# 第一次队内赛的writeup

原创

yvan的魔仙堡 于 2019-12-15 17:23:38 发布 65 收藏



这周五是第一次的队内赛，也是我第一次正式的参加一次ctf的比赛

签到题就太简单了就不讲了，简单的Crypto也就是rot13而已

然后吉奥万·巴蒂斯塔·贝拉索那题的话还真不知道就去百度了下

然后发现其实是维吉尼亚加密。

刚刚开始并没有发现有个加密密码给我们的

然后其实也是可以做的 因为那个flag的格式已经提前告知 根据flag的开头格式和加密内容的头三个字母，就可以把加密密码给求出来

然后那倒md安全性的题目上图

```php
<?php
highlight_file('index.php');
include("flag.php");
if(isset($_GET['v1'])  &&  isset($_GET['v2'])  &&  isset($_GET['v3'])){
        $v1  =  $_GET['v1'];
        $v2  =  $_GET['v2'];
        $v3  =  $_GET['v3'];
        if($v1  !=  $v2  &&  md5($v1)  ==  md5($v2)){
                if(!strcmp($v3,  $flag)){
                        echo  $flag;
                }
        }
}
```



三个且 然后strcmp 大致就是让v3=flag 然后才会返回flag

百度了下这两个函数

有个md5()函数漏洞和strcmp()函数漏洞的利用

构造下数组 ?v1[]=1&v2[]=2&v3[]=1

http://10.9.20.12:32234/?v1[]=1&v2[]=2&v3[]=1

返回正确答案

```php
<?php
highlight_file('index.php');
include("flag.php");
if(isset($_GET['v1'])  &&  isset($_GET['v2'])  &&  isset($_GET['v3'])){
        $v1  =  $_GET['v1'];
        $v2  =  $_GET['v2'];
        $v3  =  $_GET['v3'];
        if($v1  !=  $v2  &&  md5($v1)  ==  md5($v2)){
                if(!strcmp($v3,  $flag)){
                        echo  $flag;
                }
        }
}
```

TSW{Md5_1s_n0t_safe}

然后接下来就是misc的题目




刚刚看见就有点懵逼，然后一百度 有这么一个网站

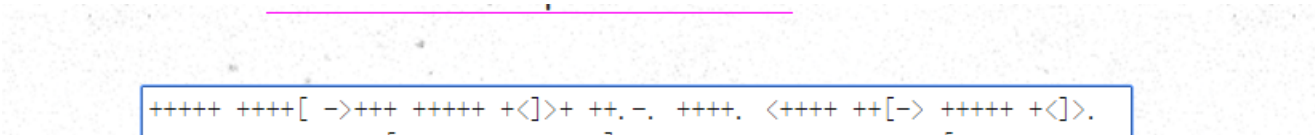
作者：蓝色的风之精灵；真米神表示对此工具的非法使用概不负责。
由 KeyFansClub 我们的梦想 提供，更多精彩不容错过！

