



## Write-Up CTF KKST2021 Kategori Mahasiswa

NAMA TIM : [Pcode]

INSTITUSI : [IIB Darmajaya]

Rabu, 15 September 2021

### Ketua Tim

- Kalingga Padel Muhamad

### Member

- 
-

## Table of Content

—	Forensic	
—	Another user (30)	
—	CVE? (30)	
—	Database (30)	
—	Secret Files (30)	
—	A files (30)	

# FORENSIC

## [Another User]

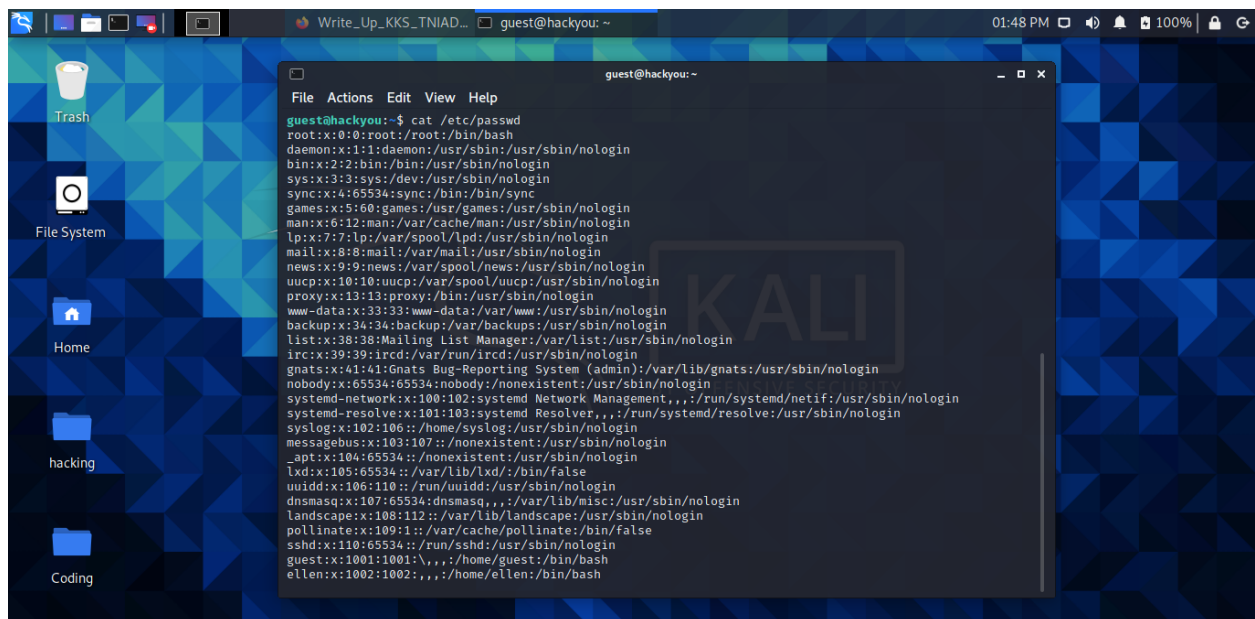
### Soal

Kami menyita sebuah mesin dari terduga pelaku peretasan 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}

Password VM : **4d1b54eeaceb5277ea022f7b42b53113**

### Pembahasan

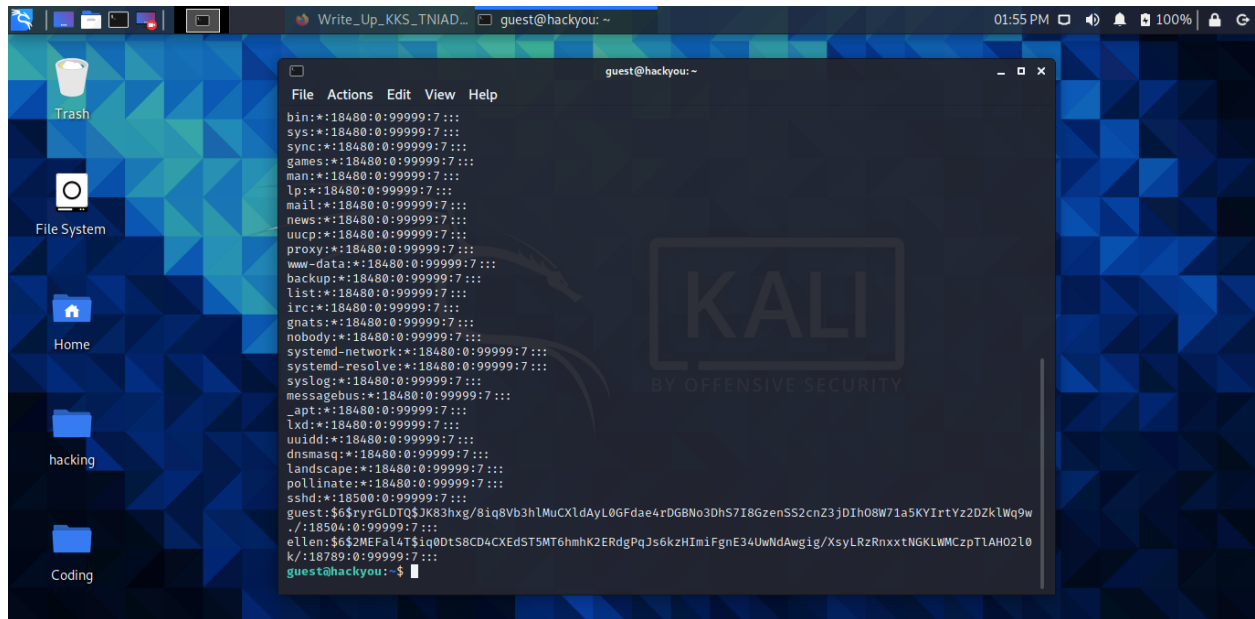
Diberikan sebuah vm dengan default user guest:guest, sesuai dengan instruksi soal, flag merupakan username dan password dari akun lain yang terdapat pada vm yang diberikan, Hal pertama yang saya lakukan adalah melihat semua akun yang terdapat pada vm dengan perintah `cat /etc/passwd` maka akan menampilkan semua informasi akun yang ada ,



