

REZKA NORHAFIZAH

WRITE UP

REVERSE 1

Diberikan sebuah soal, kemudian saya coba jalankan tetapi ternyata ketika dibuka terlihat bahwa akses ditolak. Lalu saya ketikkan **chmod +x reverse1** untuk mengubah hak akses file.

```
(kali@kali)-[~/Documents]
$ ./reverse1
zsh: permission denied: ./reverse1

(kali@kali)-[~/Documents]
$ chmod +x reverse1
```

Kemudian, saya coba jalankan lagi tetapi ternyata memerlukan password. Setelah itu, saya menggunakan tool yang bernama ltrace seperti berikut :

```
ltrace ./reverse1
_ZNSt8ios_base4InitC1Ev(0x556a761e92b9, 0xffff, 0x7ffc42ba03b8, 224) = 0
__cxa_atexit(0x7f533fbcca40, 0x556a761e92b9, 0x556a761e9060, 6) = 0
strcpy(0x7ffc42ba0163, "k0o") = 0x7ffc42ba0163
strcat("k0o", "pi_h") = "k0opi_h"
_ZNSt8ios_base4InitC1Ev(0x556a761e9080, 0x7f533fc3b6d0, 4, 0x685f69) = 0x556a761e9080
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(0x556a761e9080, 0x556a761e7010, 0, 3072) = 0x556a761e9080
_ZNSt8ios_base4InitC1Ev(0x556a761e9080, 0x7f533fc3b6d0, 0x556a761e9080, 3072) .--`..---.
) = 0x556a761e9080
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(0x556a761e9080, 0x556a761e7039, 0, 3072) = 0x556a761e9080
_ZNSt8ios_base4InitC1Ev(0x556a761e9080, 0x7f533fc3b6d0, 0x556a761e9080, 3072) .CTF:` .LKS-SMK28`
) = 0x556a761e9080
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(0x556a761e9080, 0x556a761e7058, 0, 3072) = 0x556a761e9080
_ZNSt8ios_base4InitC1Ev(0x556a761e9080, 0x7f533fc3b6d0, 0x556a761e9080, 3072) .--`..---.
) = 0x556a761e9080
_ZNSt8ios_base4InitC1Ev(0x556a761e9080, 0x7f533fc3b6d0, 0x556a761e9080, 3072)
) = 0x556a761e9080
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(0x556a761e9080, 0x556a761e7077, 0, 3072) = 0x556a761e9080
_ZNSt8ios_base4InitC1Ev(0x556a761e9080, 0x7f533fc3b6d0, 0x556a761e9080, 0x38324b4d5320534bCTF LKS SMK28) = 0x556a761e9080
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(0x556a761e9080, 0x556a761e7085, 0, 3072) = 0x556a761e9080
_ZStlsISt11char_traitsIcEERSt13basic_istreamIT_T0_ES6_PS3_(0x556a761e91a0, 0x7ffc42ba01a0, 0x7f533fcd3d0, 0x203e3a64726f7773) password:> "k0opi_h"
) = 0x556a761e91a0
strcat("k0opi_h", "ita") = "k0opi_hita"
strcat("k0opi_hita", "m_pht") = "k0opi_hitam_pht"
strcmp("k0opi_h", "k0opi_hitam_pht") = -73
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(0x556a761e9080, 0x556a761e709f, 107, 0xffff) = 0x556a761e9080
_ZNSt8ios_base4InitC1Ev(0x556a761e9080, 0x7f533fc3b6d0, 0x556a761e9080, 0x202141534942204b SMK BISA!) = 0x556a761e9080
+++ exited (status 0) +++
```

Lalu diminta untuk memasukkan sebuah inputan, saya coba ketikkan **"k0opi_h"** sesuai yang tertera di atas, dan didapat password untuk file :

```
) = 0x556a761e91a0
strcat("k0opi_h", "ita") = "k0opi_hita"
strcat("k0opi_hita", "m_pht") = "k0opi_hitam_pht"
strcmp("k0opi_h", "k0opi_hitam_pht") = -73
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(0x556a761e9080, 0x556a761e709f, 107, 0xffff) = 0x556a761e9080
_ZNSt8ios_base4InitC1Ev(0x556a761e9080, 0x7f533fc3b6d0, 0x556a761e9080, 0x202141534942204b SMK BISA!) = 0x556a761e9080
+++ exited (status 0) +++
```

