**Ez PDF**

***Forensic***

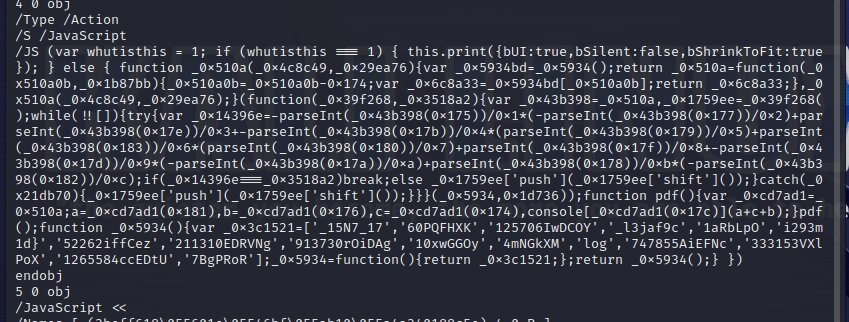
**Challenge:**

I just downloaded this PDF file from a strange site on the internet....

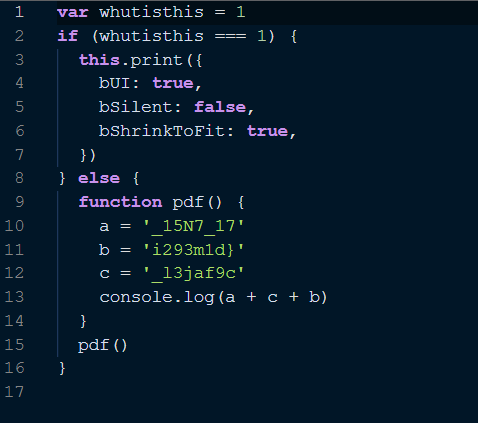
Attached - TCP1P-CTF.pdf

**Approach:**

First basic thing, using strings on the PDF file



We see this javascript code, which on one look looks obfuscated. We use a online JS deobfuscator such as “https://deobfuscate.relative.im/” and get this:



Well, not really difficult now right?

The execution of this code will reveal:

\_15N7\_17\_l3jaf9ci293m1d}

It looks like a small part of the flag, so maybe the flag is broken into pieces? hmm….

Next, we perform exiftool on the PDF file:



The creator got a very unique name, no?

It’s base64 encoded and it decodes to:

“In this question, the flag has been divided into 3 parts. You have found the first part of the flag!! TCP1P{D01n9\_F023n51C5”

which confirms that the text we got earlier, might be a part of the flag, actually, looks more like the last part of the flag because of the curly bracket at the end.

Updated flag:

TCP1P{D01n9\_F023n51C5**???**\_15N7\_17\_l3jaf9ci293m1d}

Now this is where I was stuck for the longest time, no other analysis revealed any part of the flag, and according to the question we had only 1 more missing part. I researched online and got to know we can hide images as well in the PDF, but wasn’t able to find any good tool online, so i wrote a python script :))

pdf\_file = 'TCP1P-CTF.pdf'

pdf\_document = fitz.open(pdf\_file)

for page\_num in range(len(pdf\_document)):

page = pdf\_document.load\_page(page\_num)

xObject = page.get\_images()

for img\_index, img in enumerate(xObject):

xref = img[0]

base\_image = pdf\_document.extract\_image(xref)

image\_data = base\_image["image"]

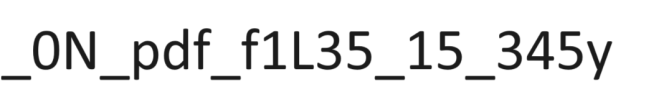
image\_filename = f"image\_{img\_index + 1}.png"

with open(image\_filename, "wb") as image\_file:

image\_file.write(image\_data)

pdf\_document.close()

Well, it finally worked out (after a shit lot of error debugging) and gave us two images, one more than what was actually visible on the file, it gave us this part of the flag:



Hence the final flag:

**Flag: TCP1P{D01n9\_F023n51C5\_0N\_pdf\_f1L35\_15\_345y\_15N7\_17\_l3jaf9ci293m1d}**

Congrats!!

Happy Hacking!