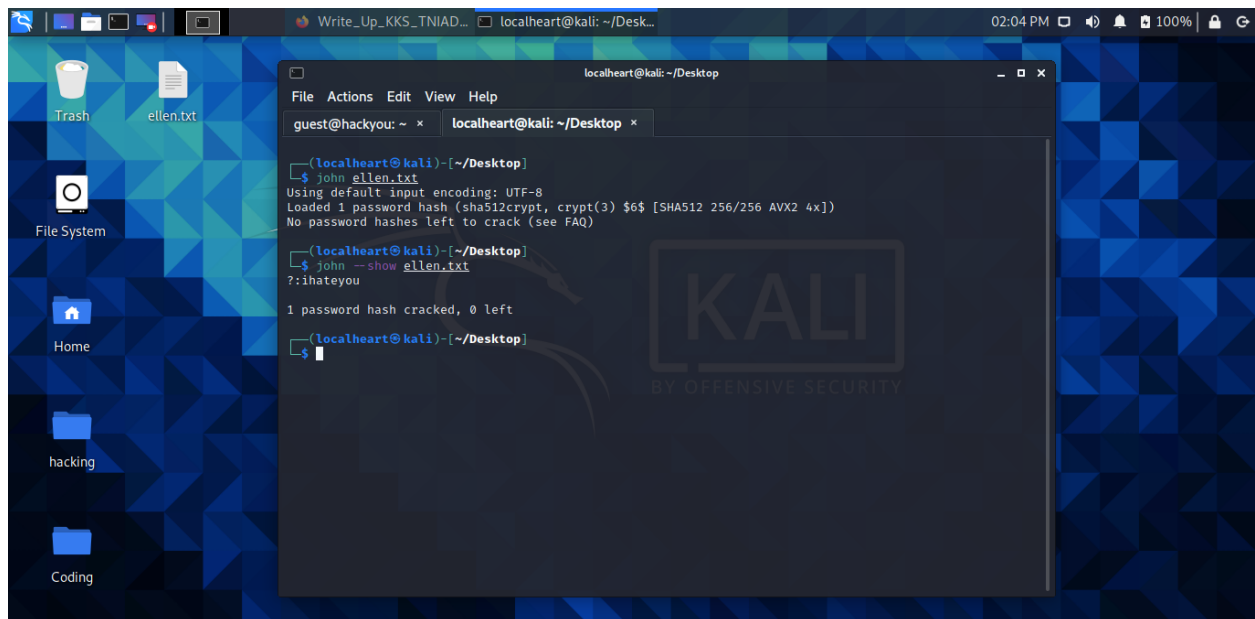
```
guest@hackyou:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
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
```

terdapat akun lain dengan username ellen:x, x adalah password, tapi passwordnya masih terenkripsi, untuk melihat x kita dapat menggunakan perintah `cat /etc/shadow` hasilnya

ellen:\$6\$2MEFa14T\$iq0DtS8CD4CXEdST5MT6hmhK2ERdgPqJs6kzHlmiFgnE34UwNdAwgig/XsYL  
RzRnxtNGKLWMCzpTIAHO210k/:18789:0:99999:7:::



lalu dilakukan decrypt menggunakan tools John the ripper



Flag : KKST2021{ellen:ihateyou}

# FORENSIC

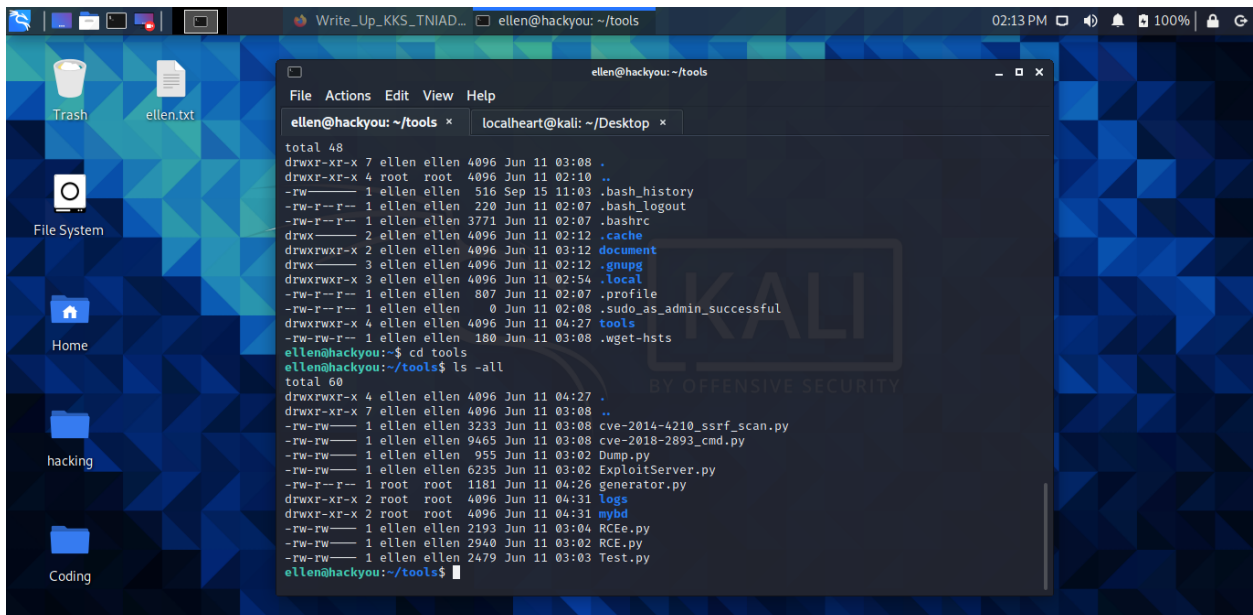
## [CVE?]

