

Forum:[Hack Forums](#)

Thread: [Can not execute when encode to shell code ..](#)

SIM-1866423 - April 10, 2015, 8:40 am

There my first hello world app with asm(Litle edit,trying bypass null bytes etc..).

PHP Code

```
<?php
section .text
    global _start

_start:
    add    edx,len
    mov    ecx,msg
    add    ebx,1        ;mov    ebx,1
    add    eax,4        ;mov    eax,4
    int    0x80

    xor    ebx,ebx      ;mov    ebx,0
    mov    al,1         ;mov    eax,1
    int    0x80
```

section .data

```
msg db    "##Hello World! #B3mB4m",0xa
len equ   $ - msg
```

When im compile script to executable file, everything going normal.

PHP Code

```
<?php
./hello
##Hello World! #B3mB4m
```

There dump info ;

PHP Code

```
<?php
hello:  file format elf32-i386
```

Disassembly of section .text:

```
08048080 <.text>:
8048080: 83 c2 16          add    $0x16,%edx
8048083: b9 98 90 04 08    mov    $0x8049098,%ecx
8048088: 83 c3 01          add    $0x1,%ebx
804808b: 83 c0 04          add    $0x4,%eax
804808e: cd 80            int    $0x80
8048090: 31 db            xor    %ebx,%ebx
```

```
8048092:  b0 01          mov  $0x1,%al
8048094:  cd 80          int  $0x80
```

When im making that shellcode cant execute ?

Already try to execute in Python/C/C++ im always get this error ;

PHP Code

```
<?php
```

```
//System :3.14-kali1-686-pae (32bit)
```

```
[php]fragmentation failure
```

I'm too hectic right now, sorry for this. So any idea why fail ? ?

LevelUp - April 10, 2015, 3:45 pm

Well firstly you can't utilise your 'message' variable in such a manner because you do not know what is going to be at address because ASLR will randomize that sections base address. You will have to instead utilise a:

Code _start:

```
    jmp popme
```

resume:

```
    etc etc
```

```
    etc etc
```

popme:

```
    call resume
```

```
    db "#Hello World! #B3mB4m",0x0d,0x0a
```

Also if you were using this as part of a buffer overflow, it would not work to use 'add <reg32>,0xwhatever' as you've done in your code because you have not zeroed out the registers yet. Instead just use:

Code xor <reg32>,<reg32>

```
mov <reg8>,0xwhatever
```

To be noted that you'll still get a segfault with making that initial change I first suggested because you must disable NX stack first by compiling with -fno-stack-protector -z execstack.

SIM-1866423 - April 10, 2015, 11:30 pm

I'm pretty new in asm,asm looks like me little higgledy-piggledy.I will try again, thanks for advice ?