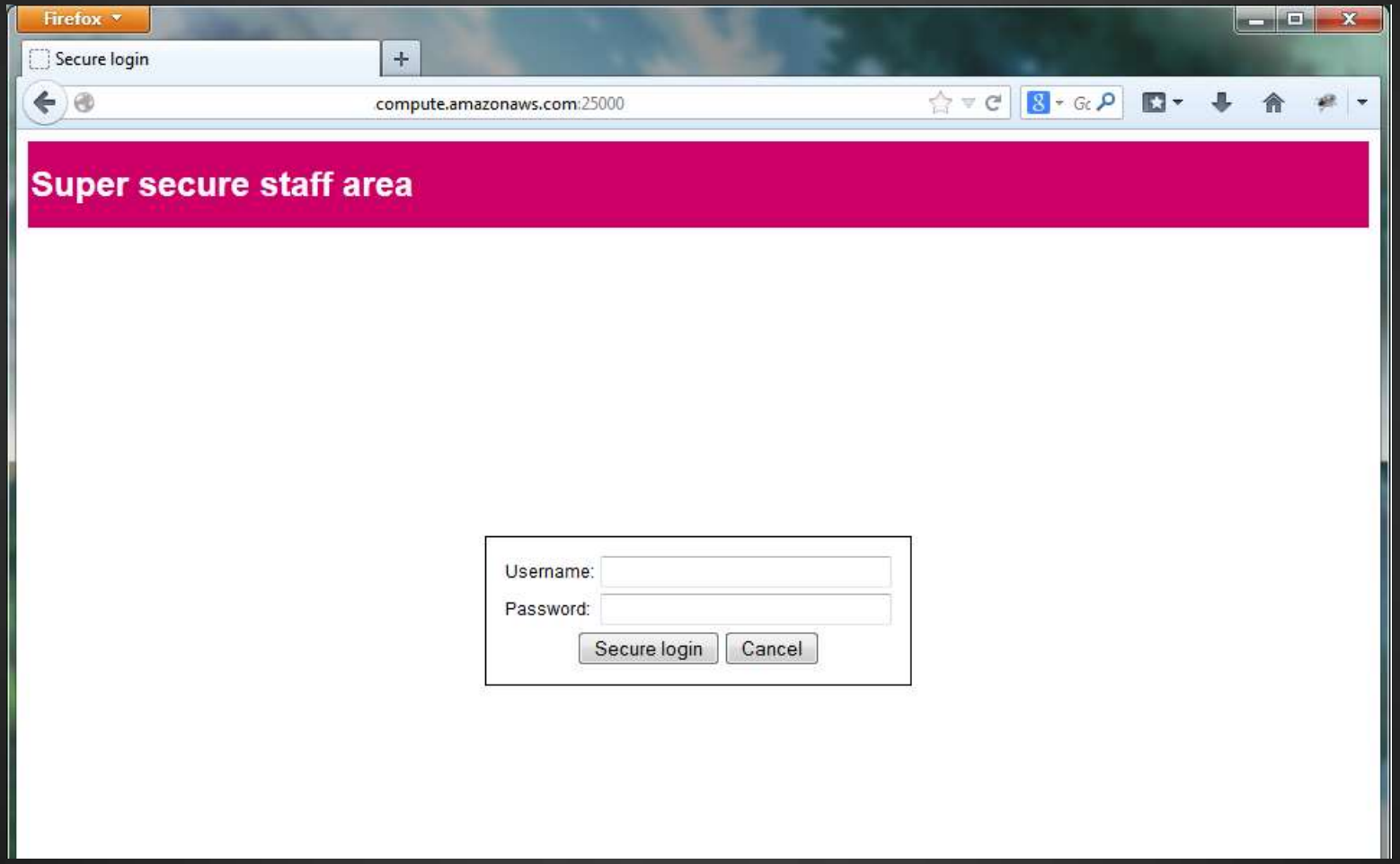
SecTalks CTF Solution 0x00

@nanomebia

Obligatory about me

- One of the four WAHCKon Organisers
  - (date pending: Start of May/end of April 2014)
  - www.wahckon.org.au
- Recently hates multiprocessing and python (you'll see)
- I like cats AND dogs (bring it)

Target: Super secure staff area



Let’s do some initial recon

```
<table border="0" style="border: 1px solid; padding: 10px">
<tr><td>Username:</td><td><input type="text" name="username"
size="30" id="userfield"></td></tr>
<tr><td>Password:</td><td><input type="password" name="password"
size="30" id="passfield"></td></tr> <tr><td colspan="2"
align="center"><input type="button" value="Secure login"
onclick="doLogin()">
<input type="button" value="Cancel"></td></tr> </table>
```

And then: JavaScript

```
// 'Secure' password system modified from
http://www.dynamicdrive.com/dynamicindex9/password.htm
function checkValid(str) {
        …
        <check if inputs are valid>
        …
        }
function doLogin(){
        …
        <do some math magic hash>
        …
        }
```

Let's take a look at doLogin()

(relevant parts only)

```
uniqueId = "d9507edf0b2eb30b1292596e4ec10d7abbf0a959";
var username = userfield.value.toLowerCase();
var password = passfield.value.toLowerCase();
passcode = 1; usercode = 1; usertot = 0; passtot = 0;
for(i = 0; i < password.length; i++) {
passtot += (i*password.charCodeAt(i)*password.charCodeAt(i));
passcode *= password.charCodeAt(i); }
for(x = 0; x < username.length; x++) {
usertot += (x*username.charCodeAt(x));
usercode *= username.charCodeAt(x); }

if(usercode == 1172188274400 && passcode == 1842055687879732800
&& usertot == 1537 && passtot == 393644) {
document.location.href =
"secure.php?tok=" + username + ":" + password + ":" + uniqueId; }
```

That's an interesting URL Forward

```
"secure.php?tok=" + username + ":" + password + ":" + uniqueId;
```

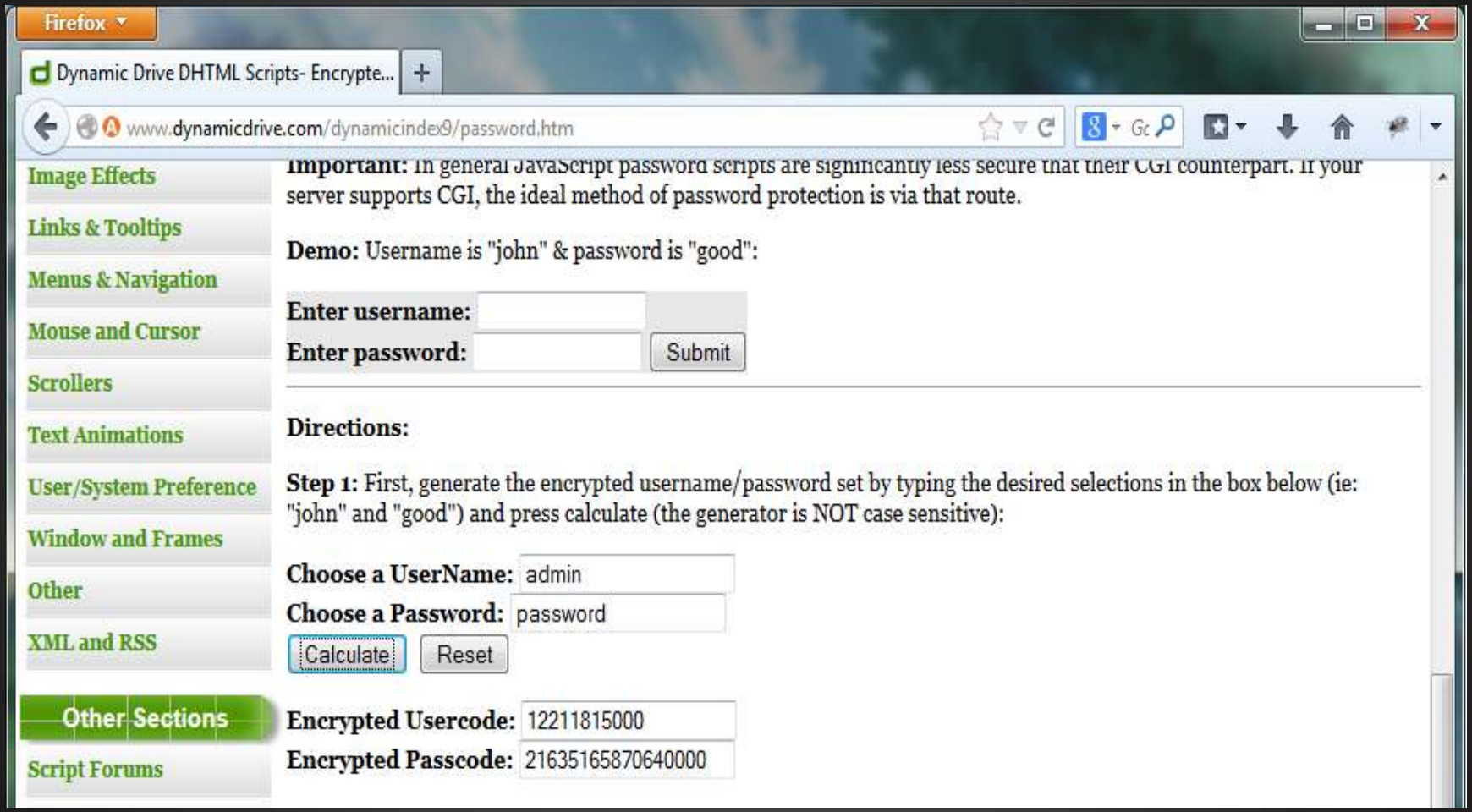
Ends up as something like this:

`http://host.com/secure.php?tok=admin:admin:d9507edf0b2eb30b1292596e4ec10d7abbf0a959`

Which Goes to:

…Damn.

