bugkuct部分writeup 持续更新

转载

weixin_30481087 于 2019-03-12 11:36:00 发布 231 收藏
文章标签： php shell javascript ViewUI
原文链接：http://www.cnblogs.com/hagendasi/p/10513415.html

6307

校赛被打击到自闭，决心好好学习。

web部分题目.

1、web2　　地址 http://123.206.87.240:8002/web2/

既然是第一个题我们应该采取查看源码的方式进行，右键之发现没有办法查看源码。遂使用命令view-source查看源码，源码中包含flag，提交即可。

2、计算器　　地址：http://123.206.87.240:8002/yanzhengma/

进入发现是一个计算题

输入结果时发现只能输入一个字符，应该是和HTML的text中的maxlength属性有关，控制台查看发现了问题所在

```
1 <input type="text" class="input" maxlength="1"/>
```

修改maxlength的值为3，再次输入结果进行验证获得flag。

3、web基础$_GET　　地址：http://123.206.87.240:8002/get/

进入时发现出题人将源码放出来了

```
1 $what=$_GET['what'];
2 echo $what;
3 if($what=='flag')
4 echo 'flag{****}';
```

用URL进行传递http://123.206.87.240:8002/get/?what=flag 即可，得到flag。

4、web基础$_POST　　链接：http://123.206.87.240:8002/post/

进入时发现同样的源代码被出题者放出来了。

```php
$what=$_POST['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
```

利用火狐的插件HackBar提交post

得到flag。

5、矛盾　　链接：http://123.206.87.240:8002/get/index1.php

进入题目发现源代码已经放出来了

```php
$num=$_GET['num'];
if(!is_numeric($num))
{
echo $num;
if($num==1)
echo 'flag{**********}';
}
```

和题目一样，这个代码乍一看就是有一点矛盾。第一层是变量不能是数字，第二层是变量必须是1。

因为php是一个弱类型语言所以我们可以构造payload

1'

1%00

1e0.1

1sdad

URL即可得到flag

6、web3　　链接：http://123.206.87.240:8002/web3/

例行工作先查看源码，在源码中发现了一个可疑的注释

```
<!--
&#75;&#69;&#89;&#123;&#74;&#50;&#115;&#97;&#52;&#50;&#97;&#104;&#74;&#75;&#45;&#72;&#83;&#49;&#49;&#73;&#73;
&#73;&#125;-->
```

将这段Unicode进行转换就拿到了flag

7、域名解析

进入题目发现了提示，听说把 flag.baidu.com 解析到123.206.87.240 就能拿到flag。

这样我们在本地C:\Windows\System32\drivers\etc\hosts 文件中将其进行解析就可以了。

```
123.206.87.240      flag.baidu.com
```

在浏览器中访问flag.baidu.com就可以得到flag。

8、你必须让他停下　　链接：http://123.206.87.240:8002/web12/

进去之后发现网页不停的刷新，查看源码

```
<script language="JavaScript">
function myrefresh(){
window.location.reload();
}
setTimeout('myrefresh()',500);
</script>
<body>
<center><strong>I want to play Dummy game with others£¡But I can't stop!</strong></center>
<center>Stop at panda ! u will get flag</center>
<center><div><img src="2.jpg" /></div></center><br><a style="display:none">flag is here~</a></body>
</html>
```

我们可以发现提示就是要我们停在某一张图片上 然后会有flag的提示

我们打开bp 然后在Rpeater进行go 然后会刷新到panda所在的图片，flag也就得到了。

9、本地包含　　链接：http://123.206.87.240:8003/

这个题目可能是挂掉了，等以后再去做吧。

10、变量　　链接：http://123.206.87.240:8004/index1.php

进入到网页见到提示 flag In the variable ! 说明flag在变量variable中。

进一步阅读出题者给出的源码

```
flag In the variable ! <?php


error_reporting(0);// 关闭php错误显示
include "flag1.php";// 引入flag1.php文件代码
highlight_file(__file__);
if(isset($_GET['args'])){// 通过get方式传递 args变量才能执行if里面的代码
    $args = $_GET['args'];
    if(!preg_match("/^\w+$/",$args)){// 这个正则表达式的意思是匹配任意 [A-Za-z0-9_] 的字符，就是任意大小写字母和0到9以及下划线组成
        die("args error!");
    }
    eval("var_dump($$args);");// 这边告诉我们这题是代码审计的题目
}
?>
```

其中$$args是一个可变变量，var_dump将变量以数组的方式进行显示。

eval("var_dump($$args);");　　首先将 var_dump($$args); 当成代码执行
var_dump($GLOBALS);

var_dump()函数将$GLOBALS数组中存放的所有变量以数组的方式输出 得到flag!

11、web5　　链接：http://123.206.87.240:8002/web5/

这个题目进去一看jspfuck，查看源码。发现了jspfuck风格的编码，拿去解码，拿到flag。

12、头等舱　　链接：http://123.206.87.240:9009/hd.php

进入题目发现没有什么提示，查看源码也没有什么发现。所以利用burpsuite进行抓包，在响应包包头发现了相关的flag。

13、网站被黑　　链接：http://123.206.87.240:8002/webshell/

题目进入之后发现那个光标的样式真好玩，玩了十分钟。

webshell就想起来要用扫描工具，利用御剑进行扫描发现了存在shell.php。访问http://123.206.87.240:8002/webshell/shell.php

进入发现需要进行登录，利用bp进行爆破之。发现pass=hack。

14、管理员系统　　链接：http://123.206.31.85:1003/

进入题目发现其需要本地IP，利用火狐插件X-Forwarded-For Header伪造ip。

在请求头里面就会出现 X-Forwarded-For: 127.0.0.1

查看源码时发现dGVzdDEyMw==　　对其进行解码是test123猜测应该是密码。

用户名admin 密码test23

得到了flag进行提交。

15、web4　　链接：http://123.206.87.240:8002/web4/、

进入页面根据提示查看源码发现了两段URL编码，将第一段进行解码得到function checkSubmit(){var a=document.getElementById("password");if("undefined"!=typeof a){if("67d709b2b

第二段进行解码得到
54aa2aa648cf6e87a7114f1"==a.value)return!0;alert("Error");a.focus();return!1}}do

两段合在一起就是function checkSubmit(){var a=document.getElementById("password");if("undefined"!=typeof a){if("67d709b2b54aa2aa648cf6e87a7114f1"==a.value)return!0;alert("Error");a.focus(

我们只要提交67d709b2b54aa2aa648cf6e87a7114f1就能得到flag

16、flag在index里　　链接：http://123.206.87.240:8005/post/

这个题目进入之后首先查看源码没有发现什么，bp也没有发现什么特殊的地方。题目的提示是flag在index中间，确实是不会了所以就百度了一下其他的大佬的做法，发现这个题目是一个本地文件包含加php伪协议利用。利用了php://filter 这里是一个十分重要的知识点。

php://filter是PHP语言中特有的协议流，作用是作为一个“中间流”来处理其他流。比如，我们可以用如下一行代码将POST内容转换成base64编码并输出。首先这是一个file关键字的get参数传递，php://是一种协议名称，php://filter/是一种访问本地文件的协议，/read=convert.base64-encode/表示读取的方式是base64编码后，resource=index.php表示目标文件为index.php。构造payload：http://120.24.86.145:8005/post/index.php?file=php://filter/read=convert.base64-encode/resource=index.php
返回base64编码的结果，在注释中发现flag。

转载于:https://www.cnblogs.com/hagendasi/p/10513415.html