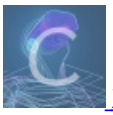
XCTF-re1-100

原创

永远是深夜有多好。 于 2022-02-01 21:06:00 发布 366 收藏

分类专栏： XCTF 文章标签： 其他

本文链接：https://blog.csdn.net/qq_37370714/article/details/122766168



静态分析

```
if ( numRead == -1 )
  break;
if ( numRead )
{
  if ( !childCheckDebugResult()
    && bufParentRead[0] == '{'
    && strlen(bufParentRead) == 42
    && !strncmp(&bufParentRead[1], "53fc275d81", 10uLL)
    && bufParentRead[strlen(bufParentRead) - 1] == '}'
    && !strncmp(&bufParentRead[31], "4938ae4efd", 10uLL)
    && confuseKey(bufParentRead, 42)
    && !strncmp(bufParentRead, "{daf29f5934938ae4efd53fc275d81053ed5be8c}", 42uLL) )
  {
    responseTrue();
  }
  else
  {
    responseFalse();
  }
}
```


已知前11字符串和31到40的字符串，通过`confuseKey`函数混淆了key

```
  return 0;
if ( strlen(szKey) != 42 )
  return 0;
if ( *szKey != '{' )
  return 0;
strncpy(szPart1, szKey + 1, 10uLL);
strncpy(szPart2, szKey + 11, 10uLL);
strncpy(szPart3, szKey + 21, 10uLL);
strncpy(szPart4, szKey + 31, 10uLL);
memset(szKey, 0, 42uLL);
*szKey = '{';
strcat(szKey, szPart3);
strcat(szKey, szPart4);
strcat(szKey, szPart1);
strcat(szKey, szPart2);
szKey[41] = '}';
return 1;
```


而这个函数混淆的顺序就是3、4、1、2按照正常顺序排序就能得到答案

```
Input key : {53fc275d81053ed5be8cdaf29f59034938ae4efd}
True
```