Let’s look at that function again



Hashing

```
for(i = 0; i < password.length; i++)
 {

        passtot += (i*password.charCodeAt(i)*password.charCodeAt(i));
        passcode *= password.charCodeAt(i);
}
for(x = 0; x < username.length; x++)
 {
        usertot += (x*username.charCodeAt(x));
        usercode *= username.charCodeAt(x);
}
```

Let’s develop some code

```
#!/usr/bin/python
#breakdict.py
import sys
brute = open(“all.lst", "r")
words = []
for line in brute:
    words.append(line.strip())
print('\nread in done\n')
z = 0
for z in range(z, len(words)):
    passcode = 1;
    usercode = 1;
    usertot = 0;
    passtot = 0;
    username = words[z]
    password = words[z]
    for i, c in enumerate(password):
        passtot += (i*ord(c)*ord(c));
        passcode *= ord(c);
    for i, c in enumerate(username):
        usertot += (i*ord(c));
        usercode *= ord(c);
    if  usercode == 1172188274400:
        print('\n\nUsername: '+username)
    if usertot == 1537
        print('\n\nUsername: '+username)
    if passcode == 18420556878797328000:
        print('\n\nPassword: '+password)
    if passtot == 393644:
        print('\n\nPassword: '+password)
print('done')
```

And then this happens:

(Output of previous code)

