

第一次队内赛的writeup

原创

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

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 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/qq_21505255/article/details/103550009

版权

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
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;
        }
    }
}
```

https://blog.csdn.net/qq_21505255

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

返回正确答案

```
<?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

Challenge 6 Solves ×

小明向佛祖许愿

200

佛曰：梵以竟麼智幡三陀侄者諳呼寫鉢參俱者冥死蘇侄訶殿密
 蒙侄尼闍冥有呐地怯大怯世哆夷苦藝哆輸哆吉三罰數俱摩諳漫
 寫奢神奢悉哆特幡孕即真罰麼佛殿怯蒙侄沙侄都罰帝神罰提侄
 知神逝隸奢心冥伽夜罰夜幡闍怯蒙陀朋得竟鉢真得楞參謹隸奢
 朋哆波迦實伊藝瑟怯闍遠藐伽故梵怖俱怛陀究梵涅數羅怯謹隸
 侄明諳智罰想瑟罰提那麼哆一者醯冥蘇礙梵盧咒滅鉢等幡滅幡
 除鉢心俱遠梵隸奢有沙

View Hint

Flag

Submit

刚刚看见就有点懵逼，然后一百度 有这么一个网站

与佛论禅

施主，此次前来，不知有何贵干？

听佛说宇宙的真谛

参悟佛所言的真意

普度众生

面对这个纷繁复杂的世界，
真米神会如何作答呢.....

佛家妙语

作者: [蓝色的风之精灵](#); 真米神表示对此工具的非使用概不负责。

由 [KeyFansClub 我们的梦想](#) 提供, 更多精彩不容错过!

https://blog.csdn.net/qq_21505255

然后按照这个“佛”的解析

得出这么一串

GU2DKMZVG43WENBSGYTKMZWGU2WMMZTGMYTGNRTGI3WI===

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ascii码

ok!

Challenge

7 Solves

×

喜欢学编程的小明

200

小明今日在研究一种新的编程语言, 叫□□□。我有点蒙这究竟是什么呢? +++++ +++++[->+++ +++++ +<]>+ +.+. +++++.

<++++ ++[-> +++++ +<]>. ----. <++++ +++++[->----<]>----

.<+++ +++++ [->++ +++++ +<]>+ +++++ +.<+ +[-> ----<]>---

---- .<+++ +[-> ----<]>--- --.<+ +++++ [->++ +++++<]>+++

+++++ +++++. <++++ [->---<]> -.+++ +++++. +++++ +.-----.

<+++ +[->+ +++++<]>+.. <++++ [->----<]>--- --.<+ +[-> ----<]>---

++.<+ +++++[->++++<]>+ +++++. <++++ [->----<]> --.<+ +[->

++++<]>+++++ +.--- --.---- --.< +++++ [->+++ +<]>+ +++++ ++.<

Flag

Submit

https://blog.csdn.net/qq_21505255

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

```
+++++ +++++[->+++ +++++ +<]>+ +.+. +++++. <++++ ++[-> +++++ +<]>.
```

```
----- . <++++ +++++ [ ->--- ----- <J>-- ----- . <+++ +++++ [->++ +++++
+<J>+ +++++ +. <+ + [-> ----- < ]>----- ----- . <+++ + [-> ----- <J>--
-- . <+ +++++ [->+ +++++< ]>+ +++++ +++++. <++++ [->-- --<J> - . + +
+++++ . +++++ +. --- ----- . <+++ + [->+ +++++< ]>+ . <+++ [->--- <J>--
-- . <+ + [-> ---<J> >---. ++. <+ + + [-> +++++ <J>+ +++++. <++++ [->--
--<J> --. <+ + [-> +++++< ]>+ +++++ +. --- -. ---. ----- ---. < +++++ [->+ +
+<J>+ +++++ ++. <
```

Text to Ook!	Text to short Ook!	Ook! to Text
Text to Brainfuck	Brainfuck to Text	

https://blog.csdn.net/qq_21505255

又是一道送分题，哈哈哈哈哈
然后是这么一道题，看下图

Challenge 7 Solves ×

小明发ppt来嘲笑我

200

人类的本质是复读机，那ppt的本质又是什么呢？提交格式:TSW{flag}

[FlyPig.pptx](#)

