Secret(放棄)

```
  └──# nmap -sCV -p 22,80,3000 -A 10.10.11.120
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-27 03:01 PDT
Nmap scan report for 10.10.11.120
Host is up (0.23s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 97:af:61:44:10:89:b9:53:f0:80:3f:d7:19:b1:e2:9c (RSA)
|   256 95:ed:65:8d:cd:08:2b:55:dd:17:51:31:1e:3e:18:12 (ECDSA)
|_  256 33:7b:c1:71:d3:33:0f:92:4e:83:5a:1f:52:02:93:5e (ED25519)
80/tcp   open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: DUMB Docs
3000/tcp open  http    Node.js (Express middleware)
|_http-title: DUMB Docs
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (96%), Linux 4.15 - 5.8 (96%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), Linux 5.3 - 5.4 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), Linux 2.6.32 (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   288.42 ms 10.10.14.1
2   288.65 ms 10.10.11.120

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.55 seconds
```

80、3000 port 網站相同

在登入用戶裡面->可進行註冊 + 登入，有子目錄

註冊用戶

介紹部分在這裡。 客戶很重要，有了客戶才會跟著客戶走。 每個人
convallis bibendum quis vitae turpis。 兩前庭直徑 lorem, vit

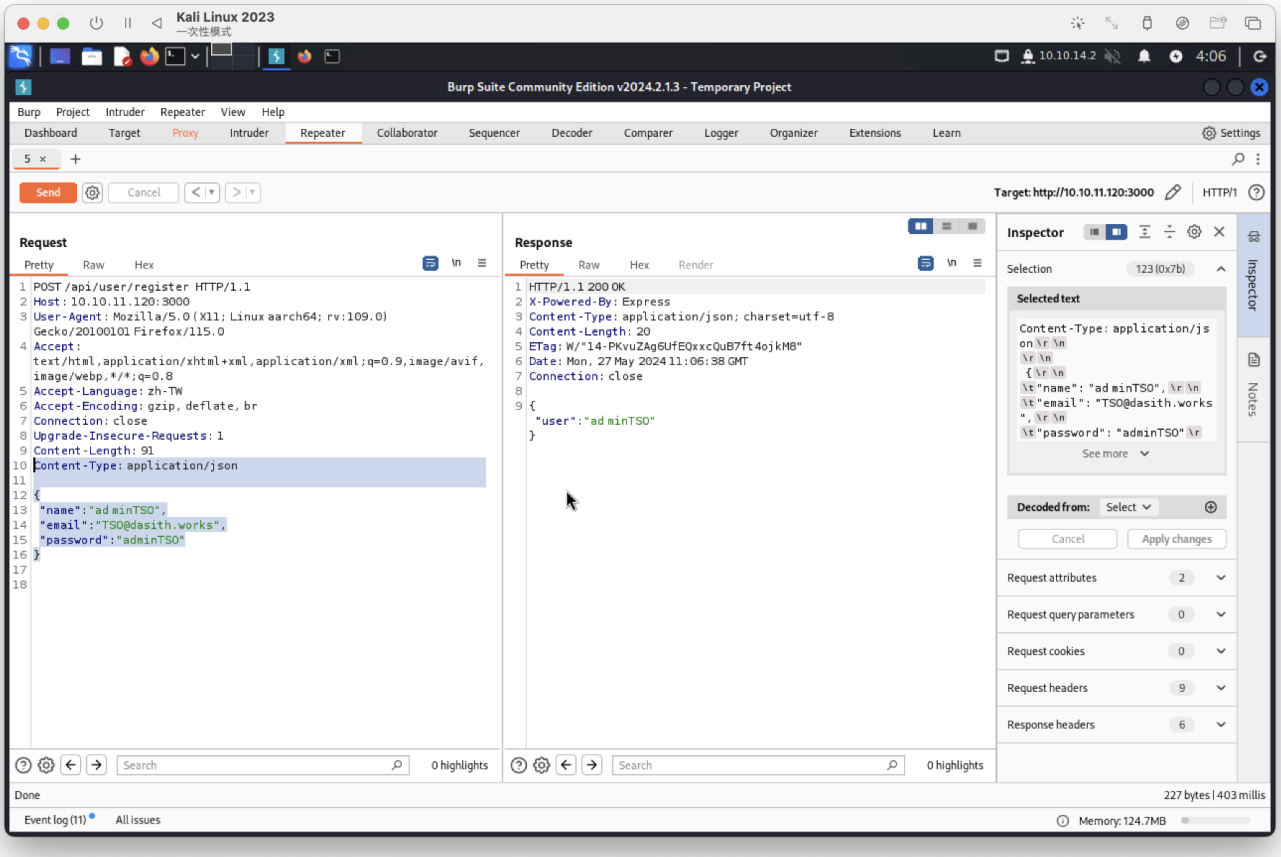
```
POST http://localhost:3000/api/user/register
```

