2020重庆市教育局网络安全攻防比赛

原创

Fstone2020 于 2020-09-15 23:49:47 发布 3232 收藏 9

分类专栏： CTF 文章标签： 密码学 信息安全

本文链接：https://blog.csdn.net/qq_42158602/article/details/108612053

一个卑微的web狗在角落瑟瑟发抖，又是一题未出。密码基本都是全秒。拿了一个一血，两个2血，misc基本和后面和队友一起做的，全是一步之遥。

想起这次的misc就睡不着，起来赶了一篇wp，记录一下。

有些题目的名字忘了，就写个序号。把将就看把，

crypto

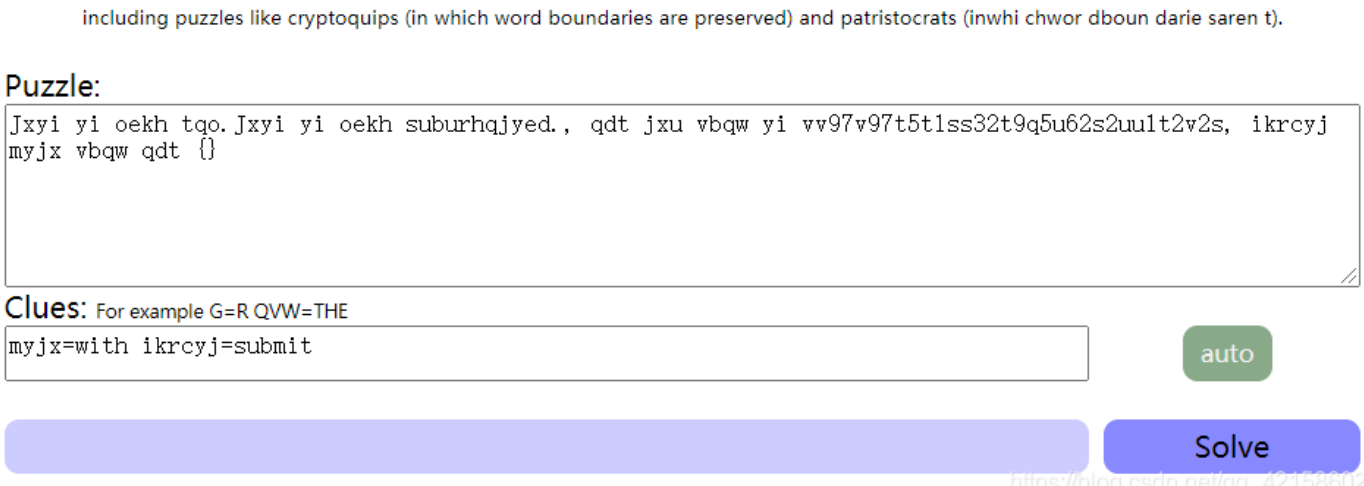
1

密文

Jxyi yi oekh tqo.Jxyi yi oekh suburhqjyed., qdt jxu vbqw yi vv97v97t5t1ss32t9q5u62s2uu1t2v2s, ikrcyj myjx vbqw qdt {}

该题是替换密码
直接用在线网站爆破

https://quipqiup.com/



多确定两个完整的单词后 结果就出来了

明文

This is your day.This is your celebration., and the flag is ff97f97d5d1cc32d9a5e62c2ee1d2f2c, submit with flag and {}

2 bullshit

这题是原题
安恒7月月赛

直接上代码

```
# flag = b'flag'

def pairing(a,b):
    shell = max(a, b)
    step = min(a, b)
    if step == b:
        flag = 0
    else:
        flag = 1
    return shell ** 2 + step * 2 + flag

def encrypt(message):
    res = ''
    for i in range(0,len(message),2):
        res += str(pairing(message[i],message[i+1]))
    return res

temp = '1186910804152291019933541010532411051999082499105051010395199519323297119520312715722'

fuzz = "abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ@_.<>?/;!$#{}-"
fuzz = list(fuzz)
print(fuzz)
flag = 'flag'
for k in range(20):
    for i in fuzz:
        for j in fuzz:
            flag_temp = flag + i + j
            # print(flag_temp)
            res = encrypt(flag_temp.encode('utf-8'))
            if res in temp:
                # print(res)
                # print(flag_temp)
                flag = flag_temp
    print(flag)
```