### Soal

Sebuah website dari perusahaan yang terjadi korban peretasan itu setelah dilakukan wawancara terhadap pengembangnya, bahasa pemrograman yang digunakan adalah PHP dan OS yang digunakan adalah Ubuntu dan web servernya 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!**

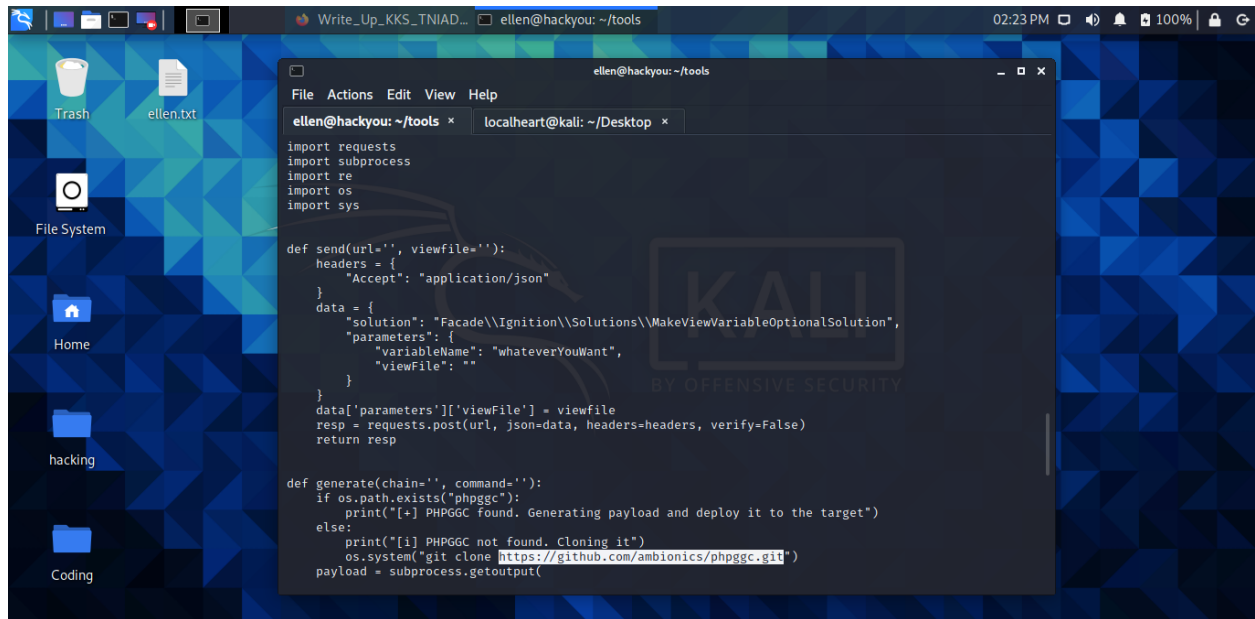
### Pembahasan

Setelah mendapatkan akun ellen pada soal sebelumnya, saya mencoba melihat directory apa saja yang terdapat pada akun ellen, sesuai soal saya harus mencari sesuatu yang berhubungan dengan CVE lalu didapatkan dir `/tools` yang terdapat 2 file dengan nama CVE

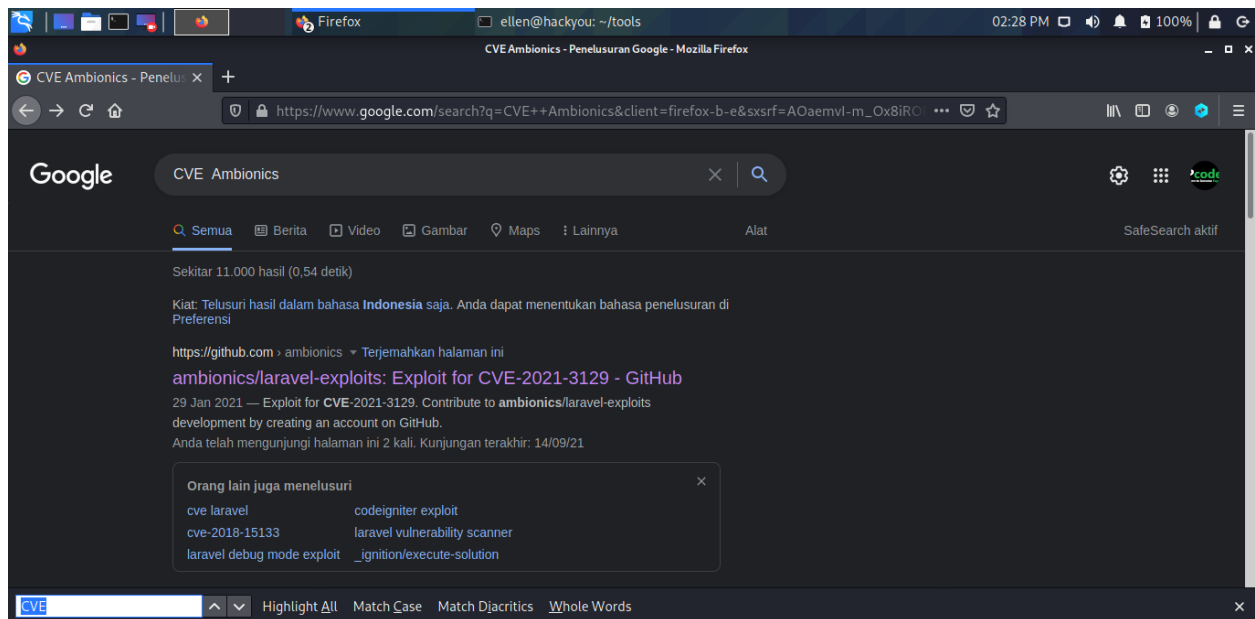


```
ellen@hackyou: ~/tools
File Actions Edit View Help
ellen@hackyou: ~/tools * localheart@kali: ~/Desktop *
total 48
drwxr-xr-x 7 ellen ellen 4096 Jun 11 03:08 .
drwxr-xr-x 4 root root 4096 Jun 11 02:10 ..
-rw-r--r-- 1 ellen ellen 516 Sep 15 11:03 .bash_history
-rw-r--r-- 1 ellen ellen 220 Jun 11 02:07 .bash_logout
-rw-r--r-- 1 ellen ellen 3771 Jun 11 02:07 .bashrc
drwx----- 2 ellen ellen 4096 Jun 11 02:12 .cache
drwxrwxr-x 2 ellen ellen 4096 Jun 11 03:12 document
drwx----- 3 ellen ellen 4096 Jun 11 02:12 .gnupg
drwxrwxr-x 3 ellen ellen 4096 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 4096 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 -all
total 60
drwxrwxr-x 4 ellen ellen 4096 Jun 11 04:27 .
drwxr-xr-x 7 ellen ellen 4096 Jun 11 03:08 ..
-rw-rw- 1 ellen ellen 3233 Jun 11 03:08 cve-2014-4210_ssrf_scan.py
-rw-rw- 1 ellen ellen 9465 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 6235 Jun 11 03:02 ExploitServer.py
-rw-r--r-- 1 root root 1181 Jun 11 04:26 generator.py
drwxr-xr-x 2 root root 4096 Jun 11 04:31 logs
drwxr-xr-x 2 root root 4096 Jun 11 04:31 mybd
-rw-rw- 1 ellen ellen 2193 Jun 11 03:04 RCEe.py
-rw-rw- 1 ellen ellen 2940 Jun 11 03:02 RCE.py
-rw-rw- 1 ellen ellen 2479 Jun 11 03:03 Test.py
ellen@hackyou:~/tools$
```

