**Epistemus:** This image goes hard, feel free to run diagnostics.



Here, we are given a photo of Patrick that seems to have a github link hiding in plain sight

We use stegsolve to accurately identify the link

A picture containing diagram

Description automatically generated

The GitHub Repository contains one file to lead challengers astray and two important files to complete the challenge:

A screenshot of a computer

Description automatically generated with medium confidence

README.md contained the following line of text:

Arire tbaan tvir lbh hc Arire tbaan yrg lbh qbja Arire tbaan eha nebhaq naq qrfreg lbh Arire tbaan znxr lbh pel Arire tbaan fnl tbbqolr Arire tbaan gryy n yvr naq uheg lbh

Since it looks like the output of a well-known substitution cipher (ROT13), I decided to use the tool CyberChef by the GCHQ and immediately found out that this … is indeed a Rickroll

The something\_in\_the\_way.rar file needs some password to extract the files within, but we do not seem to have that

There is another file named rightplace?.txt that contains:

I dｏｎ't ｔhiｎk tｈⅰs iｓ the ｒｉght plaｃe to be sｅaｒcｈіｎg ｆｏｒ ａｎｙtｈiｎg. Nothing bｕt emptiｎesｓ aｎｄ ⅴoіd. Liｔerally， ａ wastｅ οｆ time

At first look, it looks like some gibberish, but this is a classic case of Homoglyph Steganography.

Using the link: <http://holloway.co.nz/steg/>

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated

This is indeed the password for the .rar file

After extracting, we find multiple copies of a file

One specific text file has the info we need, i.e,

Bomb – copy(69) ,we just have to ctrl F the file for ‘flag’ and voila

VishwaCTF{th1ng$\_a43\_n0t\_wh4t\_th3y\_4lw4y$\_$33m}

A screenshot of a computer

Description automatically generated with medium confidence