HBCTF——WriteUp&&涨姿势（4）

原创

浅零半泣 于 2017-06-04 22:27:35 发布 580 收藏

分类专栏： CTF

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/sinat_34200786/article/details/72862165

版权

CTF 专栏收录该内容

19 篇文章 0 订阅

订阅专栏

WriteUp

1. 签到
2. 初恋

涨姿势

1. 给我flag吧

签到

原题

解题思路

```
签到无需太费神
```

打开链接看看再说

点击我获取flag

http://blog.csdn.net/sinat_34200786

惯例，右键源代码，发现关键字

```
<!DOCTYPE html PUBLIC -//W3C//DTD XHTML 1.0 Transitional//EN http://www.w3.org/TR/xhtml1/hbctf123hell0qd125.dtd>
<html xmlns:pcat>
<head>
    <meta charset="UTF-8">
    <title>这是签到题</title>
    <style>
        pcat\:input{
            font-size: 24px;
            font-weight: bold;
            color:red;
            text-decoration:underline;
        }
    </style>
</head>
 <body onload="xxoo()">
    <pcat:input id="pseudocat" value="点击我获取flag" onclick="flag()" type="button"></pcat:input>

    <script type="text/javascript">
        function xxoo(){
            var xx=document.getElementById("pseudocat");
            xx.innerHTML=xx.getAttribute("value");
        }

        function flag(){
            alert("想多了。BTW，出题人的web水平太差了，¬_¬");
        }

        function no_key(){
            window.win = window.open("http://www.chamd5.org");
            setTimeout("ooxx()",2000);
        }

        function ooxx(){
            flag();
            document.write('\x3c\x74\x69\x74\x6c\x65\x3e\x66\x6c\x61\x67\x5f\x69\x73\x5f\x6e\x6f\x74\x5f\x68\x65\x72\x65\x3c\x2f\x74\x69\x74\x6c\x65\x3e');
        }
    </script>
</body>
</html>
```

