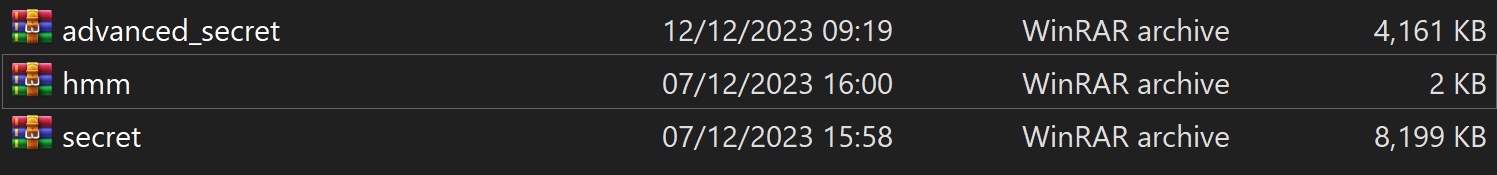
**BlackBox4 – Solution**

1. This blackbox start with these 3 rar files:



I tried to extract all of them, but only secret.rar didn’t ask for a password for doing so. The extraction was of the file **secret.exe** so I chose to run it via **cmd** with this command: **>secret.exe**

The output of this program was:

**\* Serving Flask app 'secret'**

**\* Debug mode: on**

**WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.