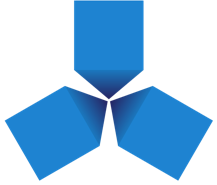
**某服务器**

**应急事件分析及溯源报告**

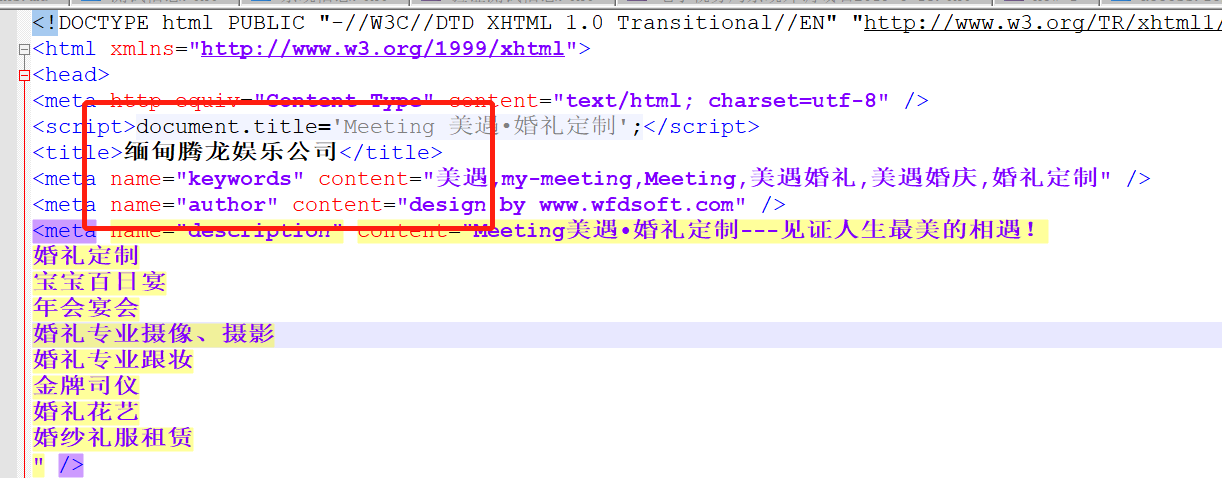


**TIDE信息安全实验室**

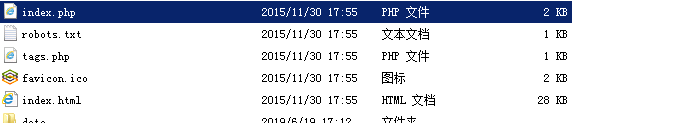
**2019年06月**

# 事件简述

2019年6月13日，接到某单位通知，某网站首页内容被篡改，网站标题被修改为缅甸腾龙娱乐公司。



文件修改时间被篡改为2015年

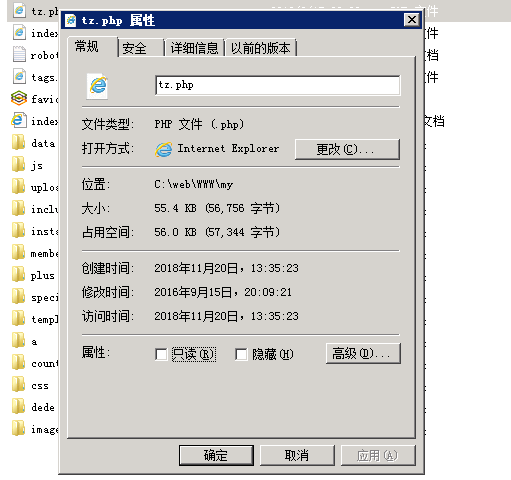




通过扫描网站目录发现如下后门文件



从后门文件创建事件以及index.php的修改时间来看，最早在18年11月20号就被上传了后门程序，并进行了首页的篡改。