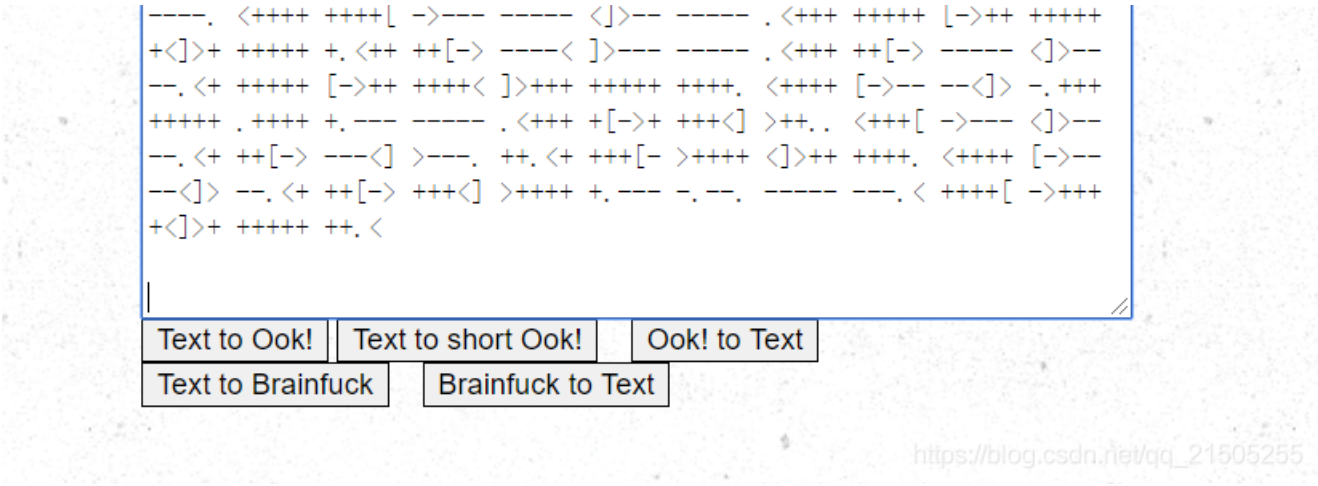


然后按照这个“佛”的解析
得出这么一串
GU2DKMZVG43WENBSGYYTKMZWGU2WMMZTGMYTGNRTGI3WI===
base16 base64都不行 然后base32试了就ok
解密出来是一串十六进制 那时候盯着看了半天还以为还有一重什么加密呢？
然后就是简单的十六进制转asc码
ok！




这么一道题目 百度下原来有个bugku？？？？？然后用的是一个brainfuck
日脑解密







又是一道送分题，哈哈哈哈哈
然后是这么一道题，看下图



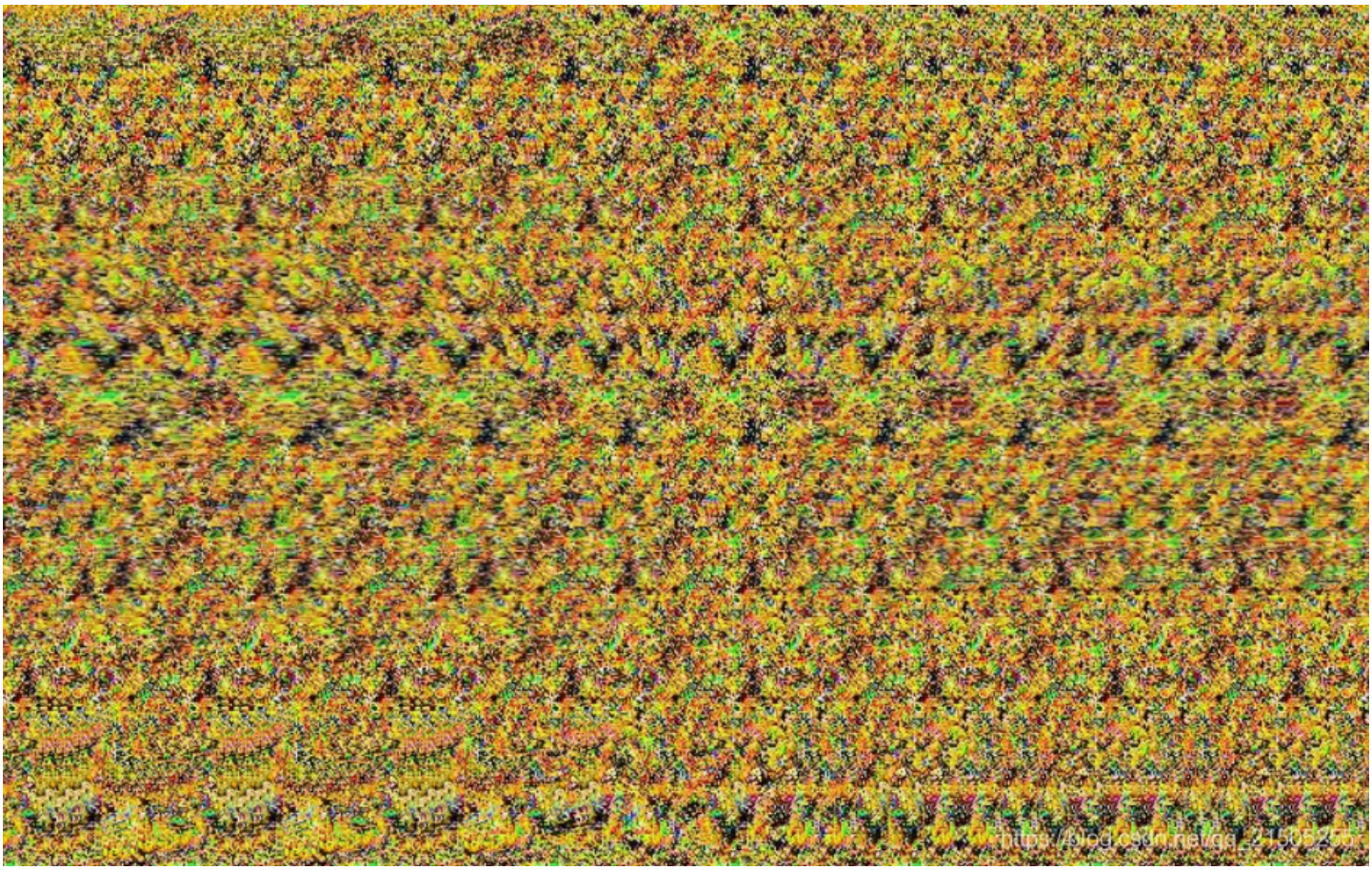
然后就是一个ppt文件，刚刚开始想还以为是ppt里面有图片然后是图片隐写的内容
然后打开ppt把里面的内容拖啊拖