Kemudian saya coba jalankan lagi menggunakan password tersebut dan didapat :

```
(kali@kali)-[~/Documents]
$ ./reverse1

.CTF:~ .LKS-SMK28~

CTF LKS SMK28
password:> k0opi_hitam_pht

LKSSMK28{01c9fsd3gt34zxxcb0eb8a42d3c534rf3c570703e3t}
```

Flag = LKSSMK28{01c9fsd3gt34zxxcb0eb8a42d3c534rf3c570703e3t}

REVERSE 2

Diberikan sebuah soal, kemudian saya lakukan hal yang sama seperti yang saya lakukan untuk reverse1, ternyata diminta memasukkan password. Lalu saya menggunakan tool ltrace dan didapat password :

```
(kali@kali)-[~/Documents]
$ ltrace ./reverse2
puts("||=====||")
)
) = 73
puts("|| //////////////////////////////////////////////////////////////////// ... || ////////////////////////////////////////////////////////////////////")
)
) = 73
puts("|| ()=====|| CTF ... || ()=====|| CTF ||")
)
) = 66
puts("|| ()=====|| LKS SM ... || ()=====|| LKS SMK 28")
)
) = 66
puts("|| //////////////////////////////////////////////////////////////////// ... || ////////////////////////////////////////////////////////////////////")
)
) = 73
puts("||=====||")
)
) = 73
puts("Password:Password:")
)
) = 10
__isoc99_scanf(0x55d3dbf2313c, 0x7ffdd395ad90, 0, 0x7f76e0577f33.)
) = 1
strcmp("0x00007fff", ".")
puts("You FailedYou Failed")
)
+++ exited (status 0) +++
) = 11
```

Kemudian saya coba jalankan lagi file tersebut dan saya masukkan password dan didapatkan flagnya :


```
(kali㉿kali)-[~/Documents]
$ ./crackme
puts("Hi!\nInput Your Password"Hi!
Input Your Password
)
= 24
malloc(18)
memset(0x55e1a7fd36b0, '\0', 18)
fgets(0x55e1a7fd36b0
"0x55e1a7fd36b0\n", 18, 0x7ff66b4bb980)
strcmp("0x55e1a7fd36b0\n", "JJJJJJJJJJJJJBxs")
puts("Password Salah!"Password Salah!
)
free(0x55e1a7fd36b0)
+++ exited (status 0) +++

(kali㉿kali)-[~/Documents]
$ ./crackme
Hi!
Input Your Password
JJJJJJJJJJJJJBxs
MANTUL, flag is LKSSMK28{JJJJJJJJJJJJJBxs}
```

Flag = LKSSMK28{JJJJJJJJJJJJJBxs}

Diberikan soal, lalu saya buka menggunakan aplikasi wireshark kemudian saya lakukan filter packet HTTP seperti berikut :

http
+
+

No.	Time	Source	Destination	Protocol	Length	Info
273	16.148757722	192.168.0.5	203.201.167.38	HTTP	354	GET /img/intro-bg.jpg HTTP/1.1
1048	19.464190600	192.168.0.5	203.201.167.38	HTTP	432	GET /peserta-lolos.php HTTP/1.1
1094	19.535954000	203.201.167.38	192.168.0.5	HTTP	1572	[CG: previous segment not captured] Continuation
1094	19.535953639	203.201.167.38	192.168.0.5	HTTP	1514	Continuation
1096	19.535977256	203.201.167.38	192.168.0.5	HTTP	1514	Continuation
1101	19.537225375	203.201.167.38	192.168.0.5	HTTP	1514	Continuation
1103	19.541818692	203.201.167.38	192.168.0.5	HTTP	1514	Continuation
1108	19.557564946	203.201.167.38	192.168.0.5	HTTP	1514	Continuation
1110	19.557584162	203.201.167.38	192.168.0.5	HTTP	1514	Continuation
1112	19.559674720	203.201.167.38	192.168.0.5	HTTP	1514	Continuation

> Frame 1108: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface wlan1, id 0