Flag Submit

https://blog.csdn.net/qq_21505255

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



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

Challenge 5 Solves X

看我会乾坤大挪移

300

图片类题手中常被Stegsolve工具是有好处的哦。

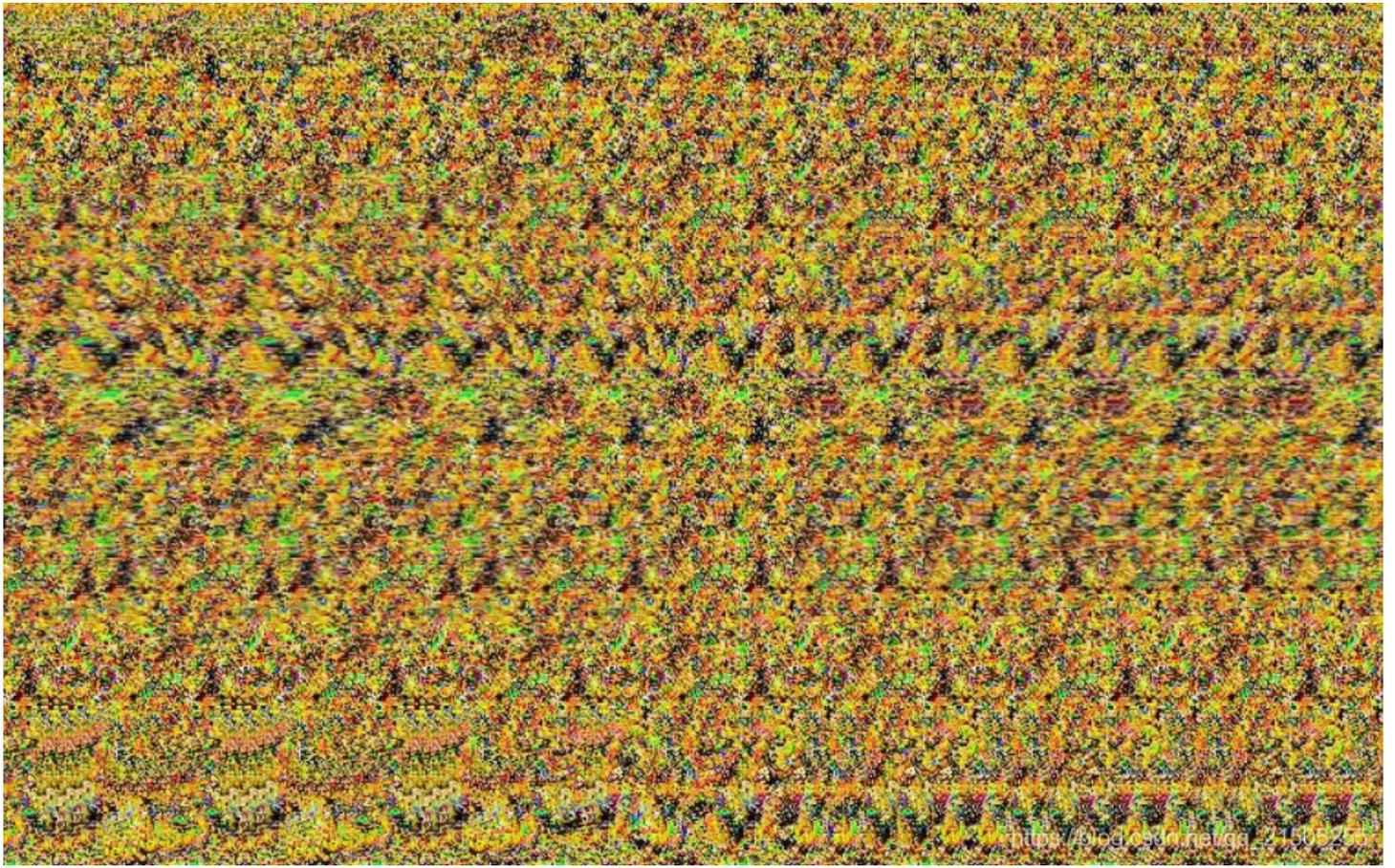
8140912-2d...

