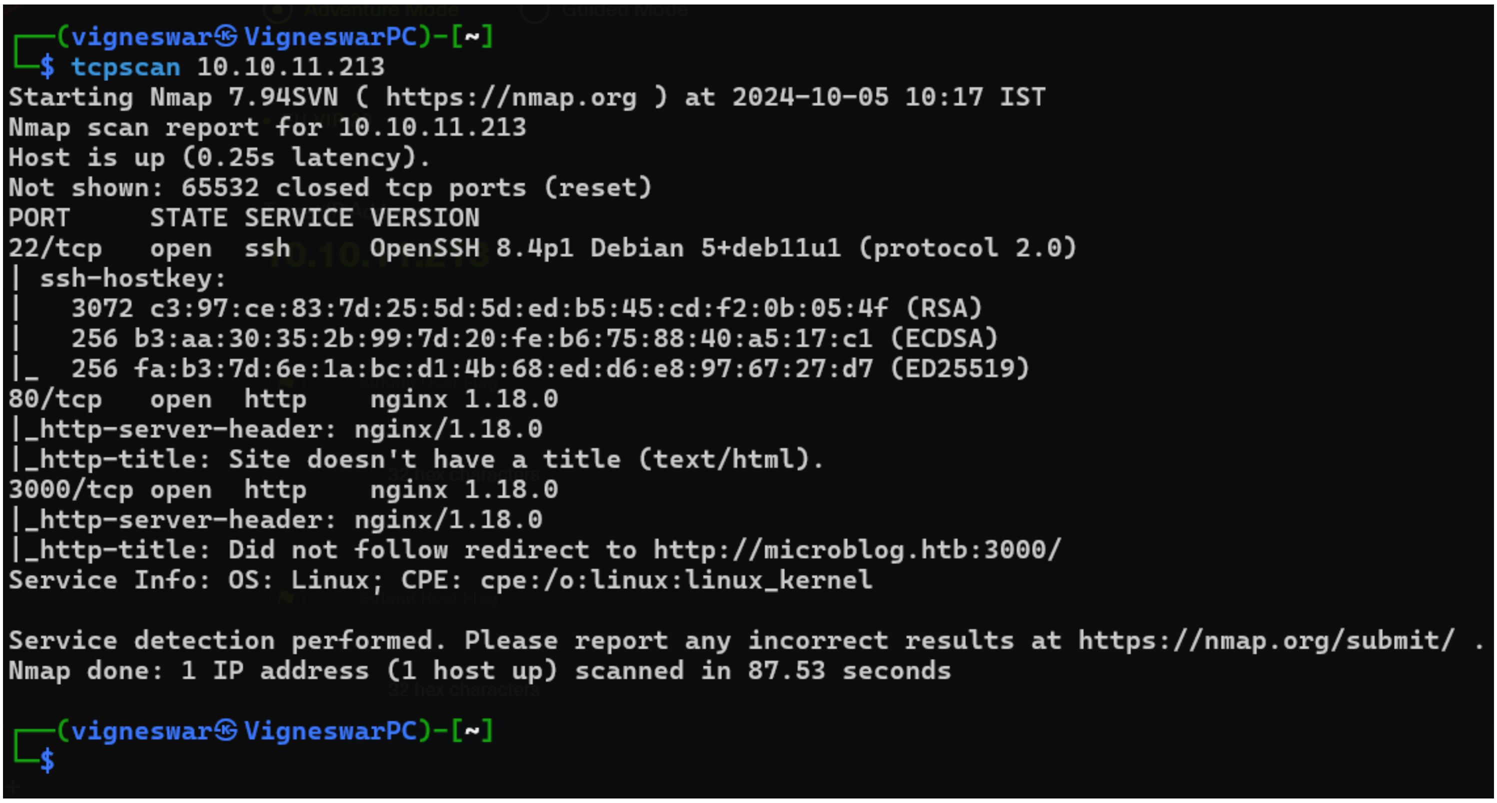
