

bugkuCTF Writeup (Web) 41-44

原创

[Troublor](#)  于 2018-02-07 20:49:41 发布  1730  收藏 1

分类专栏: [CTF](#) 文章标签: [CTF](#) [Web](#) [SQL](#) [PHP](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/troublor/article/details/79284170>

版权



[CTF 专栏收录该内容](#)

8 篇文章 1 订阅

订阅专栏

这是一个神奇的登陆框

题目

75 Solves

×

这是一个神奇的登陆框

150

http://120.24.86.145:9001/sql/

flag格式flag{}

Key

SUBMIT

<http://blog.csdn.net/troublor>

登陆框注入

这是一个神奇的登录界面

来登录试试

Username

Password

GO GO GO

<http://blog.csdn.net/troublor>

之前注入的分隔符都用的是单引号'，这道题特立独行用的是双引号。

又发现有报错的回显，于是报错注入：

一开始使用的updatexml和extractvalue这两个函数来进行的报错注入，后来发现这两个函数的报错注入有缺陷，报错信息的长度不超过32位，对于这道题来说，flag是一个md5摘要，长度正好32位，而又会用到concat函数来连接，就会显示不完全。

所以这道题的注入还是使用基于 `floor()`和`rand()` 的报错注入

payload:

```
admin_name:a1
admin_passwd:1" and (select 1 from (select count(*), concat(floor(rand(0)*2),0x23,(爆数据库信息))x from i
submit:GO GO GO
```

在“爆数据库信息”那里逐个找，就能找到flag1表的flag1字段是flag

多次

题目 15 Solves ×

多次 150

<http://120.24.86.145:9004>

本题有2个flag

flag格式 flag{}

Key

SUBMIT

<http://blog.csdn.net/troublor>

这个暂时还没做出来（忧伤）

sql注入2

题目 356 Solves ×

sql注入2

190

<http://120.24.86.145:8007/web2/>

全都tm过滤了绝望吗？

提示 !,!,=,+,-,^,%

Key

SUBMIT

<http://blog.csdn.net/troublor>

自己做没做出来，看别人的，竟然url为 <http://120.24.86.145:8007/web2/flag> 可以直接下载，无语。
下载下来就是flag。。。

题目

173 Solves

×

wordpress

200

<http://wp.bugku.com/>

出题花了10分钟，应该很简单的，
进网站看看就明白了。

需要用到渗透测试第一步信息收集

Key

SUBMIT

<http://blog.csdn.net/troublor>

信息收集，嗯，就开始扒博客，幸亏文章就一点点，
看到有一个文章说flag在这里，并且下面给了两个字符串

SUN某的 BLOG

又一个WordPress站点

2017年2月17日 由SUN

flag在这里

wp wzTrzYRdbrbyjAx

上面这2是什么东东?

<http://blog.csdn.net/troublor>

抱着试试看的心态去访问phpmyadmin还成功了，这还真是信息搜集啊
数据库里东西很容易就找到了

The screenshot shows the phpMyAdmin interface for a MySQL database named 'wp'. The current table selected is 'flag'. The SQL query entered is:

```
SELECT *  
FROM `flag`  
LIMIT 0, 30
```

The interface shows the table structure for 'flag' with the following columns:

flag
KEY (flag_089_admin)

At the bottom of the interface, there is a URL: <http://blog.csdn.net/troublor>