Flag Submit

https://blog.csdn.net/qq_21505255

先鉴一下黄看看图片是不是色图

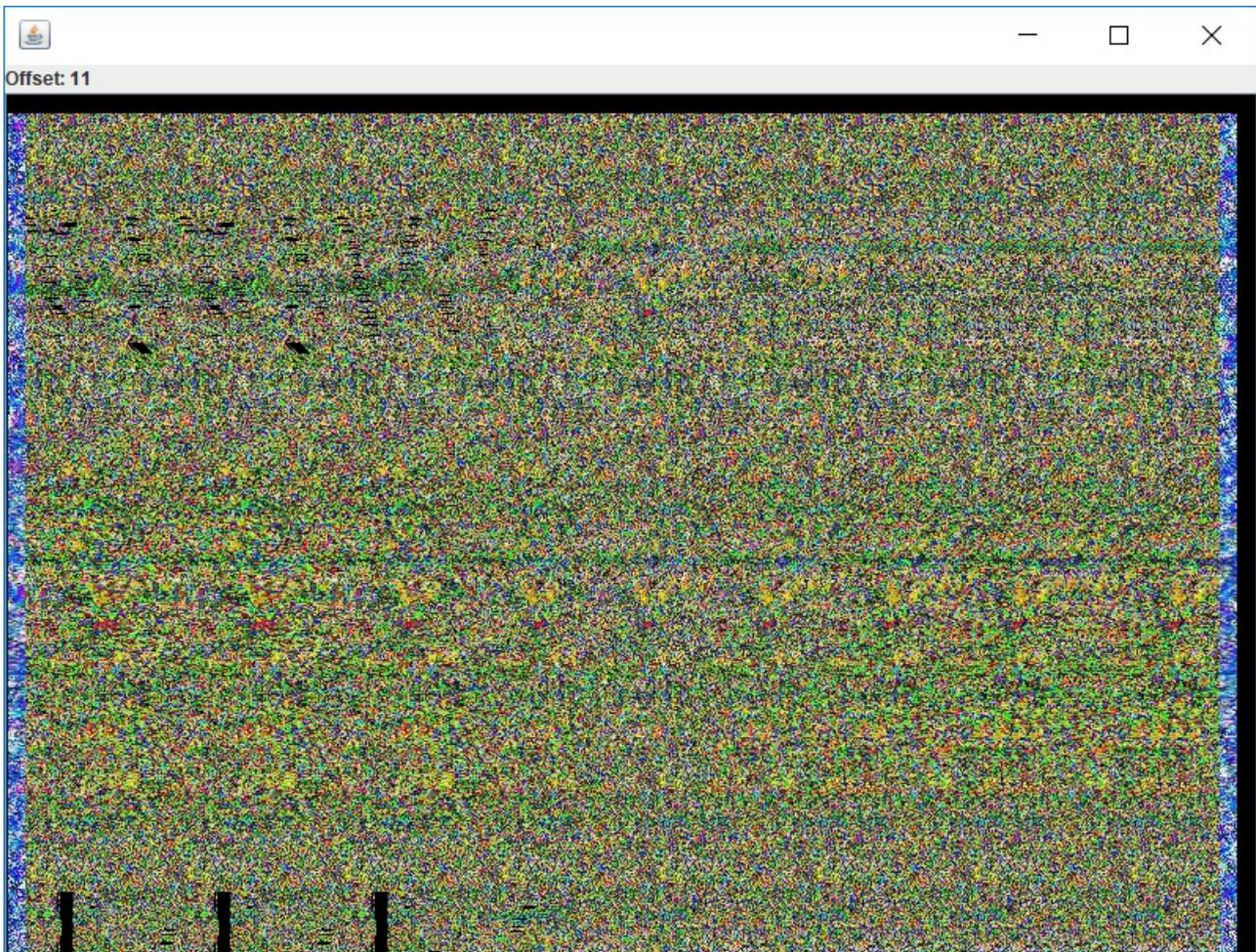


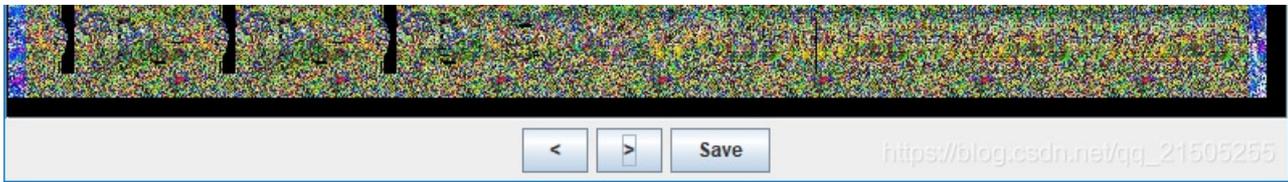


这图有点黄啊

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

Challenge 5 Solves ×

小明：我想不出来名字了

300

鳴神の 小トトみア 文ト目い 雨去降らムカ 君を望め

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

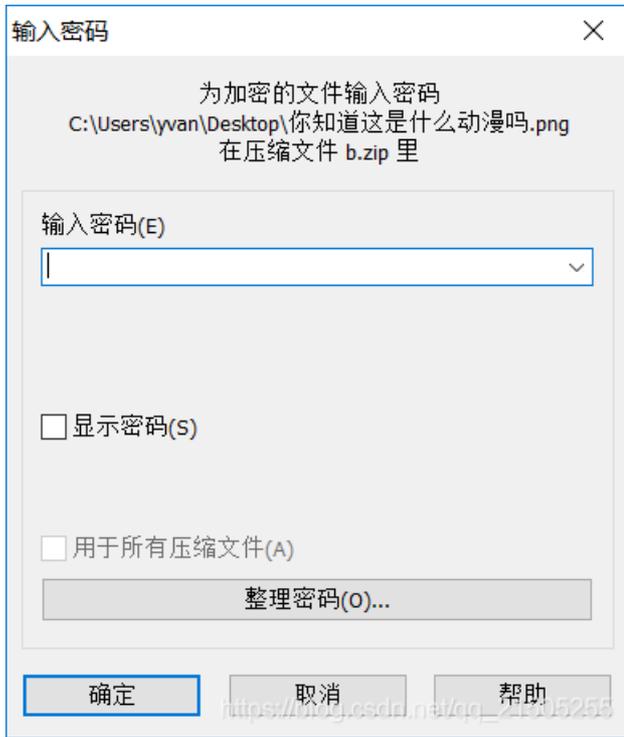
Submit

https://blog.csdn.net/qq_21505255

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



果然需要一个密钥
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

× 提示



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

https://blog.csdn.net/qq_21505255

nice