最近一次后门是在19年5月21号上传，由于系统只是保留了19年的日志，所以，本次重点分析5月21号这次攻击。

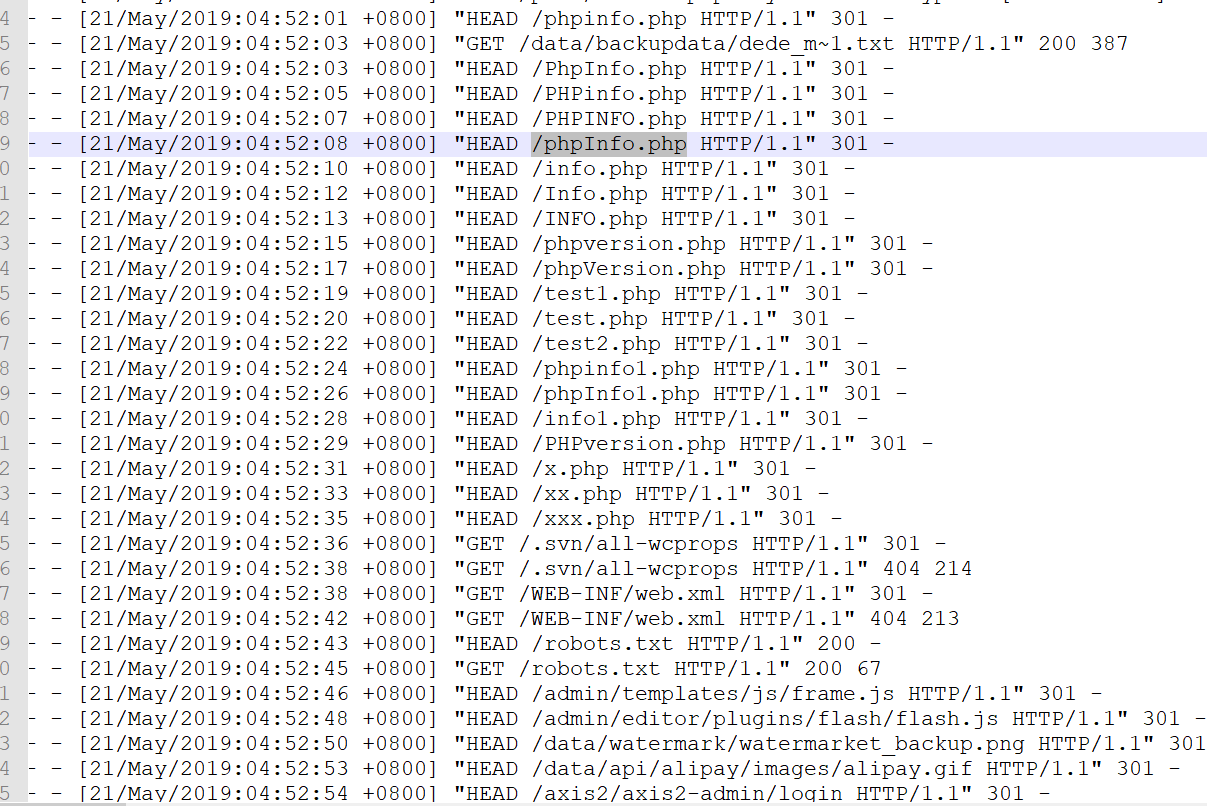
# 排查过程

## 系统状态

对系统当前连接进行查看，未发现异常连接，未发现服务器与非正常ip地址建立连接。查看任务管理器未发现占用较高cpu、内存的异常进程。

## 日志分析

从5月21号日志可见，攻击者进行了一轮目录枚举

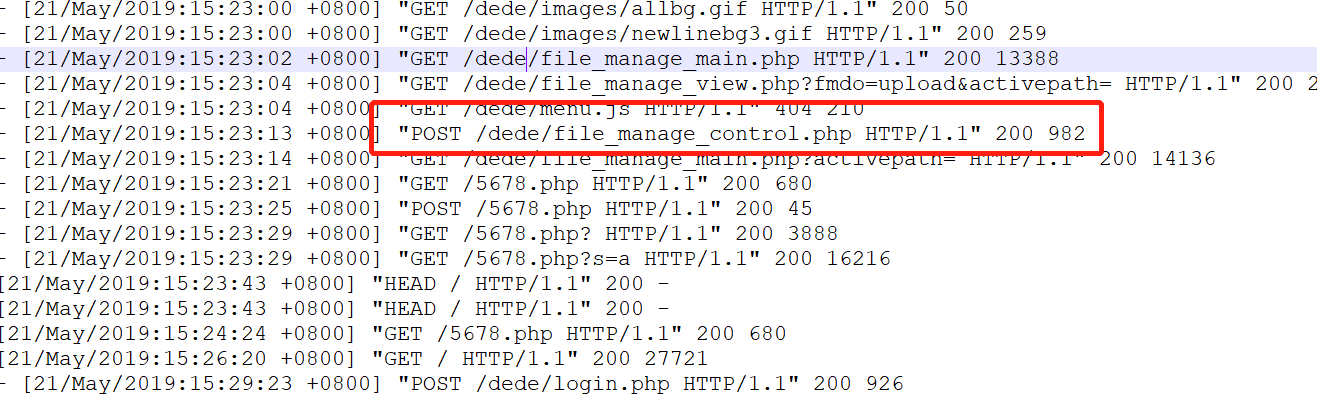


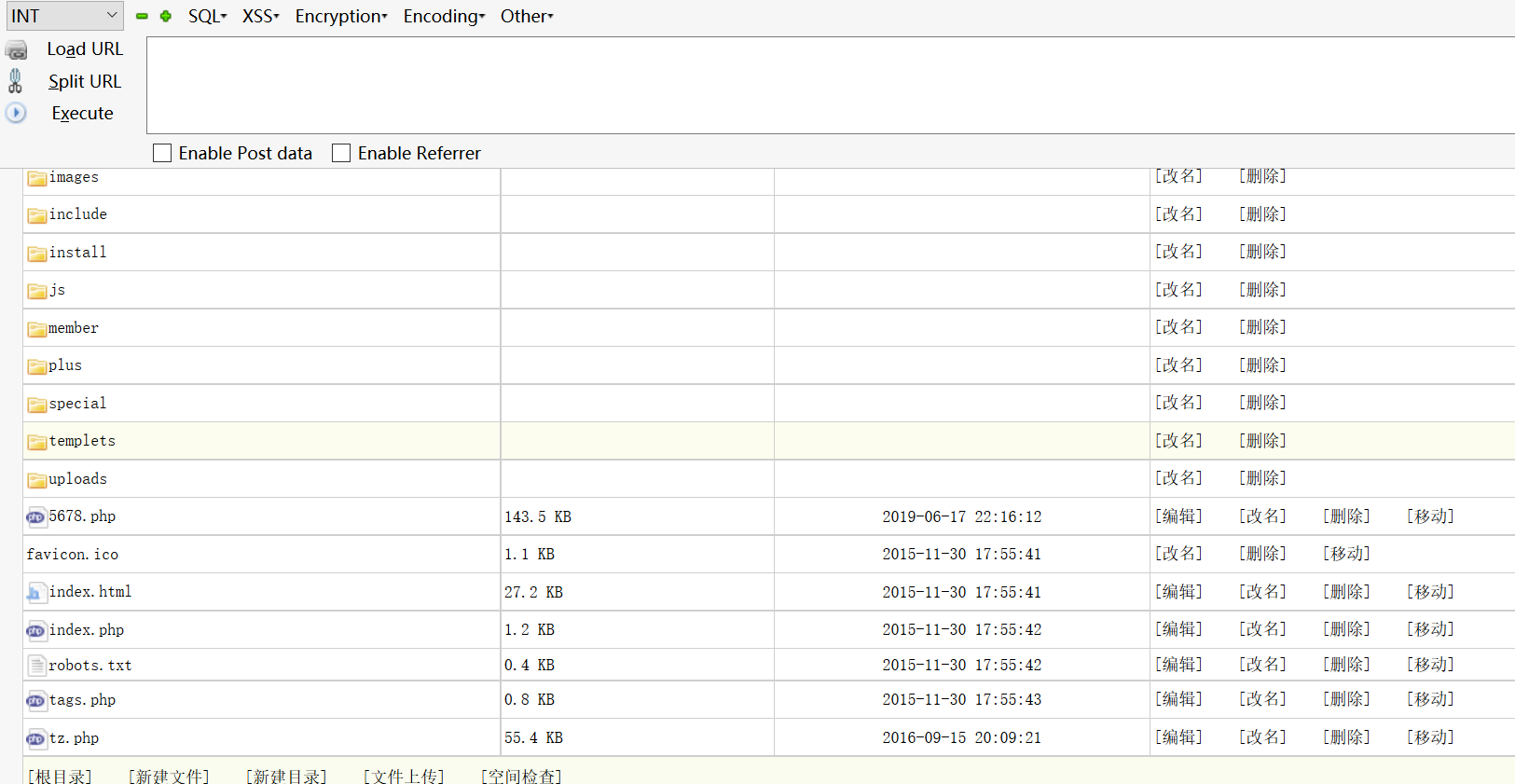
攻击者利用织梦cms apche+win环境下的短文件名泄露漏洞，可获取管理员密码。

