**Super SSH**

Can you ssh as ctf-player to titan.picoctf.net at port 49566 to get the flag? You'll also need the password 1db87a14. If asked, accept the fingerprint with yes.

run in the command line

$ ssh -p 49566 ctf-player@titan.picoctf.net

a.k.a ssh -p <port> <username>@<url>

agree (yes) to fingerprint

enter password

**Bookmarklet**

Why search for the flag when I can make a bookmarklet to print it for me?

*Useful resources:*

https://www.freecodecamp.org/news/what-are-bookmarklets/

*Solution:*

Make a new bookmark in a way that allows you to type in the URL

In the space for adding a url, copy and paste the javascript given on the webpage

**Verify**

Had to netcat in for some reason wouldn't work when downloading the files

sha256sum files/\* >> sha.txt

grep to find file that matches checksum (for me this was 2cdcb2de)

decrypt.sh /files/2cdcb2de

produces flag

**Scan surprise**

Netcat in then scan the QR code (I used my phone)

**CanYouSee**

Viewed the metadata of the image

Chucked the things that looked strange into magic on cyberchef

This was the resource in the end

**Endianness**

I think I changed the c code to make it generate the big / little endian representations for me bc I just could not be bothered to convert then by hand

Copy in edited.c

**WebDecode**

The inspect the page (usually control + i)

Then looked for unusual stuff – the notify\_true field in the HTML for the about page section for class=’about’ looks strange.

The I chucked it into magic on cyber tool – turns out to be base 85 (I think)

**Secret of the Polgyglot**

Opened as a pdf that gave me the second half of the page

Looked at metadata that led me to GIMP but I think any image viewer might let this work (it’s just I had GIMP already)

First part through an image viewer (GIMP)

Then just a normal pdf viewer (firefox) for second part

**Binary Search**

Connect with netcat then use a binary search to find the correct number (i.e. guess 500, then half higher or lower)

<https://www.khanacademy.org/computing/computer-science/algorithms/binary-search/a/binary-search>

**format string 0**

Launched the challenge instance and then selected the menu items that had particularly unusual characters in ‘i.e. % something’.

Gr%114d\_Cheese

Cla%sic\_Che%s%steak

**commitment issues**

run $git to make sure that i had git installed

in drop-in

unzip the file using unzip command

$ git init

$ git log

this told me that the user name and email i want to emulate were picoCTF and ops@picoctf.com and gave me the commit number I wnated to revert to

$ git config --global user.email ops@picoctf.com

$ git config --global user.name picoCTF

$ git add .

$ git commit -m "putting the changes in here so that I can revert to a prior one"

$ git revert 42942c9c605b30100f5d859ef6e172027447c0db

$ cat message.txt

**time machine**

in drop in

git init

git log

the flag was then the message that came with the last commit

**Blame game**

unzip challenge.zip

cd drop-in

git init

git log -p -- message.py

This shows all the changes made to the message.py file

looked at the authors who have made the changes -- one of the author names is the flag!

**Collaborative Development**

unzip challenge.zip

cd drop-in

git init

git branch

This tells us that there are 3 branches! Let's change into the three branches and see what they have

git checkout feature/part-1

This gives us the first part of the flag in flag.py

checkout the other two features to form the whole flag :)

**heap 0**

Wrote a really long set of stuff to the heap (option 2) so it overflowed into the secure variables and let me print the flag :)

**heap 1**

the trick here is to look at the win condition (the safe var = pico) and then to write the right length of muck so that it only just overflows into the safe var (picopicopicopicopicopicopicopicopico)

**dont-you-love-banners**

*Have not completed, am struggling here*

*I suspect this will be useful:* [*GTFOBins*](https://gtfobins.github.io/) *but idk if it is*

The password is found by netcatting into the insecure server.

My\_Passw@rd\_@1234

Then answer the questions (DEFCON, John Draper)

Can't seem to find anything with sudo permissions??

<https://vimeo.com/showcase/3416096/video/133002251>

This looks like a promising start – watch it later