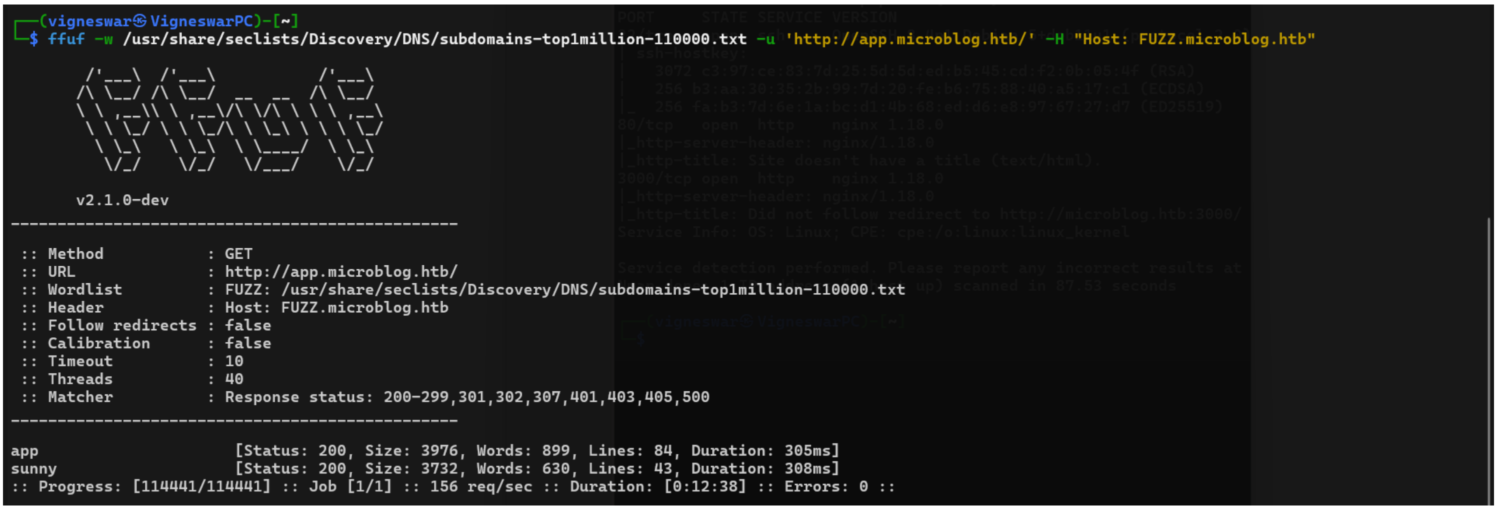
Information Gathering