通过访问<http://xxx.xxx.xxx//data/backupdata/dede_m~1.txt>,获取admin账号，并成功登录系统

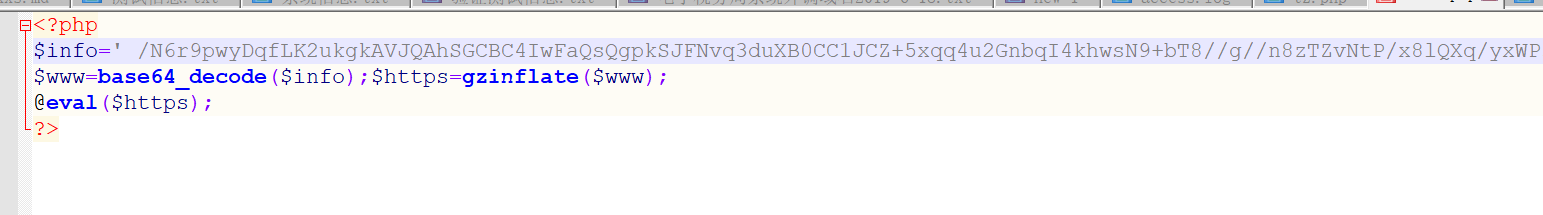


在后台访问dede/file\_manage\_view.php?fmdo=upload&activepath=路径，进行恶意文件上传，上传5678.php成功，上传时间为5月21。

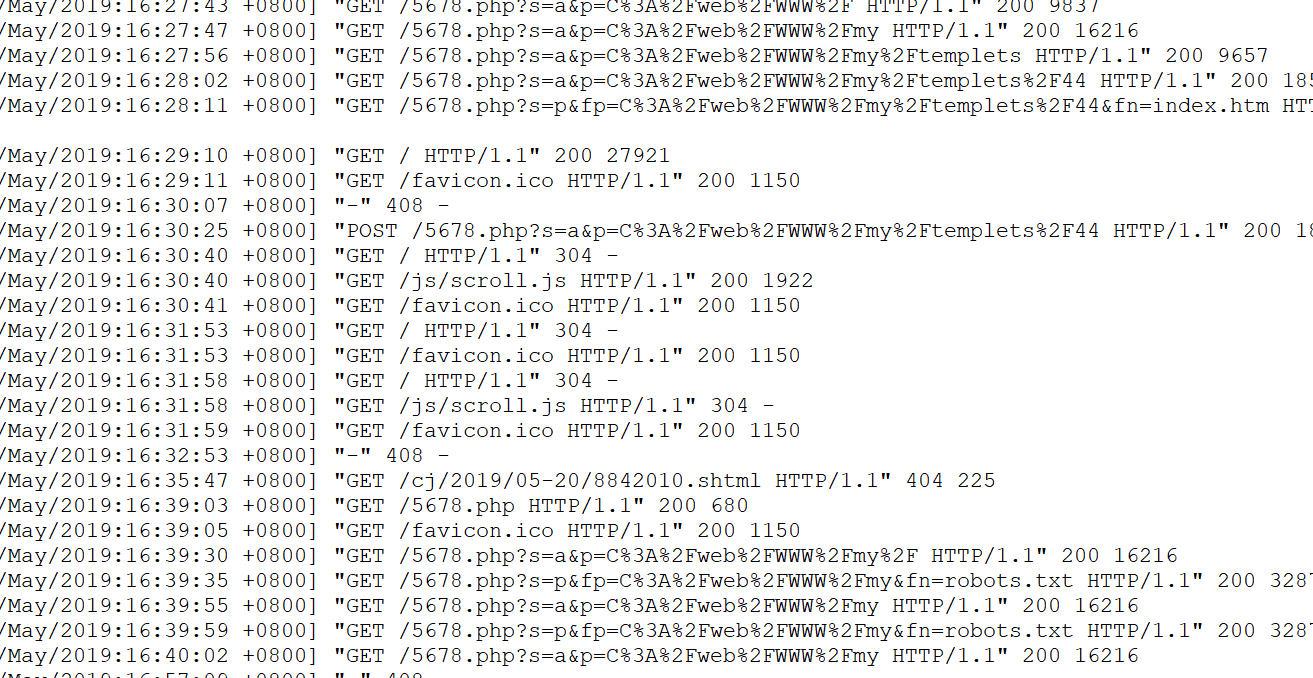




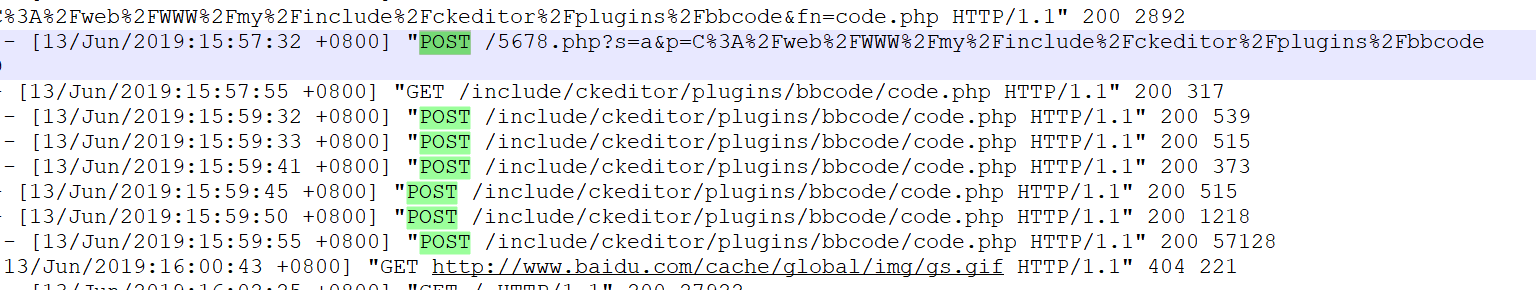
后门5678.php的具体内容如下，该后门还是很有意思的，大多数时间也是放在该后门的分析上了。



