MISC

- Base全家福
  由题目可知为base系列解码，先将将密文
  R1k0RE1OWldHRTNFSU5SVkc1QkRLTlpXR1VaVENOUlRHTVlETVJCV0dVMlVN
  TlpVR01ZREtSUlVIQTJET01aVUdSQ0RHTVpWSVlaVEVNWlFHTVpER01KWElR
  PT09PT09
  进行base64解码得到
  GY4DMNZWGE3EINRVG5BDKNZWGUZTCNRTGMYDMRBWGU2UMNZUGMYD
  KRRUHA2DOMZUGRCDGMZVIYZTEMZQGMZDGMJXIQ======
  再进行base32解码得到
  6867616D657B57653163306D655F74305F4847344D335F323032317D
  最后进行base16解码得到
  flag: hgame{We1c0me_t0_HG4M3_2021}

- 不起眼压缩包的养成的方法
  首先拿到图片，查看其属性。在备注中发现：Secret hidden IN picture.于是想到图片中藏了一个压缩包。用ubuntu使用foremost将图片分离，得到一个加密压缩包。密码未知，想到寻找密码。将图片拖入winhex，得到密码的信息。

0x4qE_03a7087b48c94b748a...

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	ANSI ASCII
00630840	53	A4	A8	57	F4	0D	C6	66	C9	AA	73	BB	D4	9D	S¤¨Wô ÆfÉªs»Ô
00630854	3F	18	7D	50	E9	5C	73	C0	5E	D4	42	DB	2D	6D	? }Pé\sÀ^ÔBÛ-m
00630868	56	37	69	7D	01	BE	23	60	1B	9C	B0	50	4B	01	V7i} ¾#` œ°PK
00630882	02	14	00	14	00	09	00	00	00	09	B3	3C	52	1C	³<R
00630896	00	D9	AF	7F	00	00	00	73	00	00	00	0F	00	24	Ù¯ s $
00630910	00	00	00	00	00	00	00	20	00	00	00	00	00	00	
00630924	00	4E	4F	20	50	41	53	53	57	4F	52	44	2E	74	NO PASSWORD.t
00630938	78	74	0A	00	20	00	00	00	00	00	01	00	18	00	xt
00630952	1A	D8	33	42	81	F5	D6	01	87	A6	F6	9E	44	F6	Ø3B õÖ ‡¦öžDö
00630966	D6	01	D9	A8	F7	D3	7C	F5	D6	01	50	4B	01	02	Ö Ù¨÷Ó|õÖ PK
00630980	14	00	14	00	09	00	00	00	C0	AC	3D	52	5D	0F	À¬=R]
00630994	B7	0B	41	03	00	00	35	03	00	00	09	00	24	00	· A 5 $
00631008	00	00	00	00	00	00	20	00	00	00	AC	00	00	00	¬
00631022	70	6C	61	69	6E	2E	7A	69	70	0A	00	20	00	00	plain.zip
00631036	00	00	00	01	00	18	00	C0	F4	D1	F4	43	F6	D6	ÀôÑôCöÖ
00631050	01	91	23	D3	9D	44	F6	D6	01	73	1D	D1	F4	43	'#Ó DöÖ s ÑôC
00631064	F6	D6	01	50	4B	05	06	00	00	00	00	02	00	02	öÖ PK
00631078	00	BC	00	00	00	14	04	00	00	2A	00	EF	BB	BF	¼ * ï»¿
00631092	50	61	73	73	77	6F	72	64	20	69	73	20	70	69	Password is pi
00631106	63	75	72	65	20	49	44	2E	20	28	55	70	20	74	cure ID. (Up t
00631120	6F	20	38	20	64	69	67	69	74	73	29				o 8 digits)

