writeup-collision

原创

charlie_heng 于 2016-11-21 20:22:55 发布 371 收藏

分类专栏： 二进制-逆向工程 文章标签： 逆向工程

题目如下

Daddy told me about cool MD5 hash collision today.
I wanna do something like that too!

ssh col@pwnable.kr -p2222 (pw:guest)

先连上去看下有什么东西
发现有个col.c 代码如下

```c
#include <stdio.h>
#include <string.h>
unsigned long hashcode = 0x21DD09EC;
unsigned long check_password(const char* p){
    int* ip = (int*)p;
    int i;
    int res=0;
    for(i=0; i<5; i++){
        res += ip[i];
    }
    return res;
}

int main(int argc, char* argv[]){
    if(argc<2){
        printf("usage : %s [passcode]\n", argv[0]);
        return 0;
    }
    if(strlen(argv[1]) != 20){
        printf("passcode length should be 20 bytes\n");
        return 0;
    }

    if(hashcode == check_password( argv[1] )){
        system("/bin/cat flag");
        return 0;
    }
    else
        printf("wrong passcode.\n");
    return 0;
}
```

很明显要构造一个长度为20的字符串，然后每4位转换为int相加之后的值为0x21DD09EC

一开始没想到要溢出，直接除以5发现数字太小，根本构造不出来，后面想到之后构造了一下就出来了

字符串为 ah_mah_lah_mam_mhc_m ，这题应该有多解，一开始其实想直接爆破的。。但是想了想时间复杂度，明显太大爆破不了。。。

输入./col ah_mah_lah_mam_mhc_m

拿到flag
daddy! I just managed to create a hash collision :)

（吐槽下。。这flag好奇葩。。。）