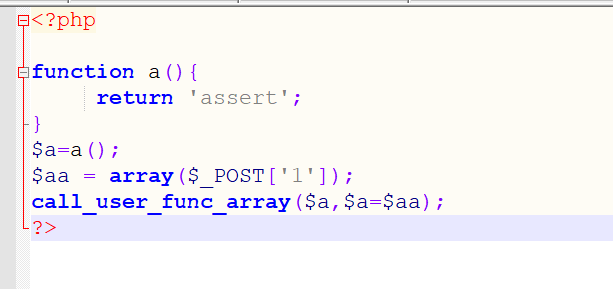
从日志中可见攻击者利用5678.php做了一系列查询操作



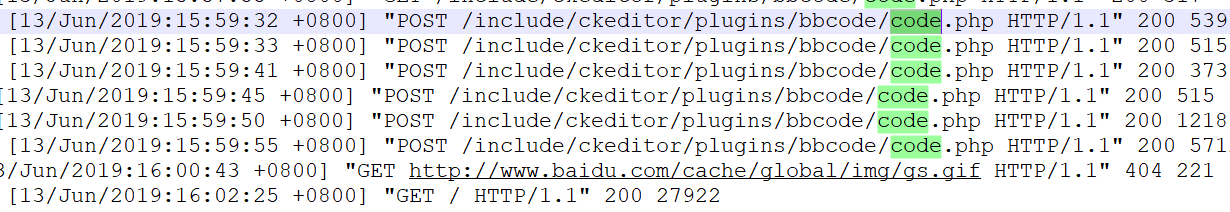
在6月13号的时候，攻击者通过访问5678.php，上传了code.php一句话木马。

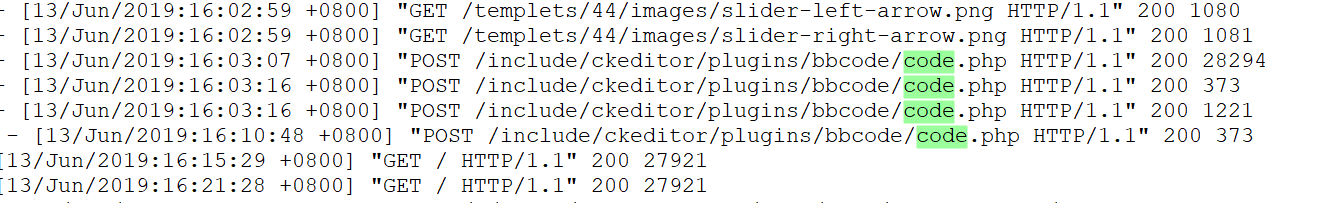


code.php具体内容如下，该菜刀马同样也是免杀马，测试了下win10自带的防护、D盾都无法查杀出来是后门文件。



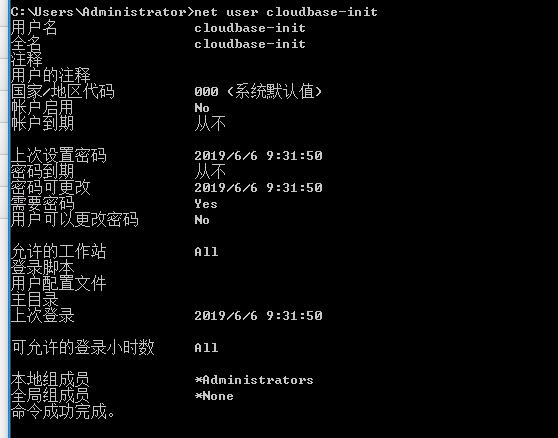
继续分析日志，从日志来看，攻击者又通过连接code.php做了一些操作，但是具体行为无法判断