  可知密码为8位，archpr爆破得密码为70415155，打开压缩包中的txt文件，发现一段英文。先放着，然后打开plain.zip，发现里面有flag.zip和之前一样的txt。由此想到明文攻击。将上个压缩包的txt文件压缩成zip形式作为明文文件，将flag.zip作为攻击对象。但是会报“在选定的档案中没有匹配的文件”错。可知压缩类型出错，联想到

txt中的"By the way, I only storge it",将txt的选择存储的压缩形式，攻击成功。得到口令C8uvP$DP。打开flag.zip，得到加密的flag.txt。将文件拖入winhex得到一串密文。html解密后得到flag。

flag:hgame{2IP_is_Usefu1_and_Me9umi_i5_W0r1d}

- Galaxy

  wireshark打开附件，分析http得到galaxy.png。查看图片属性，没发现flag，看到图片的宽高不同，由此想到修改图片的宽高。将图片拖入winhex进行修改，得到flag，但是图片中的显示的不是完整的flag，导致交的时候交了很多次，最后发现是漏了下划线。

  flag:hgame{Wh4t_A_W0nderfu1_Wa11paper}

- Word RE:MASTER

  打开文件，看到brain fuck,首先想到brain fuck与后面的一串英文字符相结合，但是挣扎一段时间后无果。开始各种尝试，比如word隐藏字符之类的。在将word拖入winhex之后发现16进制文件头为50 4B 也就是压缩包的形式。改文件后缀名为zip，在压缩包中寻找到许多brainfuck类型的密文，连接后，用brainfuck解码得到maimai.docx的密码：DOYOUKNOWHIDDEN?

  打开文件后得到一张图片，其他什么都没有。但是查看到有word隐藏的字符，是几行空白字符，联想图片的提示，百度得snow解密。下载专门解密的snow.exe文件，将密文复制进txt文件。将txt文件与snow.exe放在同一目录下，执行

  ```
  或批处理文件。

  C:\Users\user>D:\ctf\misc\snow\SNOW.EXE -C D:\ctf\misc\snow\1.txt
  hgame{Cha11en9e_Whit3_P4ND0R4_P4R4D0XXX}
  ```

  得到flag。

  flag:hgame{Cha11en9e_Whit3_P4ND0R4_P4R4D0XXX}

WEB

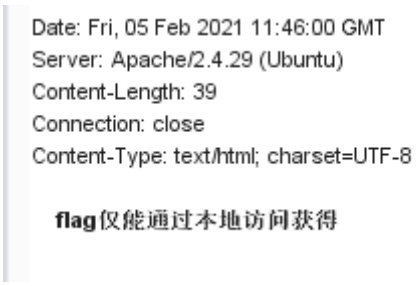
- Hitchhiking_in_the_Galaxy

  bp抓包，将HitchhikerGuide.php包send to repeater,将请求改为post。按照要求将user-agent改为指定引擎后出现

  ```
  HTTP/1.1 200 OK
  Date: Fri, 05 Feb 2021 11:43:47 GMT
  Server: Apache/2.4.29 (Ubuntu)
  Vary: Accept-Encoding
  Content-Length: 148
  Connection: close
  Content-Type: text/html; charset=UTF-8

  你知道吗？<a href="https://github.com/wuhan005">茄子</a>特别要求：你得从他的<a
  href="https://cardinal.ink/">Cardinal</a>过来
  ```

  将referer后面改为https://cardinal.ink/



添加X-Forwarded-For: 127.0.0.1，伪造访问ip
得到flag。
flag: hgame{s3Cret_0f_HitCHhiking_in_the_GAl@xy_i5_dOnT_p@nic!}

- watermelon
  按F12，修改页面布局，然后靠物理外挂（拖动左右窗口）强行玩到2000分（虽然有点舍不得，毕竟第一次这么高，但还是自爆了），然后网页弹出flag
  不过正常应该是js修改做的，事后百度了。

flag: hgame{do_you_know_cocos_game?}

- 智商检测鸡
  做了一百道定积分，然后得到了flag。。。。。。
  做的时候，由于每次定积分的类型差不多，于是写了一个简单的脚本
  ' ' '
  int main(){
  double a,b,c,e,f;
  scanf("%lf%lf%lf%lf",&a,&b,&e,&f);
  c=a*0.5*(e*e-f*f)+b*(e-f);
  printf("%.2f",c);
  return 0;
  }
  ' ' '
  a,b,c,d,口算然后带入。