http://blog.csdn.net/sinat_34200786

其实套路就在这里，很多人连签到都没做出来就是因为对ASCII码不敏感，'123he110qd125' 中的两个数字很明显是对应的123—'{

初恋

原题

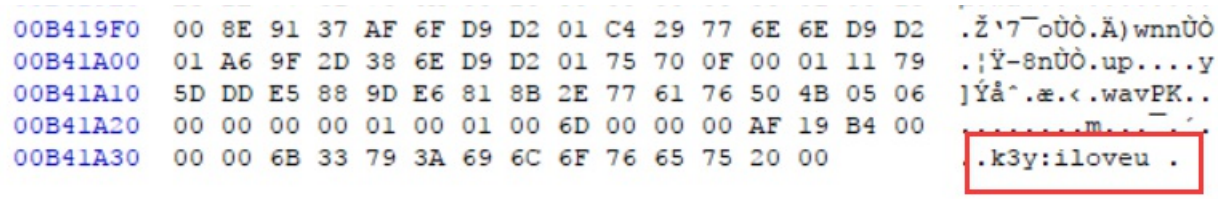
http://blog.csdn.net/sinat_34200786

解题思路

也许需要一个工具

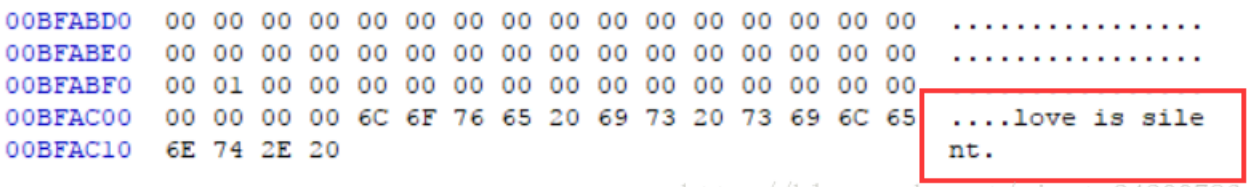
WriteUp

惯例拿到数据先仍HxD里面，意外发现key



http://blog.csdn.net/sinat_34200786

解压得到的WAV也仍HxD里看看，获得神秘提示

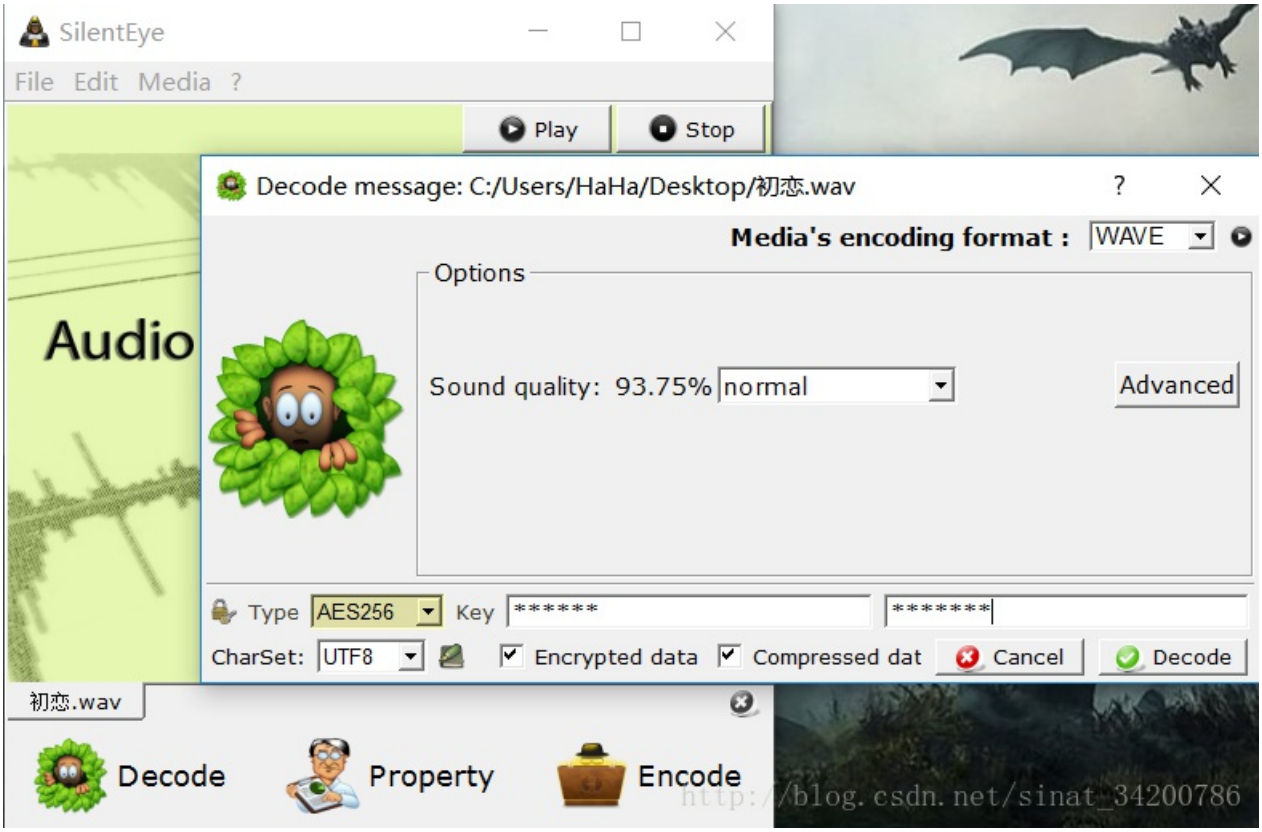


http://blog.csdn.net/sinat_34200786

先是用Audacity一阵折腾，没有发现有价值的东西，这时才想起神秘提示，搜一下看看

http://blog.csdn.net/sinat_34200786

原来是SlientEye，下载个玩玩，key就是最开始得到的key



得到个flag.txt

打开，发现是base64编码，解码即可

备注

```
很多人在解这题时都不知道key在哪，而我一早就发现了key却不知道在哪用，直到后来发现了SlientEye。。
```

给我flag吧

原题

解题思路

```
改分离出来的数据就分离出来，然后需要一点脑洞？
```

WriteUp

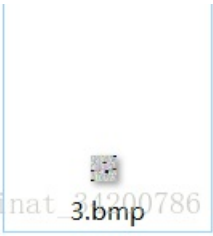
```
解压出图片后仍Binwalk里看看
```

```
root@kali: ~
文件(F)  编辑(E)  查看(V)  搜索(S)  终端(T)  帮助(H)
root@kali:~# binwalk 给我flag吧.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
30            0x1E            TIFF image data, big-endian, offset of first image
 directory: 8
10331         0x285B          JPEG image data, EXIF standard
10343         0x2867          TIFF image data, big-endian, offset of first image
 directory: 8
11089         0x2B51          Copyright string: "Copyright (c) 1998 Hewlett-Pack