3

这题是一个base64的换表

直接附上一个b64加解密的脚本

```
# coding:utf-8

# s = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"


s = "PackmybxwthfivdzenlqorjugspACKMYBXWTHFIVDZENLQORJUGS0123456789+/"

def base64_encode(inputs):
    # 将字符串转化为2进制
    bin_str = []
    for i in inputs:
```

```
    for i in inputs:
        x = str(bin(ord(i))).replace('0b', '')
        bin_str.append('{:0>8}'.format(x))
    # print(bin_str)
    # 输出的字符串
    outputs = ""
    # 不够三倍数，需补齐的次数
    nums = 0
    while bin_str:
        # 每次取三个字符的二进制
        temp_list = bin_str[:3]
        # print(temp_list)
        if (len(temp_list) != 3):
            nums = 3 - len(temp_list)
            while len(temp_list) < 3:
                temp_list += ['0' * 8]
        temp_str = "".join(temp_list)
        # print(temp_str)
        # 将三个8字节的二进制转换为4个十进制
        temp_str_list = []
        for i in range(0, 4):
            temp_str_list.append(int(temp_str[i * 6:(i + 1) * 6], 2))
        # print(temp_str_list)
        if nums:
            temp_str_list = temp_str_list[0:4 - nums]

        for i in temp_str_list:
            outputs += s[i]
        bin_str = bin_str[3:]
    outputs += nums * '='
    print(outputs)


def base64_decode(inputs):
    # 将字符串转化为2进制
    bin_str = []
    for i in inputs:
        if i != '=':
            x = str(bin(s.index(i))).replace('0b', '')
            bin_str.append('{:0>6}'.format(x))
    # print(bin_str)
    # 输出的字符串
    outputs = ""
    nums = inputs.count('=')
    while bin_str:
        temp_list = bin_str[:4]
        temp_str = "".join(temp_list)
        # print(temp_str)
        # 补足8位字节
        if (len(temp_str) % 8 != 0):
            temp_str = temp_str[0:-1 * nums * 2]
        # 将四个6字节的二进制转换为三个字符
        for i in range(0, int(len(temp_str) / 8)):
            outputs += chr(int(temp_str[i * 8:(i + 1) * 8], 2))
        bin_str = bin_str[4:]
    print(outputs)



base64_decode('sIUXs3LUgSgUdjsHvIo5vbm2gSH3g2o3iTrXi2o3vjo3i2o0vx0=')
```

ps: 前几天刚把base64原理看了一下，顺便撸了一个能用的脚本

4 rsa

这题就是一个简单的rsa

直接上代码

```
import gmpy2
from Crypto.Util.number import getPrime,inverse,bytes_to_long,long_to_bytes

phi_t = 0x9360ce5eb573dcdb85af4cef9468a29323aa9d26f8cef9a2b004f3d9922c12c45f74b85c00db81fa34de4714a6a95b676618a3
ea8155df7095056c079531233f3e80cc372263ccaf4d42e5b7aa637586b673e30820a2d7eba201691371e138e4b3e45ed756cc6faac6e6f4
686dfb56e7fcd361ac312d0f7110e76f8fee5cff75894e8a2f4e50ffd0ef9db7f0eb685a6b3038892a96b355ea1d154b77db6e97a3facd36
dd8ee14b94cb98a21f4cea1412e7c72ea4cad530995ade3f5aae3444204dfc0d6ede436427
e= 0x2e43a6e5
n= 0x9360ce5eb573dcdb85af4cef9468a29323aa9d26f8cef9a2b004f3d9922c12c45f74b85c00db81fa34de4714a6a95b676618a3ea815
5df7095056c079531233f3e80cc372263ccaf4d42e5b7aa637586b673e30820a2d7eba201691371e138e4b3e45eda7d04ff5b6a850dd6c5d
5dcaab3588c8acc1b56794cbef1337664afd984d491d8134e3c1d661414278836b76e0de6a4e9a16f1c3f6abe86448dd065f317515d09888
955eba578c5579381f59a5355584d1b2003c93660ada247f13db12aadc74a6801803b
c= 0x49c627fa815685ad85060c0891e2cd04b5cd722cd82cc809835cb43da79b21ce547f4139da69a67e201c5f4643ff91306b92ae7d1e3
cc96a01e7074c7016058bf607038061fc3a99b6ac3ae1eaf6a3fddcc70303ed56281896183a4cd98c18e5f0378bf18d6a09c685c6fefdd0c
0914b4b22e183ac5c88d5674b54141ef8291855bc394296b8031c0b0b6ec26889871137b91224321bb0d2a89ae1cf84eeba9fe459d0b8dff
7fb1aadbae839956dfdfef5b0a8dbdfe8fd2613228e75f45195ee24cfa58b85a57e0f


pandq = (n-phi_t)//2+2
print(pandq)

phi = n-pandq+1
d = inverse(e,phi)
print(d)
m = pow(c,d,n)

print(long_to_bytes(m))
```