saya sempat mensubmit 2 CVE tersebut ternyata incorrect wkwwk, ternyata hanya jebakan sesuai deskripsi soal CVE nya berhubungan dengan bahasa pemrograman PHP dan hanya terdapat 1 file yaitu Test.py karena di dalam file Test.py terdapat request yang mengarah laravel dan perintah git clone ke repository <https://github.com/ambionics/phpggc>



lalu browsing di google dengan keyword **CVE Ambionics** maka didapatkan



Flag : KKST2021{CVE-2021-3129}

# FORENSIC

## [Database]

### Soal

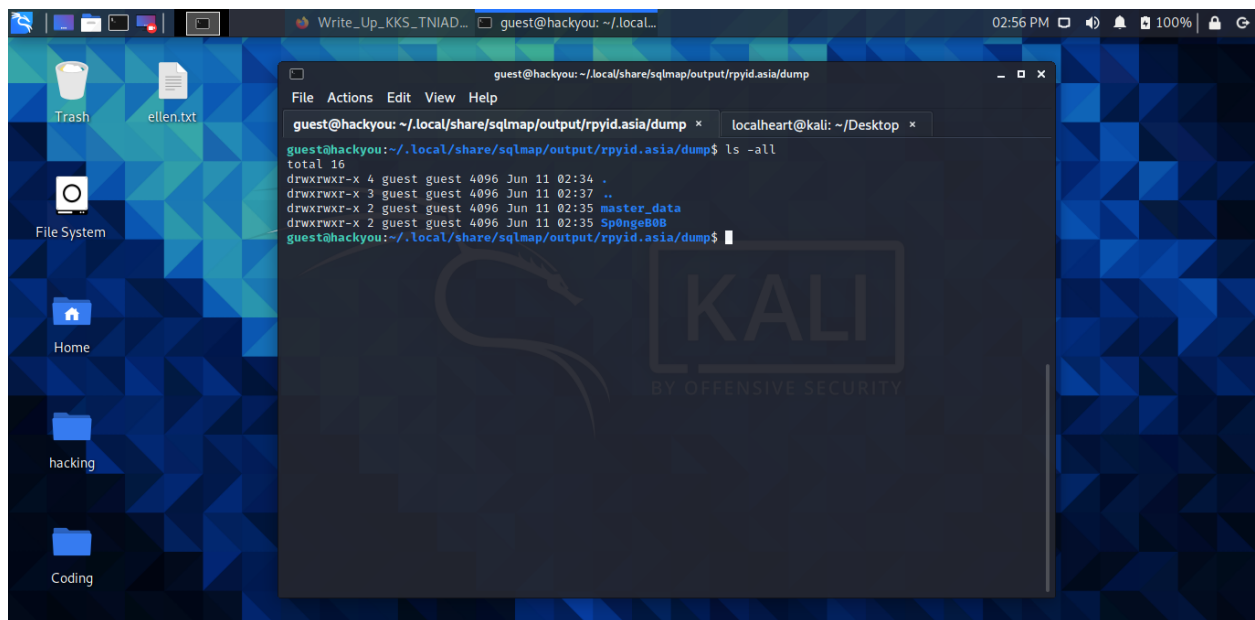
Perusahaan tersebut mengatakan databasenya di dump oleh terduga pelaku ini, dapatkan kamu memberitahu kami apa saja database yang terduga dump? Lalu, apa tabel yang terakhir di-dump oleh terduga? dan berapa banyak datanya? dan dari database apa?

