2021年蓝帽杯部分WP

原创

Oooption 于 2021-05-03 17:03:09 发布 1090 收藏 2

分类专栏： CTF 文章标签： 安全

本文链接：https://blog.csdn.net/weixin_46685211/article/details/116372408

文章目录

前言

一、One_Pointer_php

1.反序列化漏洞

2.分析题目中获得文件

二、冬奥会_is_coming

1.前言

2.题目

总结

前言

2021年“蓝帽杯”题目复盘，感觉题目难度挺大的，小白选择性记录目前能看懂的部分，不是完整WP,自己的学习记录。需要完整WP的可以翻一翻其他大师傅的文章。

一、One_Pointer_php

本次比赛有两个web题，第一个居然是个玩游戏的，game渣渣直接掉线。第二个就是这个很多层的题目。目前值看懂了第一层反序列化，后续的操作先挖个坑。

1.反序列化漏洞

解释：

序列化是将变量转换为可保存或传输的字符串的过程；反序列化就是在适当的时候把这个字符串再转化成原来的变量使用。这两个过程结合起来，可以轻松地存储和传输数据，使程序更具维护性。

函数：

serialize和unserialize

例子：

```php
<?php
//创建一个数组
$a = array('a' => 'Apple' ,'b' => 'banana' , 'c' => 'Coconut');
//序列化数组
$s = serialize($a);
echo $s;
//输出结果：a:3:{s:1:"a";s:5:"Apple";s:1:"b";s:6:"banana";s:1:"c";s:7:"Coconut";}
echo '<br /><br />';
//反序列化
$o = unserialize($s);
print_r($o);
//输出结果 Array ( [a] => Apple [b] => banana [c] => Coconut )
?>
```

其中：

（1）a:3表示数组a中有三个对象

（2）s:1:"a"表示字符串长度为1，内容为a。

2.分析题目中获得文件

下载压缩包获得两个php文件：

user.php

```php
<?php
class User{
 public $count;
}
?>
```

创建了一个User对象，里面有一个变量count

add_api.php

```php
<?php
include "user.php";
if($user=unserialize($_COOKIE["data"])){
 $count[++$user->count]=1;
 if($count[]=1){
  $user->count+=1;
  setcookie("data",serialize($user));
 }else{
  eval($_GET["backdoor"]);
 }
}else{
 $user=new User;
 $user->count=1;
 setcookie("data",serialize($user));
}
?>
```

为了学习这些php的语句，先配置了一上午的php环境（好家伙）

$_COOKIE语句学习链接：https://blog.csdn.net/sm20170867238/article/details/90762010

```
$user=unserialize($_COOKIE["data"])
```

表示获取cookie为data的序列，解序列赋给user，里面有一个count的变量，手动赋值。

```
$count[++$user->count]=1;
```

表示对count数组中的第n+1位赋值为1
由于第五排的一个赋值操作，不需要绕过第五排的赋值操作才能进入else的后门程序，所以使用PHP溢出来跨过。
构造序列：

```
O:4:"User":1:{s:5:"count";i:9223372036854775806;}
#i表示int
#s表示string，要加上字符串的长度
```

最后记得修改cookie的名字为data

二、冬奥会_is_coming

1.前言

初次接触MISC的题目，下载工具：
1、kali 感觉功能很强大，但是目前不会用。初始用户名和密码都是kali
2、MP3Stego 一个可以对MP3文件进行解码和编码的工具，使用是将要处理的文件拉入.exe文件目录下，在当前文件夹打开cmd
解密：