misc

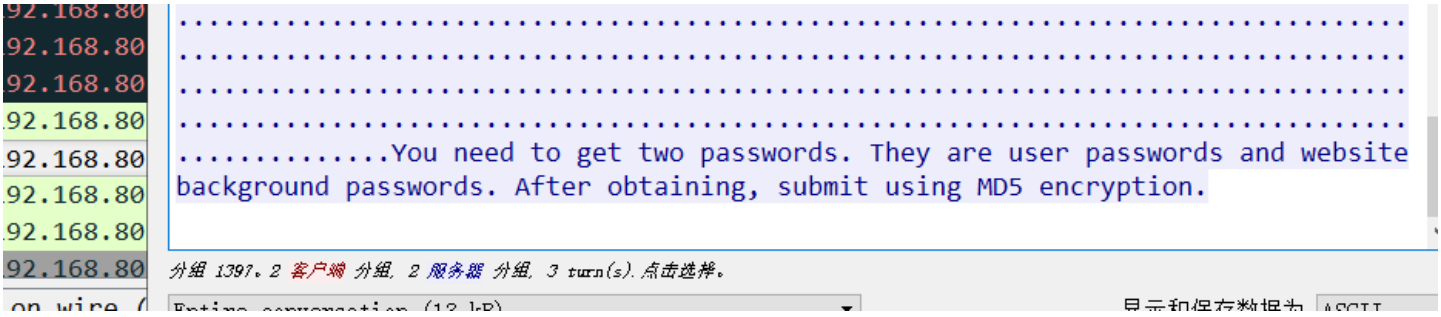
我们队一题没出，每题都差一点点，成功掉出前11 /哭

难啊~ 难啊~

1

给了一个包，直接丢进鲨鱼（英文忘了 别问我 反正就是一条鲨鱼）里面

在hint.php中找到提示 说需要两个密码，然后两个密码的的md5作为flag提交



看见两个php伪协议读取两个文件

```
430 GET /css/bootstrap.css HTTP/1.1
563 GET /contact.php HTTP/1.1
568 GET /about.php?file=php://filter/read=string.rot13/resource=/etc/shadow HTTP/1.1
574 GET /about.php?file=php://filter/read=convert.base64-encode/resource=test.sql HTTP/1.1
576 GET /about.php?file=php://filter/read=convert.base64-encode/resource=footer.php HTTP/1.1
526 GET /about.php?file=index.php HTTP/1.1
```

/etc/shadow中得到第一个密码 但是是加密的 用

```
pgs:$6$NXa3ixa0$MWZrFvwSm2VoRLIg5twVGZmJtWqX4PIcdxyC.4mWidRnYgy3HmZ1lejm63mnUG3YrcNZmzszdujiGRnmBRZFE1:18345:0:99999:7:::
```

用 John the Ripper 工具进行解密， 我们没有解出来 /哭
kali自带 不用另行下载

据说解出来是

> newcount

第二个在sql中

通过sql可以看见 创建了一个admin表，插入了一条数据

```
drop database if exists `test`;
create database `test`;
use test;

DROP TABLE IF EXISTS `admin`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `admin` (
  `user_id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `user_name` varchar(255) NOT NULL DEFAULT '',
  `user_pass` varchar(255) NOT NULL DEFAULT '',
  PRIMARY KEY (`user_id`)
) ENGINE=MyISAM AUTO_INCREMENT=4 DEFAULT CHARSET=utf8;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `admin`
--

LOCK TABLES `admin` WRITE;
/*!40000 ALTER TABLE `admin` DISABLE KEYS */;
INSERT INTO `admin` VALUES (1,'admin','AA00A');
/*!40000 ALTER TABLE `admin` ENABLE KEYS */;
UNLOCK TABLES;

--
-- Table structure for table `news`
--

DROP TABLE IF EXISTS `news`;
```

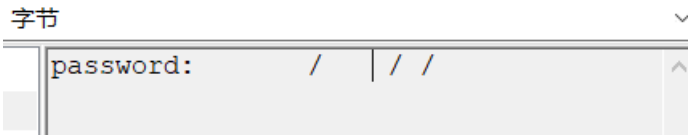

所以 第二个密码是

> AA00A

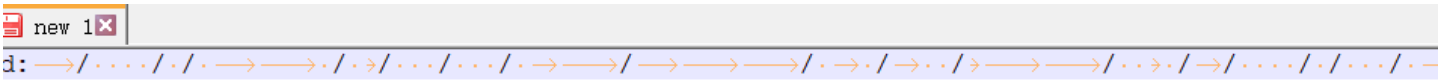
把两个合起来md5一下就行了

2 flag.rar

这有个password的提示



查看 不可见字符 发现是莫斯加密



解出
THEPASSWORDOFTHESAFEIS???

做到这里我们就开始爆破4位密码，爆破了5 6个小时没一点动静 / 难受

结果应该是还要加上前面 /哭了

3 一道杂项题

这题真的可惜 了，比赛中我都点进了那个介绍pyc隐写的文章了，然后没看，去做领另外两道杂项了。 群里一说，我一百度，还是那篇文章 。 淦！ /吐血

flag.pyc 反编译后没啥看的 就是一个base58的加密解密程序，给了一个密文，提示flag在pyc中

直接用工具stegosaurus解密

工具介绍
https://www.freebuf.com/sectool/129357.html

直接用那个命令使用有点问题 附上我在win10试出来的命令

> python3 .\stegosaurus.py .\flag.pyc -x

赛后才出来 /气