Json 主體範例

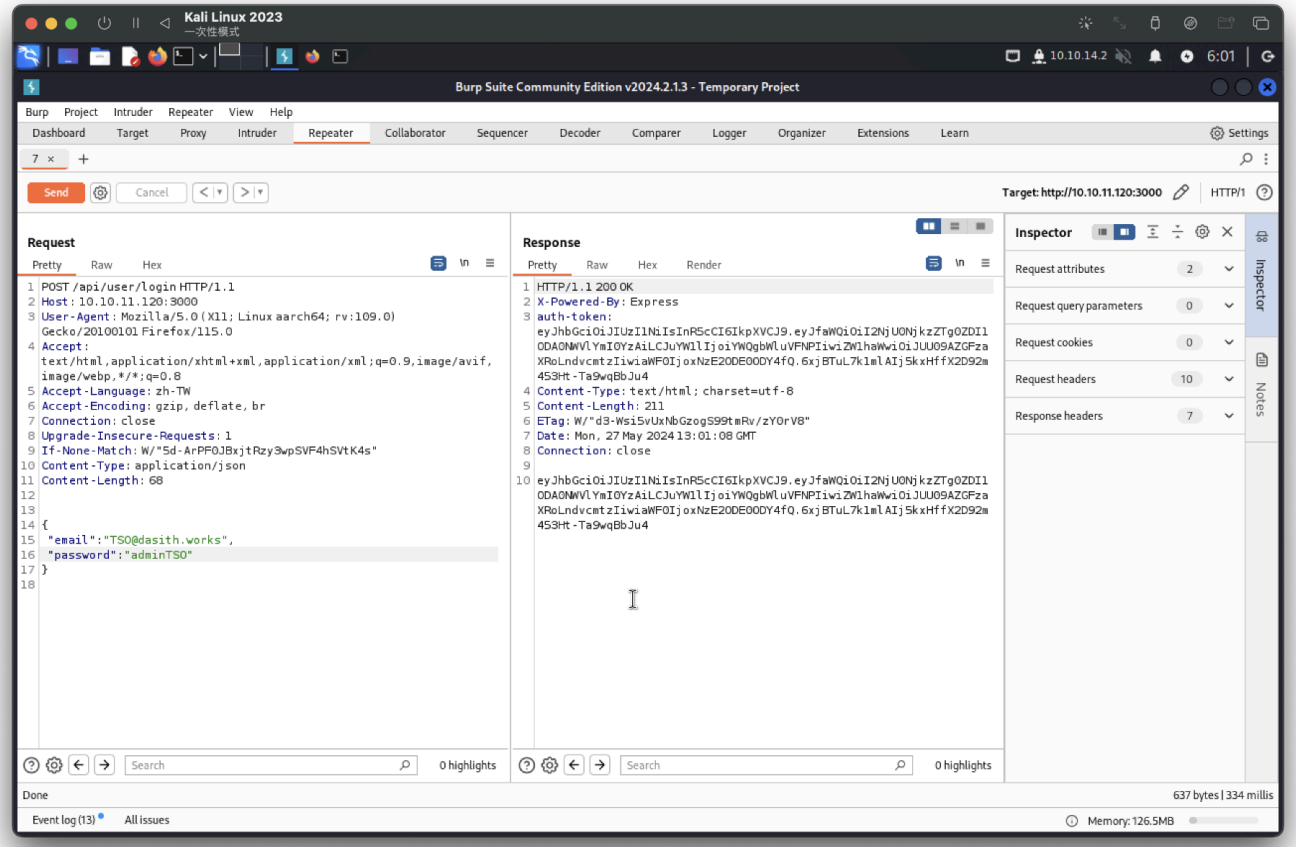
```
{
        "name": "dasith",
        "email": "root@dasith.works",
        "password": "Kekc8swFgD6zU"
}
```

