# i春秋-百度杯十月场-vld

转载

weixin_30391339 于 2018-11-01 22:56:00 发布 51 收藏
原文链接：http://www.cnblogs.com/whitehawk/p/9893222.html


查看源码，有提示，index.php.txt ， 进入得到文本。

---

不太看得懂，后来百度，大致就是，flag1=.....&flag2=.....&flag3=..... ,传给index.php.

得到下一步，1chunqiu.zip。下载下来，查看源码。

可能知识太少，没看出什么，参考一下大佬的答案后，得知利用两个地方可以构造注入：

---

---

addslashes()这个函数，能使%00转义为\0,而trim()函数又消除username与number相同的字符串。

构造：number=0&username=a%00' or updatexml(1,concat(2,(select database()),2),1)%23&password=1&submit=submit

注入语句，脑补。。。。

转载于:https://www.cnblogs.com/whitehawk/p/9893222.html