**

**\* Running on http://127.0.0.1:5000**

**Press CTRL+C to quit**

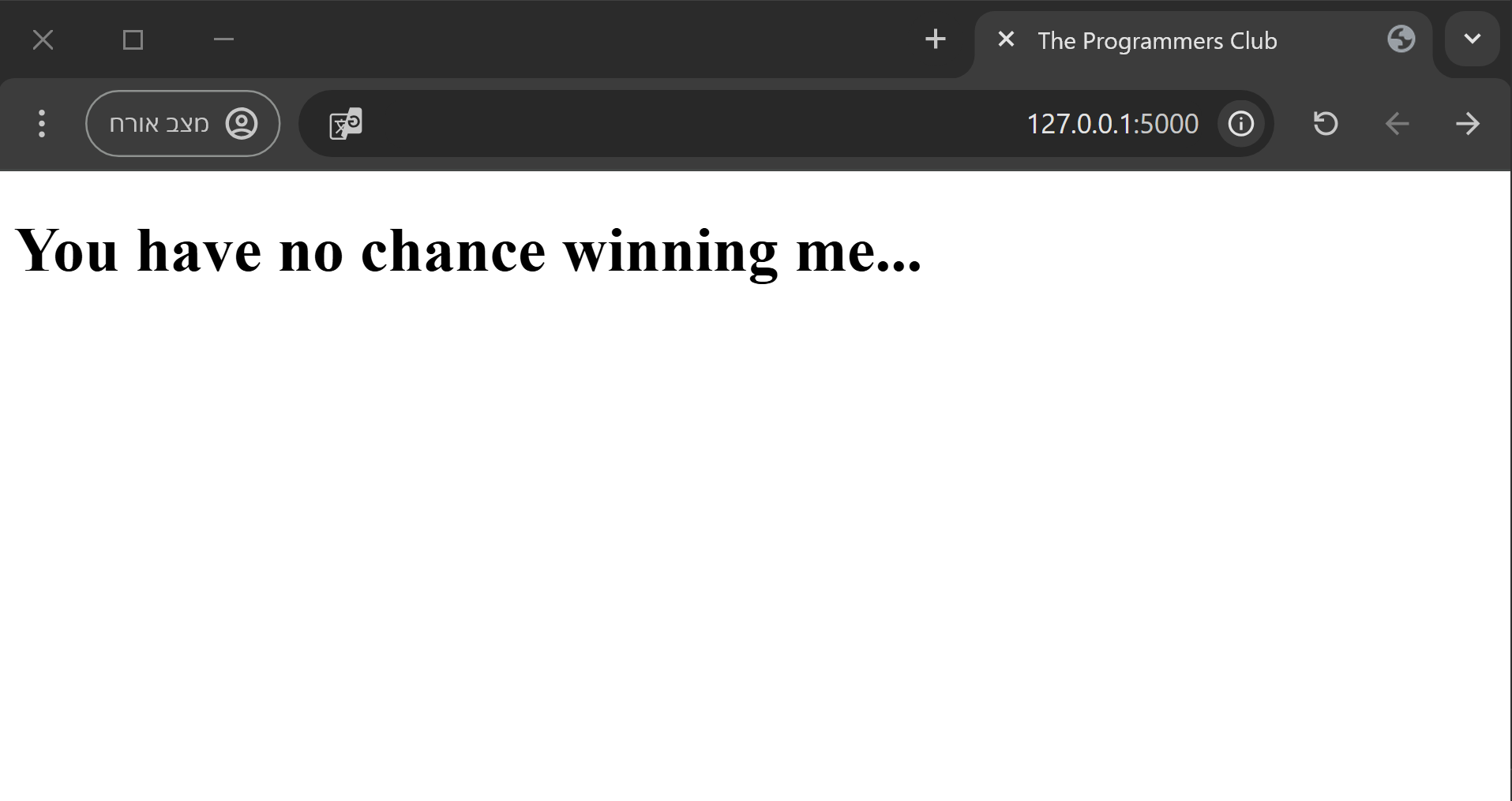
**\* Restarting with stat**

**\* Debugger is active!**

**\* Debugger PIN: 555-912-949**

From here I understood that a **http** **server** was run on the **localhost(127.0.0.1)** with port number **5000**.

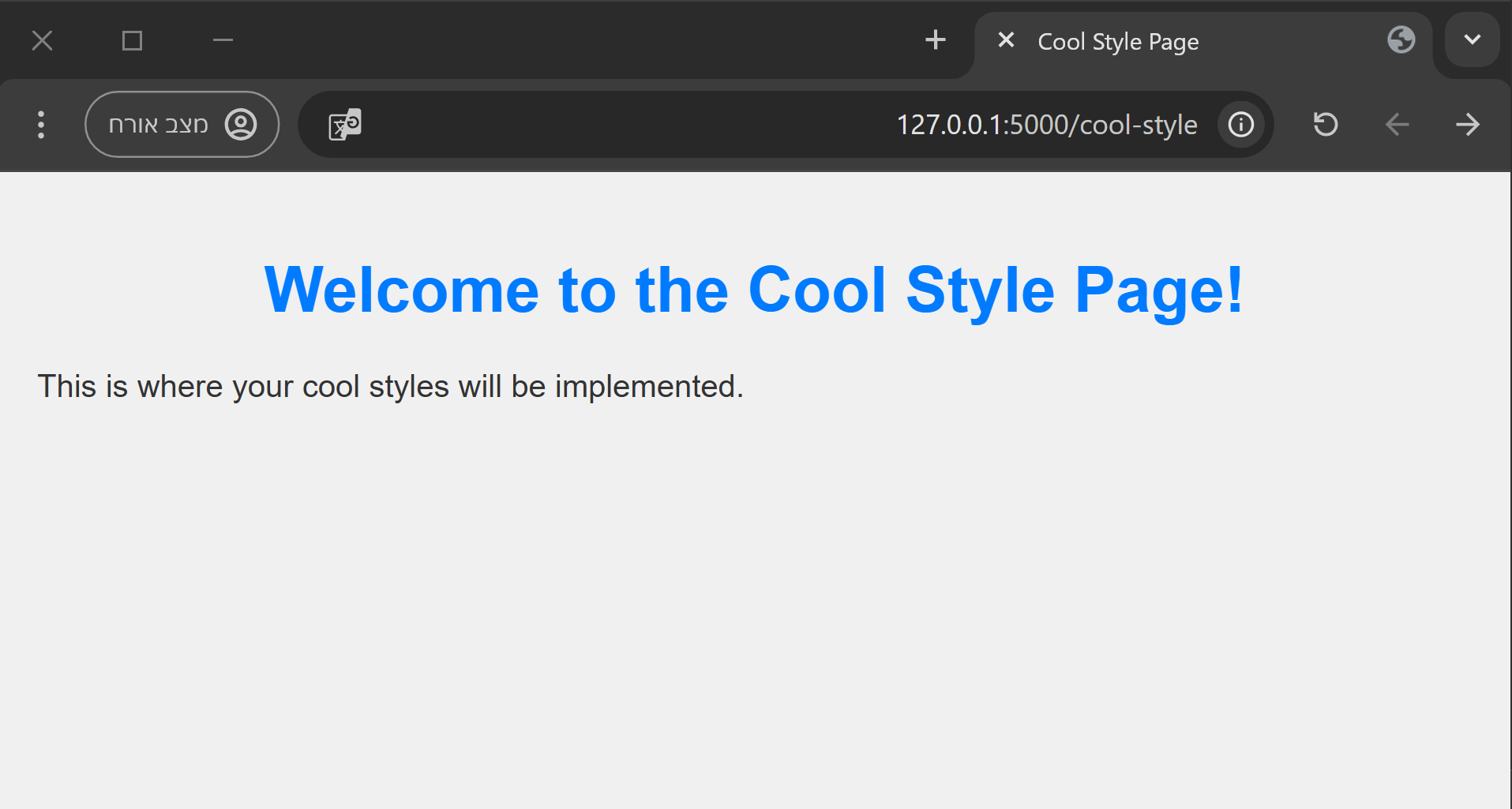
1. Then, I tried to connect this server with my browser(**google chrome**), and this is the opening page of the website:



1. After watching the **inspector** settings of this website, I found a new page of the website, “**cool-style**”, via this line in the http code of the default page:

<h1 css="http://127.0.0.1:5000/cool-style">You have no chance winning me...</h1>

**This new page:**

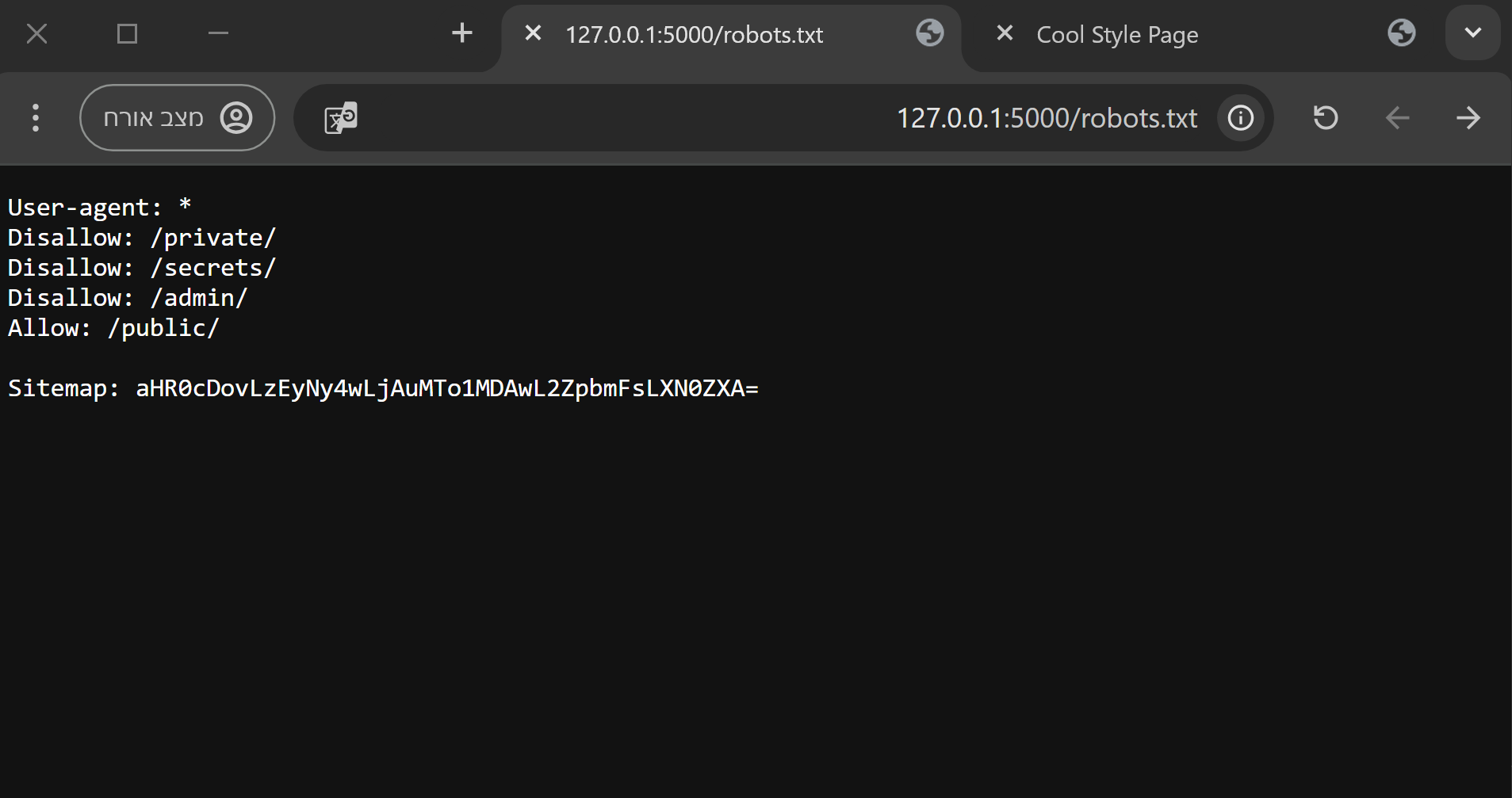


1. In the next step, I found inside the html code of this page this line:

**<!-- U2FsdGVkX19CmDLOm05upIE+T+IIVK+A71BblFe5tWAahq2x6+P8w5oWOzM2DGf5 -->**

The value inside the comment seems like a **hashed/encrypted** value but I will work with it later.