KKST2021{nama\_db:tabel:jumlah\_data:db}

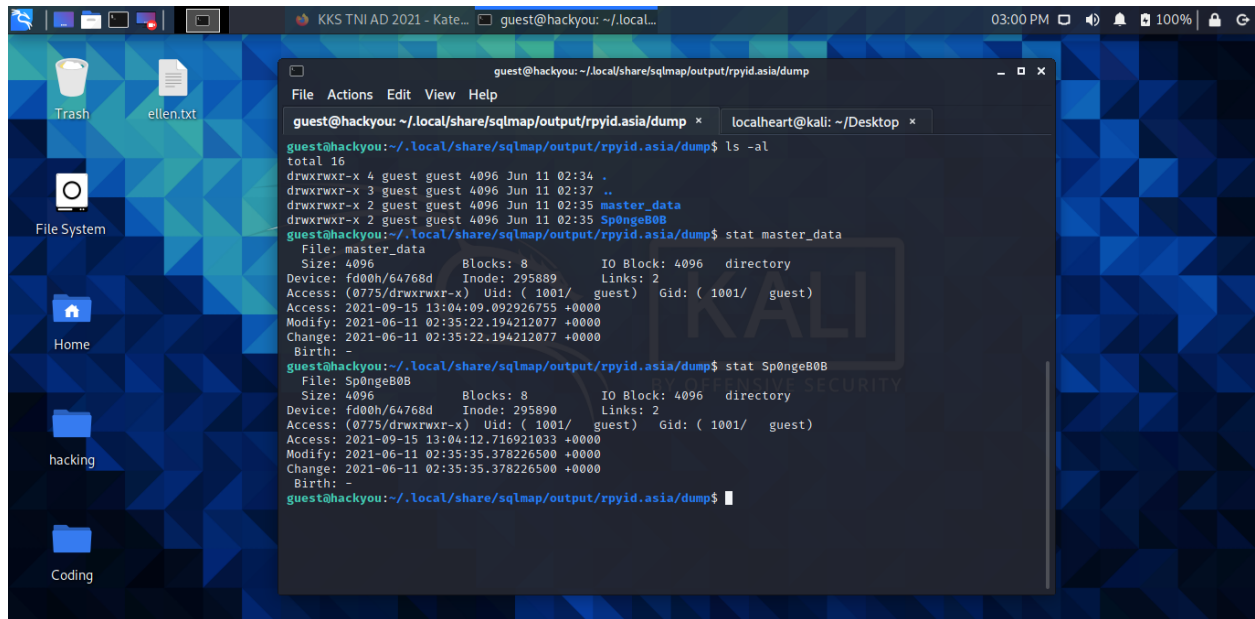
KKST2021{nama\_db,nama\_db,nama\_db:tabel:jumlah\_data:db}

### Pembahasan

Seperti tadi saya diharuskan mencari sesuatu di dalam vm yang berhubungan dengan database kali ini terdapat pada akun guest dengan alamat directory

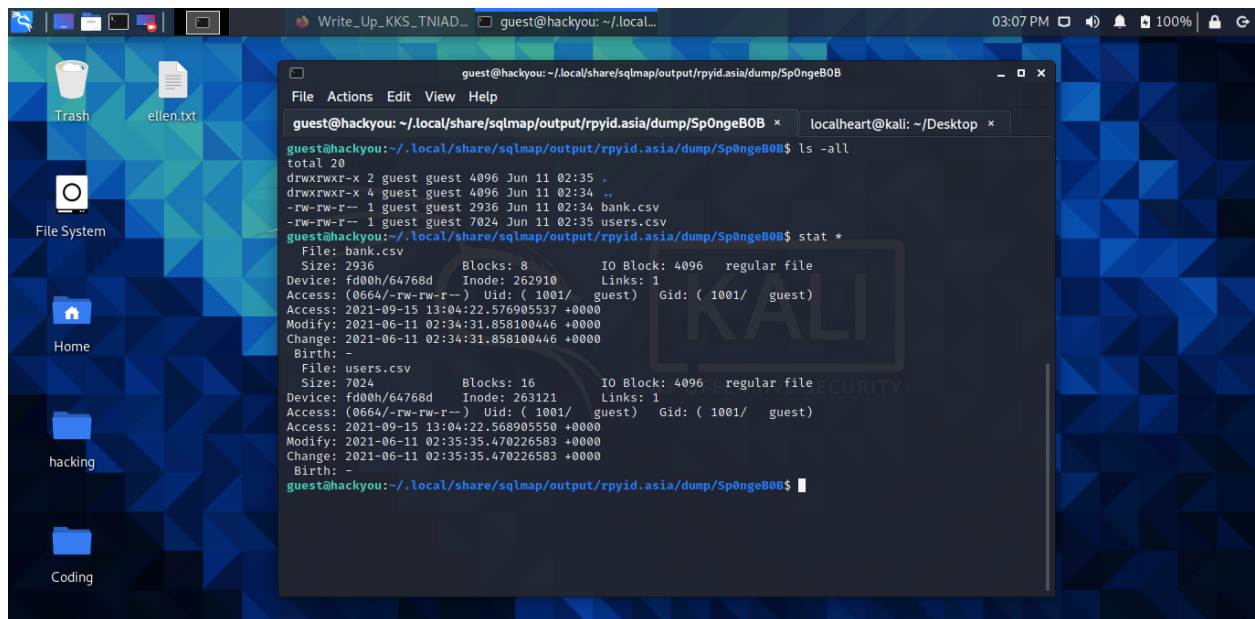


disini master\_data dan Sp0ngeB0B adalah 2 db yang di dump untuk melihat db terakhir yang di dump saya menggunakan perintah stat dengan command



```
guest@hackyou: ~/local/share/sqlmap/output/rpyid.asia/dump
guest@hackyou:~/local/share/sqlmap/output/rpyid.asia/dump$ ls -al
total 16
drwxrwxr-x 4 guest guest 4096 Jun 11 02:34 .
drwxrwxr-x 3 guest guest 4096 Jun 11 02:37 ..
drwxrwxr-x 2 guest guest 4096 Jun 11 02:35 master_data
drwxrwxr-x 2 guest guest 4096 Jun 11 02:35 Sp0ngeB0B
guest@hackyou:~/local/share/sqlmap/output/rpyid.asia/dump$ stat master_data
  File: master_data
  Size: 4096          Blocks: 8          IO Block: 4096   directory
Device: fd00h/64768d Inode: 295889    Links: 2
Access: (0775/drwxrwxr-x)  Uid: ( 1001/   guest)   Gid: ( 1001/   guest)
Access: 2021-09-15 13:04:09.092926755 +0000
Modify: 2021-06-11 02:35:22.194212077 +0000
Change: 2021-06-11 02:35:22.194212077 +0000
 Birth: -
guest@hackyou:~/local/share/sqlmap/output/rpyid.asia/dump$ stat Sp0ngeB0B
  File: Sp0ngeB0B
  Size: 4096          Blocks: 8          IO Block: 4096   directory
Device: fd00h/64768d Inode: 295890    Links: 2
Access: (0775/drwxrwxr-x)  Uid: ( 1001/   guest)   Gid: ( 1001/   guest)
Access: 2021-09-15 13:04:12.716921033 +0000
Modify: 2021-06-11 02:35:35.378226500 +0000
Change: 2021-06-11 02:35:35.378226500 +0000
 Birth: -
guest@hackyou:~/local/share/sqlmap/output/rpyid.asia/dump$
```

