[原创] 看雪CTF Q2题目提交 优

顾何 1

举报

2019-6-5 14:58 269

战队名称：iret
队长QQ：450566546
参赛题目：CrackMe
题目答案：KanXue2019ctf_st
详细的题目设计说明和破解思路以及其他需要说明的各个问题：
该题目为base64魔改的CrackMe
首先定义了一个自定义的base64编码table：

```
#define TABLE1 "tuvwxTUlmnopqrs7YZabcdefghij8yz0123456VWXkABCDEFGHIJKLMNOPQRS9+/"
```

然后定义了一个单个字符加密的方法：

```
static char charEncrypt(int data)
{
    char *table = TABLE1;
    data = table[data];
    if(data>=65 && data<=90)
    {
        data = (155-data) ;
        return  (char)data;
    }
    if(data>=97&&data<=122)
    {
        data = (data-64);
        return  (char)data;
    }
    if(data>=48&&data<=57)
    {
        data = (data + 50) ;
        return  (char)data;
    }
    if(data==43)
    {
        data = 119;
        return  (char)data;
    }
    if(data==47)
        data = 121;
    return  (char)data;
}
```

接下来使用c语言实现了base64编码，不仅使用修改后的编码table，还会在赋值的时候调用单个字符加密方法将字符加密后赋值。

破解思路：本题的重点在于单个字符的变换强度。真实的编码table从头到尾不会在内存中显示。所以攻击者需要先将断点设置在charEncrypt处，找出编码的变换规则，然后找到修改过后的编码table，根据变换规则推导出真正的编码table。

完整代码：

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <errno.h>
#include <inttypes.h>
#define TABLE1 "tuvwxTUlmnopqrs7YZabcdefghij8yz0123456VWXkABCDEFGHIJKLMNOPQRS9+/"

/*base64编/解码用的基础字符集*/


static char charEncrypt(int data)
{
    char *table = TABLE1;
```

```
        data = (155-data) ;
        return  (char)data;
    }
    if(data>=97&&data<=122)
    {
        data = (data-64);
        return  (char)data;
    }
    if(data>=48&&data<=57)
    {
        data = (data + 50) ;
        return  (char)data;
    }
    if(data==43)
    {
        data = 119;
        return  (char)data;
    }
    if(data==47)
        data = 121;
    return  (char)data;
}

static int base64_encode( const uint8_t *bindata, char *base64, int binlength)
{
    int i, j;
    uint8_t current;
    for ( i = 0, j = 0 ; i < binlength ; i += 3 ) {
        current = (bindata[i] >> 2) ;
        current &= (uint8_t)0x3F;
        base64[j++] = charEncrypt((int)current);
        current = ( (uint8_t)(bindata[i] << 4 ) ) & ( (uint8_t)0x30 ) ;
        if ( i + 1 >= binlength ) {

            base64[j++] = charEncrypt((int)current);
            base64[j++] = '=';
            base64[j++] = '=';
            break;
        }
        current |= ( (uint8_t)(bindata[i+1] >> 4) ) & ( (uint8_t) 0x0F );

        base64[j++] = charEncrypt((int)current);
        current = ( (uint8_t)(bindata[i+1] << 2) ) & ( (uint8_t)0x3C ) ;
        if ( i + 2 >= binlength ) {

            base64[j++] = charEncrypt((int)current);
            base64[j++] = '=';
            break;
        }
        current |= ( (uint8_t)(bindata[i+2] >> 6) ) & ( (uint8_t) 0x03 );
        base64[j++] = charEncrypt((int)current);
        current = ( (uint8_t)bindata[i+2] ) & ( (uint8_t)0x3F ) ;

        base64[j++] = charEncrypt((int)current);
    }
    base64[j] = '\0';
    return j;
}
int main (int argc, char **argv)
{
    char str1[55];
    printf("please enter Serial:");
    scanf(" %s",str1);
    if(strlen(str1)>=50)
    {
        printf("error\n");
        exit;
    }
    char *base64_str = calloc(1, 1024);
    base64_encode(str1, base64_str, strlen(str1));
    char *str = "!NGV%,$h1f4S3%2P(hkQ94==";
    if(!strcmp(str,base64_str))
    {
        printf("Success\n");
    } else{
        printf("Please Try Again\n");
    }

    free(base64_str);
    system("pause");
    return 0;
}
```

[公告]看雪.纽盾 KCTF 2019晋级赛Q3攻击方规则，9月10日开赛，华为P30 Pro、iPad、kindle等你来拿！

最后于 2019-6-24 18:23 被kanxue编辑，原因:

上传的附件：

Kanxue.exe （27.61kb，2次下载）

1 0

☆ 收藏 赞 打赏 分享

最新回复 (0)

勇士小蓝

内容

回帖 表情 高级回复

返回

©2000-2019 看雪学院 | Based on Xiuno BBS
域名：加速乐 | SSL证书：亚洲诚信 | 安全网易云易盾| 同盾反欺诈

公众号：ikanxue | 关于我们 | 联系我们 | 企业服务
Processed: **0.028**s, SQL: **17** / 京ICP备10040895号-17

首页 论坛 专栏 课程 发现