1) Found open ports



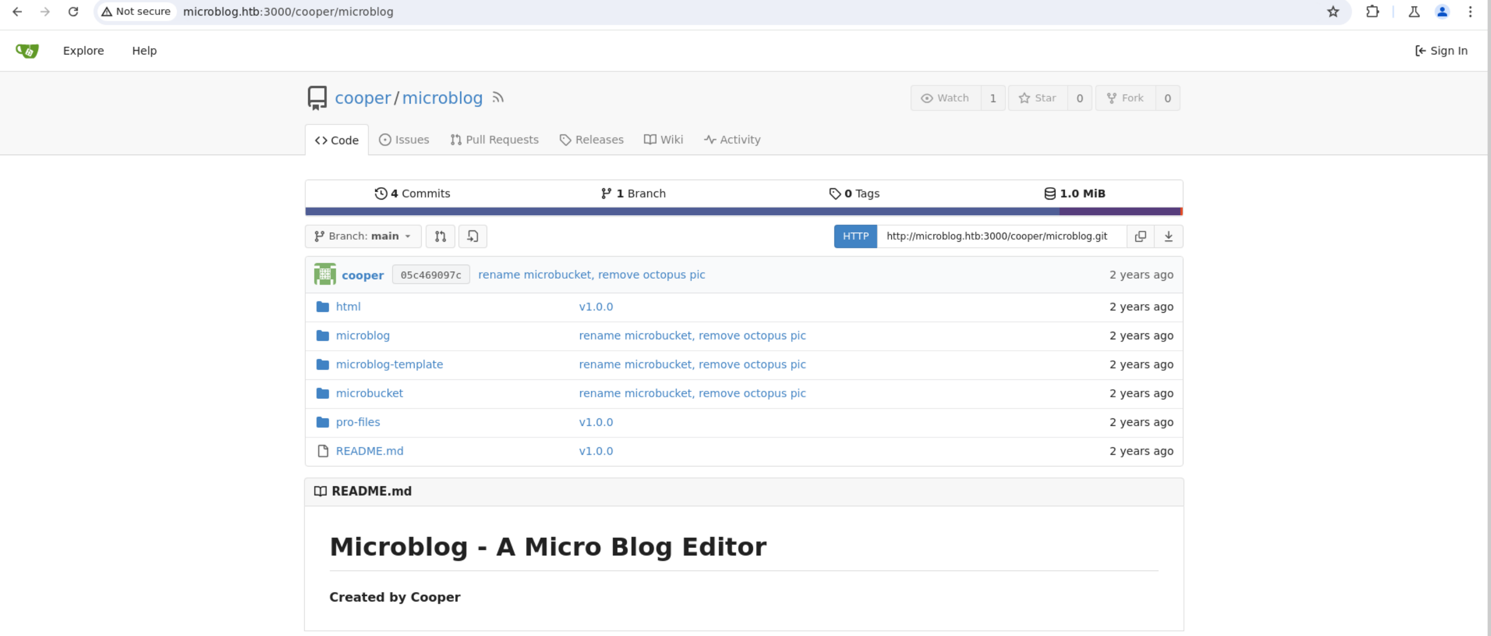
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.11.213
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-05 10:17 IST
Nmap scan report for 10.10.11.213
Host is up (0.25s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 c3:97:ce:83:7d:25:5d:5d:ed:b5:45:cd:f2:0b:05:4f (RSA)
|   256 b3:aa:30:35:2b:99:7d:20:fe:b6:75:88:40:a5:17:c1 (ECDSA)
|_  256 fa:b3:7d:6e:1a:bc:d1:4b:68:ed:d6:e8:97:67:27:d7 (ED25519)
80/tcp   open  http    nginx 1.18.0
|_http-server-header: nginx/1.18.0
|_http-title: Site doesn't have a title (text/html).
3000/tcp open  http    nginx 1.18.0
|_http-server-header: nginx/1.18.0
|_http-title: Did not follow redirect to http://microblog.htb:3000/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 87.53 seconds

┌──(vigneswar㉿VigneswarPC)-[~]
└─$
```

2) Found vhosts



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -u 'http://app.microblog.htb/' -H "Host: FUZZ.microblog.htb"

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://app.microblog.htb/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.microblog.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

app                     [Status: 200, Size: 3976, Words: 899, Lines: 84, Duration: 305ms]
sunny                   [Status: 200, Size: 3732, Words: 630, Lines: 43, Duration: 308ms]
:: Progress: [114441/114441] :: Job [1/1] :: 156 req/sec :: Duration: [0:12:38] :: Errors: 0 ::
```