1. Afterwards, I opened the **robots.txt** file(which is the sitemap file of the website) with this url: **http://127.0.0.1:5000/robots.txt** . The result is:



1. I saw this encryption: “**aHR0cDovLzEyNy4wLjAuMTo1MDAwL2ZpbmFsLXN0ZXA=**” in the **robots.txt** which I tried to decode using this **py** script:

import base64

def decrypt(s:str):

    # The function gets a string.

    # The function returns the given string after getting decrypted.

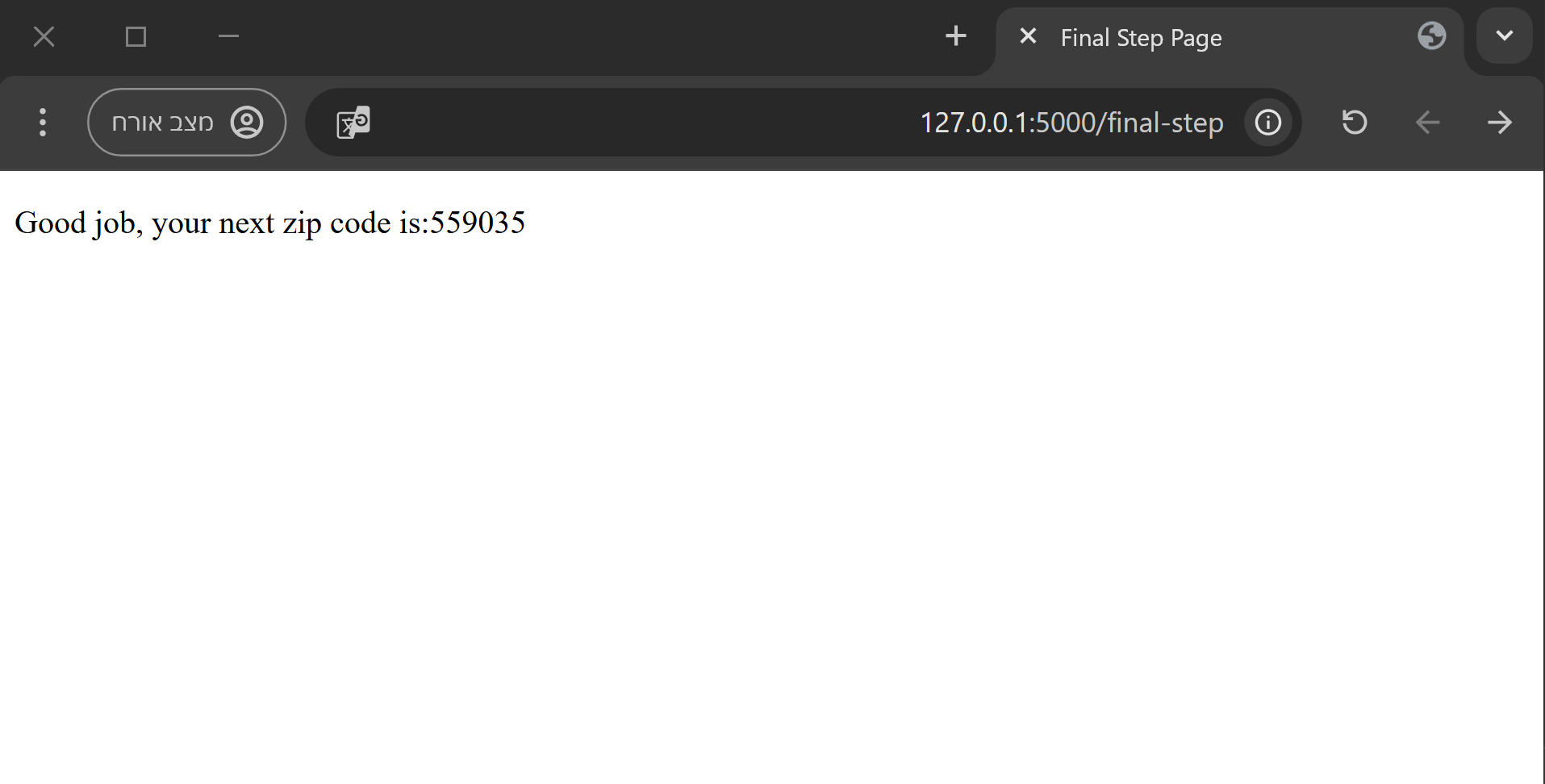
    return base64.b64decode(s.encode()).decode()