> Ethernet II, Src: D-Link-14:97:40 (80:26:89:14:97:40), Dst: Tp-Link_2e:8e:e4 (c0:25:9e:2e:8e:e4)

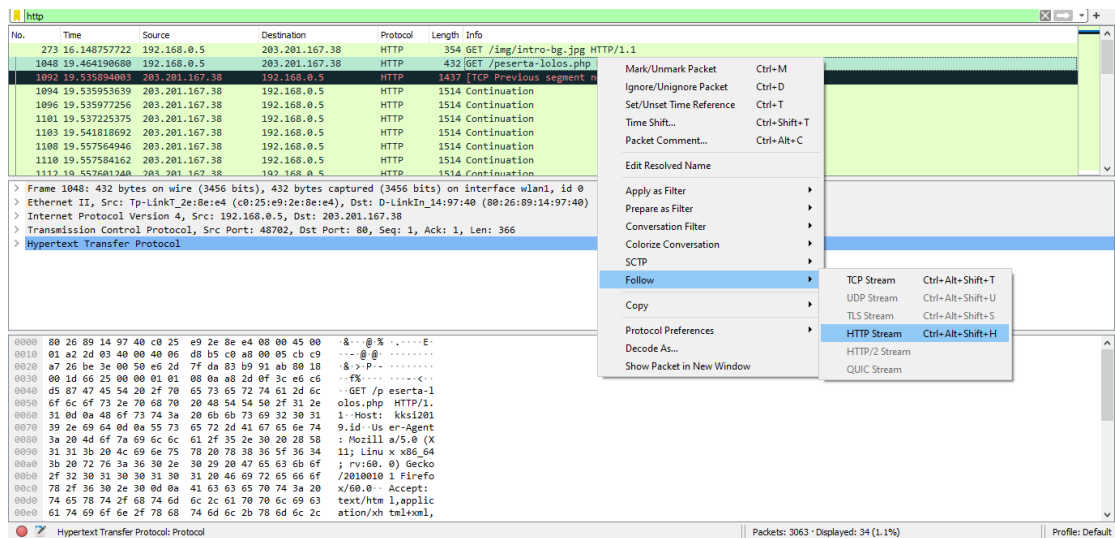
> Internet Protocol Version 4, Src: 203.201.167.38, Dst: 192.168.0.5

> Transmission Control Protocol, Src Port: 80, Dst Port: 48702, Seq: 17300, Ack: 367, Len: 1448