ard Company"
23541         0x5BF5          Copyright string: "Copyright (c) 1998 Hewlett-Pack
ard Company"
33644         0x836C          Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#">
 <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xml
ns:stEvt=
111600        0x1B3F0         PC bitmap, Windows 3.x format,, 16 x 16 x 24

root@kali:~#
```

http://blog.csdn.net/sinat_34200786

里面有一张JPG，一张BMP图，用HxD分离出来分析

1.jpg



3.bmp

og.csdn.net/sinat_34200786

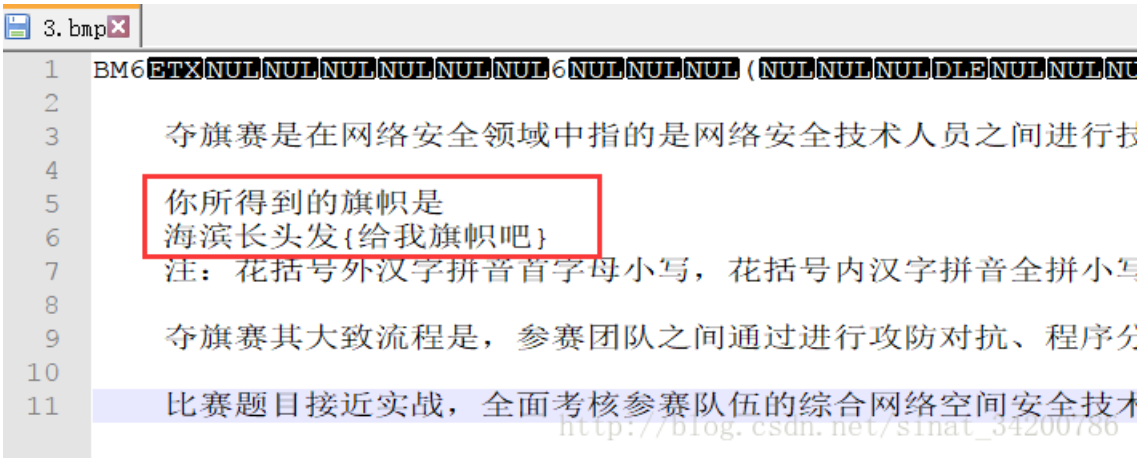
分析结果如何呢？HxD没发现，Stegosolve没发现，最后Ps都上了也没发现
怎么看这都是很正常的图片

再检查一遍可以发现Bmp图片的数据偏少

```
000002D0  BD A1 A3 B4 CB B4 CE B1 C8 C8 FC C4 DC B9 BB B6  ½¡£´Ë´Î±ÈÈüÄÜ¹»¶
000002E0  CD C1 B6 D1 A1 CA D6 B5 C4 CD F8 C2 E7 BF D5 BC  ÍÁ¶Ñ¡ÊÖµÄÍøÂç¿Õ¼
000002F0  E4 B0 B2 C8 AB BC BC CA F5 A3 AC C8 C3 B2 CE C8  ä°²È«¼¼Êõ£¬ÈÃ²ÎÈ
00000300  FC D1 A1 CA D6 CD A8 B9 FD B1 C8 C8 FC B7 A2 CF  üÑ¡ÊÖÍ¨¹ý±ÈÈü·¢Ï
00000310  D6 D7 D4 BC BA B5 C4 C8 B1 CF DD A3 AC BF C9 D2  Ö×Ô¼ºµÄÈ±ÏÝ£¬¿ÉÒ
00000320  D4 D3 D0 C4 BF B5 C4 B2 E9 C2 A9 B2 B9 C8 B1 A1  ÔÓÐÄ¿µÄ²éÂ©²¹È±¡
00000330  A3 00 00 00 00 00                                 £.....
```

http://blog.csdn.net/sinat_34200786

这时用notepad看看？



涨姿势点

将数据用GBK编码后再加上一个BMP文件头使文件看起来就是一个BMP图像文件，做多了隐写题的人反而可能做不出