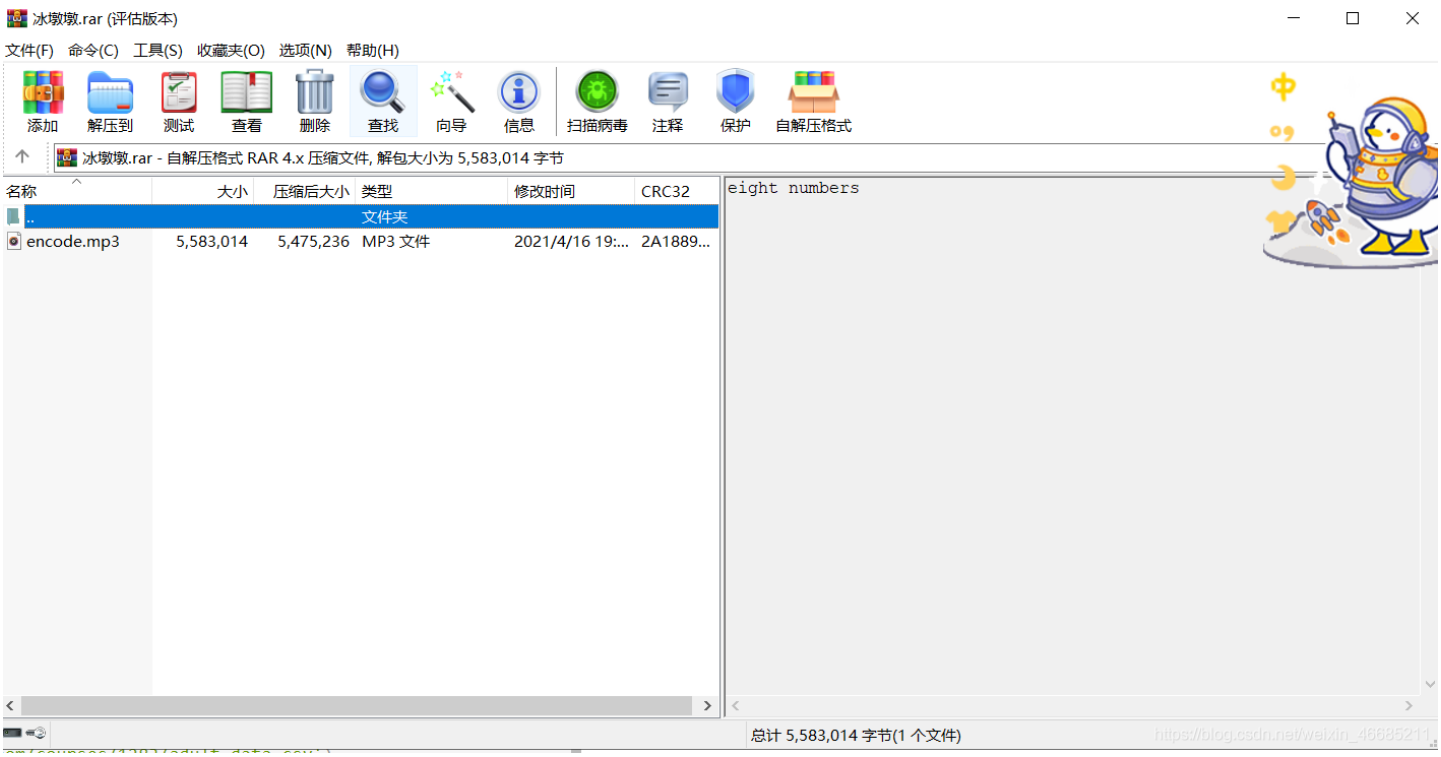
```
decode -X sound.mp3 -P 123
```

加密

```
encode -E data.txt sound.wav sound.mp3 -P 123
```

2.题目

首先获得一个图片，发现这个图片的体积非常大。考虑是隐藏了一些文件在里面，所以使用.rar进行解压获得一个mp3的文件，以及提示是八位密码。



猜测八位密码是冬奥会开幕日期:20220204即MP3Stego的解压密码。
使用MP3Stego解压后得到一串十六进制的符号。

```
\xe2\x9c\x8c\xef\xb8\x8e \xe2\x98\x9d\xef\xb8\x8e\xe2\x99\x93\xef\xb8\x8e\xe2\xa7\xab\xef\xb8\x8e\xe2\x98\x9f\xe
f\xb8\x8e\xe2\x97\x86\xef\xb8\x8e\xe2\x99\x8c\xef\xb8\x8e \xe2\x9d\x92\xef\xb8\x8e\xe2\x99\x8f\xef\xb8\x8e\xe2\x
97\xbb\xef\xb8\x8e\xe2\x96\xa1\xef\xb8\x8e\xe2\xac\xa7\xef\xb8\x8e\xe2\x99\x93\xef\xb8\x8e\xe2\xa7\xab\xef\xb8\x
8e\xe2\x96\xa1\xef\xb8\x8e\xe2\x9d\x92\xef\xb8\x8e\xe2\x8d\x93\xef\xb8\x8e \xe2\x96\xa0\xef\xb8\x8e\xe2\x99\x8b\
xef\xb8\x8e\xe2\x9d\x8d\xef\xb8\x8e\xe2\x99\x8f\xef\xb8\x8e\xe2\x99\x8e\xef\xb8\x8e \xf0\x9f\x93\x82\xef\xb8\x8e
\xe2\x99\x8d\xef\xb8\x8e\xe2\x99\x8f\xef\xb8\x8e\xf0\x9f\x8f\xb1\xef\xb8\x8e\xe2\x99\x8f\xef\xb8\x8e\xe2\x99\x8b
\xef\xb8\x8e\xf0\x9f\x99\xb5 \xe2\x99\x93\xef\xb8\x8e\xe2\xac\xa7\xef\xb8\x8e \xe2\x9d\x96\xef\xb8\x8e\xe2\x99\x
8f\xef\xb8\x8e\xe2\x9d\x92\xef\xb8\x8e\xe2\x8d\x93\xef\xb8\x8e \xe2\x99\x93\xef\xb8\x8e\xe2\x96\xa0\xef\xb8\x8e\