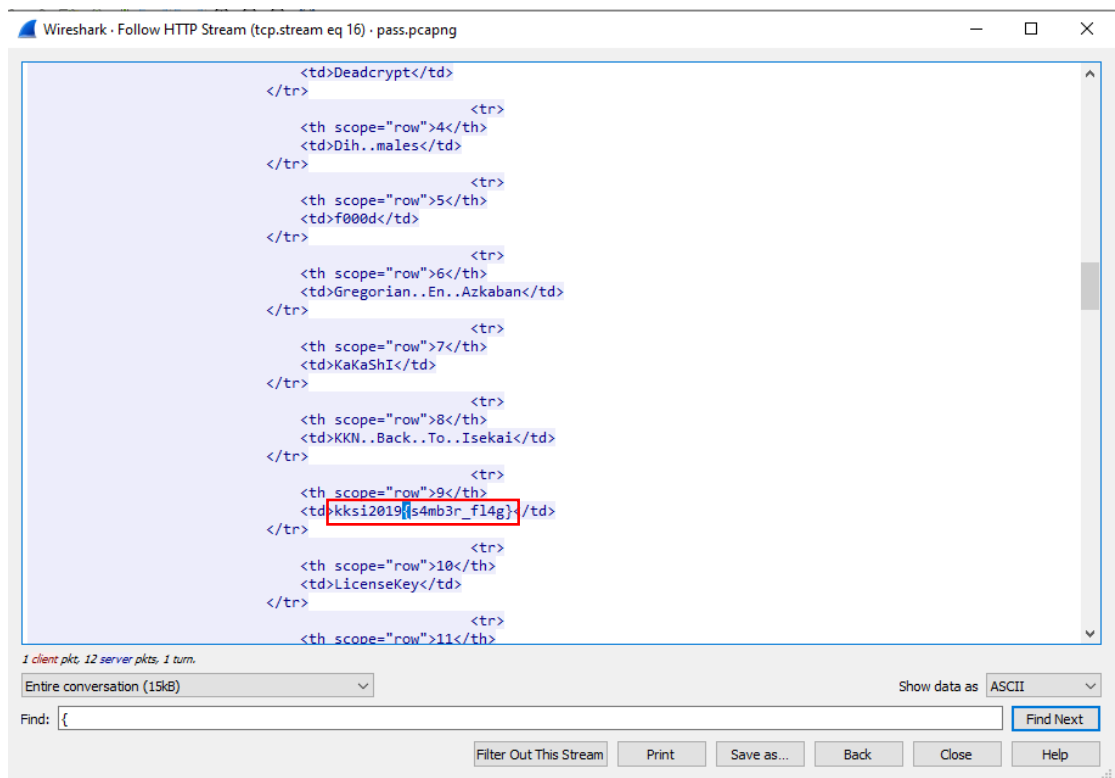
> Hypertext Transfer Protocol

```

0000  c0 25 e9 2e 8e e4 80 26 89 14 97 40 08 00 45 00  %..&...<@<-E-
0010  05 dc 4a f7 40 00 37 06 bf 87 cb c9 a7 26 c0 a8  ...3@7-....<-
0020  00 05 00 50 be 3e 83 b9 d5 3e e6 2d 81 48 80 10  ...P>>>->-H-
0030  00 7a 4f f1 00 00 01 01 08 0a e6 c6 08 0a a8 2d  <N.....<-
0040  0f 84 84 20 20 20 20 20 20 20 20 20 20 20 20 20  <tr>
0050  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0060  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0070  20 3c 7a 68 20 7a 63 6f 70 05 3d 22 72 6f 77 22  <th sco pen"row"
0080  7a 31 3a 3c 2f 7a 68 3e 0a 20 20 20 20 20 20 20  >14</th> <-
0090  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
00a0  20 20 20 20 20 20 20 20 20 3c 7a 64 3e 7a 69 6d  <td>tim
00b0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <hehe</td> >-
00c0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
00d0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
00e0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
00f0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0100  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0110  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0120  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0130  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0140  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0150  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0160  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0170  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0180  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0190  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
01a0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
01b0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
01c0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
01d0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
01e0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
01f0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0200  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0210  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0220  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0230  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0240  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0250  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0260  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0270  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0280  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
0290  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
02a0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
02b0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
02c0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  <-
02d0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  &
```



Dan didapat flag :



Flag = kks2019{s4mb3r_fl4g}

BONGKARZZZ

Diberikan file, lalu saya coba buka ternyata diperlukan username dan password. Kemudian saya mencari username dan password untuk file tersebut. Saya coba menggunakan perintah strings tetapi tidak kunjung ditemukan juga. Selanjutnya saya coba menggunakan radare2 dan saya lakukan analyze terhadap file.

```
(kali㉿kali)-[~/Documents]
$ r2 -d ./bongkarzzz
Process with PID 1455 started...
= attach 1455 1455
bin.baddr 0x08048000
Using 0x08048000
asm.bits 32
glibc.fc_offset = 0x00148
[0xf7f960b0]> aaa
[x] Analyze all flags starting with sym. and entry0 (aa)
[x] Analyze function calls (aac)
[x] Analyze len bytes of instructions for references (aar)
[x] Check for vtables
[TOFIX: aaft can't run in debugger mode.ions (aaft)
[x] Type matching analysis for all functions (aaft)
[x] Propagate noreturn information
[x] Use -AA or aaaa to perform additional experimental analysis.
```

Lalu, untuk melihat list function saya ketikkan afl dan disana terlihat ada main function.

```
[0xf7f960b0]> afl
0x08048380 1 33 entry0
0x08048360 1 6 sym.imp.__libc_start_main
0x080483c0 4 43 sym.deregister_tm_clones
0x080483f0 4 53 sym.register_tm_clones
0x08048430 3 30 sym.__do_global_dtors_aux
0x08048450 4 43 → 40 entry.init0
0x08048560 1 2 sym.__libc_csu_fini
0x080483b0 1 4 sym.__x86.get_pc_thunk.bx
0x08048564 1 20 sym._fini
0x080484f0 4 97 sym.__libc_csu_init
0x0804847b 4 115 main
0x080482f4 3 35 sym._init
0x08048350 1 6 loc.imp.__gmon_start__
0x08048330 1 6 sym.imp.printf
0x08048340 1 6 sym.imp.puts
0x08048370 1 6 sym.imp.__isoc99_scanf
```

