Level09

Two files are present is present in home directory of the `level09` user witch are a binary named `level09` and a `token` file. The `token` file is **world redable**. The **SUID** bit is set on the `level09` binary and owner is user `flag09` on both files.

Tests

- Use the `cat` command on the token file outputs `f4kmm6p|=�p�n��DB�Du{��`
- Execute the `level09` binary outputs `You need to provied only one arg.`
- Executing the `level09` binary with `token` as argument outputs `tpmhr`.

The last test looks like this binary file outputs the string passed as first argument to `stdout` in an altered form. The first letter is **t** the second letter is shifted one letter up from **o** to **p**, the third letter shifter two letters up, and so on...

```
t  o  k  e  n
t  p  m  h  r
|  |  |  |  |
+0 +1 +2 +3 +4
```

The `token` file contents is probably the output of the original that has been passed trough the `level09` binary.

With a simple **python** script, we are able to **reverse this** with a loop that subtracts it's value on each letter, prints the character and increments it's value by one. The resulting string should be the original token.

```python
#!/usr/bin/python
import sys

i = 0

with open('token', 'r') as file:
        for line in file:
                for char in line:
                        if char == '\n':
                                break
                        sys.stdout.write(chr(ord(char) - i))
                        i = i + 1
                sys.stdout.write('\n')
        file.close()
```

The token obtained works to login as user `flag09` and we are able to launch the `getflag` command.

```
level09@SnowCrash:/tmp$ ./rev.py
f3iji1ju5yuevaus41q1afiuq
level09@SnowCrash:/tmp$ su flag09
Password:
Don't forget to launch getflag !
flag09@SnowCrash:~$ getflag
Check flag.Here is your token : s5cAJpM8ev6XHw998pRWG728z
```