

i春秋“百度杯”CTF比赛 九月场 SQLi

原创

「已注销」于 2018-09-13 12:55:10 发布 913 收藏

分类专栏: [春秋](#)

友链: <https://cutt.ly/7777aaaa>

本文链接: https://blog.csdn.net/include_heqile/article/details/82686332

版权



[春秋](#) 专栏收录该内容

19 篇文章 0 订阅

订阅专栏

<https://www.ichunqiu.com/battalion?t=1&r=0>

这道题相当坑爹,我是看了 [writeup](#) 才知道该怎么做

进入题目链接后查看源代码,提示说注入点是 `login.php`,但是这个注入点是假的,累死你也注不出来任何内容,看一下题目链接和点进去之后浏览器搜索框上的链接,两者其实是不一样的:

题目链接: <http://bc9dbb2a422b452ca6bcdf4aad8f3ec9ad845a95d8748f6.game.ichunqiu.com>

进去之后搜索框里显示的链

接: <http://bc9dbb2a422b452ca6bcdf4aad8f3ec9ad845a95d8748f6.game.ichunqiu.com/b68a89d1c4a097a9d8631b3ac45e8979.php>

如果我们使用 `burpsuite` 看一下 `http history` 的话就会发现网站做了一次 `302` 重定向操作,然后我们会在回复报文的 `header` 中发现 `page` 字段,上面会提示我们真正的注入点位置

The screenshot shows the Burp Suite interface with the HTTP history tab selected. The selected request is a GET request to the URL mentioned in the text. The response tab is also open, showing the following headers:

```
HTTP/1.1 302 Found
Server: nginx/1.10.2
Date: Thu, 13 Sep 2018 04:44:13 GMT
Content-Type: text/html
Content-Length: 97
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19
page: login.php?id=1
location: ./b68a89d1c4a097a9d8631b3ac45e8979.php
```

The HTML body shows a loading spinner: `<html><title>Loading...</title></head></html>`

然后就可以进行 `sql` 注入了,题目甚至都给出了显位的个数,而且没有对 `'` 做任何过滤,只是过滤了 `,`,使用 `SQL` 中的 `join` 关键字即可:这是我在本地 `sql` 数据库中做的测试

```
select * from sqlitest where id=' ' union select * from (select 1)a join (select 2)b;
```

```
+-----+
| id | name |
+-----+
|  1 |  2  |
+-----+
```

把上面的 1 和 2 替换成自己的注入语句即可



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)