xe2\xa7\xab\xef\xb8\x8e\xe2\x99\x8f\xef\xb8\x8e\xe2\x9d\x92\xef\xb8\x8e\xe2\x99\x8f\xef\xb8\x8e\xe2\xac\xa7\xef\
xb8\x8e\xe2\xa7\xab\xef\xb8\x8e\xe2\x99\x93\xef\xb8\x8e\xe2\x96\xa0\xef\xb8\x8e\xe2\x99\x91\xef\xb8\x8e\xf0\x9f\
x93\xac\xef\xb8\x8e \xf0\x9f\x95\x88\xef\xb8\x8e\xe2\x99\x92\xef\xb8\x8e\xe2\x8d\x93\xef\xb8\x8e \xe2\x96\xa0\xe
f\xb8\x8e\xe2\x96\xa1\xef\xb8\x8e\xe2\xa7\xab\xef\xb8\x8e \xe2\xa7\xab\xef\xb8\x8e\xe2\x99\x8b\xef\xb8\x8e\xf0\x
9f\x99\xb5\xe2\x99\x8f\xef\xb8\x8e \xe2\x99\x8b\xef\xb8\x8e \xe2\x97\x8f\xef\xb8\x8e\xe2\x96\xa1\xef\xb8\x8e\xe2
\x96\xa1\xef\xb8\x8e\xf0\x9f\x99\xb5 \xe2\x99\x8b\xef\xb8\x8e\xe2\xa7\xab\xef\xb8\x8e \xe2\x99\x93\xef\xb8\x8e\x
e2\xa7\xab\xef\xb8\x8e\xe2\x9c\x8d\xef\xb8\x8e
```

这个是utf-8编码，或者是说这个是一个字节的表示方式。在python里面直接进行解码。

```
print(b"...".decode(utf-8))
```

得到一串wingding字符,使用一个在线解码器进行解码：https://lingojam.com/WingdingsTranslatorwingding在线解码

```
✌▯ 👆▯👀▯▯▯👎▯◆▯♌▯ ❒▯♏▯▯▯▫▯▯▯👀▯▯▯▫▯❒▯🖃▯ ■▯♋▯❍▯♏▯♎▯ ▯▯♍▯♏▯▯▯♏▯♋▯▯ 👀▯▯▯ ❖▯♏▯❒▯🖃▯ 👀▯■▯▯▯♏▯❒▯♏▯▯▯▯▯
👀▯■▯♑▯▯▯ ▯▯♒▯🖃▯ ■▯▫▯▯▯ ▯▯♋▯▯♏▯ ♋▯ ●▯▫▯▫▯▯ ♋▯▯▯ 👀▯▯▯✍▯
```

Wingdings 是一个符号字体系列，它将许多字母渲染成各式各样的符号，用途十分广泛。
得到一串英文提示：

A GitHub repository named 1cePeak is very interesting.
Why not take a look at it?

