PyCON.tw 2013

# About

- a.k.a. xatier
- 平凡無奇的大學生
- 喜好自由軟體和資訊安全技術
- Python 只是輔助 (?)

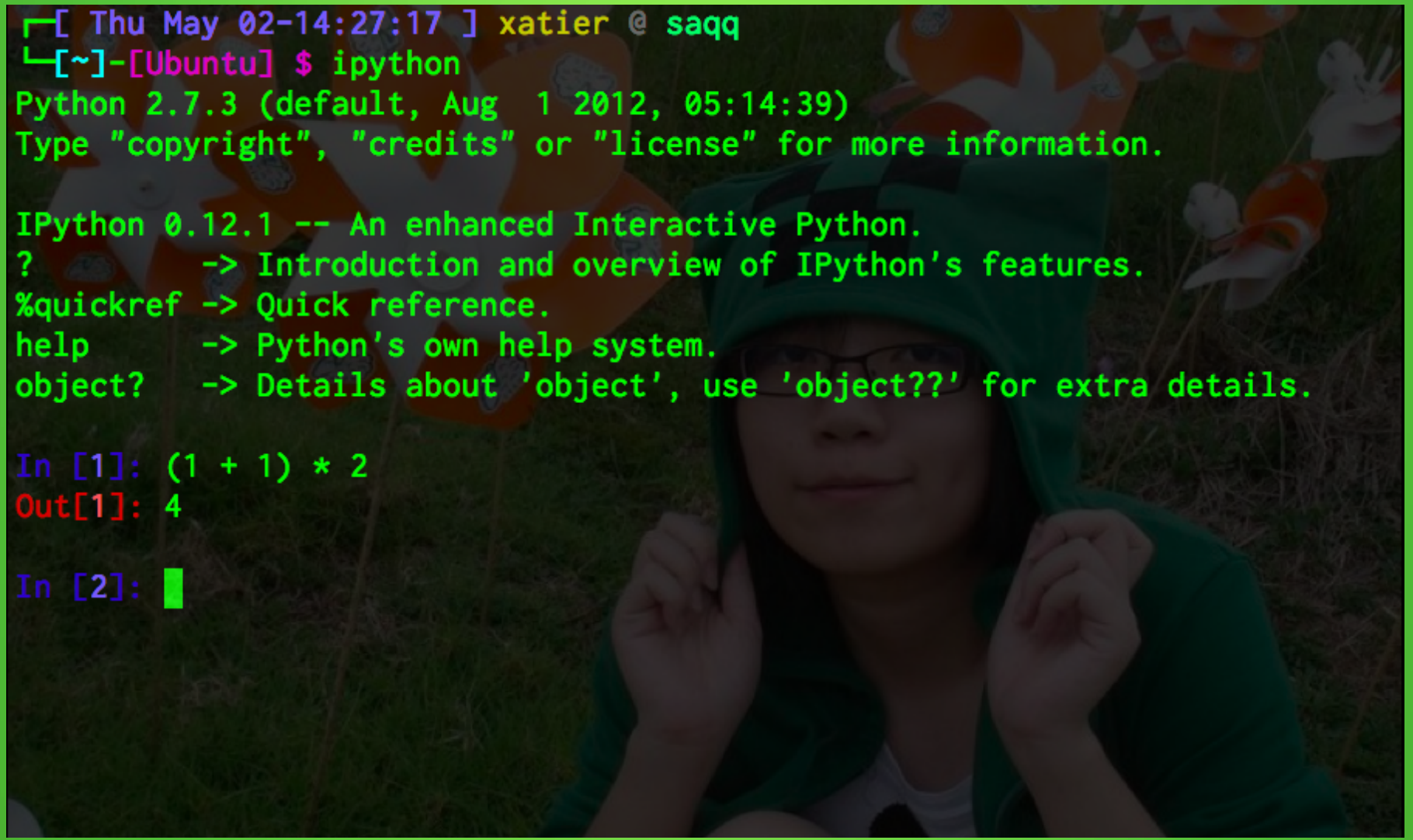
# 工商服務

晚點 BoF 八號場地

強者我學長 Dr. Ken 大大

- 講題『Mining Interest Topics from Plurk by using Python』

# 最常拿 Python 來...


┌─[ Thu May 02-14:27:17 ] xatier @ saqq
└─[~]-[Ubuntu] $ ipython
Python 2.7.3 (default, Aug  1 2012, 05:14:39)
Type "copyright", "credits" or "license" for more information.
IPython 0.12.1 -- An enhanced Interactive Python.
?         -> Introduction and overview of IPython's features.
%quickref -> Quick reference.
help      -> Python's own help system.
object?   -> Details about 'object', use 'object??' for extra details.
In [1]: (1 + 1) * 2
Out[1]: 4
In [2]:

# We Love Python

- Easy to Learn
- Easy to Read
  - Easy to Hack (?)
- Cross platform
- Builtin tools
- Libraries

"This (Programming), of course, is the fundamental hacking skill. If you don't know any computer languages, I recommend starting with Python. It is cleanly designed, well documented, and relatively kind to beginners. Despite being a good first language, it is not just a toy; it is very powerful and flexible and well suited for large projects."

– *How to become a hacker* (ESR)

(compare to C) ..... "With today's machines as powerful as they are, this is usually a bad tradeoff — it's smarter to use a language that uses the machine's time less efficiently, but your time much more efficiently. Thus, Python."

- *How to become a hacker* (ESR)

# 小試身手

decrypt

# decrypt

```
import crypt


crypt.crypt(word, salt) -> string

word will usually be a user's password. salt is a 2-
character string

which will be used to select one of 4096 variations of
DES. The characters

in salt must be either ".", "/", or an alphanumeric
character. Returns

the hashed password as a string, which will be
composed of characters from

the same alphabet as the salt.
```

