Remove函数：

if ( v2 <= 0x63 && (v1 = (\_DWORD \*)garden\_qword\_202040[v2]) != 0LL )

{

\*v1 = 0;

free(\*(void \*\*)(garden\_qword\_202040[v2] + 8LL));

result = puts("Successful");

}

将指定flower的name字段free,并且将in\_use字段置0

Clean函数：

v0 = garden\_qword\_202040;

do

{

v1 = (\_DWORD \*)\*v0;

if ( \*v0 && !\*v1 )

{

free(v1);

\*v0 = 0LL;

--total\_202024;

}

++v0;

}

while ( v0 != &garden\_qword\_202040[100] );

当flower的in\_use字段为0时，将当前flower清除free

初步思路：

1.泄露strtol函数地址

2.计算system函数地址

3.将strtol地址修改为system地址

4.Getshell