read in done
Username: maggie
Username: Maggie
Username: canela
Username: candid
Username: daybed
Username: decode
Username: defame
Username: homage
Username: inlaid
Username: lexica
Username: locale
Username: manege
Username: sahara
Username: thence
Username: venice
Username: whence
Username: wooded
Username: zenana
Username: Sahara
Username: Venice
Username: abraid
Username: adenia
Username: aerage
Username: arcked
Username: baggie
Username: befame
Username: behale
Username: birded
Username: caribe
Username: cilice
Username: eatage
Username: feriae
Username: girded
Username: golfed
Username: helide
Username: hexade
Username: hooded
Username: jalapa
Username: kalema
Username: kambal
Username: keened
Username: kipage
Username: lemnad
Username: lorcha
Username: macaco
Username: medici
Username: miladi
Username: muscae
Username: panela
Username: peened
Username: pereia
Username: piemag
Username: pipage
Username: reckla
Username: recode
Username: rehale
Username: rifled
Username: salaam
Username: salema
Username: sambal
Username: sipage
Username: sorbed
Username: stalag
Username: tarama
Username: themed
Username: unlaid
Username: uvalha
Username: waggie
Username: weened
Username: wolfed
Username: zincic
Username: Abanic
Username: Aralia
Username: Balaam
Username: Balija
Username: Dipala
Username: Geikia
Username: Medici
Username: Mexica
Username: Padina
Username: Poiana
Username: Salaam
Username: Sambal
Username: Tupaia
Password: Volgograd
Username: Watala
Username: Zambal
Username: Belege
Username: Gerede
Username: Kueche
Username: alinea
Username: archai
Username: bipede
Username: corcha
Username: defila
Username: demoda
Username: e'mise
Username: etoffa[Decode error - output not utf-8]
Username: evidee
Username: felide
Username: focale
Username: foncee
Username: forgea
Username: girafe
Username: glande
Username: gorgea
Username: milice
Username: ratage
Username: silice
Username: trac[Decode error - output not utf-8]
Username: vocale
Username: vocife
Username: amiche
Username: badata
Username: becchi
Username: biscia
Username: blande
Username: gelide
Username: giocai
Username: gridai
Username: lecchi
Username: liscia
Username: pecchi
Username: pedane
Username: pieghe
Username: proced
Username: saldo`
Username: scambi
Username: secchi
Username: solcai
Username: stoffa
Username: vecchi
Username: aerede
Username: anfald
Username: anslaa
Username: arbejd
Username: skoede
Username: abanic
Username: affich
Username: aralia
Username: ardeid
Username: balaam
Username: balija
Username: berede
Username: corbed
Username: curace
Username: dipala
Username: domage
Username: flabra
Username: geikia
Username: kokama
Username: mexica
Username: morcha
Username: onlaid
Username: padina
Username: pareja
Username: pheeal
Username: poiana
Username: ramack
Username: relide
Username: romage
Username: suegee
Username: tupaia
Username: vidame
Username: watala
Username: zambal
Username: Azelea
Username: Bueche
Username: Daggna
Username: Denice
Username: Docena
Username: Jalapa
Username: Janela
Username: Jenice
Username: Josefa
Username: Kerala
Username: Moomba
Username: Muscae
Username: Natala
Username: Oralia
Username: Salema
Username: Sateia
Username: Secchi
Username: Slifka
Username: Sorcha
Username: Szeged
Username: Tudela
Username: Vivica
Username: Zahara
Username: -cidal
Password: wall-girt
Username: afgaan
Username: bladig
Username: bofbal
Username: daggie
Username: elande
Username: gedane
Username: gerede
Username: hofbal
Username: inhaal
Username: josefa
Username: laggie
Username: nadele
Username: nadraf
Username: bijela
Username: cijela
Username: cosica
Username: debele
Username: dijela
Username: dosade
Username: falija
Username: ferala
Username: galija
Username: kradje
Username: ledima
Username: mariama
Username: milana
Username: napadi
Username: navece
Username: posade
Username: slenga
Username: suicka
Username: svidja
Username: tijela
Username: uvidja
Username: vidila
Username: zenice
Username: debata
Username: dedici
Username: denice
Username: dohoda
Username: doklad
Username: fixace
Username: hadaji
Username: hajena
Username: iranec
Username: jerabi
Username: klenbe
Username: laicke
Username: locika
Username: mijela
Username: nabije
Username: najedi
Username: nejake
Username: oceane
Username: padaji
Username: pajdal
Username: pohoda
Username: poklad
Username: pomala
Username: predci
Username: reakci
Username: ridila
Username: sedici
Username: senice
Username: slibna
Username: svatba
Username: svedla
Username: tajena
Username: tocena
Username: tulaka
Username: udajna
Username: uvedla
Username: uzenac
Username: velela
Username: vlhk[Decode error - output not utf-8]
Username: vydana
Username: zabije
Username: zadaji
Username: zadina
Username: zasoba
Username: zatala
Username: zelela
Username: znajic
Username: zridka
Username: zvedla
Username: abctae
Username: bbctae
Username: biachi
Username: deneka
Username: finlad
Username: gaebel
Username: garlad
Username: gretaa
Username: haluaa
Username: herala
Username: hipiae
Username: huikea
Username: ilke[Decode error - output not utf-8]
Username: isomaa
Username: kahila
Username: kaluaa
Username: katala
Username: keriae
Username: kiveae
Username: kotkaa
Username: kujala
Username: kuvaae
Username: ladata
Username: lakkia
Username: laskea
Username: libyaa
Username: liksaa
Username: madina
Username: matala
Username: meriae
Username: muikea
Username: olevaa
Username: otavaa
Username: patala
Username: periae
Username: polkea
Username: potkaa
Username: pyhiae
Username: raesae
Password: rytkoelae
Username: sakkia
Username: skaane
Username: steffe
Username: stefka
Username: takkia
Username: tapana
Username: telmae
Username: tilana
Username: uralia
Username: veriae
Username: vibeke
Username: viej[Decode error - output not utf-8]
Username: votkaa
Username: yskiae
Username: fegoga
Username: qijide
Username: szeged
Username: vitaja
Username: barama
Username: chinfa
Username: decchi
Username: ekimae
Username: fecchi
Username: futaga
Username: hatabi
Username: hiraka
Username: kaechi
Username: kajika
Username: karama
Username: katage
Username: ketaka
Username: kowaga
Username: mahara
Username: majika
Username: manmae
Username: matage
Username: midara
Username: mikoda
Username: mitida
Username: mypace
Username: nabera
Username: nachan
Username: nafuda
Username: oibane
Username: okkana
Username: ookama
Username: puraha
Username: sabaki
Username: seriae
Username: setaka
Username: sitida
Username: suhama
Username: syagai
Username: tabaki
Username: tahara
Username: tanebi
Username: tatage
Username: tatiae
Username: tebata
Username: tinama
Username: tiraka
Username: watage
Username: yahara
Username: yasoba
Username: accidi
Username: adibam
Username: aeriae
Username: caesae
Username: clarae
Username: decabo
Username: istaec
Username: itabam
Username: minaci
Username: nitida
Username: niveae
Username: occidi
Username: perage
Username: redeam
Username: sedeam
Username: stabam
Username: bidige
Password: femtiende
Username: flenga
Username: gjelde
Username: kerala
Username: kjelde
Username: snodde
Username: stanga
Username: tjelde
Username: asceci
Username: aukcja
Username: bocika
Username: buicka
Username: chadek
Username: debina
Username: diabel
Username: emocja
Username: hulaka
Username: karcic
Username: kaucja
Username: klania
Username: kopcia
Username: lezace
Username: peciak
Username: powaga
Username: sadata
Username: sekcie
Username: trefic
Username: ulegaj
Username: witaja
Username: wyciag
Username: wydana
Username: znecal
Username: abasi`
Username: adarce
Username: ama\ar
Username: atenea
Username: babera
Username: badina
Username: cabera
Username: carama
Username: catifa
Username: celaje
Username: chifla
Username: chirca
Username: docena
Username: elemi`
Username: exarca
Username: fenice
Username: fogaje
Username: garama
Username: gehena
Username: glabra
Username: guasca
Username: huasca
Username: jabera
Username: ladina
Username: llande
Username: monfi`
Username: muare`
Username: pelaje
Username: queche
Username: rabera
Username: rebina
Username: renana
Username: ro`sea
Username: sarama
Username: tacaco
Username: tanela
Username: valija
Username: velaje
Username: zalema
Username: asiibe
Username: furaha
Username: hapana
Username: kiraka
Username: mabaki
Username: mahame
Username: mapana
Username: orodha
Username: usiibe
Username: wabaki
Username: walafi
Username: aatala
Username: aeckla
Username: befara
Username: faebod
Username: haedan
Username: maekla
Username: nydana
Username: vaebel
Username: veckla
Username: birkac
Username: burgac
Username: dalgic
Username: delege
Username: garibe
Username: icecek
Username: iskala
Username: kaleci
Username: karaci
Username: kinama
Username: nerede
Username: perdah
Username: sancak
Username: sinama
Username: slavca
Username: yenice
Username: Furaha
Username: Hapana
Username: Usiibe
Username: ki-ton
Username: ku-pon
Username: askede
Username: elskab
Username: fjelde
Username: hujede
Username: iskage
Username: latifa
Username: lerede
[Decode error - output not utf-8]
r
Username: renhed
[Decode error - output not utf-8]
Username: sebina
Username: spejde
Username: tebina
Username: thanja
Username: tjalfe
Username: tvebak
Username: udkald
Username: ulande
Username: vivica
Username: wibeke
Username: ydende
Username: zebina
[Decode error - output not utf-8]
[Decode error - output not utf-8]
[Decode error - output not utf-8]
Username: afreed
Username: bedane
Username: bralde
Username: plande
Username: toepad
Username: zomede
Username: a"chze
Username: fernab
Username: weitab
Username: amjadi
Username: asiaci
Username: bipala
Username: calija
Username: camack
Username: catala
Username: chavda
Username: civaia
Username: civica
Username: dianah
Username: eccidi
Username: faraci
Username: focena
Username: gaggie
Username: gariga
Username: giachi
Username: hadidi
Username: haebel
Username: imbuca
Username: inedie
Username: isoida
Username: jahara
Username: libici
Username: lupaia
Username: madidi
Username: menadi
Username: moiana
Username: otarda
Username: papaie
Username: penice
Username: piscia
Username: redima
Username: refila
Username: riduca
Username: rosica
Username: saighe
Username: sariga
Username: silana
Username: somala
Username: sterba
Username: suleha
Username: tadina
Username: taighe
Username: toboga
Username: uebele
Username: umiche
Username: vedici
Username: zahara
Username: Saebel
Username: afalla
Username: ahmmad
Username: akkana
Username: alxfac
Username: aridai
Username: baaang
Username: baasha
Username: banaei
Username: banela
Username: beardd
Username: binnbb
Username: biomac
Username: bmckee
Username: braaan
Username: bueche
Username: bwfaak
Username: cahady
Username: cecchi
Username: cenice
Username: channa
Username: cheich
Username: chemed
Username: chinae
Username: cimehc
Username: cinnbb
Username: ckclah
Username: cliffe
Username: colmac
Username: datage
Username: degrad
Username: detafe
Username: dsachg
Username: echobe
Username: ecuded
Username: edibam
Username: eegrad
Username: elbboc
Username: elteeb
Username: eteffe
Username: gesicc
Username: getbdf
Username: gislab
Username: gitega
Username: gmckee
Username: gnbich
Username: goiana
Username: greeff
Username: gueche
Username: hcoice
Username: hibeam
Username: hoplab
Username: hscpad
Username: hufana
Username: idload
Username: iecode
Username: inband
Username: infodb
Username: innnba
Username: jalema
Username: janela
Username: japana
Username: jenice
Username: jhugdb
Username: jmckee
Username: juleha
Username: kaared
Username: kadhal
Username: kerage
Username: leekfe
Username: lineee
Username: lobmag
Username: loomba
Username: lupica
Username: mahlah
Username: majuba
Username: matchc
Username: matnab
Username: mbanic
Username: mbfeld
Username: memabk
Username: merdah
Username: michlb
Username: misbah
Username: mlabme
Username: mpomba
Username: motecc
Username: mwgkcc
Username: nadina
Username: nafasa
Username: naifeh
Username: natala
Username: necchi
Username: nekoea
Username: nenana
Username: nghlgb
Username: ngineb
Username: oralia
Username: palapa
Username: pathcd
Username: pfiidf
Username: pinnbb
Username: purace
Username: pushab
Username: radata
Username: raybed
Username: rchaoc
Username: rebraf
Username: recchi
Username: renice
Username: rokama
Username: sadhal
Username: saedan
Username: sahibi
Username: saxida
Username: sebata
Username: sebele
Username: sedasa
Username: sedima
Username: semalc
Username: serifa
Username: setcbg
Username: sfreed
Username: smadej
Username: sorcha
Username: stavaa
Username: subpad
Username: sufice
Username: tabera
Username: tcuded
Username: teckla
Username: tegdif
Username: tescee
Username: thebie
Username: tmalib
Username: tmscce
Username: tomala
Username: tragid
Username: tralia
Username: tudela
Username: usasac
Username: vadeqa
Username: verbef
Username: vilana
Username: vislab
Password: volgograd
Password: volgograd
Username: wehsac
Username: wesfdd
Username: wobcke
Username: xalapa
Username: xhence
Username: xlbiff
Username: yachad
Username: yelrab
Username: ytlaef
Username: zecchi
Username: zilaie
Username: zmsagc
Username: AmiNet
Username: CHtsHx
Username: CHttKu
Username: CJzBrq
Username: DDiehl
Username: DeCaro
Username: DeJong
Username: DeMark
Username: DeVita
Username: KORies
Username: LeGore
Username: Nibiki
Username: NSFnet
Username: NexTel
Username: ST-low
Username: XStack
Username: aaWhen
Username: dpa/AFP
Username: e'libs
Username: fladdr
Username: flceil
Username: flexec
Username: flfeof
Username: flmodf
Username: flrcmd
Username: g'luck
Username: h/ware
Username: hEhuee
Username: ha-way
Username: hcEdit
Username: n'save
Username: no-tax
Username: noFunc
Username: so-hot
Username: su-xin
Username: to-any
Username: tv-set
Username: x'none
Username: AGU-NET
Username: AIT-NET
Username: AMR-NET
Username: API/SPI
Username: BIT-NET
Username: CICS/OS
Username: CIT-NET
Username: DEV-NET
Username: DIT-NET
Username: DJN-NET
Username: ESO-NET
Username: EU-CNET
Username: EUNET-X
Username: FR-FMSH
Username: HKS-NET
Username: IIT-NET
Username: IWM-NET
Username: KIT-NET
Username: LIN-TER
Username: LKS-NET
Username: MC/AMEX
Username: MCW-NET
Username: MGU-NET
Username: MIT-NET
Username: MKS-NET
Username: NFS/UDP
Username: OIT-NET
Username: OSO-NET
Username: PAK-ZIM
Username: PROTO-T
Username: SMR-NET
Username: SUN-NET
Username: TGU-NET
Username: TRAV-OR
Username: TST-RGN
Username: UNIV-UK
Username: USF-MSL
Username: VUN-NET
Username: WRAP-UP
Username: YIT-NET
Username: ZIT-NET
done
[Finished in 50.4s]