# decrypt

- Dictionary Attack
- /usr/share/dict/words
- GGvxb.e7Ygnlg

# decrypt

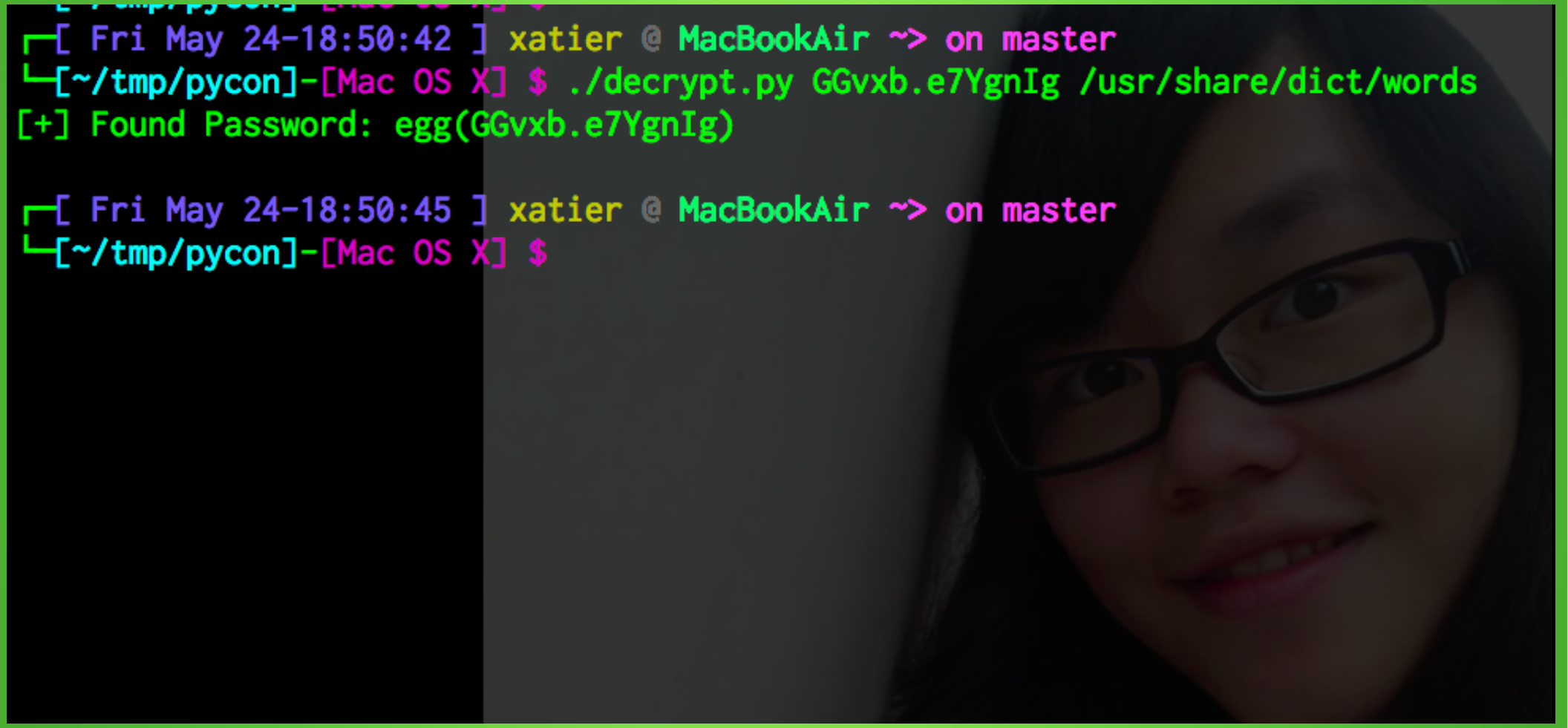
```
import crypt
import sys

def testPass(cryptPass, dic):
    salt = cryptPass[0:2]
    dictFile = open(dic, 'r')

    for word in dictFile.readlines():
        word = word.strip('\n')
        ced = crypt.crypt(word, salt)
        if (ced == cryptPass):
            print "[+] Found Password: " + word + "(" + cryptPass + ")\n"
            return

    print "[-] Password Not Found.\n"
    return
```

# decrypt


[ Fri May 24-18:50:42 ] xatier @ MacBookAir ~> on master
[~/tmp/pycon]-[Mac OS X] $ ./decrypt.py GGvxb.e7YgnIg /usr/share/dict/words
[+] Found Password: egg(GGvxb.e7YgnIg)
[ Fri May 24-18:50:45 ] xatier @ MacBookAir ~> on master
[~/tmp/pycon]-[Mac OS X] $

# Brute force

- http://pvanhoof.be/files/bruteforce.c

- `import itertools`

# Brute force

- http://pvanhoof.be/files/bruteforce.c

- `import itertools`

```
def f(S, l):
    for j in ("".join(i) for i in (itertools.combinations_with_replacement(S, l))):
        print j
```

# APIs

- socket API 跟 C 用起來幾乎一模一樣
- ctypes 標準庫提供 C/dll/so 跨接的橋樑
- 物件、流程控制等可省下更多時間

# Hacking Skype

- main.db
  - 你想要的通通都在這邊 （？
  - 聯絡人、聊天紀錄 ... 等
- Unix like 系統很棒的

# Lots of tools

- http://www.dirk-loss.de/python-tools.htm

scapy
dpkt
Immunity Debugger
IDAPython
Lldb (llvm's debugger)
.....

# python-nmap

- http://xael.org/norman/python/python-nmap/
- Nmap 工具的 Python binding
- 搭配 IPython shell 一同服用
- GPL licensed

# Inspired by

- Nicolle Neulist: Write your own tools with python! Derbycon2012
- Gray Hat Python: Python Programming for Hackers and Reverse Engineers
- Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers

# Thank you