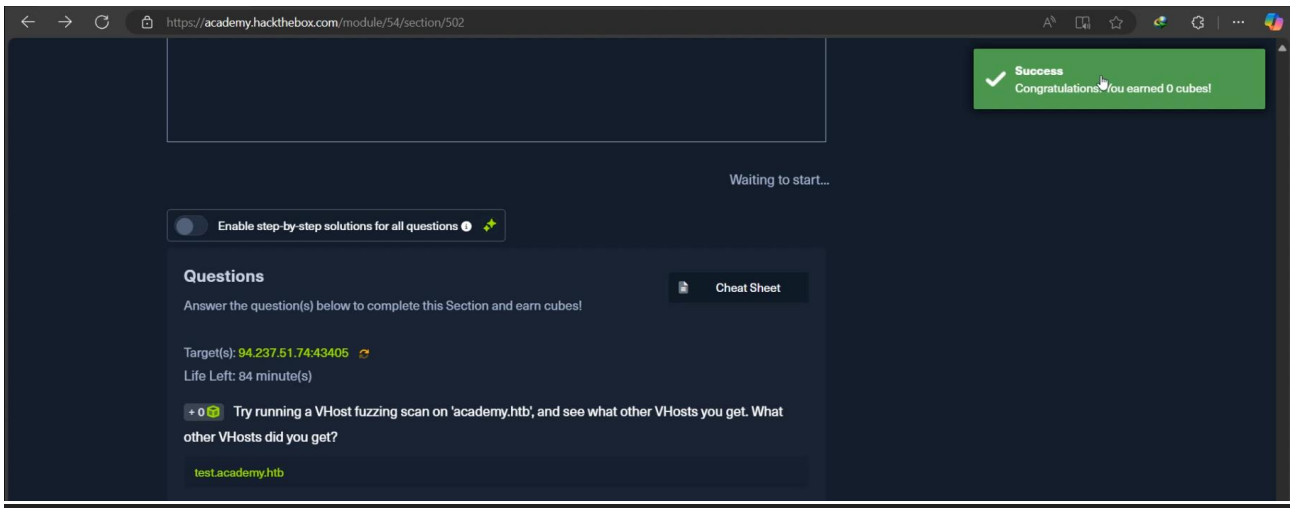





- Tại đây kết quả trả về với size là 986 rất nhiều, ta tiến hành lọc nó, thay đổi thông số -fs là 986:



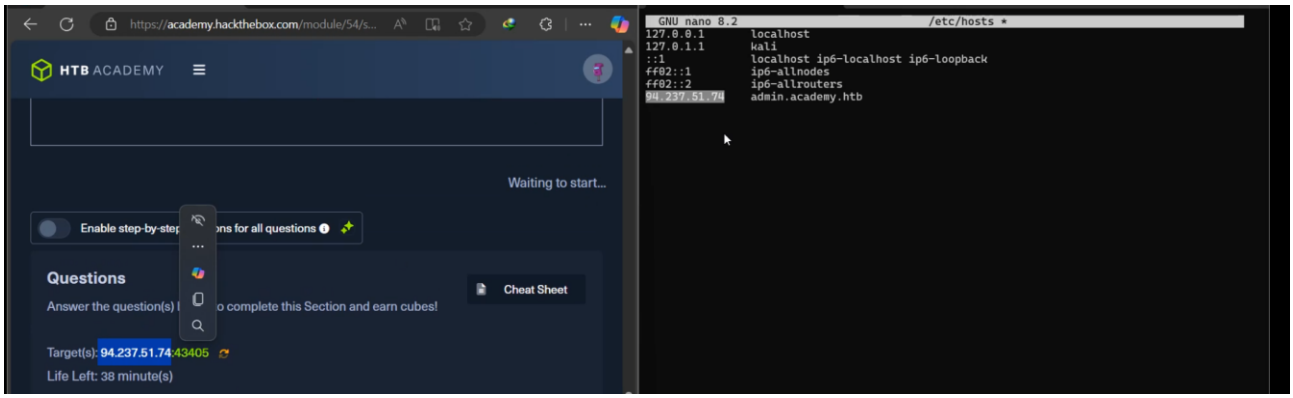

=> Kết quả trả về là “test”