So, Now what?

```
#!/usr/bin/python
#break6nodict.py
import sys
import itertools
from string import ascii_lowercase
chars = ascii_lowercase
for i in itertools.product(chars,repeat=6):
    usercode = 1
    usertot = 0
    username = ''.join(i)
    for i, c in enumerate(username):
        usertot += (i*ord(c))
        usercode *= ord(c)
    if  ((usercode == 11721882744400) and (usertot == 1537)):
        f=open("c:\Users\Andrew\Desktop\user6test2.txt", "a")
        f.write(username+'\n')
        f.close()
        print('\n\nUsername: '+username)
print('done')
```

And of course…

```
#!/usr/bin/python
#break9nodict.py
import sys
import itertools
from string import ascii_lowercase
chars = ascii_lowercase
for i in itertools.product(chars,repeat=9):
    passcode = 1
    passtot = 0
    password = ''.join(i)
    for i, c in enumerate(password):
        passtot += (i*ord(c)*ord(c))
        passcode *= ord(c)
    if  ((passcode == 18420556878797328000) and (passtot == 393644)):
        f=open("c:\Users\Andrew\Desktop\pass9test2.txt", "a")
        f.write(password+'\n')
        f.close()
        print('\n\nPassword: '+password)
print('done')
```

Break6.py + breakdict.py

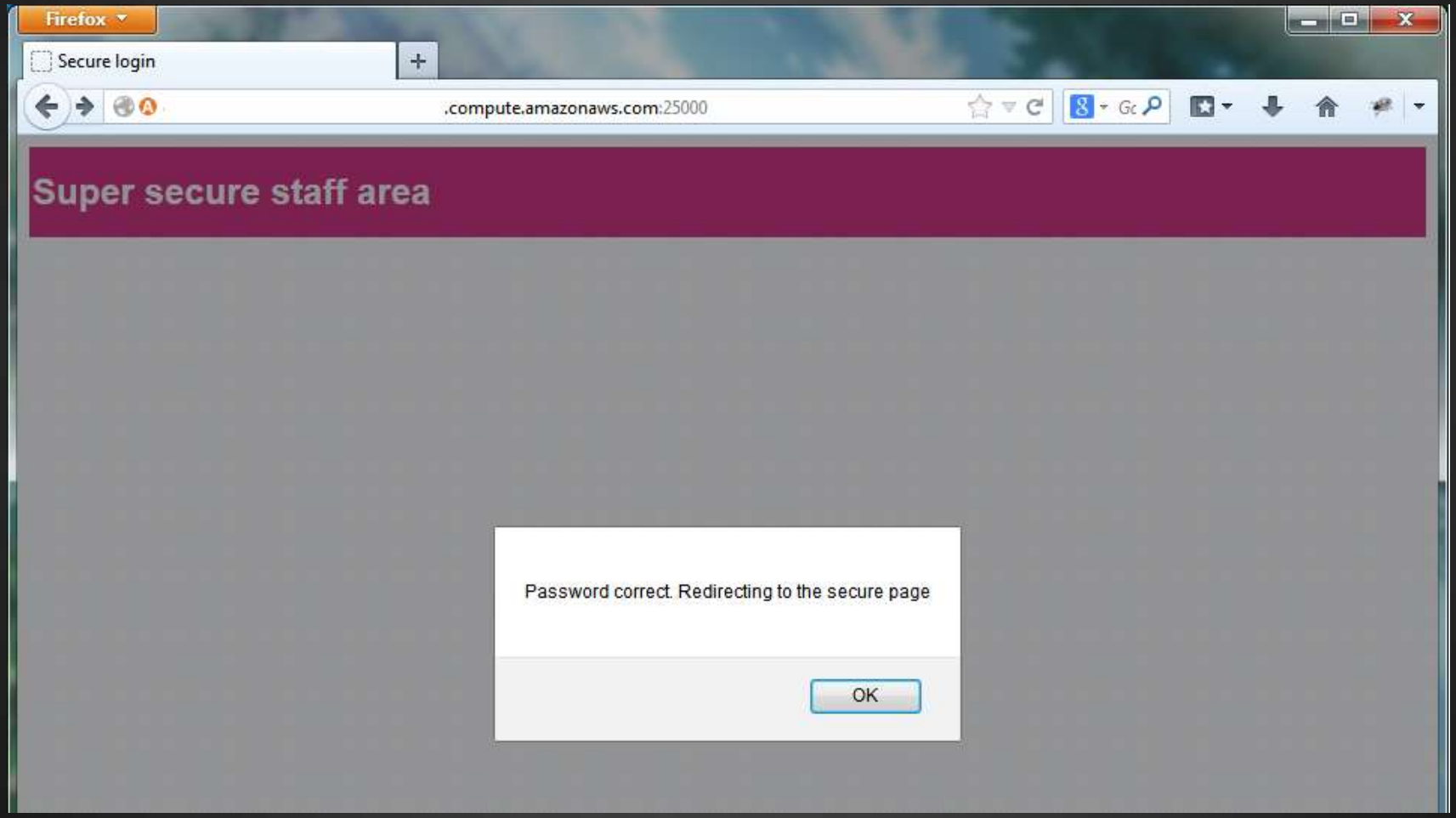
Usernames:

1. adyhac
2. ahnnac
3. annach
4. daycha
5. hncaan
6. naanch

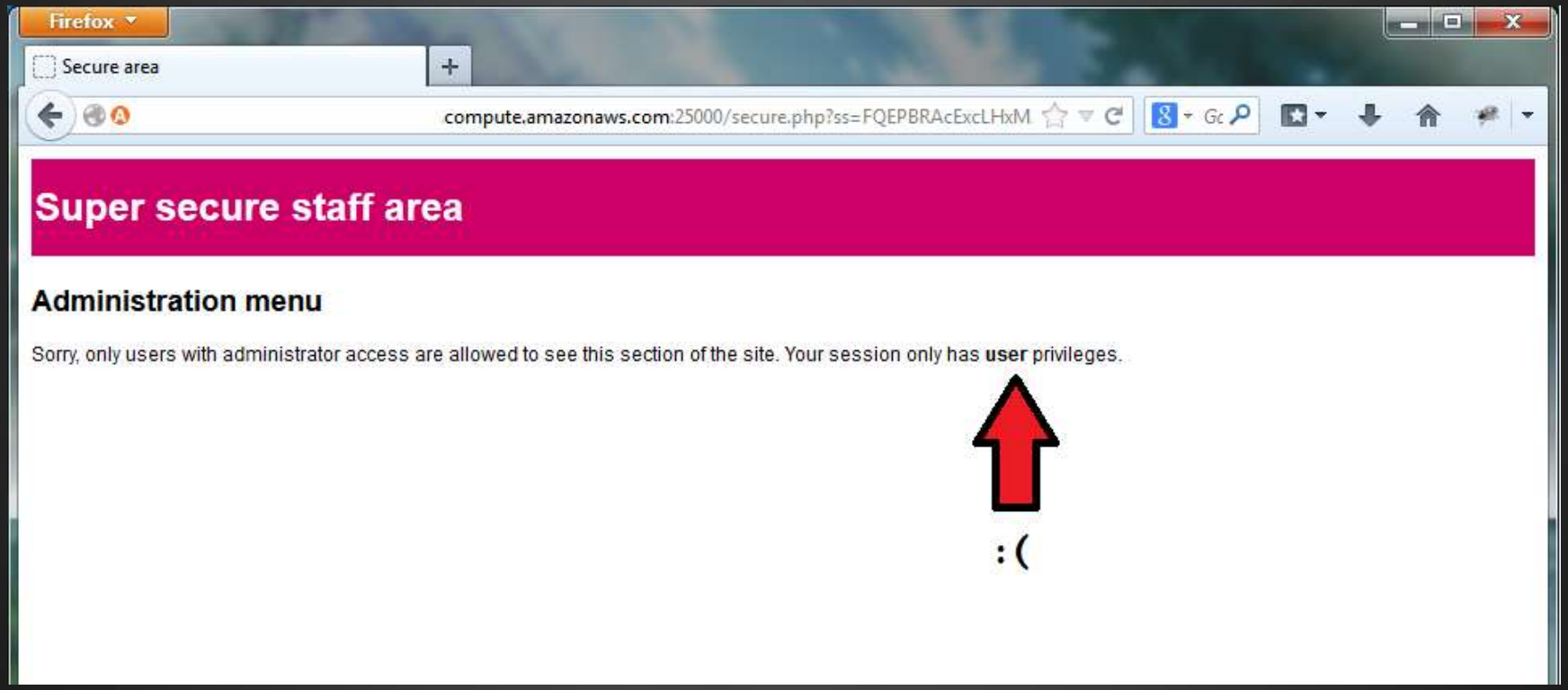
Passwords:

1. volgograd
2. volgograd
3. Volgograd
4. wall-girt
5. rytkoelae
6. femtiende

The winning combination: annach/volgograd



The coveted prize



Regroup:

- Sadly, Source code is boring (Everything being done Server Side)
- That URL looks interesting:

```
secure.php?ss=FQEPBRAcExcLHxMABhYSEB
MFXUZEWAQAFUQNUwERR18DVUFNXVRdRRFbBA
dCRAtWBREWCVEFSkFWHREAER0=
```

- Lets Play with it.

