百度杯”CTF比赛 九月场SQLi ---------i春秋

转载

weixin_30907523 于 2019-07-07 11:46:00 发布 62 收藏
文章标签： php 数据库
原文链接：http://www.cnblogs.com/zhangyukui/p/11145840.html

题目链接：https://www.ichunqiu.com/battalion

打开链接，创建题目，进入题目环境

发现界面没有显示东西

查看一下源代码

```
1 <html>
2 <head><title>Loading...</title></head>
3 <body>
4     <!-- login.php?id=1 -->
5 </body>
6 </html>
```

发现源代码里注释了一条信息，login.php?id=1,访问一下

welcome admin~ 1 welcome admin~</br>

只返回了一条句子welcome admin~，尝试注入，结果没什么发现

进行抓包，访问index.php,在主界面获取到一个信息

```
HTTP/1.1 200 OK
Date: Sun, 07 Jul 2019 00:52:19 GMT
Content-Type: text/html
Content-Length: 0
Connection: close
refresh: 0;url=./b68a89d1c4a097a9d863lb3ac45e8979.php
X-Via-JSL: b[redacted]
X-Cache: bypass
```

刚开始以为和URL上显示一样，仔细一看才发现，它把1换成了l，访问一下这个界面,进行抓包

HTTP/1.1 302 Found
Date: Sun, 07 Jul 2019 01:00:58 GMT
Content-Type: text/html
Content-Length: 57
Connection: close
page: l0gin.php?id=1
location: ./b68a89d1c4a097a9d8631b3ac45e8979.php
X-Via-JSL: 1d2d85a,-
X-Cache: bypass

看到上面多了一行l0gin.php?id=1,进行访问

id	username
1	flag

通过检测发现过滤了逗号，百度查一下替换逗号的方式，构造语句,查询数据库

id	username
sqli	5.5.50-0ubuntu0.14.04.1

查表

id	username
users	5.5.50-0ubuntu0.14.04.1

查字段

id	username
id,username,flag_9c861b688330	5.5.50-0ubuntu0.14.04.1

看到有一个flag，提交显示错误，那就查看这个字段

id	username
flag{0d5bc449-1660-4642-ac4d-49194ea44d03}	5.5.50-0ubuntu0.14.04.1

得到正确flag

转载于:https://www.cnblogs.com/zhangyukui/p/11145840.html