=> Vhost là test.academy.htb

## Task: Parameter Fuzzing – GET

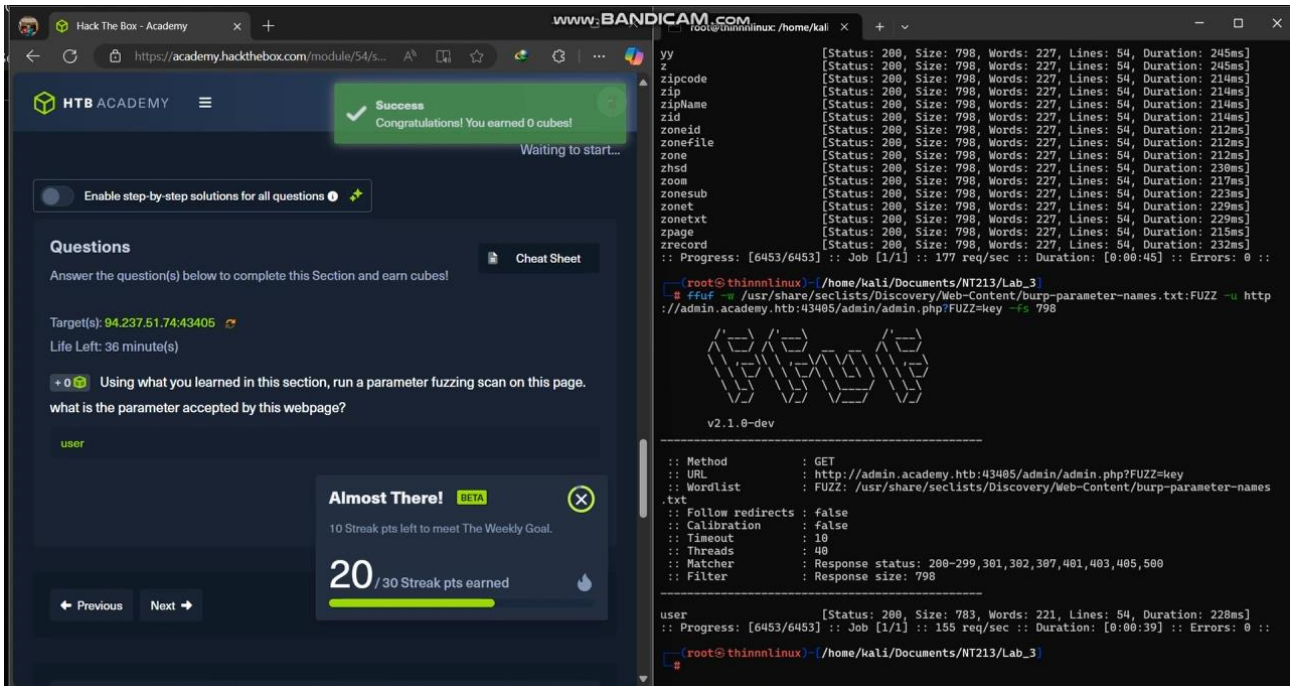
- Video thực hiện: https://youtu.be/k2a2XRLteao
- Cấu hình hosts:




- Chạy với thông số -fs 100, ta thấy được kết quả trả về với size 798 rất nhiều:

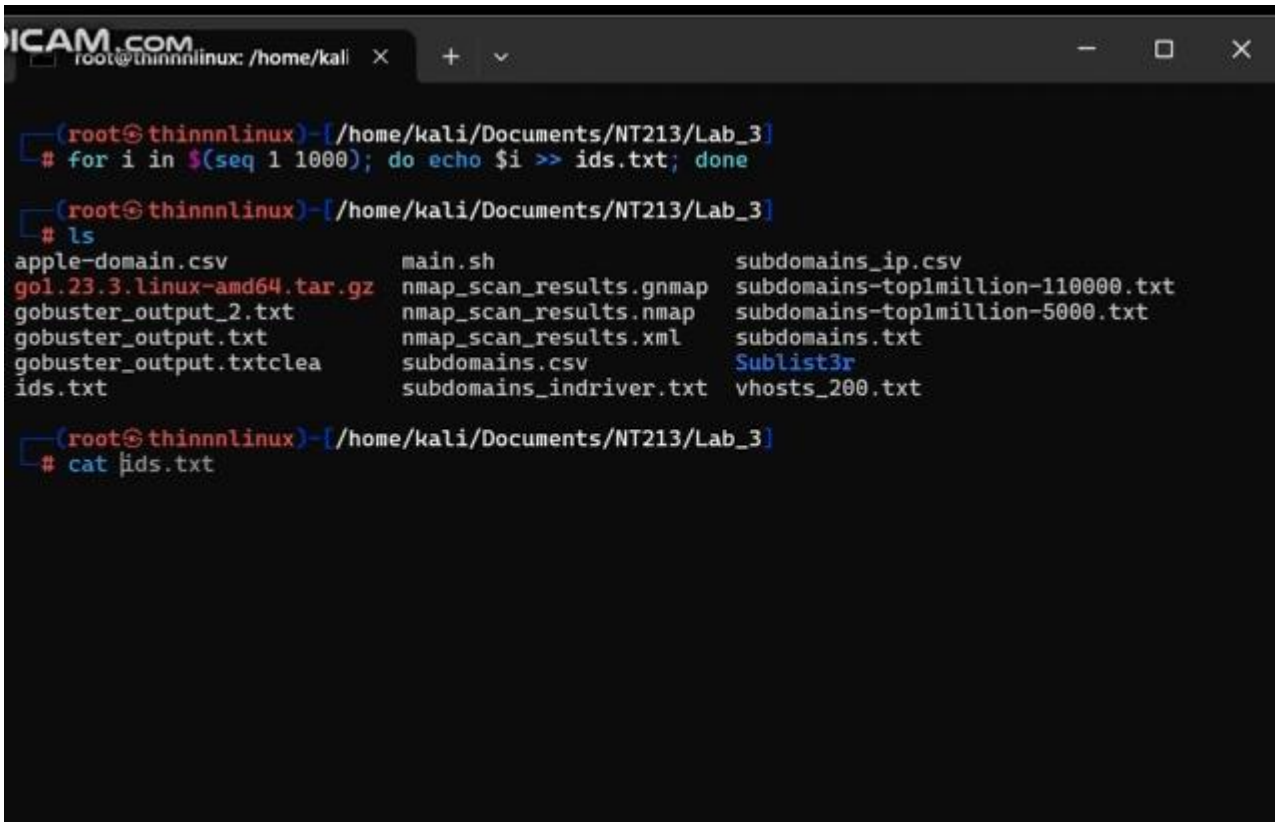
```
┌──(root㉿thinnnlinux)-[/home/kali/Documents/NT213/Lab_3]
└─# ffuf -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u http
://admin.academy.htb:43405/admin/admin.php?FUZZ=key -fs 100

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://admin.academy.htb:43405/admin/admin.php?FUZZ=key
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/burp-parameter-names
.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 100
________________________________________________

16                      [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 208ms]
AMOUNT                  [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 208ms]
15                      [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 209ms]
21                      [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 212ms]
Artist                  [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 213ms]
Article                 [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 211ms]
AddAuthItemForm         [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 212ms]
A                       [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 213ms]
Albania                 [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 226ms]
AUTH                    [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 225ms]
AudioPlayerSubmit       [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 222ms]
AuthChildForm           [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 222ms]
AuthItem                [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 222ms]
AuthItemChild           [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 233ms]
BIGGER                  [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 233ms]
BackURL                 [Status: 200, Size: 798, Words: 227, Lines: 54, Duration: 233ms]
```

- Chạy lại với -fs=798, ta được kết quả trả về là user




## Task: Value Fuzzing

- Video thực hiện: https://youtu.be/hg-F7Mqlh0c
- Tạo file text 1000 số:



