漏洞银行逆向工程系列讲座（一） —— 暴力流学汇编

内存寻址方式

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

目录

[bx]

- mov ax,[bx]　　什么意思？
- ax=[ds*10H+bx]

loop

2的11次方怎么算？

```
mov ax,2
add ax,2
 ...(9次)
add ax,bx
```

```
happy:  mov ax,2
        mov cx,10
        add ax,2
        loop happy
```

and和or指令

and ax,f0f0h (ax and 11110000 11110000B)

or ax,ff00h (ax or 11111111 00000000B)

大写字母变小写字母

```
mov cx,10

mov al,[bx]

and al,11101111B

inc bx

loop --
```

内存寻址方式

mov　　ax,[bx+200h]　　什么意思

si，di寄存器是什么

mov ax,[100h]　　[ds*10h+100h]

mov ax,[bx]　　[ds*10h+bx]

mov ax,[si]　　[ds*10h+si]

mov ax,[bp+100h][ss*10h+bp+100h]

mov ax,[si+bx+100h]　　[ds*10h+si+bx+100h]

内存寻址方式

寻址方式	格式
直接寻址	[100h]
寄存器间接寻址	[bx] [bp] [si/di]
寄存器相对寻址	[bx+100h] [bp+100h] [si/di+100h]
基址变址寻址	[bx+si/di] [bp+si/di]
相对基址变址寻址	[bx+si/di+100h] [bp+si/di+100h]

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