3) Found gitea instance with source code



Not secure microblog.htb:3000/cooper/microblog

Explore Help Sign In

cooper/microblog

Watch 1 Star 0 Fork 0

Code Issues Pull Requests Releases Wiki Activity

4 Commits 1 Branch 0 Tags 1.0 MiB

Branch: main

HTTP http://microblog.htb:3000/cooper/microblog.git

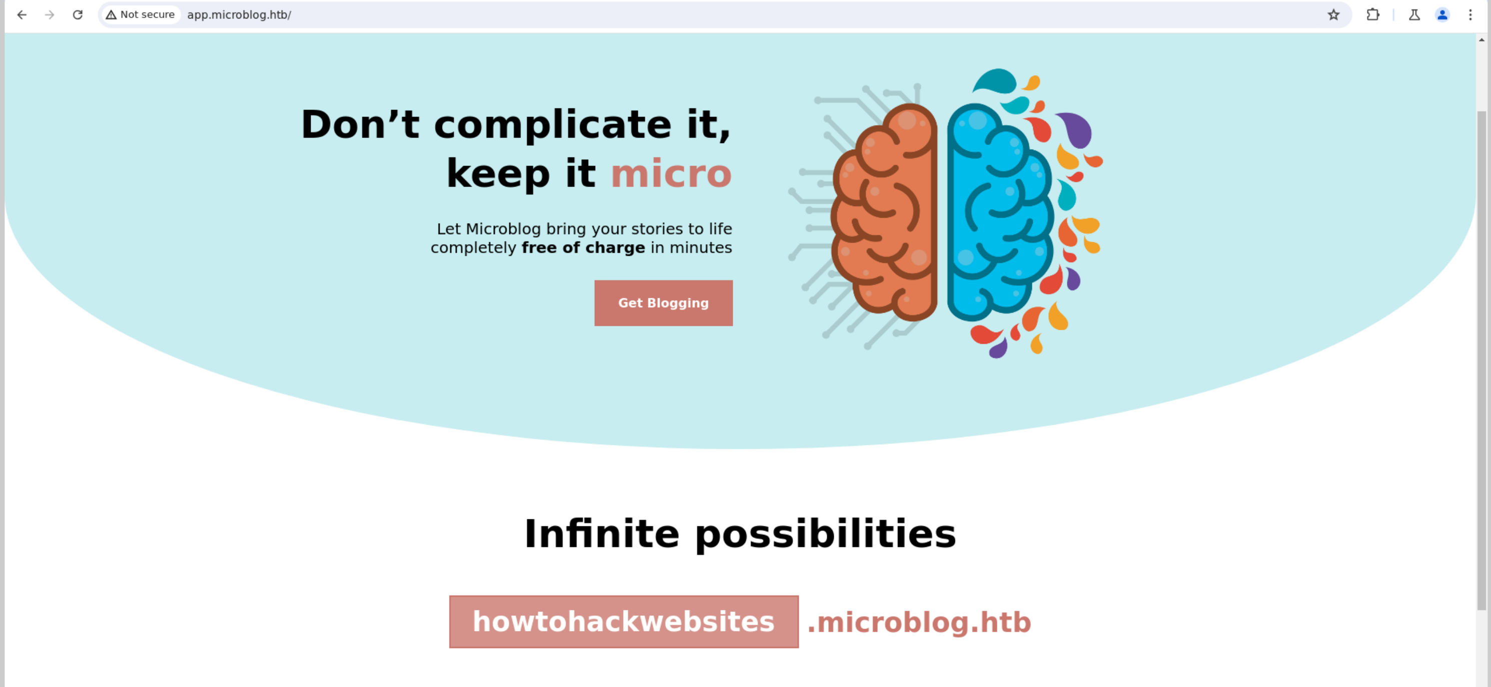
cooper 05c469097c	rename microbucket, remove octopus pic	2 years ago
html	v1.0.0	2 years ago
microblog	rename microbucket, remove octopus pic	2 years ago
microblog-template	rename microbucket, remove octopus pic	2 years ago
microbucket	rename microbucket, remove octopus pic	2 years ago
pro-files	v1.0.0	2 years ago
README.md	v1.0.0	2 years ago