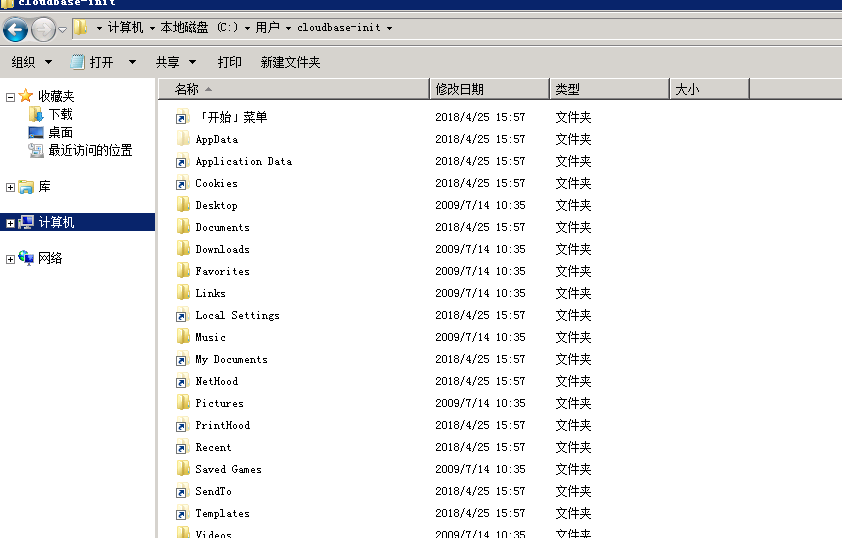


## 异常用户分析

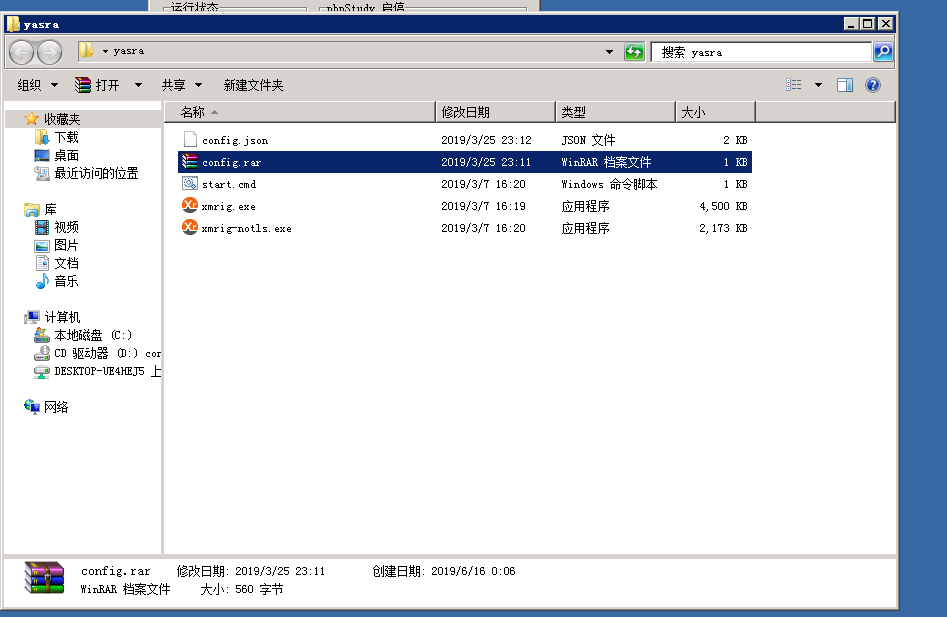
通过查看用户发现系统上存在cloudbase-init异常用户，最后一次登录时间为6月6 号。



