xctf中re题配套知识点

原创

jovy-rtt 于 2019-12-06 14:57:26 发布 238 收藏 1
分类专栏： CTF 文章标签： ctf 小白学习之路

本文链接：https://blog.csdn.net/zmx2473162621/article/details/103416005

关于ida的用法上：

可以右键函数名称，来直接搜索main函数

关于ida中伪代码的一些函数：

1. sprintf（）

sprintf指的是字符串格式化命令，函数声明为 int sprintf(char *string, char *format [,argument,…]);，主要功能是把格式化的数据写入某个字符串中，即发送格式化输出到 string 所指向的字符串。sprintf 是个变参函数。使用sprintf 对于写入buffer的字符数是没有限制的，这就存在了buffer溢出的可能性。解决这个问题，可以考虑使用 snprintf函数，该函数可对写入字符数做出限制

- **string–** 这是指向一个字符数组的指针，该数组存储了 C 字符串。
- **format–** 这是字符串，包含了要被写入到字符串 str 的文本。它可以包含嵌入的 format 标签，format 标签可被随后的附加参数中指定的值替换，并按需求进行格式化。format 标签属性是%[flags][width][.precision][length]specifier
- **[argument]…**：根据不同的 format 字符串，函数可能需要一系列的附加参数，每个参数包含了一个要被插入的值，替换了 format 参数中指定的每个 % 标签。参数的个数应与 % 标签的个数相同。
- **功能** 把格式化的数据写入某个字符串缓冲区。

本题之后就是把后边的那个字符，变成十六进制数值的字符形式，如：v4为‘0’->‘0x30’就是这种格式

2. strcat（）

- 中文名：**字符串连接函数**
- 原型 ：**extern char *strcat(char *dest, const char *src);**
- **功能**：把src所指向的字符串（包括“\0”）复制到dest所指向的字符串后面（删除*dest原来末尾的“\0”*）。*要保证*dest足够长，以容纳被复制进来的*src。*src中原有的字符不变。返回指向dest的指针。

在本题中就是把那个的单个字符加到v10上，相当于：flag+=s[i]

python中函数：

- chr（）函数是可以把一个数字代表的ASCII码变成字符

```
>>> chr(98)
'b'
>>>
```

相应的，

- ord（）函数可以把一个字符的ASCII输出

```
>>> chr(98)
'b'
>>> ord('0')
48
>>>
```

- hex()把十进制装换 成十六进制字符

```
>>> hex(56)
'0x38'
>>>
```

- oct()把十进制转换为八进制字符

```
>>> oct(10)
'0o12'
>>>
```

- bin()把十进制装换为二进制字符

```
>>> bin(10)
'0b1010'
>>>
```

- 注意字符是str

```
>>> type(oct(10))
<class 'str'>
>>>
```

以上这些都是内置函数

而对于python的这个bytes，就是一个字节的序列，也就是一个一个字节来算的，可以结合地址的概念来理解，也可以记着，char是一个字节，int是4个，一个字节是8个比特位；
简单来说：
比如我定义一个s=b'0123'
其实就是0占一个字节，1占一个字节...并且**字节类型不支持修改**

而对于bytes的方法有很多，在官方的help下，对bytes就有385行，

```
>>> help(bytes)
```

Squeezed text (385 lines).

所以就说一点吧；

- bytes.fromhex（）
  直接用例子来说明吧

bytes.fromhex(“3034”)
结果是b’04’

然后对于

- hex（）
  bytes.hex(b’hello’)
  结果是’68656c6c6f’ 68->h 65->e 6c->l 6f->o

对于其他的题…正在补充