terlihat db Sp0ngeB0B adalah db terakhir yang di dump, terdapat 2 table yang di dump pada db Sp0ngeB0B yaitu bank.csv dan user.csv, sama seperti cara di atas untuk melihat table yang terakhir di dump saya menggunakan command stat, disini table user adalah tabel terakhir yang di dump dengan jumlah data 40, untuk melihat data saya menggunakan Google Spreadsheet



```
guest@hackyou: ~/local/share/sqlmap/output/rpyid.asia/dump/Sp0ngeB0B
guest@hackyou:~/local/share/sqlmap/output/rpyid.asia/dump/Sp0ngeB0B$ ls -all
total 20
drwxrwxr-x 2 guest guest 4096 Jun 11 02:35 .
drwxrwxr-x 4 guest guest 4096 Jun 11 02:34 ..
-rw-rw-r-- 1 guest guest 2936 Jun 11 02:34 bank.csv
-rw-rw-r-- 1 guest guest 7024 Jun 11 02:35 users.csv
guest@hackyou:~/local/share/sqlmap/output/rpyid.asia/dump/Sp0ngeB0B$ stat *
  File: bank.csv
  Size: 2936          Blocks: 8          IO Block: 4096   regular file
Device: fd00h/64768d Inode: 262910    Links: 1
Access: (0664/-rw-rw-r--) Uid: ( 1001/   guest)   Gid: ( 1001/   guest)
Access: 2021-09-15 13:04:22.576905537 +0000
Modify: 2021-06-11 02:34:31.858100446 +0000
Change: 2021-06-11 02:34:31.858100446 +0000
 Birth: -
  File: users.csv
  Size: 7024          Blocks: 16         IO Block: 4096   regular file
Device: fd00h/64768d Inode: 263121    Links: 1
Access: (0664/-rw-rw-r--) Uid: ( 1001/   guest)   Gid: ( 1001/   guest)
Access: 2021-09-15 13:04:22.568905550 +0000
Modify: 2021-06-11 02:35:35.470226583 +0000
Change: 2021-06-11 02:35:35.470226583 +0000
 Birth: -
guest@hackyou:~/local/share/sqlmap/output/rpyid.asia/dump/Sp0ngeB0B$
```

Jlka diurutkan maka **Flag : KKST2021{master\_data,Sp0ngeB0B:users:40:Sp0ngeB0B}**



# FORENSIC

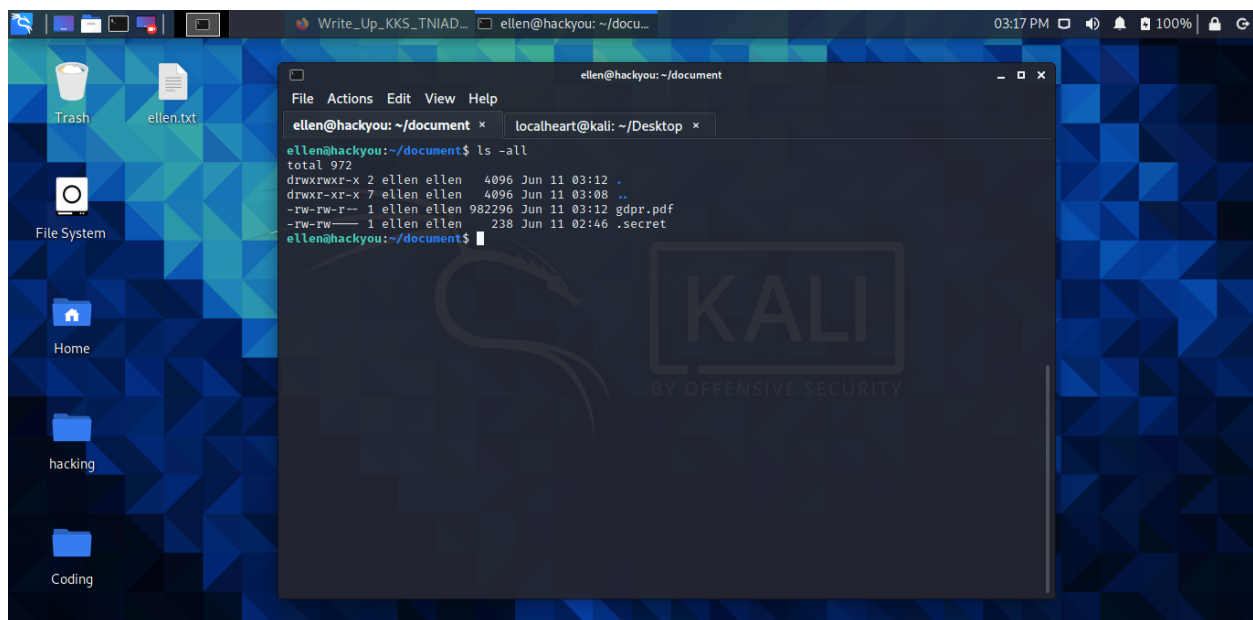
## [Secret Files]

### Soal

Saat melakukan interogasi 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!