查看用户配置文件，该用户第一次登录时间应该在2018年4月25日

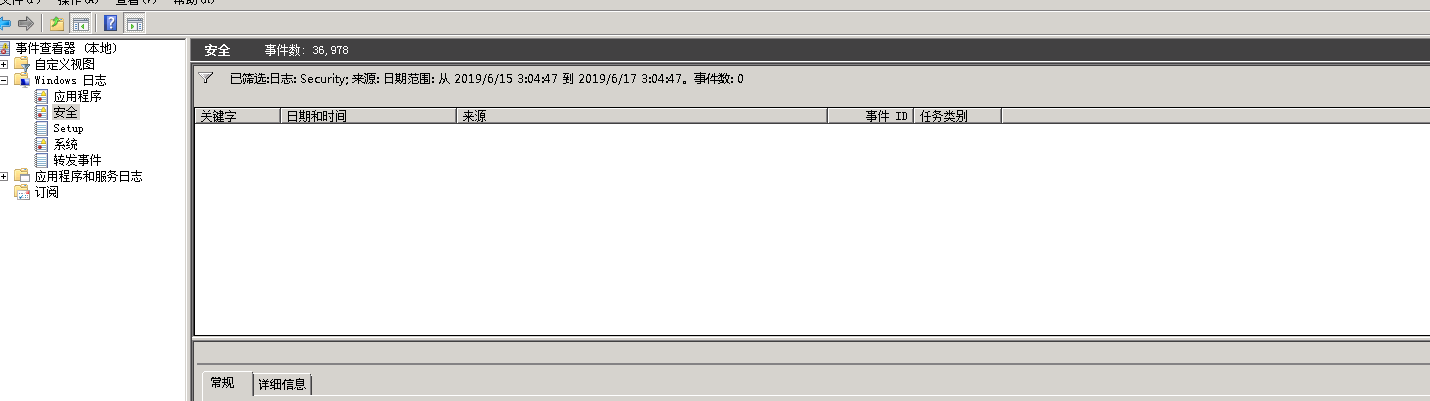


其桌面上被传入了xmrig挖矿软件，文件建立时间为6月16号。

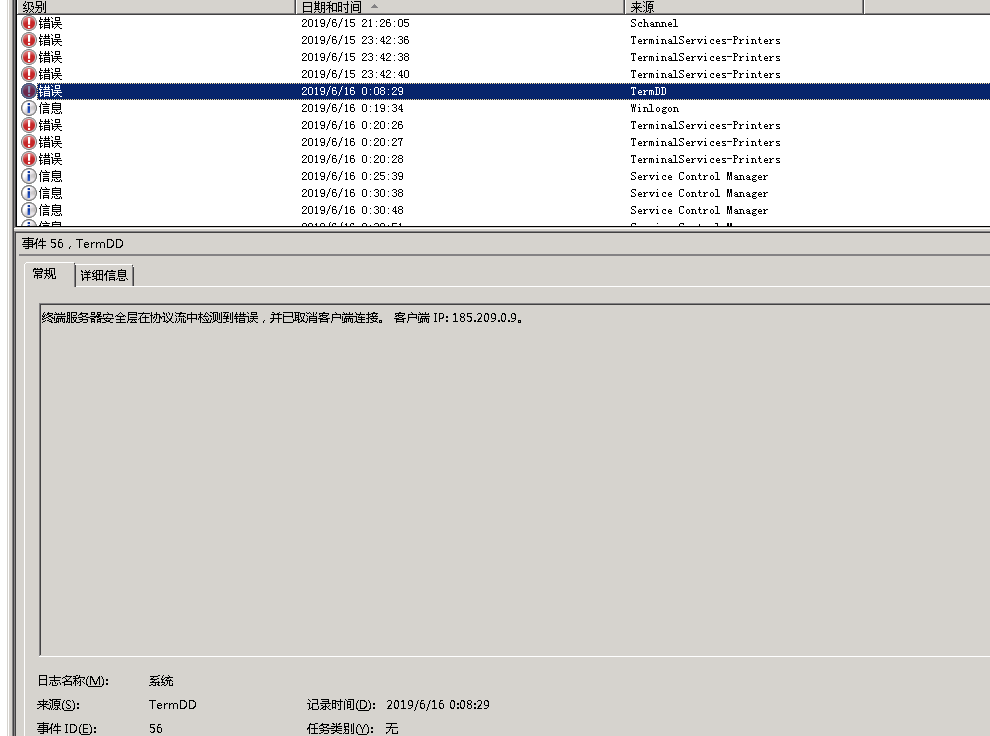


关于这个挖矿软件无法确实是如何上传的，攻击者要么是通过3389远程链接进行拷贝或是通过浏览器下载、要么是通过后门上传，简单排查过程如下：

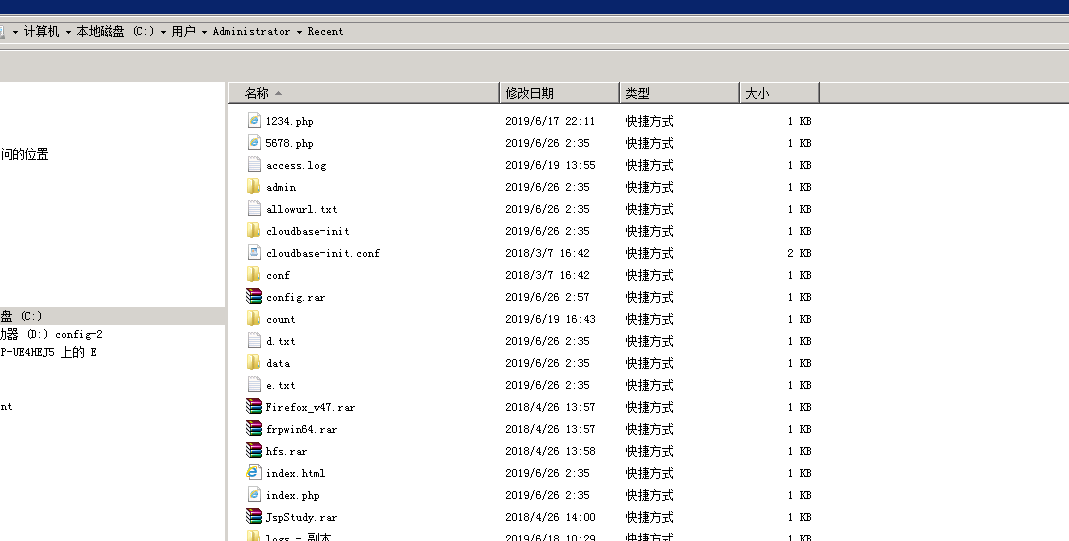
根据文件建立时间了，看了相关日志，发现这段时间没有用户登录系统



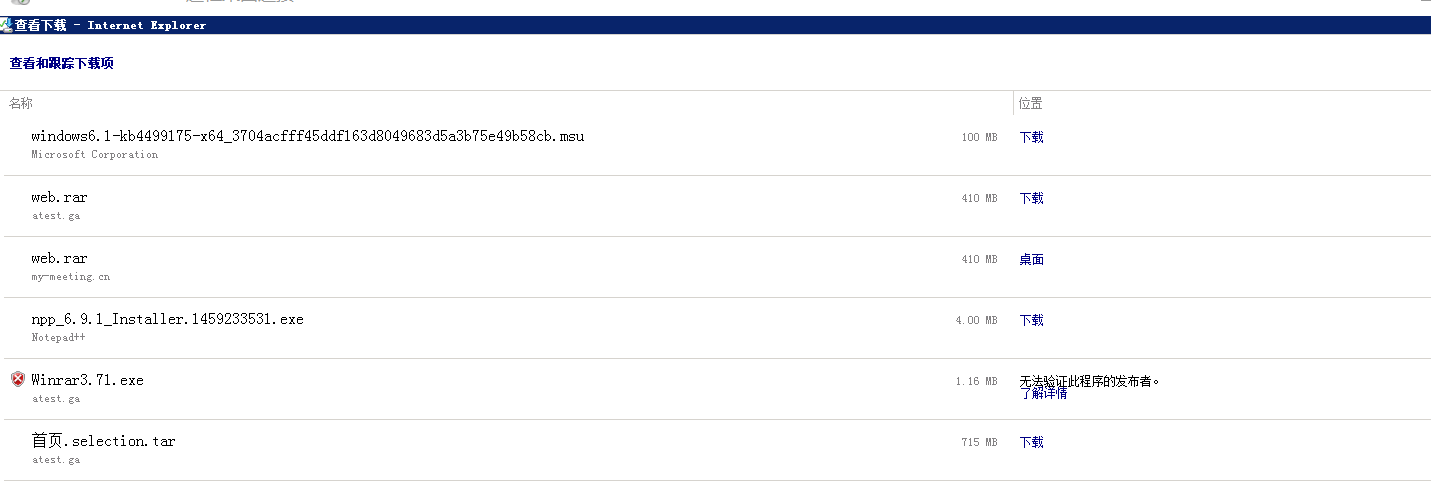
查看系统日志，发现存在一条 termdd 56日志，时间是6月16日0点08分，虽然和挖矿软件时间接近，但是该日志并未显示登录成功。



