咸鱼的ROP笔记

pop/ret

pop:

将后一个内存地址中的数据放到$ebp中

ret:

ret = pop + jump

将后一个内存地址中的数据放到$ebp中，并跳转到这个数据所代表的地址

于是 *'a'*140+p32(pop_ret)+p32(0)+ +p32(pop_ret)+p32(0)+p32(write)*就是酱紫的

		pop执行ING	ret执行ING	pop执行ING	ret执行ING
Overflow ('a'*140)	POP/RET	p32(0)	POP/RET	p32(0)	WRITE
溢出到$ebp	将pop/ret写入$ebp	POP将p32(0)放入$ebp 此时$esp=[$esp+4]	RET先将第二个POP/RET放入$ebp，再执行POP/RET 此时$esp=[$esp+8]	POP将p32(0)放入$ebp 此时$esp=[$esp+12]	RET先将WRITE放入$ebp，再执行WRITE 此时$esp=[$esp+16]
	POP/RET分两步进行		POP/RET分两步进行		

更正

RET是把数据放到$eip里去

$eip是指令寄存器 存放的永远是下一条要执行的语句地址

POP [参数] 就是把数据放到【参数】寄存器里去