抓包後進行註冊，需要post請求，

因為json，所以`Content-Type`也要改



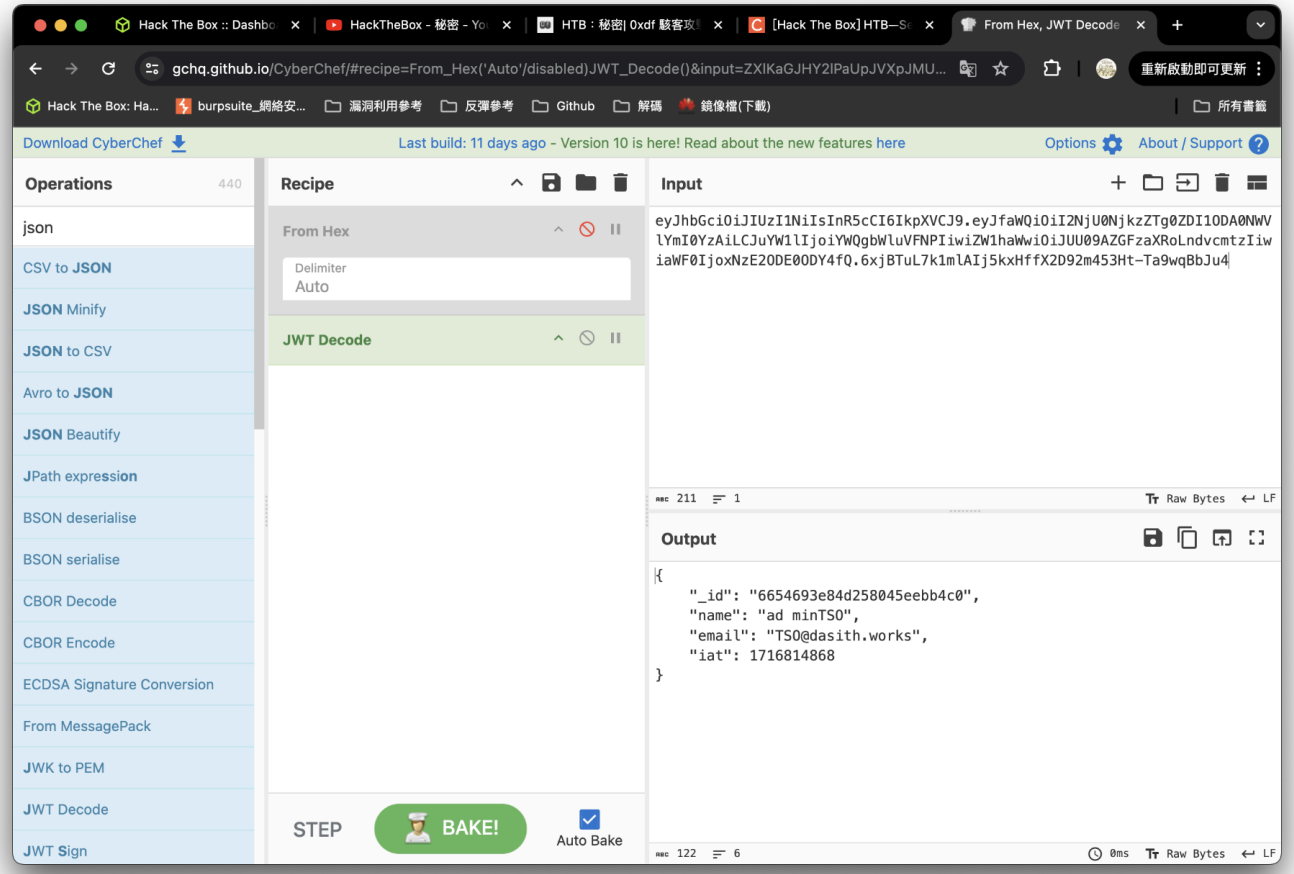
繼續按照網站過程執行



得到auth-token

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI2NjU0NjkzZTg0ZDI1ODA0NWVlYmI0YzAiLCJuYW1lIjoiYWQgbWluVFNPIiwiZW1haWwiOiJUU09AZGFzaXRoLndvcmtzIiwiaWF0IjoxNzE2ODE0ODY4fQ.6xjBTuL7k1mlAIj5kxHffX2D92m453Ht-Ta9wqBbJu4
```

進行json解密查看是否一致



按照網站執行，在標頭放token有異常，參考別人也是一樣。。