if \_\_name\_\_ == "\_\_main\_\_":

    print(decrypt("aHR0cDovLzEyNy4wLjAuMTo1MDAwL2ZpbmFsLXN0ZXA="))

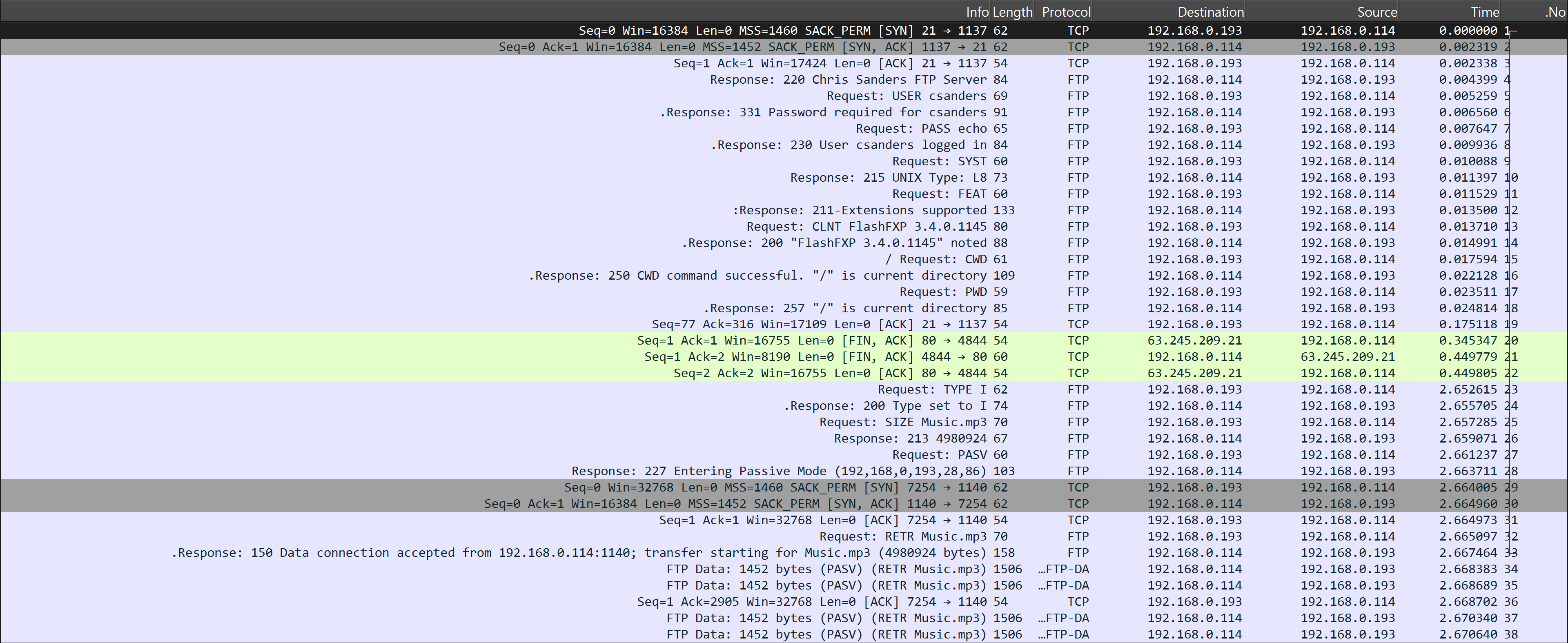
The output is: “**http://127.0.0.1:5000/final-step**” which seems like a url for a new page on this website.