RE

- helloRe
  将文件拖入ida，根据判断语句找到main函数

```
  v12 = 15i64;
  LOBYTE(Memory) = 0;
  v1 = sub_1400017C0(std::cout, "hello, enter your flag please!");
  v2 = std::basic_ostream<char,std::char_traits<char>>::operator<<(v1, sub_140001990);
  sub_1400017C0(v2, "> ");
  sub_140001BD0(std::cin, &Memory);
  sub_1400017C0(std::cout, "checking flag ");
  sub_140001290(200i64);
  if ( v11 != 22 )
LABEL_13:
    sub_140001480();
  v3 = v12;
  v4 = (void **)Memory;
  do
  {
    v5 = &Memory;
    if ( v3 >= 0x10 )
      v5 = v4;
    if ( (*((_BYTE *)v5 + v0) ^ (unsigned __int8)sub_140001430()) != byte_140003480[v0] )
      goto LABEL_13;
    ++v0;
  }
  while ( v0 < 22 );
  v6 = std::basic_ostream<char,std::char_traits<char>>::operator<<(std::cout, sub_14000199
  v7 = sub_1400017C0(v6, &unk_140003470);
  std::basic_ostream<char,std::char_traits<char>>::operator<<(v7, sub_140001990);
  if ( v3 >= 0x10 )
```

根据判断语句可知flag逐位与sub_140001430的值异或等于byte_140003480各位的值，sub_140001430的值为FF,byte_140003480各位值为97h, 99h, 9Ch, 91h, 9Eh, 81h, 91h, 9Dh, 9Bh, 2 dup(9Ah)，ABh, 81h, 97h, 0AEh, 80h, 83h, 8Fh, 94h, 89h, 99h，97h。异或得到flag

flag:hgame{hello_re_player}

- pypy

  由代码可知为py字节码，百度相关知识，一步步吃力地翻译。得到一段代码，分析可得大致加密方法

  然后运行脚本：

  ```
  s='30466633346f59213b4139794520572b45514d61583151576638643a'
  cipher=''
  text=''
  for i in range(0,len(s)//2):
  cipher+=chr(int(s[2*i:2*i+2],16)^i)
  for i in range(0,len(cipher)//2):
  text=text+cipher[2*i+1]+cipher[2*i]
  print(text)
  ```

  flag:hgame{G00dj0&_H3r3-I Y@Ur_ L@G!~!~}

PWN

- whitegive
  分析代码，可知password为程序中"paSsw0rd"的值，将第二个文件拖入ida，找到对应的值

```
.rodata:000000000040200E aLd             db '%ld',0             ; DATA XREF: main+39↑o
.rodata:0000000000402012 aPassw0rd       db 'paSsw0rd',0        ; DATA XREF: main+51↑o
```

  转为10进制得password：4202514
  nc连接，输入密码，cat flag

```
leon@leon-virtual-machine:~$ nc 182.92.108.71 30210
password:4202514
you are right!
ls
bin
dev
flag
lib
lib32
lib64
usr
whitegive
cat flag
hgame{W3lCOme_t0_Hg4m3_2222Z222zO2l}
SS
```

Crypto

- まひと
  摩斯密码解码，ascii码转换
  base 64
  Vigenere-Liki:}VkmvJb!1XtAxe!hpM1{M+9xqzrTM_Nj~cRg4x
  维吉尼亚
  }KccnYt!1NlPpu!zeE1{C+9pfrhLB_Fz~uGy4n
  栅栏6位
  }!!Ch~K1z+LucNe9BGclEp_ynP1fF4Yp{rzntu
  左右反转
  utnzr{pY4Ff1Pny_pElcGB9eNcuL+z1K~hC!!}
  凯撒13
  hgame{cL4Ss1Cal_cRypTO9rAphY+m1X~uP!!}
- transformer
  爆破txt内容得：The lift bridge console system has only used password login since 2003, the password is "hgame{ea5y_f0r_fun^3nd&he11o_}",Don't forget to add the year at the end.
  flag:hgame{ea5y_f0r_fun^3nd&he11o_2021}