进入GitHub上看看有啥？
打开只有下载了文件，获得：

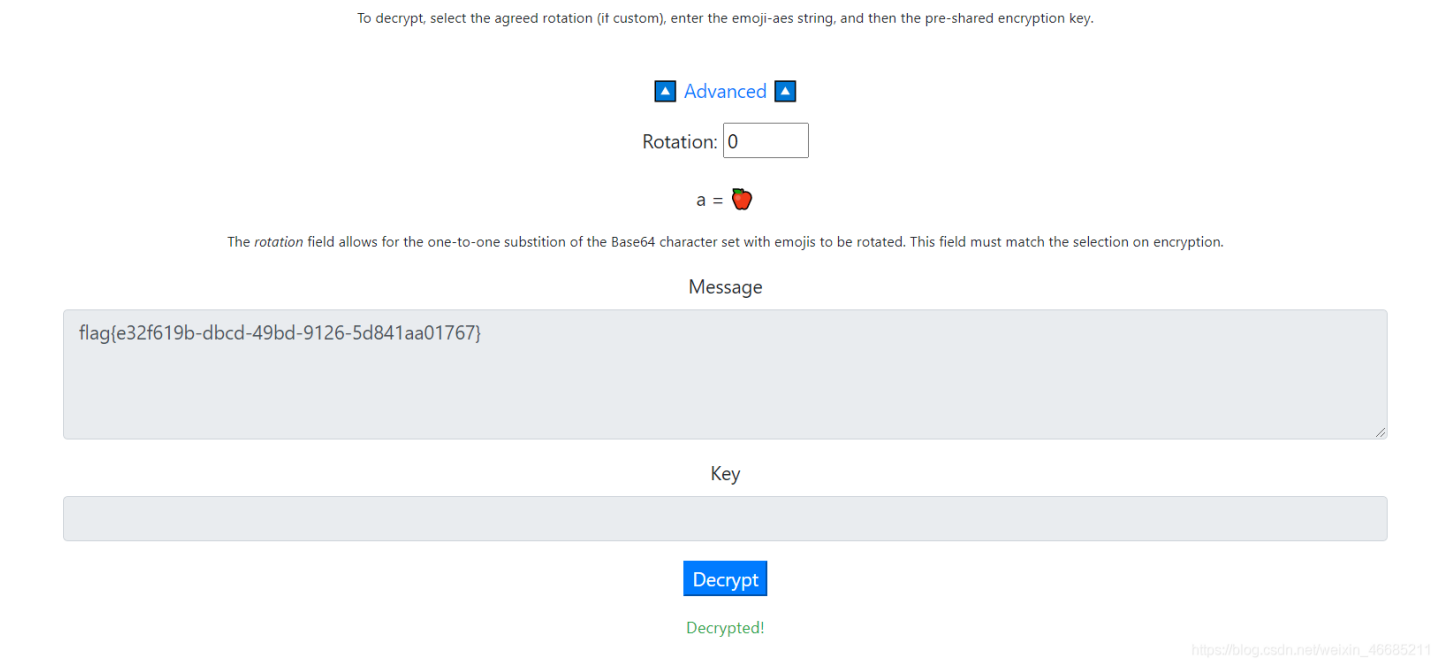
```
#!/bin/sh
echo How_6ad_c0uld_a_1cePeak_be? >&2
```