README.md

Microblog - A Micro Blog Editor

Created by Cooper

4) Checked the websites



Not secure app.microblog.htb/

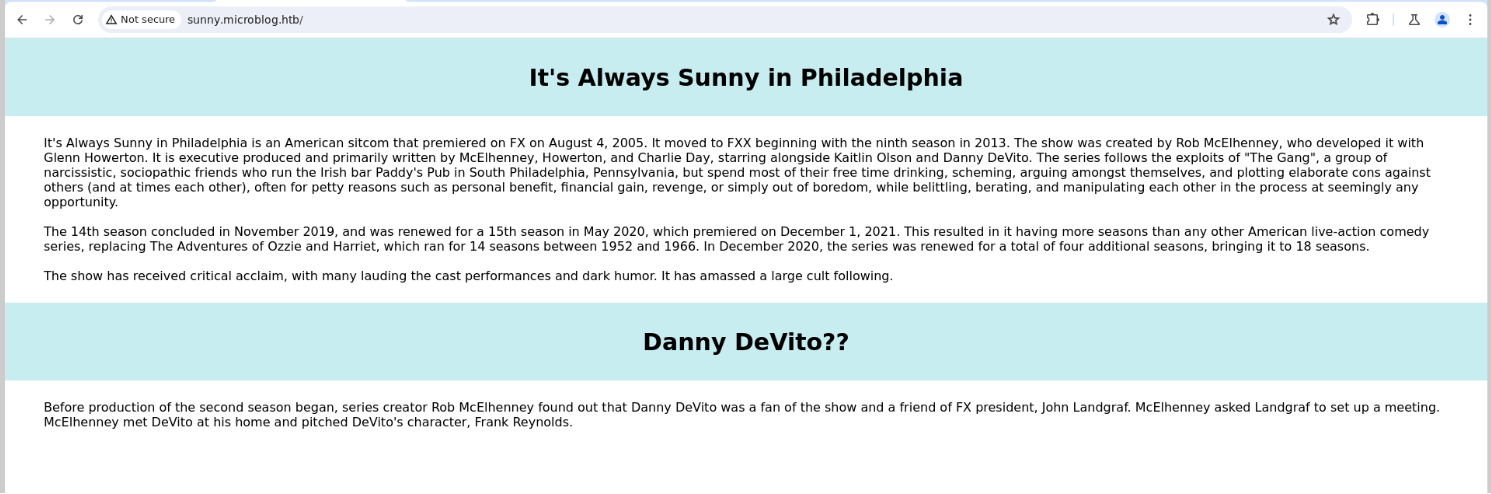
Don't complicate it, keep it micro

Let Microblog bring your stories to life completely **free of charge** in minutes

Get Blogging

Infinite possibilities

howtohackwebsites .microblog.htb



Not secure sunny.microblog.htb/

It's Always Sunny in Philadelphia

It's Always Sunny in Philadelphia is an American sitcom that premiered on FX on August 4, 2005. It moved to FXX beginning with the ninth season in 2013. The show was created by Rob McElhenney, who developed it with Glenn Howerton. It is executive produced and primarily written by McElhenney, Howerton, and Charlie Day, starring alongside Kaitlin Olson and Danny DeVito. The series follows the exploits of "The Gang", a group of narcissistic, sociopathic friends who run the Irish bar Paddy's Pub in South Philadelphia, Pennsylvania, but spend most of their free time drinking, scheming, arguing amongst themselves, and plotting elaborate cons against others (and at times each other), often for petty reasons such as personal benefit, financial gain, revenge, or simply out of boredom, while belittling, berating, and manipulating each other in the process at seemingly any opportunity.

The 14th season concluded in November 2019, and was renewed for a 15th season in May 2020, which premiered on December 1, 2021. This resulted in it having more seasons than any other American live-action comedy series, replacing The Adventures of Ozzie and Harriet, which ran for 14 seasons between 1952 and 1966. In December 2020, the series was renewed for a total of four additional seasons, bringing it to 18 seasons.

The show has received critical acclaim, with many lauding the cast performances and dark humor. It has amassed a large cult following.

Danny DeVito??

Before production of the second season began, series creator Rob McElhenney found out that Danny DeVito was a fan of the show and a friend of FX president, John Landgraf. McElhenney asked Landgraf to set up a meeting. McElhenney met DeVito at his home and pitched DeVito's character, Frank Reynolds.