拨开云雾见真相

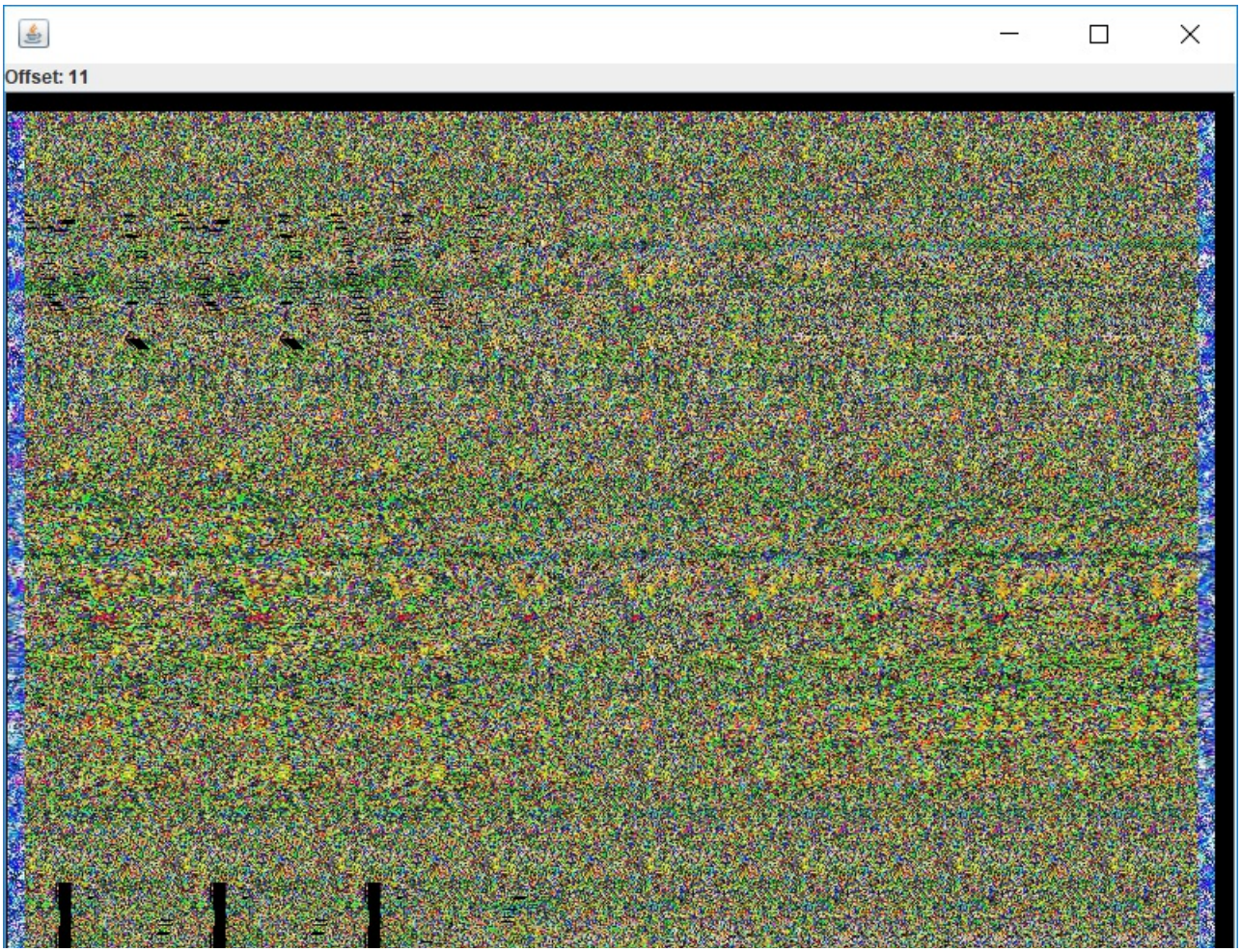

然后十六进制打开，里面有一个flag.txt文件
打开kali
binwalk -e root/desktop/FlyPig.pptx
ok然后对应文件夹下面会有一个文件夹里面就会有一个flag.txt文件
就是有点恶心 都是回车
然后是一张图片题

