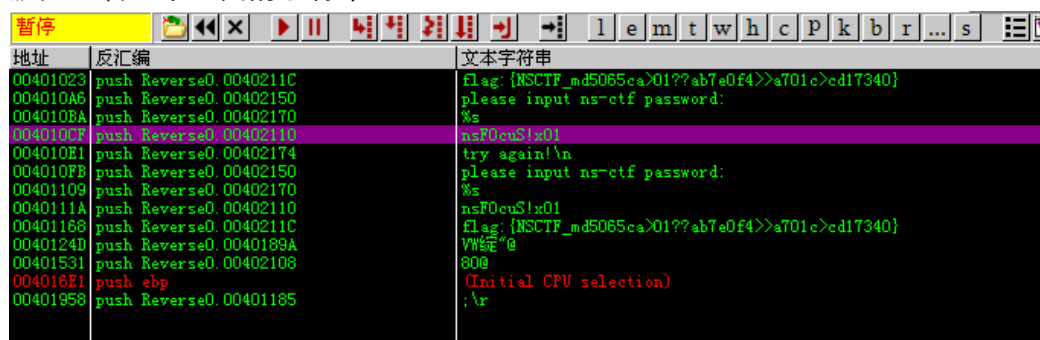


Reverse 100

程序运行后提示 **please input ns-ctf password:** 要求输入密码，随便试了下错误，于是用 OD 和 IDA 分析。

用 PEiD 查到发现加了 ASPack 2.12 的壳，这个壳比较简单，直接用 OllyDump 手动脱壳，虽然脱下的程序无法直接运行，但对解题没什么影响。这个壳的手动脱法很简单，在网上搜一下就能找到了。

脱壳后看一下里面的字符串



地址	反汇编	文本字符串
00401023	push Reverse0.0040211C	Flag: {NSCTF_md5065ca>01??ab7e0f4>>a701c>cd17340}
004010A6	push Reverse0.00402150	please input ns-ctf password:
004010BA	push Reverse0.00402170	%s
004010CF	push Reverse0.00402110	nsF0cuS!x01
004010E1	push Reverse0.00402174	try again!\n
004010FB	push Reverse0.00402150	please input ns-ctf password:
00401109	push Reverse0.00402170	%s
0040111A	push Reverse0.00402110	nsF0cuS!x01
00401168	push Reverse0.0040211C	Flag: {NSCTF_md5065ca>01??ab7e0f4>>a701c>cd17340}
0040124D	push Reverse0.0040189A	VW%定"@
00401531	push Reverse0.00402108	80@
004016E1	push ebp	(Initial CPU selection)
00401958	push Reverse0.00401185	;\r

长成这样，啥也不说直接先试试 **nsF0cuS!x01**

程序退出，得到 Flag，和里面的那个字符串一样：**flag: {NSCTF_md5065ca>01??ab7e0f4>>a701c>cd17340}**

提交发现不对，于是打开 IDA 找到对应的位置看看

```

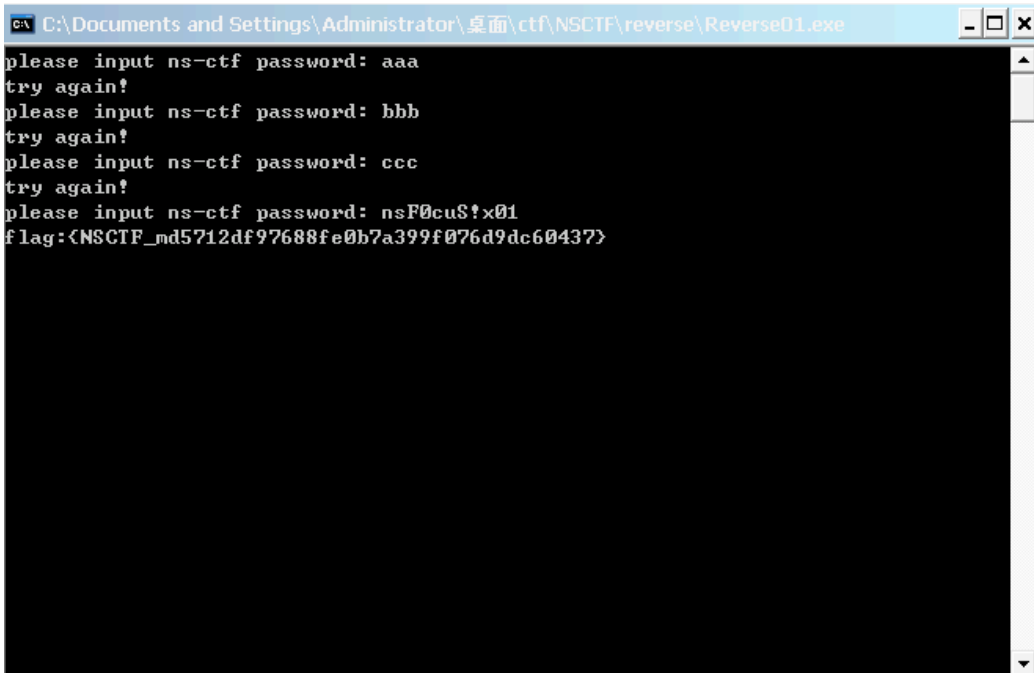
v800006FE("please input ns-ctf password: ");
v80000721("%s", &v4);
for ( i = 1; v8000073C("nsF0cu$!x01", &v4, 11); ++i )
{
    v800006FE("try again!\n");
    sub_4019B4(&v4, 0, 256);
    v800006FE("please input ns-ctf password: ");
    v80000721("%s", &v4);
}
v1 = &v4;
dword_403368 = 1;
do
    v2 = *v1++;
while ( v2 );
if ( v1 != &v5 )
{
    if ( i > 3 )
    {
        sub_401000();
        return 0;
    }
    v800006FE("flag:<NSCTF_md5065ca>01??ab7e0f4>>a701c>cd17340}");
}

```

Decode Here



发现当 $i > 3$ 时会执行 decode，那么就先输错三次吧。



```

C:\Documents and Settings\Administrator\桌面\ctf\NSCTF\reverse\Reverse01.exe
please input ns-ctf password: aaa
try again!
please input ns-ctf password: bbb
try again!
please input ns-ctf password: ccc
try again!
please input ns-ctf password: nsF0cu$!x01
flag:<NSCTF_md5712df97688fe0b7a399f076d9dc60437}

```

flag:{NSCTF_md5712df97688fe0b7a399f076d9dc60437}