漏洞银行逆向工程系列课程（一） —— 暴力流学汇编

第五课_标志寄存器

主讲：K1ght（漏洞银行安全专家）

讲师互动丨课后交流丨资料共享 二进制学习圈：**542285506**

漏洞银行微信公众号：**BUG_BANK**

漏洞银行 | BUGBANK
www.bugbank.cn

标志寄存器

CF——进位标志（Carry Flag）。若CF=1，表示算术运算时产生进位或借位，否则CF=0。移位指令会影响CF。

PF——奇偶标志（Parity Flag）。若PF=1，表示操作结果中“1”的个数为偶数，否则PF=0。这个标志位主要用于检查数据传送过程中的错误。

AF——辅助进位标志（Auxiliary Carry Flag）。若AF=1表示字节运算产生低半字节向高半字节的进位或借位，否则AF=0。辅助进位也称半进位标志，主要用于BCD码运算的十进制调整。

ZF——全零标志（Zero Flag）。若ZF=1，表示操作结果全为零，否则ZF=0。

SF——符号标志（Sign Flag）。若SF=1，表示符号数运算后的结果为负数，否则SF=0。

标志寄存器

OF——溢出标志（Overflow Flag）。若OF=1，表示当进行算术运算时，结果超过了最大范围，否则OF=0。

IF——中断允许标志（Interrupt Enable Flag）。若IF=1，则CPU可以响应外部可屏蔽中断请求；若IF=0，则CPU不允许响应中断请求。IF的状态可由中断指令设置。

DF——方向标志（Direction Flag）。若DF=1，表示执行字符串操作时按着从高地址向低地址方向进行；否则DF=0。DF位可由指令控制。

TF——单步标志（Trace Flag）。又称跟踪标志。该标志位在调试程序时可直接控制CPU的工作状态。当TF=1时为单步操作，CPU每执行一条指令就进入内部的单步中断处理，以便对指令的执行情况进行检查；若TF=0，则CPU继续执行程序。

ZF标志

全零标志（Zero Flag）。若ZF=1，表示操作结果全为零，否则ZF=0。

```
mov ax,1

sub  ax,1          (ZF = 0)
```

影响标志寄存器的指令：add,sub,mul,div,inc,or,and

不影响标致寄存器的指令：mov,push,pop

PF标志

奇偶标志（Parity Flag）。若PF=1，表示操作结果中“1”的个数为偶数，否则PF=0。这个标志位主要用于检查数据传送过程中的错误。

```
mov     al,1

add     al,10

or      al,8
```

SF标志

符号标志（Sign Flag）。若SF=1，表示符号数运算后的结果为负数，否则SF=0

```
Mov             al,ff

Add             al,1
```

add是无符号加，但是当有进位的时候还是会影响奇偶标志

CF 标志

进位标志（Carry Flag）。若CF=1，表示算术运算时产生进位或借位，否则CF=0。移位指令会影响CF。

```
mov     al,ff

add     al,1
```

同样的两句话，进位的1到了CF；

OF标志

溢出标志（Overflow Flag）。若OF=1，表示当进行算术运算时，结果超过了最大范围，否则OF=0。

```
Mov         al,ff

Add         al,1
```

溢出了，所以OF也会变

adc

带进位的加

```
mov     ax,2
mov     bx,1
sub     bx,ax
adc     ax,1
```

sbb

带借位的减法

```
Sbb         ax,bx       (ax=ax-bx-CF)


mov         ax,2
mov         bx,1
sub         bx,ax
sbb         ax,1
```

cmp指令

不保存结果的sub

```
cmp     ax,ax     (ax-ax=0;  ZF=1,PF=1,SF=0,CF=0,OF=0)

mov     ax,2
mov     bx,3
cmp     ax,bx
```

检测比较结果的条件转移指令

JC	如果进位位被置位则跳转	进位标志 = 1	JB，JNAE	JNC
JZ	如果0标志被置位则跳转	0标志 = 1	JE	JNZ
JB	如果低于(<)则跳转	进位标志 = 1	JC，JNAE	JNB
JA	如果超过(>)则跳转	进位标志 = 0，0标志 = 0	JNBE	JNA
JBE	如果低于或等于(<=)则跳转	进位标志 = 1或0标志 = 1	JNA	JNBE
JE	如果相等(=)则跳转	0标志=1	JZ	JNE
JG	如果大于(>)则跳转	符号标志=溢出标志或0标志=0	JNLE	JNG

TEST命令

Test对两个参数(目标，源)执行AND逻辑操作,并根据结果设置标志寄存器,结果本身不会保存。TEST AX,BX 与 AND AX,BX 命令有相同效果

Test的一个非常普遍的用法是用来测试一方寄存器是否为空:

test ecx, ecx

jz somewhere

如果ecx为零,设置ZF零标志为1,Jz跳转

加入漏洞银行二进制学习圈　**QQ群号：542285506**

获取**免费课件**｜结交**讲师伙伴**｜紧跟**后续课程**

微信公众号：BUG_BANK

漏洞银行 | BUGBANK
www.bugbank.cn