Lalu saya menemukan nilai pembandingnya :

```
[0xf7f960b0]> pdf @main
; DATA XREF from entry0 @ 0x8048397
115: int main (int argc, char **argv, char **envp);
; FILE *fp;
; var int32_t var_ch @ ebp-0xc
; var int32_t var_4h @ ebp-0x4
; arg char **argv @ esp+0x34
0x0804847b      8d4c2404      lea ecx, [argv]
0x0804847f      83e4f0        and esp, 0xffffffff
0x08048482      ff71fc        push dword [ecx - 4]
0x08048485      55            push ebp
0x08048486      89e5          mov ebp, esp
0x08048488      51            push ecx
0x08048489      83ec14        sub esp, 0x14
0x0804848c      83ec0c        sub esp, 0xc
0x0804848f      6880850408    push str.Cari_Username_:_ ; 0x8048580 ; "Cari Userna
me : "
0x08048494      e897feffff    call sym.imp.printf ; int printf(const char *f
ormat)
0x08048499      83c410        add esp, 0x10
0x0804849c      83ec08        sub esp, 8
0x0804849f      8d45f4        lea eax, [var_ch]
0x080484a2      50            push eax
0x080484a3      6891850408    push 0x8048591
0x080484a8      e8c3feffff    call sym.imp.__isoc99_scanf ; int scanf(const char *fo
rmat)
0x08048499      83c410        add esp, 0x10
0x0804849c      83ec08        sub esp, 8
0x0804849f      8d45f4        lea eax, [var_ch]
0x080484a2      50            push eax
0x080484a3      6891850408    push 0x8048591
0x080484a8      e8c3feffff    call sym.imp.__isoc99_scanf ; int scanf(const char *fo
rmat)
0x080484ad      83c410        add esp, 0x10
0x080484b0      8b45f4        mov eax, dword [var_ch]
0x080484b3      3de01e1100    cmp eax, 0x111ee0
0x080484b8      7412          je 0x80484cc
0x080484ba      83ec0c        sub esp, 0xc
0x080484bd      6894850408    push str.Cari_Password_:_ ; 0x8048594 ; "Cari Passwo
rd :("
0x080484c2      e879feffff    call sym.imp.puts ; int puts(const char *s)
0x080484c7      83c410        add esp, 0x10
0x080484ca      eb15          jmp 0x80484e1
0x080484cc      83ec08        sub esp, 8
0x080484cf      68d9a46500    push 0x65a4d9
0x080484d4      68a6850408    push 0x80485a6
0x080484d9      e852feffff    call sym.imp.printf ; int printf(const char *f
ormat)
0x080484de      83c410        add esp, 0x10
; CODE XREF from main @ 0x80484ca
0x080484e1      b800000000    mov eax, 0
0x080484e6      8b4dfc        mov ecx, dword [var_4h]
0x080484e9      c9            leave
0x080484ea      8d61fc        lea esp, [ecx - 4]
0x080484ed      c3            ret
```

Dan saya konversikan nilai pembanding tersebut ke desimal :

Hexadecimal to Decimal converter

From

To

Hexadecimal

Decimal

Enter hex number

111ee0

16

= Convert

✕ Reset

↕ Swap

Decimal number

1122016

10

Saya coba angka tersebut untuk username dan ternyata didapat password nya juga :