Changing the ss token

FQEPBRAcExcLHxMABhYSEBMFXUZEWAQAFUQNUwERR18DVUFNXVRdRRFbBAdCRAtWBREWCVEFSkFWHREAER0

- = “user”

FQEPBRAcExcLHxMABhYSEBMFXUZEWAQAFUQNUwERR18DVUFNXVRdRRFbBAdCRAtWBREWCVEFSkFWHQA

- = “d”

FQEPBRAcExcLHxMABhYSEBMFXUZEWAQAFUQNUwERR18DVUFNXVRdRRFbBAdCRAtWBREWCVEFSkFWHQb

- = “b”

FQEPBRAcExcLHxMABhYSEBMFXUZEWAQAFUQNUwERR18DVUFNXVRdRRFbBAdCRAtWBREWCVEFSkFWHQ1

- = “i”

FQEPBRAcExcLHxMABhYSEBMFXUZEWAQAFUQNUwERR18DVUFNXVRdRRFbBAdCRAtWBREWCVEFSkFWHT1

- = “Y ”

FQEPBRAcExcLHxMABhYSEBMFXUZEWAQAFUQNUwERR18DVUFNXVRdRRFbBAdCRAtWBREWCVEFSkFWHT'1

- = “Y”

One or two character codes after WH

- Only a few valid “Leading” Characters (Q, T, etc.)
- Combination will change what value is in the “permissions” area
- Trying to find “admin”

Head Banging

- Realised I was essentially brute forcing it manually
- Decided this was pretty silly
- So…