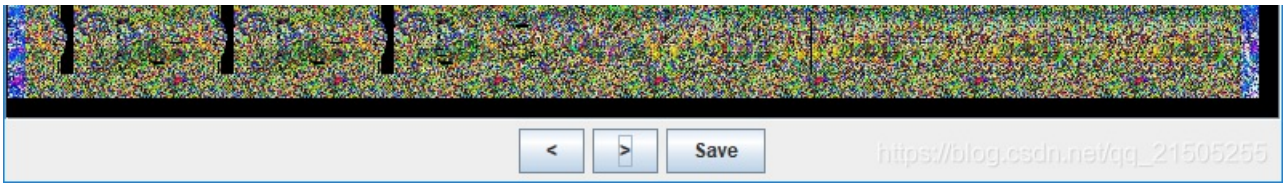
---


先鉴一下黄看看图片是不是色图

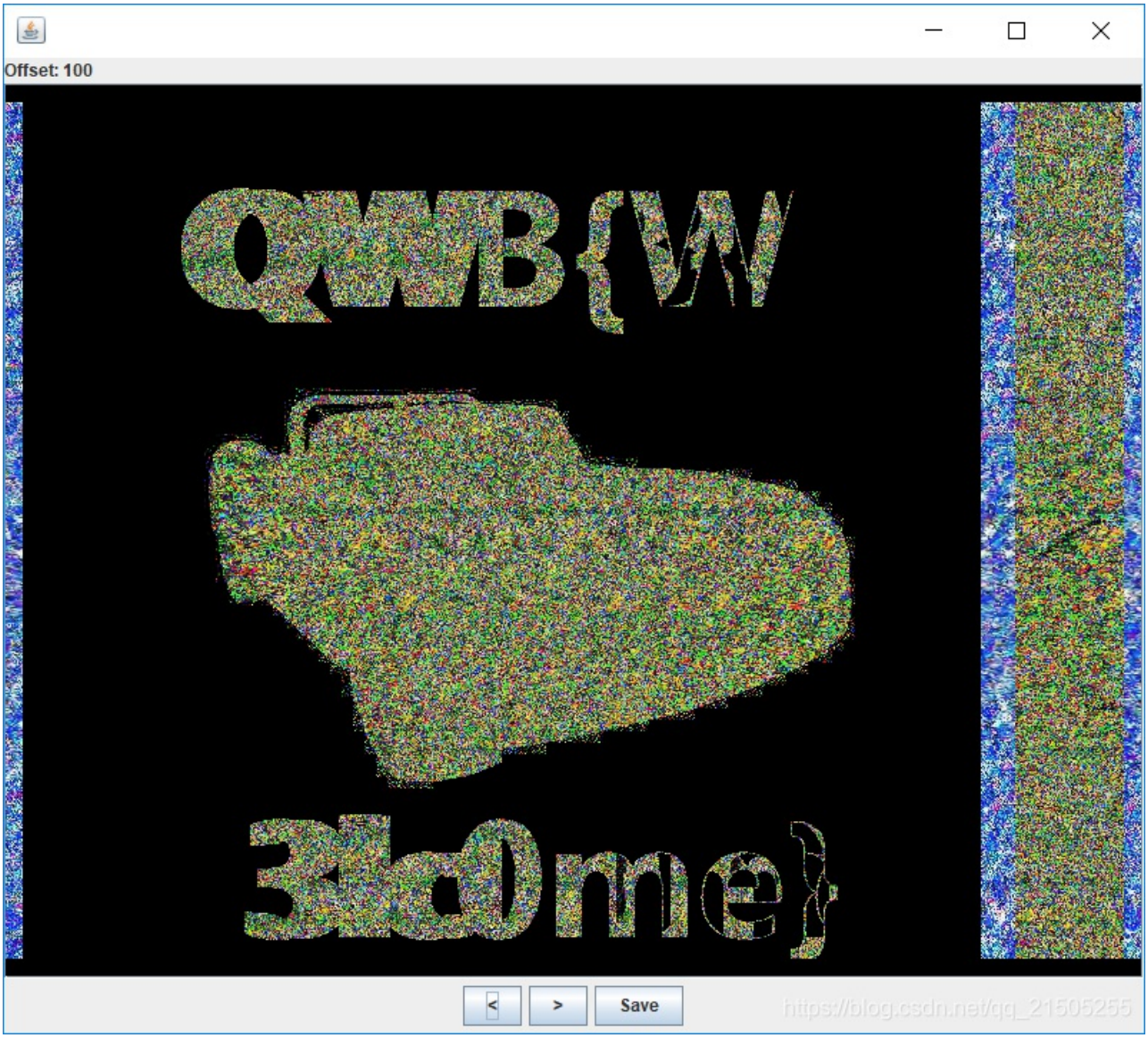


这图有点黄啊
工具提示stegsolve
在这里插入图片描述






我就慢慢移吧
在这里插入图片描述




ok
这就出来
然后是这么一道题目

ん
鳴神の　少しとよみて　降らずとも　我は止まらん　妹し留めば
以上内容与答题无关

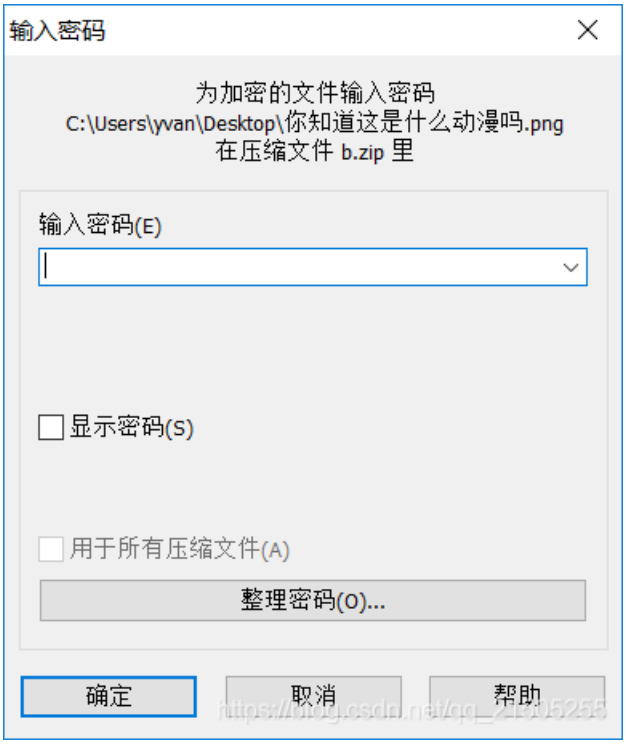

Flag

Submit



这也不是色色的图片
习惯性看下详情信息


有个password
？谁的password？
改成zip试试




果然需要一个秘钥

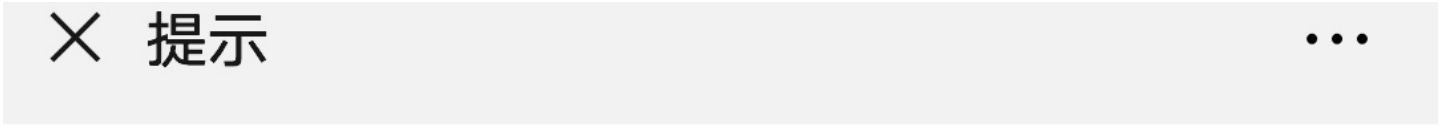
password输入

错误？

全部输入进去

OK

里面是一个二维码
打开微信扫一扫直接出结果




已扫描到以下内容

言の葉の庭

TSW{Noting_for_nothing}

扫描所得内容并非微信提供，请谨慎使用

如需使用，可通过复制操作获取内容

详情 | 举报



nice