### Pembahasan

Seperti tadi saya diharuskan mencari sesuatu di dalam vm yang berhubungan dengan Secret Files kali ini terdapat pada akun ellen dengan alamat directory

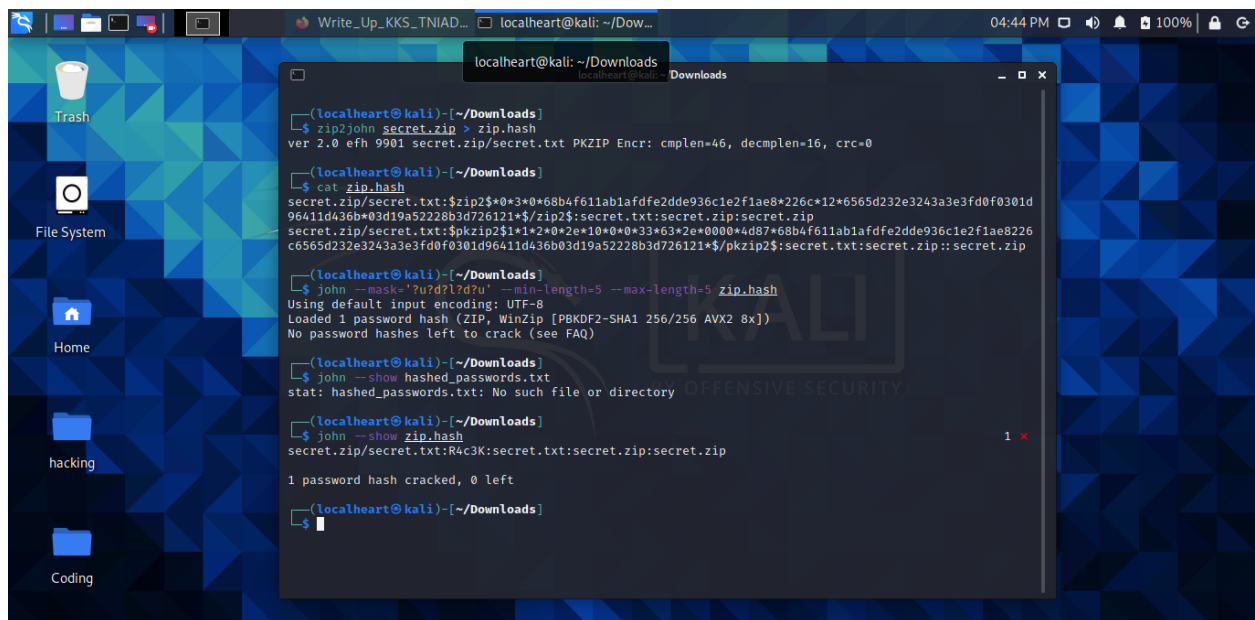


terdapat sebuah file .secret yang mana file tersebut adalah file zip yang terkunci, lalu kita crack password nya menggunakan john the ripper dengan command

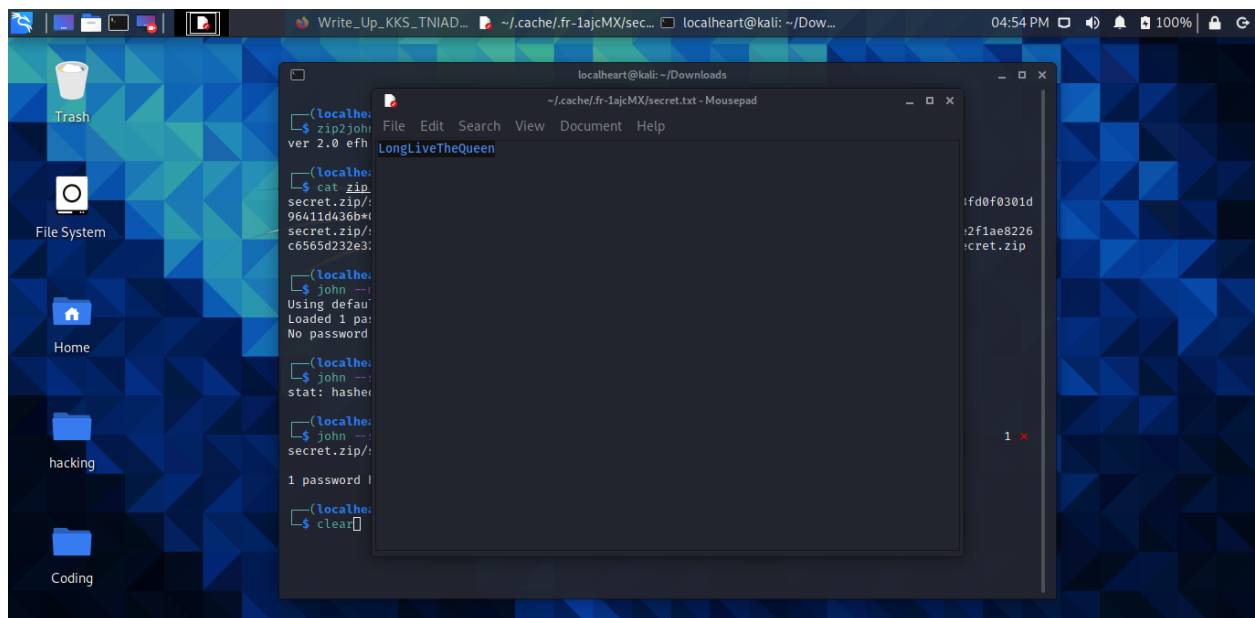
```
zip2john > secret.zip > hash.zip
```

```
john --mask='?u?d?!?d?u' --min-length=5 --max-length=5 zip.hash
```

masking sesuai dengan ketentuan soal saya pelajari dari <https://miloserdov.org/?p=5031>