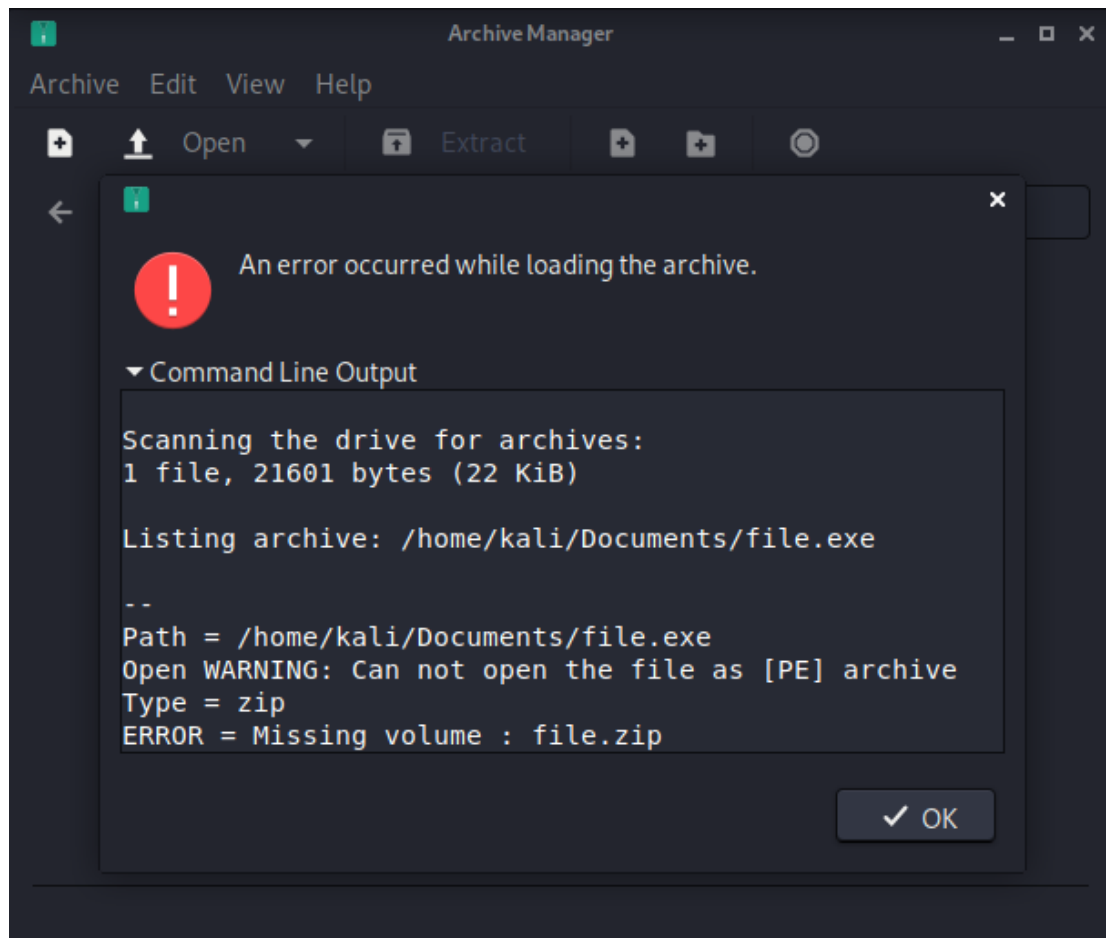
```
(kali㉿kali)-[~/Documents]
$ ./bongkarzzz
Cari Username : 1122016
6661337
```

Username : 1122016

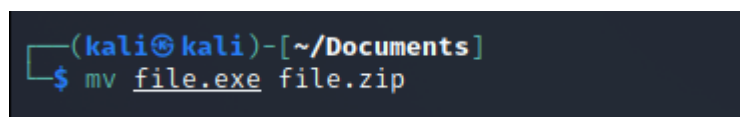
Password : 6661337

FILE.EXE

Setelah diberikan file, saya coba buka tetapi ternyata didapat error seperti berikut :



Dari gambar di atas dapat dilihat terdapat hint yang menunjukkan bahwa file tersebut adalah file dengan ekstensi zip, maka saya ubah nama file tersebut ke file.zip :



Lalu saya coba buka dan ternyata ada dua file yang tersimpan di sana yaitu sebagai berikut :

Text (ASCII / ANSI)

LKSSMK28{crack1n9_docum3nT}

Convert

Highlight Text

Hexadecimal

4c 4b 53 53 4d 4b 32 38 7b 63 72 61 63 6b 31 6e 39
5f 64 6f 63 75 6d 33 6e 54 7d

BASE64

TEtTU01LMjh7Y3JhY2sxbjlfZG9jdW0zbIR9

Flag = LKSSMK28{crack1n9_docum3nT}