1. The page looks like this:



I used the zip code, **559035**, from this page to extract the **hmm.rar** folder. The folder contained a file named “**ftp.pcap**” which is a packet sniffing file.

1. I opened this file with Wireshark program and found those packets:



The **TCP** stream of packets **1 – 19, 23-28 and 32-33** which contains this content:

220 Chris Sanders FTP Server

USER csanders

331 Password required for csanders.

PASS echo

230 User csanders logged in.

SYST

215 UNIX Type: L8

FEAT

211-Extensions supported:

CLNT

MDTM

PASV

REST STREAM

SIZE

211 End.

CLNT FlashFXP 3.4.0.1145

200 "FlashFXP 3.4.0.1145" noted.

CWD /

250 CWD command successful. "/" is current directory.

PWD

257 "/" is current directory.

TYPE I

200 Type set to I.

SIZE Music.mp3

213 4980924

PASV

227 Entering Passive Mode (192,168,0,193,28,86)

RETR Music.mp3

150 Data connection accepted from 192.168.0.114:1140; transfer starting for Music.mp3 (4980924 bytes).

After analyzing this content, I understood that it describes a connection between a user named “**csanders**” with the password “**echo**” using the host: “**192.168.0.114**” with the port: “**1140**“ and an **ftp** server with the address: “**192.168.0.193:2886**”. During the communication with the server, the user has logged in and downloaded an **mp3** file named “**Music.mp3**”.

The next **TCP** stream of packets **29-31 and 34-38** contains this content:

ID3......vTALB...&...Unknown Album (2/26/2006 11:12:20 AM)TIT2.......Track 2MCDI...(..3.+.9.6.+.4.B.0.C.+.8.7.E.7.+.D.D.4.2...TRCK.......2TCON.......UnknownPRIV......PeakValue..[..PRIV......AverageLevel..

..TPE1.......Unknown ArtistTLEN.......207720..........................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................@.....K...... p.......... ..%.....................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................@.....K....N. p.......... ..%.....................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................@.....K....N. p.......... ..%............................................................................................................................................................................................................................................................................................................................................................................................................................................

Which is less readable but according to the previous, it’s probably the stream of the downloading of the **Music.mp3** file.

1. After thinking about the first stream, I wanted to try and extract the advanced\_secret.rar folder with the password “**echo**” and it worked! The extraction gave me the program “advanced\_secret.exe” which I run using the cmd. The program printed me this:

**>advanced\_secret.exe**

**Listening on localhost:<random>**

10. I understood that it is probably another server that runs on the localhost(**127.0.0.1**) with a random port, so I searched this **process’ ID** in the **task manager** to find its port in **netstat**: 

**>netstat -ano | findstr 25352**

**TCP 127.0.0.1:8753 0.0.0.0:0 LISTENING 25352**

The port is: **8753**

11. From this step, I wrote this **py** script to create a socket with the server:

import socket

HOST, PORT = "127.0.0.1", 8753

# A tcp socket:

s = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

s.connect((HOST, PORT))

And while running it I sniffed the connection packets using Wireshark and this is their stream results:

CTF\_PROGRAMMERS\_CLUB\_FLAG\_534543234