lalu membuka secret.zip dengan password yang sudah di dapatkan



Flag : KKST2021{LongLiveTheQueen}

# FORENSIC

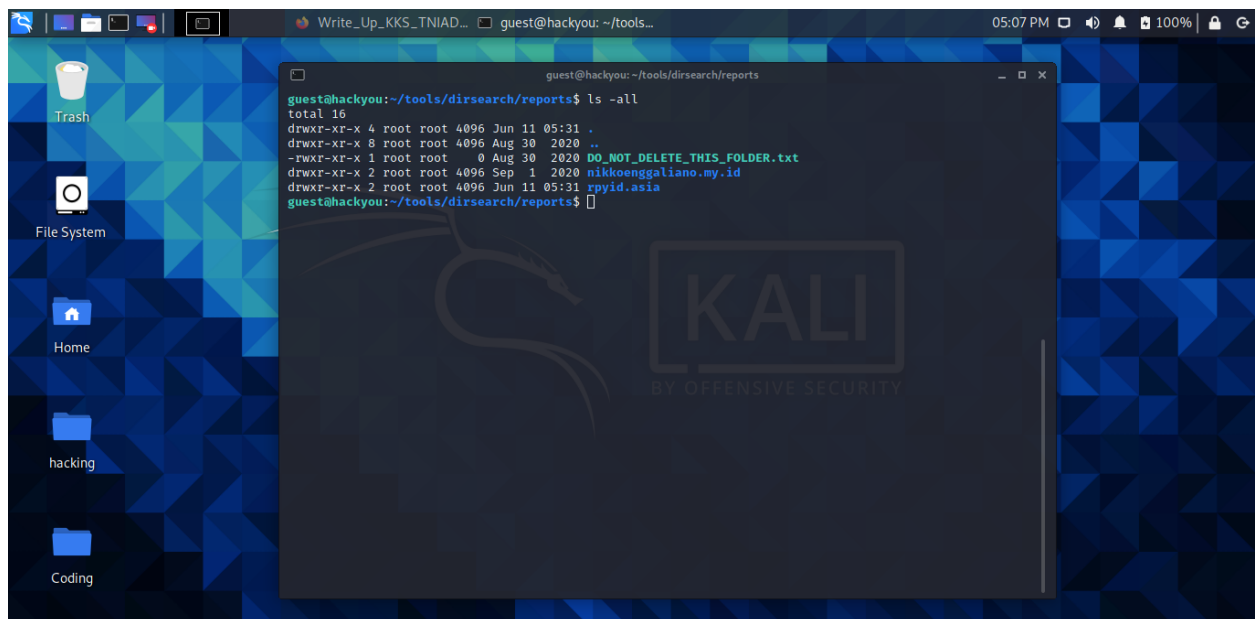
## [A Files]

### Soal

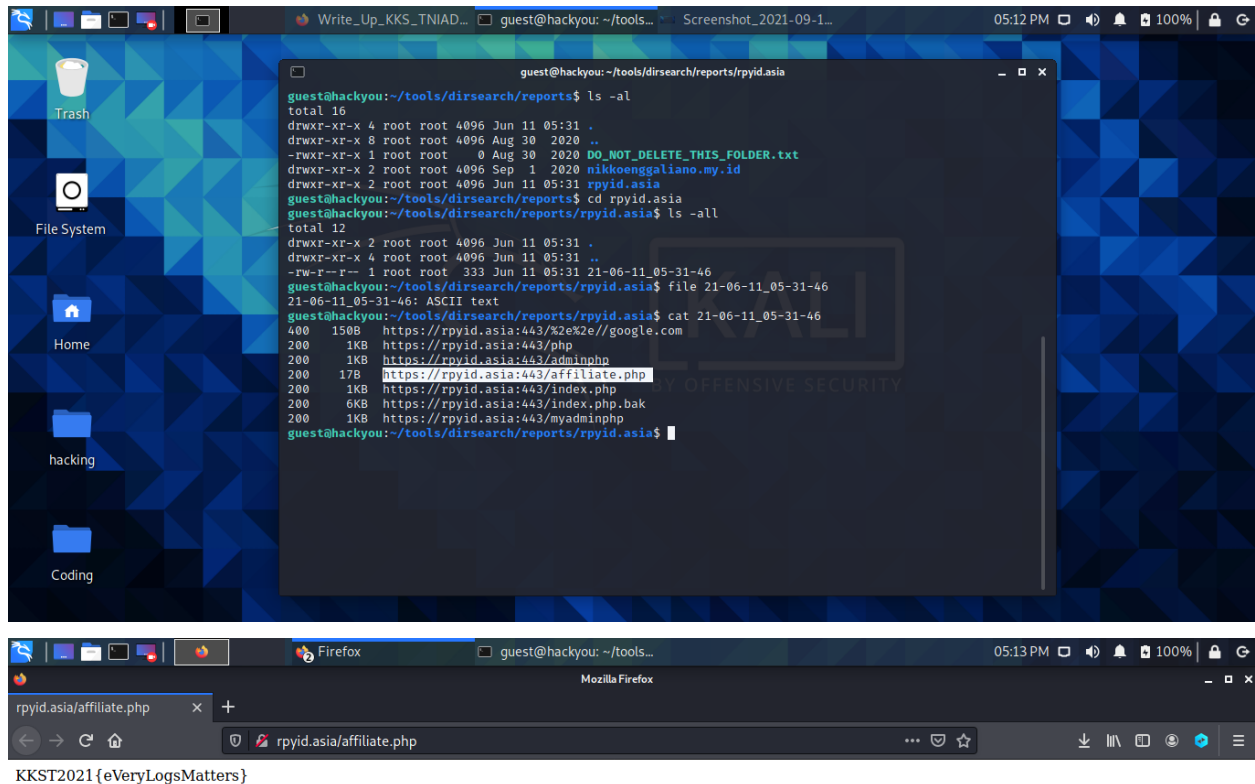
Terduga ini sebelum melakukan pementasan, melakukan proses scanning di website kami, dia menemukan sebuah file yang menjadi awal masuk pementasannya, temukan apa filenya dan apa isinya di web kami.

### Pembahasan

Untuk kali ini cukup mudah karena sudah jelas di soal terdapat kata scanning jadi ini tidak jauh jauh dari tools dir search, untuk tools dirsearch terdapat pada akun guest dengan alamat directory



terdapat 2 website hasil scanning, setelah saya cari ternyata flag berada pada dir rpyid.asia dan terdapat file dengan nama 21-06-11\_05-31-46, yang ternyata file txt .lalu baca isi file dengan perintah cat maka akan muncul hasil dari scan, buka hasil scan di web browser dan ditemukan flag pada <http://rpyid.asia/affiliate.php>



**Flag : KKST2021{eVeryLogsMatters}**