之后只用winhex查看mp3的文件，发现了一段cipher的编码。

```
19 1A B0 91 62 C4 3D 34  93 0C 00 63 69 70 68 65   °‘bÄ=4“  ciphe
72 3A F0 9F 99 83 F0 9F  92 B5 F0 9F 8C BF F0 9F  r:ðŸ™ƒðŸ’µðŸŒ¿ðŸ
8E A4 F0 9F 9A AA F0 9F  8C 8F F0 9F 90 8E F0 9F  Ž¤ðŸšªðŸŒ ðŸ ŽðŸ
A5 8B F0 9F 9A AB F0 9F  98 86 F0 9F 8E 83 E2 9C  ¥‹ðŸš«ðŸ˜†ðŸŽƒâœ
85 E2 8C A8 F0 9F 94 AA  E2 9D 93 F0 9F 9A AB F0  …â¨ðŸ”ªâ “ðŸš«ð
9F 90 8D F0 9F 99 83 F0  9F 94 AC E2 9C 89 F0 9F  Ÿ ðŸ™ƒðŸ”¬âœ‰ðŸ
91 81 F0 9F 98 86 F0 9F  8E 88 F0 9F 90 98 F0 9F  ‘ ðŸ˜†ðŸŽˆðŸ ˜ðŸ
8F 8E F0 9F 90 98 F0 9F  90 98 F0 9F 98 82 F0 9F   ŽðŸ ˜ðŸ ˜ðŸ˜‚,ðŸ
98 8E F0 9F 8E 85 F0 9F  96 90 F0 9F 90 8D E2 9C  ˜ŽðŸŽ…ðŸ– ðŸ  âœ
89 F0 9F 8D 8C F0 9F 8C  AA F0 9F 90 8E F0 9F 8D  ‰ðŸ ŒðŸŒªðŸ ŽðŸ
B5 E2 9C 85 F0 9F 9A AA  E2 9C 96 E2 98 83 F0 9F  µâœ…ðŸšªâœ–â˜ƒðŸ
91 A3 F0 9F 91 89 E2 84  B9 F0 9F 94 AA F0 9F 8D  ‘£ðŸ‘‰â„¹ðŸ”ªðŸ
8E F0 9F 94 84 F0 9F 91  A3 F0 9F 9A AA F0 9F 98  ŽðŸ”„ðŸ‘‰£ðŸšªðŸ˜
81 F0 9F 91 A3 F0 9F 92  B5 F0 9F 90 85 F0 9F 8D   ðŸ‘‰£ðŸ’µðŸ …ðŸ
B5 F0 9F 94 AC F0 9F 9B  A9 F0 9F 98 87 F0 9F 96  µðŸ”¬ðŸ©ðŸ˜‡ðŸ–
90 F0 9F 96 90 F0 9F 8E  85 E2 9C 85 F0 9F 8F 8E   ðŸ– ðŸŽ…âœ…ðŸ Ž
F0 9F 91 8C F0 9F 9A A8  F0 9F 98 86 F0 9F 8E A4  ðŸ‘ŒðŸšª¨ðŸ˜†ðŸŽ¤
F0 9F 8E 85 F0 9F A6 93  F0 9F 8C BF F0 9F A6 93  ðŸŽ…ðŸ¦“ðŸŒ¿ðŸ¦“
F0 9F 99 83 E2 9C 96 F0  9F 8D 8C F0 9F 9B A9 F0  ðŸ™ƒâœ–ðŸ ŒðŸ©ð
9F 98 82 F0 9F 91 91 F0  9F 8C 8F E2 98 83 F0 9F  Ÿ˜‚,ðŸ‘‘ðŸŒ â˜ƒðŸ
98 87 F0 9F 98 8D F0 9F  9B A9 F0 9F 9A B9 F0 9F  ˜‡ðŸ˜ ðŸ©ðŸšªðŸ
98 80 F0 9F 8D 8C F0 9F  8E 88 F0 9F 92 A7 F0 9F  ˜€ðŸ ŒðŸŽˆðŸ’§ðŸ
97 92 F0 9F 97 92                                —’ðŸ—’
```


复制Hex Value然后在在线工具里面转成字符串的形式。

通过一个神奇的emoji解码工具：https://aghorler.github.io/emoji-aes/
结合之前找到的密码How_6ad_c0uld_a_1cePeak_be?进行解码



得到flag

总结

多学多学