…More python

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
#breakurl.py
import urllib
from bs4 import BeautifulSoup
from string import digits, ascii_uppercase, ascii_lowercase
import itertools
chars = digits + ascii_uppercase + ascii_lowercase
base = "http://ec2-54-252-220-234.ap-southeast-2.compute.amazonaws.com:25000/secure.php?"
base = base+"ss=FQEPBRAcExcLHxMABhYSEBMFXUZEWAQAFUQNUwERR18DVUFNXVRdRRFbBAdCRAtWBREWCVEFSkFWH"
print base
def brute(c1):
        url = base+c1+c2
        txt = urllib.urlopen(url).read()
        soup = BeautifulSoup(txt)
        try:
                res = soup.b.string.encode('utf-8', 'replace')
        except AttributeError:
                res = "null"
        if (res == "a"):
                print ('\n\nchar: '+res+'\n\nurl :'+url+'\n\n')
                f=open("c:\Users\Andrew\Desktop\urlbreak.txt", "a")
                f.write(res+'\n')
                f.write('\nurl: '+url)
                f.close()
for i in itertools.product(chars):
        brute(str(i[0]))
```

Prize!

http://ec2-54-252-220-234.ap-southeast-2.compute.amazonaws.com:25000/secure.php?ss=FQEPBRAcExcLHxMABhYSEBMFXUZEWAQAFUQNUwERR18DVUFNXVRdRRFbBAdCRAtWBREWCVEFSkFWHQUXGQYP

BUT WAIT

Did you think it was over? You are sorely mistaken

Can we do this faster?

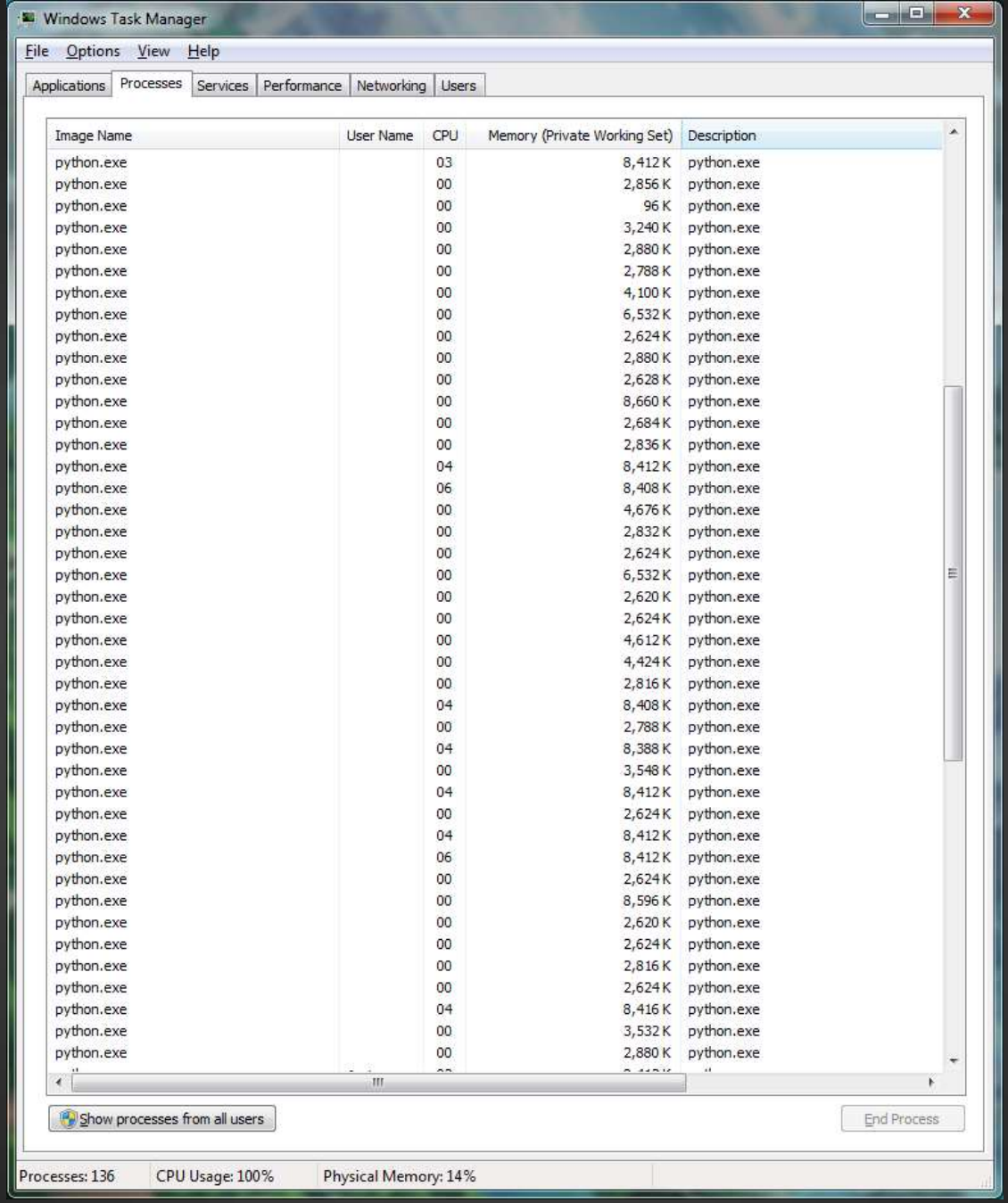
- break6.py is pretty slow (3h)
- break9.py didn’t even finish!
- Can we fix this?

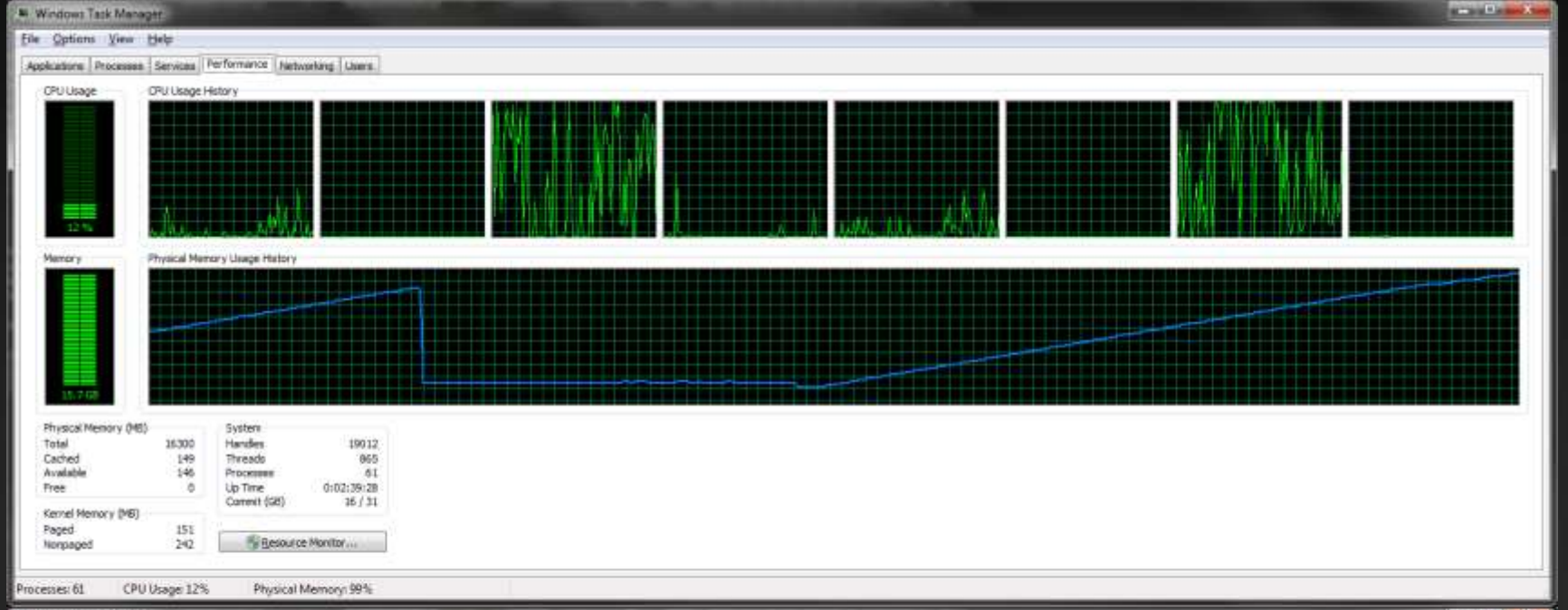
Enter: Multiprocessing

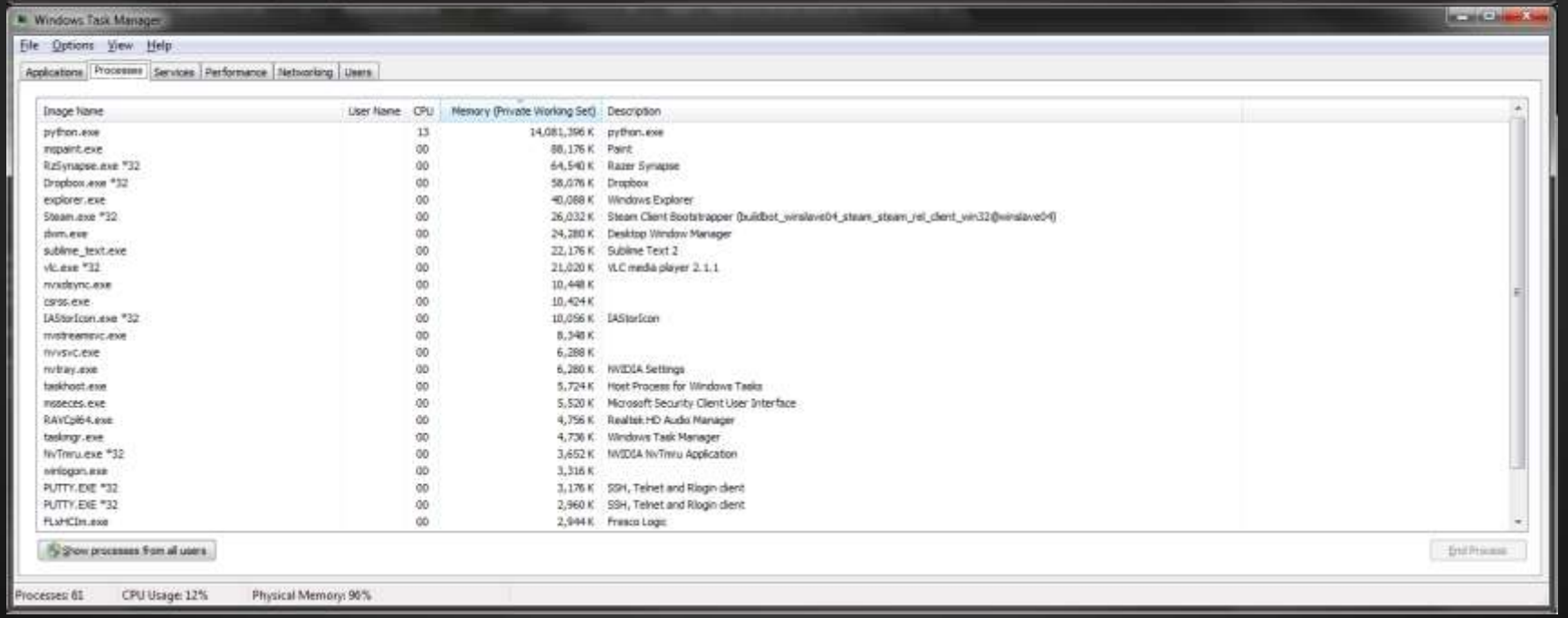
If you thought that bullshit was a nightmare, just you wait.

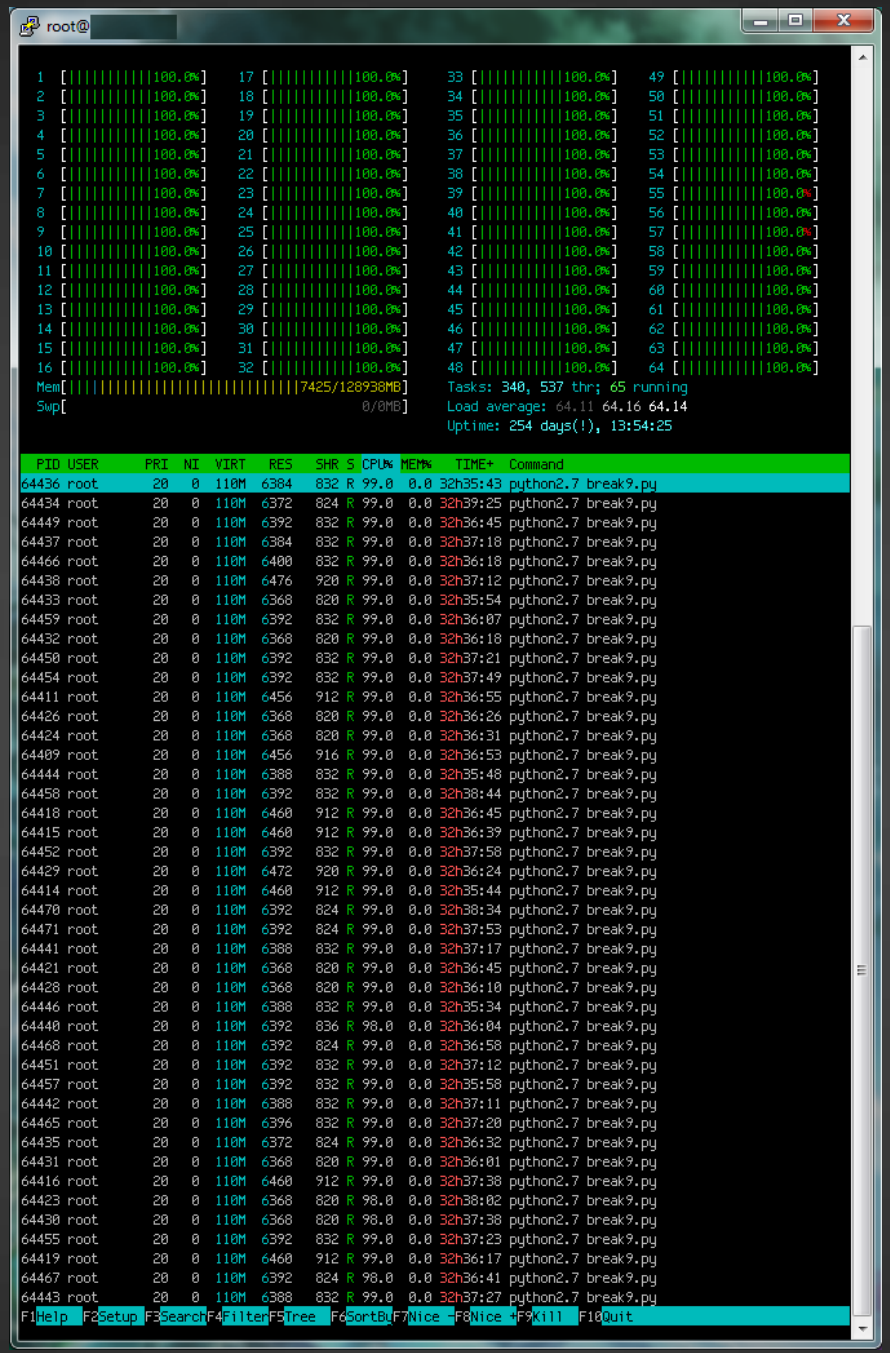
Idea: distribute that load

- Multi core CPU's
- Lets use them
- It can't be that hard right?


Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
Image Name User Name CPU Memory (Private Working Set) Description
python.exe 03 8,412 K python.exe
python.exe 00 2,856 K python.exe
python.exe 00 96 K python.exe
python.exe 00 3,240 K python.exe
python.exe 00 2,880 K python.exe
python.exe 00 2,788 K python.exe
python.exe 00 4,100 K python.exe
python.exe 00 6,532 K python.exe
python.exe 00 2,624 K python.exe
python.exe 00 2,880 K python.exe
python.exe 00 2,628 K python.exe
python.exe 00 8,660 K python.exe
python.exe 00 2,684 K python.exe
python.exe 00 2,836 K python.exe
python.exe 04 8,412 K python.exe
python.exe 06 8,408 K python.exe
python.exe 00 4,676 K python.exe
python.exe 00 2,832 K python.exe
python.exe 00 2,624 K python.exe
python.exe 00 6,532 K python.exe
python.exe 00 2,620 K python.exe
python.exe 00 2,624 K python.exe
python.exe 00 4,612 K python.exe
python.exe 00 4,424 K python.exe
python.exe 00 2,816 K python.exe
python.exe 04 8,408 K python.exe
python.exe 00 2,788 K python.exe
python.exe 04 8,388 K python.exe
python.exe 00 3,548 K python.exe
python.exe 04 8,412 K python.exe
python.exe 00 2,624 K python.exe
python.exe 04 8,412 K python.exe
python.exe 06 8,412 K python.exe
python.exe 00 2,624 K python.exe
python.exe 00 8,596 K python.exe
python.exe 00 2,620 K python.exe
python.exe 00 2,624 K python.exe
python.exe 00 2,816 K python.exe
python.exe 00 2,624 K python.exe
python.exe 04 8,416 K python.exe
python.exe 00 3,532 K python.exe
python.exe 00 2,880 K python.exe
Show processes from all users
End Process
Processes: 136 CPU Usage: 100% Physical Memory: 14%


Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
CPU Usage
CPU Usage History
12 %
Memory
Physical Memory Usage History
15.7 GB
Physical Memory (MB)
Total 16300
Cached 149
Available 146
Free 0
Kernel Memory (MB)
Paged 151
Nonpaged 242
System
Handles 19012
Threads 865
Processes 61
Up Time 0:02:39:28
Commit (GB) 16 / 31
Resource Monitor...
Processes: 61 CPU Usage: 12% Physical Memory: 99%


Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
Image Name User Name CPU Memory (Private Working Set) Description
python.exe 13 14,081,396 K python.exe
mspaint.exe 00 88,176 K Paint
RzSynapse.exe *32 00 64,540 K Razer Synapse
Dropbox.exe *32 00 58,076 K Dropbox
explorer.exe 00 40,088 K Windows Explorer
Steam.exe *32 00 26,032 K Steam Client Bootstrapper (buildbot_winslave04_steam_steam_rel_client_win32@winslave04)
dwm.exe 00 24,280 K Desktop Window Manager
sublime_text.exe 00 22,176 K Sublime Text 2
vlc.exe *32 00 21,020 K VLC media player 2.1.1
nvxdsync.exe 00 10,448 K
csrss.exe 00 10,424 K
IAStorIcon.exe *32 00 10,096 K IAStorIcon
nvstreamsvc.exe 00 8,348 K
nvvsvc.exe 00 6,288 K
nvtray.exe 00 6,280 K NVIDIA Settings
taskhost.exe 00 5,724 K Host Process for Windows Tasks
msseces.exe 00 5,520 K Microsoft Security Client User Interface
RAVCpl64.exe 00 4,756 K Realtek HD Audio Manager
taskmgr.exe 00 4,736 K Windows Task Manager
NvTmru.exe *32 00 3,652 K NVIDIA NvTmru Application
winlogon.exe 00 3,316 K
PUTTY.EXE *32 00 3,176 K SSH, Telnet and Rlogin client
PUTTY.EXE *32 00 2,960 K SSH, Telnet and Rlogin client
FLxHCIm.exe 00 2,944 K Fresco Logic
Show processes from all users
End Process
Processes: 61 CPU Usage: 12% Physical Memory: 99%


root@
1 [||||||||||100.0%] 17 [||||||||||100.0%] 33 [||||||||||100.0%] 49 [||||||||||100.0%]
2 [||||||||||100.0%] 18 [||||||||||100.0%] 34 [||||||||||100.0%] 50 [||||||||||100.0%]
3 [||||||||||100.0%] 19 [||||||||||100.0%] 35 [||||||||||100.0%] 51 [||||||||||100.0%]
4 [||||||||||100.0%] 20 [||||||||||100.0%] 36 [||||||||||100.0%] 52 [||||||||||100.0%]
5 [||||||||||100.0%] 21 [||||||||||100.0%] 37 [||||||||||100.0%] 53 [||||||||||100.0%]
6 [||||||||||100.0%] 22 [||||||||||100.0%] 38 [||||||||||100.0%] 54 [||||||||||100.0%]
7 [||||||||||100.0%] 23 [||||||||||100.0%] 39 [||||||||||100.0%] 55 [||||||||||100.0%]
8 [||||||||||100.0%] 24 [||||||||||100.0%] 40 [||||||||||100.0%] 56 [||||||||||100.0%]
9 [||||||||||100.0%] 25 [||||||||||100.0%] 41 [||||||||||100.0%] 57 [||||||||||100.0%]
10 [||||||||||100.0%] 26 [||||||||||100.0%] 42 [||||||||||100.0%] 58 [||||||||||100.0%]
11 [||||||||||100.0%] 27 [||||||||||100.0%] 43 [||||||||||100.0%] 59 [||||||||||100.0%]
12 [||||||||||100.0%] 28 [||||||||||100.0%] 44 [||||||||||100.0%] 60 [||||||||||100.0%]
13 [||||||||||100.0%] 29 [||||||||||100.0%] 45 [||||||||||100.0%] 61 [||||||||||100.0%]
14 [||||||||||100.0%] 30 [||||||||||100.0%] 46 [||||||||||100.0%] 62 [||||||||||100.0%]
15 [||||||||||100.0%] 31 [||||||||||100.0%] 47 [||||||||||100.0%] 63 [||||||||||100.0%]
16 [||||||||||100.0%] 32 [||||||||||100.0%] 48 [||||||||||100.0%] 64 [||||||||||100.0%]
Mem[||||||||||||||||||||||||||7425/128938MB]
Swp[0/0MB]
Tasks: 340, 537 thr; 65 running
Load average: 64.11 64.16 64.14
Uptime: 254 days(!), 13:54:25
PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command
64436 root 20 0 110M 6384 832 R 99.0 0.0 32h35:43 python2.7 break9.py
64434 root 20 0 110M 6372 824 R 99.0 0.0 32h39:25 python2.7 break9.py
64449 root 20 0 110M 6392 832 R 99.0 0.0 32h36:45 python2.7 break9.py
64437 root 20 0 110M 6384 832 R 99.0 0.0 32h37:18 python2.7 break9.py
64466 root 20 0 110M 6400 832 R 99.0 0.0 32h36:18 python2.7 break9.py
64438 root 20 0 110M 6476 920 R 99.0 0.0 32h37:12 python2.7 break9.py
64433 root 20 0 110M 6368 820 R 99.0 0.0 32h35:54 python2.7 break9.py
64459 root 20 0 110M 6392 832 R 99.0 0.0 32h36:07 python2.7 break9.py
64432 root 20 0 110M 6368 820 R 99.0 0.0 32h36:18 python2.7 break9.py
64450 root 20 0 110M 6392 832 R 99.0 0.0 32h37:21 python2.7 break9.py
64454 root 20 0 110M 6392 832 R 99.0 0.0 32h37:49 python2.7 break9.py
64411 root 20 0 110M 6456 912 R 99.0 0.0 32h36:55 python2.7 break9.py
64426 root 20 0 110M 6368 820 R 99.0 0.0 32h36:26 python2.7 break9.py
64424 root 20 0 110M 6368 820 R 99.0 0.0 32h36:31 python2.7 break9.py
64409 root 20 0 110M 6456 916 R 99.0 0.0 32h36:53 python2.7 break9.py
64444 root 20 0 110M 6388 832 R 99.0 0.0 32h35:48 python2.7 break9.py
64458 root 20 0 110M 6392 832 R 99.0 0.0 32h38:44 python2.7 break9.py
64418 root 20 0 110M 6460 912 R 99.0 0.0 32h36:45 python2.7 break9.py
64415 root 20 0 110M 6460 912 R 99.0 0.0 32h36:39 python2.7 break9.py
64452 root 20 0 110M 6392 832 R 99.0 0.0 32h37:58 python2.7 break9.py
64429 root 20 0 110M 6472 920 R 99.0 0.0 32h36:24 python2.7 break9.py
64414 root 20 0 110M 6460 912 R 99.0 0.0 32h35:44 python2.7 break9.py
64470 root 20 0 110M 6392 824 R 99.0 0.0 32h38:34 python2.7 break9.py
64471 root 20 0 110M 6392 824 R 99.0 0.0 32h37:53 python2.7 break9.py
64441 root 20 0 110M 6388 832 R 99.0 0.0 32h37:17 python2.7 break9.py
64421 root 20 0 110M 6368 820 R 99.0 0.0 32h36:45 python2.7 break9.py
64428 root 20 0 110M 6368 820 R 99.0 0.0 32h36:10 python2.7 break9.py
64446 root 20 0 110M 6388 832 R 99.0 0.0 32h35:34 python2.7 break9.py
64440 root 20 0 110M 6392 836 R 98.0 0.0 32h36:04 python2.7 break9.py
64468 root 20 0 110M 6392 824 R 99.0 0.0 32h36:58 python2.7 break9.py
64451 root 20 0 110M 6392 832 R 99.0 0.0 32h37:12 python2.7 break9.py
64457 root 20 0 110M 6392 832 R 99.0 0.0 32h35:58 python2.7 break9.py
64442 root 20 0 110M 6388 832 R 99.0 0.0 32h37:11 python2.7 break9.py
64465 root 20 0 110M 6396 832 R 99.0 0.0 32h37:20 python2.7 break9.py
64435 root 20 0 110M 6372 824 R 99.0 0.0 32h36:32 python2.7 break9.py
64431 root 20 0 110M 6368 820 R 99.0 0.0 32h36:01 python2.7 break9.py
64416 root 20 0 110M 6460 912 R 99.0 0.0 32h37:38 python2.7 break9.py
64423 root 20 0 110M 6368 820 R 98.0 0.0 32h38:02 python2.7 break9.py
64430 root 20 0 110M 6368 820 R 98.0 0.0 32h37:38 python2.7 break9.py
64455 root 20 0 110M 6392 832 R 99.0 0.0 32h37:23 python2.7 break9.py
64419 root 20 0 110M 6460 912 R 99.0 0.0 32h36:17 python2.7 break9.py
64467 root 20 0 110M 6392 824 R 98.0 0.0 32h36:41 python2.7 break9.py
64443 root 20 0 110M 6388 832 R 99.0 0.0 32h37:27 python2.7 break9.py
F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice - F8Nice + F9Kill F10Quit

I Spoke to the Python god

15:46 <Nanomebia> so uhh how much do you know about multiprocessing in python?

16:11 <swarley> a little, why

16:11 <swarley> what do you need mp for

16:11 <Nanomebia> i upgraded one of my scripts to mp so it would go faster

16:12 <swarley> nice

16:12 <swarley> does it work

16:12 <Nanomebia> nfi

- We exchanged wise words

break6optimised.py