查看recent也未发现相关行为



查看了浏览器的历史记录，未发现相关内容

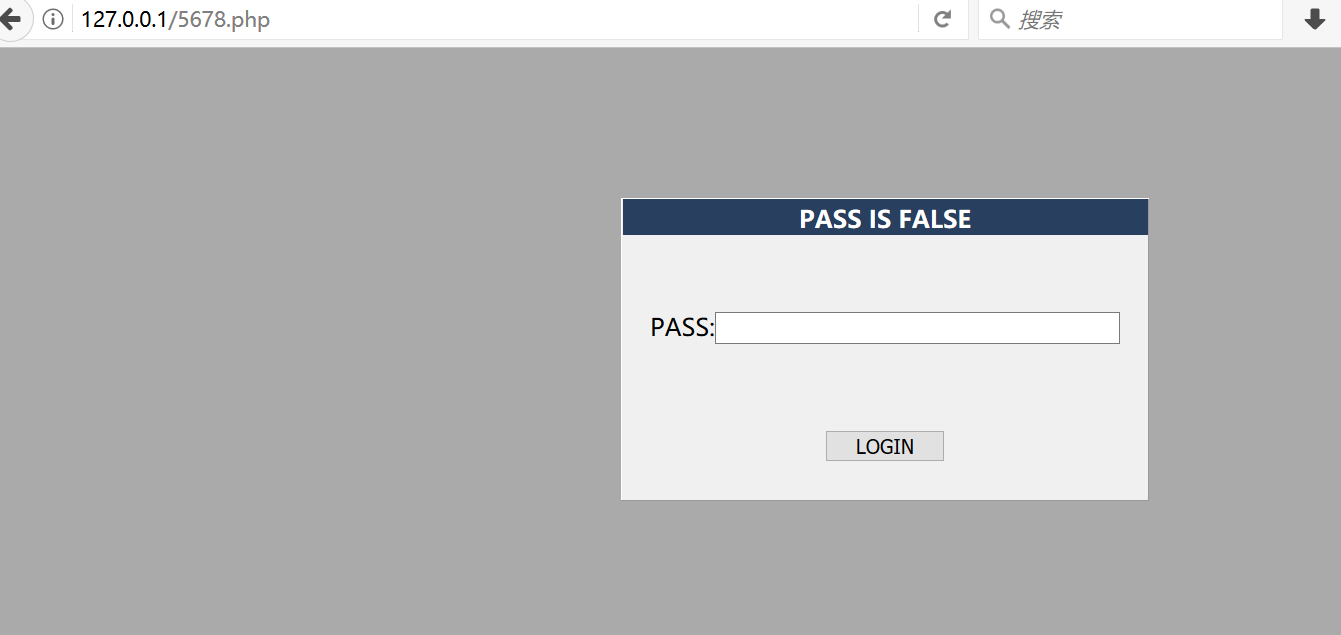


在来看看系统日志，查看15号日志未发现登录通过shell连接系统，16号日志也未发现异常。

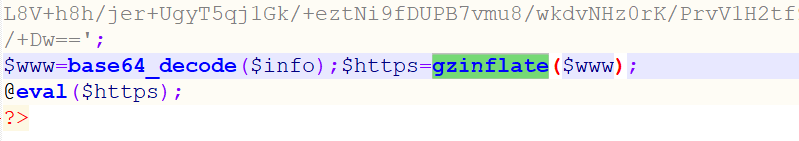


## 后门木马分析

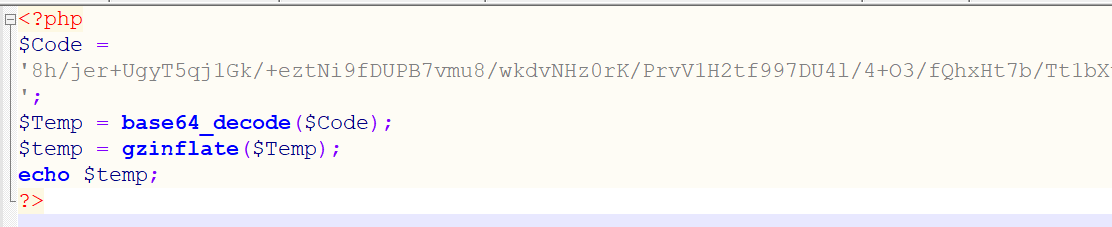
最后来简单分析下发现的5678.php的后门木马，本地搭建测试环境，木马访问如下：



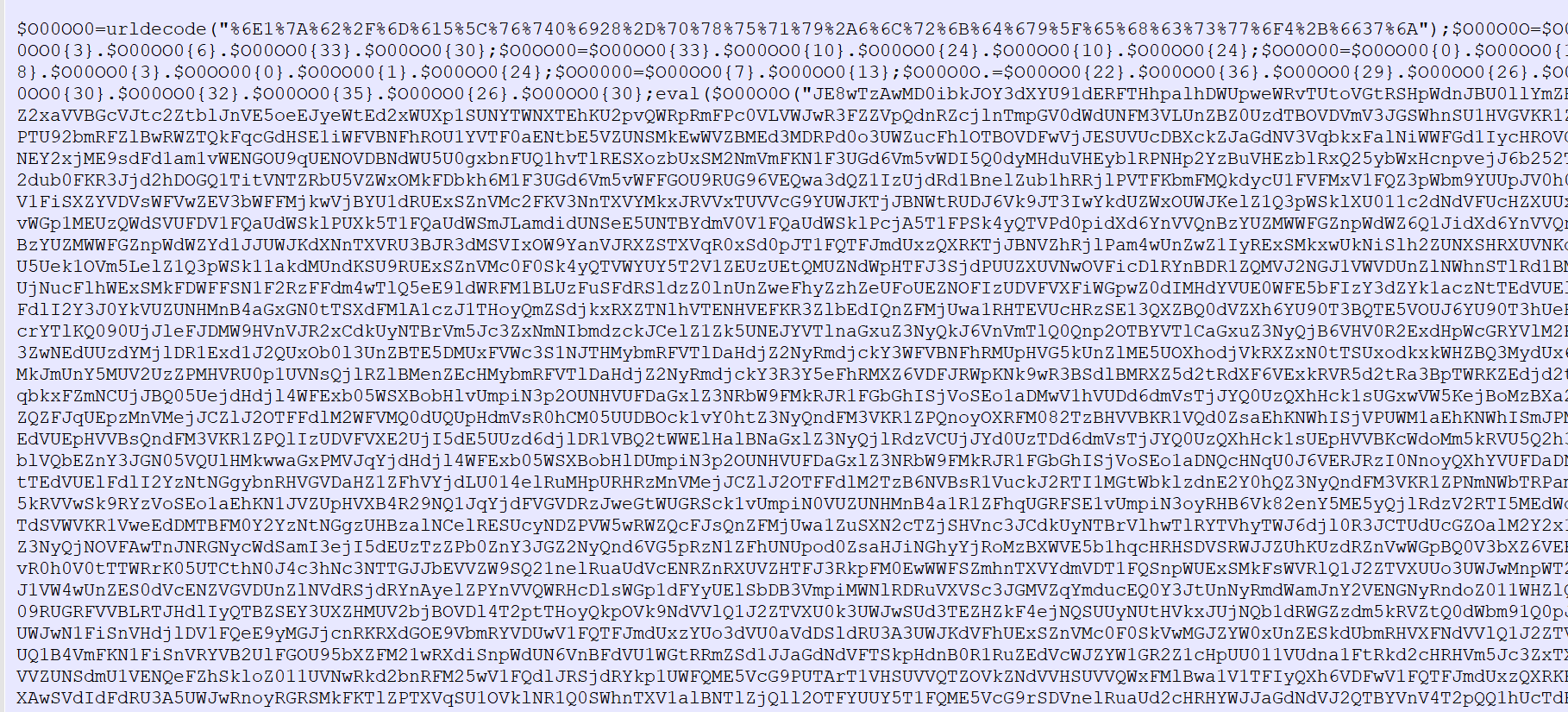
万事俱备只差password，从5678.php的具体内容来看，就是先对info内容进行base64解码，然后又利用gzinflate函数进行解压，然后执行，然而还是不知道密码。