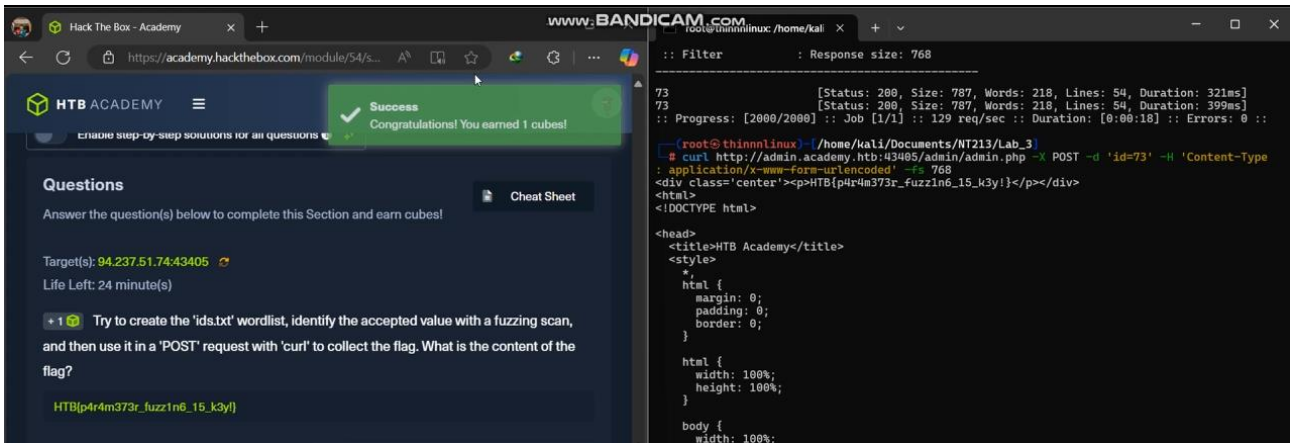
- Chạy với lệnh bên dưới, ta set -fs = 100, kết quả trả về cho ta size=768 khá nhiều

```
┌──(root㉿thinnnlinux)-[/home/kali/Documents/NT213/Lab_3]
└─# ffuf -w ids.txt:FUZZ -u http://admin.academy.htb:43405/admin/admin.php -X POST -d 'id=F
UZZ' -H 'Content-Type: application/x-www-form-urlencoded' -fs 100

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : http://admin.academy.htb:43405/admin/admin.php
 :: Wordlist         : FUZZ: /home/kali/Documents/NT213/Lab_3/ids.txt
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Data             : id=FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 100
________________________________________________

31                      [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 217ms]
25                      [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 255ms]
16                      [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 248ms]
7                       [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 249ms]
39                      [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 248ms]
17                      [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 250ms]
28                      [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 251ms]
8                       [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 251ms]
10                      [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 251ms]
26                      [Status: 200, Size: 768, Words: 219, Lines: 54, Duration: 250ms]
:: Progress: [50/2000] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
```

- Chạy lại với -fs=768, ta được id = 73:

```
┌──(root㉿thinnnlinux)-[/home/kali/Documents/NT213/Lab_3]
└─# ffuf -w ids.txt:FUZZ -u http://admin.academy.htb:43405/admin/admin.php -X POST -d 'id=FUZZ' -H 'Content-Type: application/x-www-form-urlencoded' -fs 768

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : http://admin.academy.htb:43405/admin/admin.php
 :: Wordlist         : FUZZ: /home/kali/Documents/NT213/Lab_3/ids.txt
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Data             : id=FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 768
________________________________________________

73                      [Status: 200, Size: 787, Words: 218, Lines: 54, Duration: 321ms]
73                      [Status: 200, Size: 787, Words: 218, Lines: 54, Duration: 399ms]
:: Progress: [2000/2000] :: Job [1/1] :: 129 req/sec :: Duration: [0:00:18] :: Errors: 0 ::
```

- sử dụng lệnh curl với id như trên để lấy flag:



**Skills Assessment - Web Fuzzing**

*** Question 1:**

Video thực hiện: https://youtu.be/Mz6u69jz6VE

*** Question 2:**

Video thực hiện: https://youtu.be/KhjZE_UszWc