```
#!/usr/bin/python
#break6multiprocessing.py
import sys
import itertools
import multiprocessing
from multiprocessing import Process, Queue
from string import ascii_lowercase
import time
def work(s):
    usercode = 1
    usertot = 0
    username = ''.join(s)
    for i, c in enumerate(username):
        usertot += (i*ord(c))
        usercode *= ord(c)
    if  ((usercode == 1172188274400) and (usertot == 1537)):
        return username
    else:
        return 0
def brute(s, queue):
    chars = ascii_lowercase
    while True:
        try:
            if not s.empty():
                q = s.get(block = False)
                for i in itertools.product(chars,repeat=3):
                    try:
                        w = q+i
                        res = work(w)
                        if (res != 0):
                            queue.put((res))
                    except:
                        pass
            else:
                break
        except:
            pass
def write(queue, fname):
    fhandle = open(fname, "a")
    while not queue.empty():
        try:
            username = queue.get()
            print >>fhandle, username
        except:
            break
    fhandle.close()
def main():
    chars = ascii_lowercase
    nthreads = multiprocessing.cpu_count()
    fname = "user6multiprocOPTIMISED2.txt"
    print 'using: '+str(nthreads)+' threads'
    print 'outputting to: '+fname
    writerQueue = multiprocessing.Queue()
    workQueue = multiprocessing.Queue()
    writProc = Process(target = write, args = (writerQueue, fname))
    for e in itertools.product(chars,repeat=3):
        workQueue.put((e), block=False)
    print 'work loaded'
    workProc = [Process(target = brute , args = (workQueue, writerQueue))
for i in xrange(nthreads)]
    for p in workProc:
        p.start()
    for p in workProc:
        p.join()
    print 'write started'
    writProc.start()
    writProc.join ()
    print('done')
if __name__ == '__main__':
    main()
```

Execute time:

```
using: 8 threads
outputting to:
user6multiprocOPTIMISED2.txt
work loaded
write started
done
[Finished in 161.3s]
```

The grunt work:

```
def work(s):
    usercode = 1
    usertot = 0
    username = ''.join(s)
    for i, c in enumerate(username):
        usertot += (i*ord(c))
        usercode *= ord(c)
    if  ((usercode == 11721882744400) and (usertot == 1537)):
        return username
    else:
        return 0
```

Brute it:

```
def brute(s, queue):
    chars = ascii_lowercase
    while True:
        try:
            if not s.empty():
                q = s.get(block = False)
                for i in itertools.product(chars,repeat=3):
                    try:
                        w = q+i
                        res = work(w)
                        if (res != 0):
                            queue.put((res))
                    except:
                        pass
            else:
                break
        except:
            pass
```

A tricky issue:

```
def write(queue, fname):
    fhandle = open(fname, "a")
    while not queue.empty():
        try:
            username = queue.get()
            print >>fhandle, username
        except:
            break
    fhandle.close()
```

How it comes together:

```
def main():
    chars = ascii_lowercase
    nthreads = multiprocessing.cpu_count()
    fname = "user6multiprocOPTIMISED2.txt"
    print 'using: '+str(nthreads)+' threads'
    print 'outputting to: '+fname
    writerQueue = multiprocessing.Queue()
    workQueue = multiprocessing.Queue()
    writProc = Process(target = write, args = (writerQueue, fname))
    for e in itertools.product(chars,repeat=3):
        workQueue.put((e), block=False)
    print 'work loaded'
    workProc = [Process(target = brute , args = (workQueue, writerQueue)) for i in xrange(nthreads)]
    for p in workProc:
        p.start()
    for p in workProc:
        p.join()
    print 'write started'
    writProc.start()
    writProc.join ()
    print('done')
if __name__ == '__main__':
    main()
```

break9optimised.py

- Still not fast enough
- Takes a long time (168h – only on shpzzzzzz)
  - Attack space: 5,429,503,678,976 keys
  - 8,977,353/second (64 cpus)
  - 140,271/second (1 cpu)
- Looked at GPU acceleration
- Didn’t want to commit suicide just yet

Recap

- Only needed to brute force username, password was in dictionary
- One or Two character codes to generate “admin”
- Multiprocessing can be really useful, or really really annoying

Oh, and one last thing…

- Remember the original JS?

```
uniqueId = "d9507edf0b2eb30b1292596e4ec10d7abbf0a959";
```

- Threw hashcat at it with some GPU power.
- Took just over 7 days
- Result:
- Sha1 of “1360155063”

SecTalks CTF Solution 0x00

@nanomebia

Github: https://github.com/nanomebia/sectalksctf0x00

(solution scripts)