那就先利用base64\_decode解码、在gzinflate解压，看看输出个啥



具体结果输出如下，看着是一脸茫然，输出的这是些什么东东



虽然很长，乍一看不知道是啥，但是其实就是就是一段php代码，执行了7句代码，生成如下参数

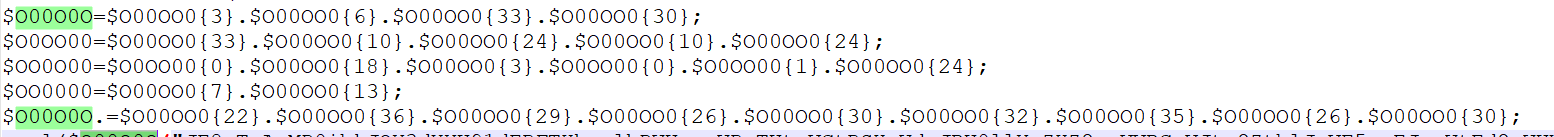
第一步先是利用urldecode生成$O00OO0，



echo $O00OO0,输出的结果如下：

n1zb/ma5\vt0i28-pxuqy\*6lrkdg9\_ehcswo4+f37j

第二步生成$O00O0O



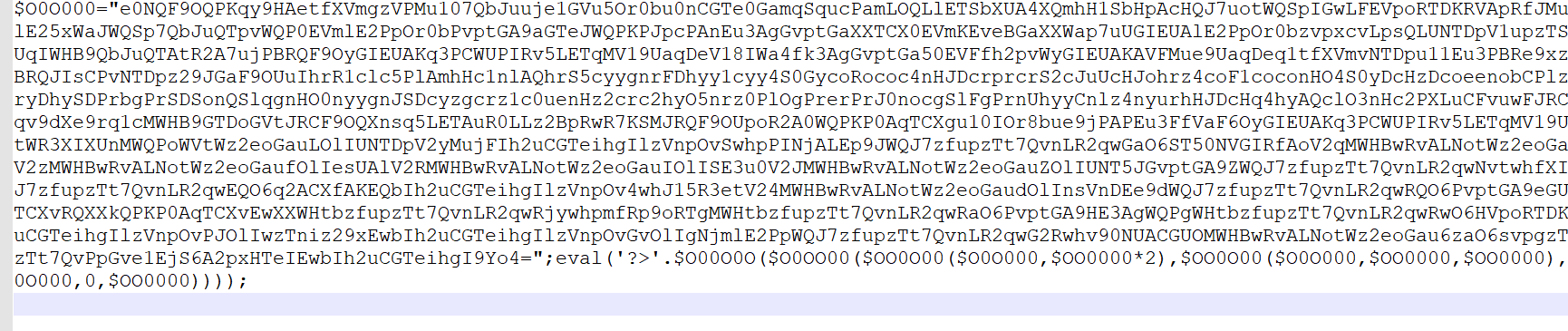
echo $O00O0O,输出结果如下：

base64\_decode

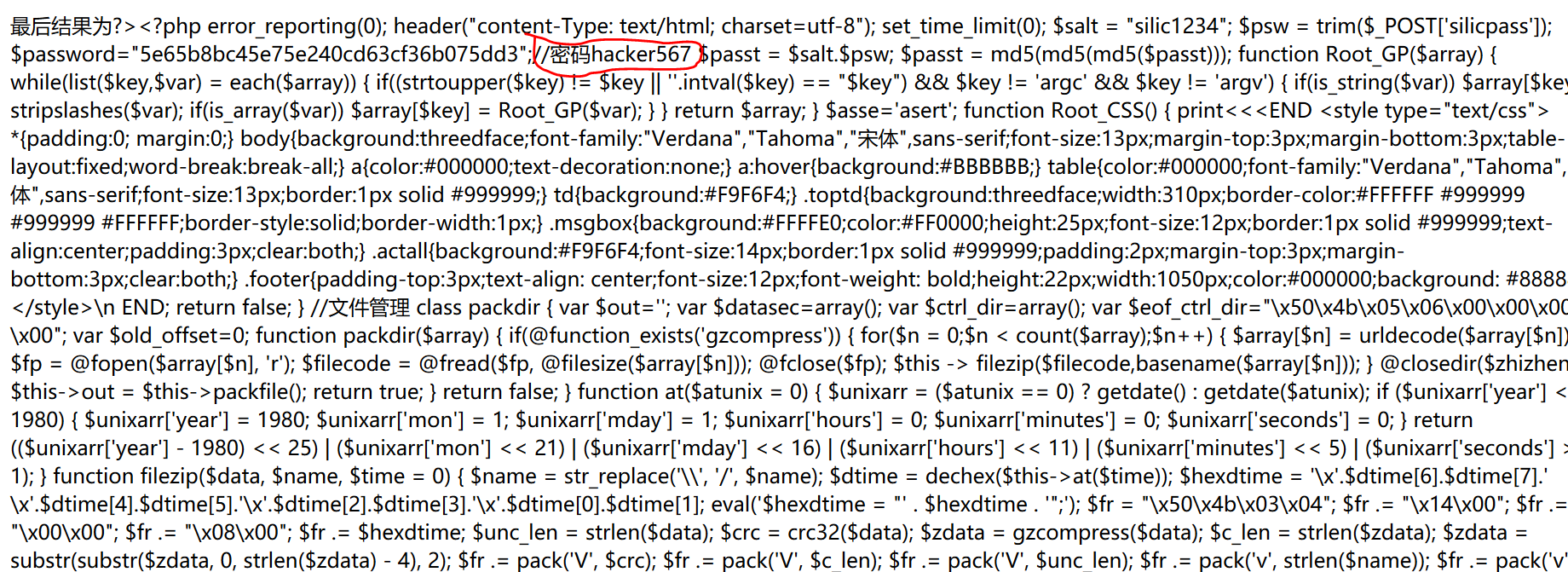
最后将eval替换为echo，$O00O0O替换为base64\_decode，



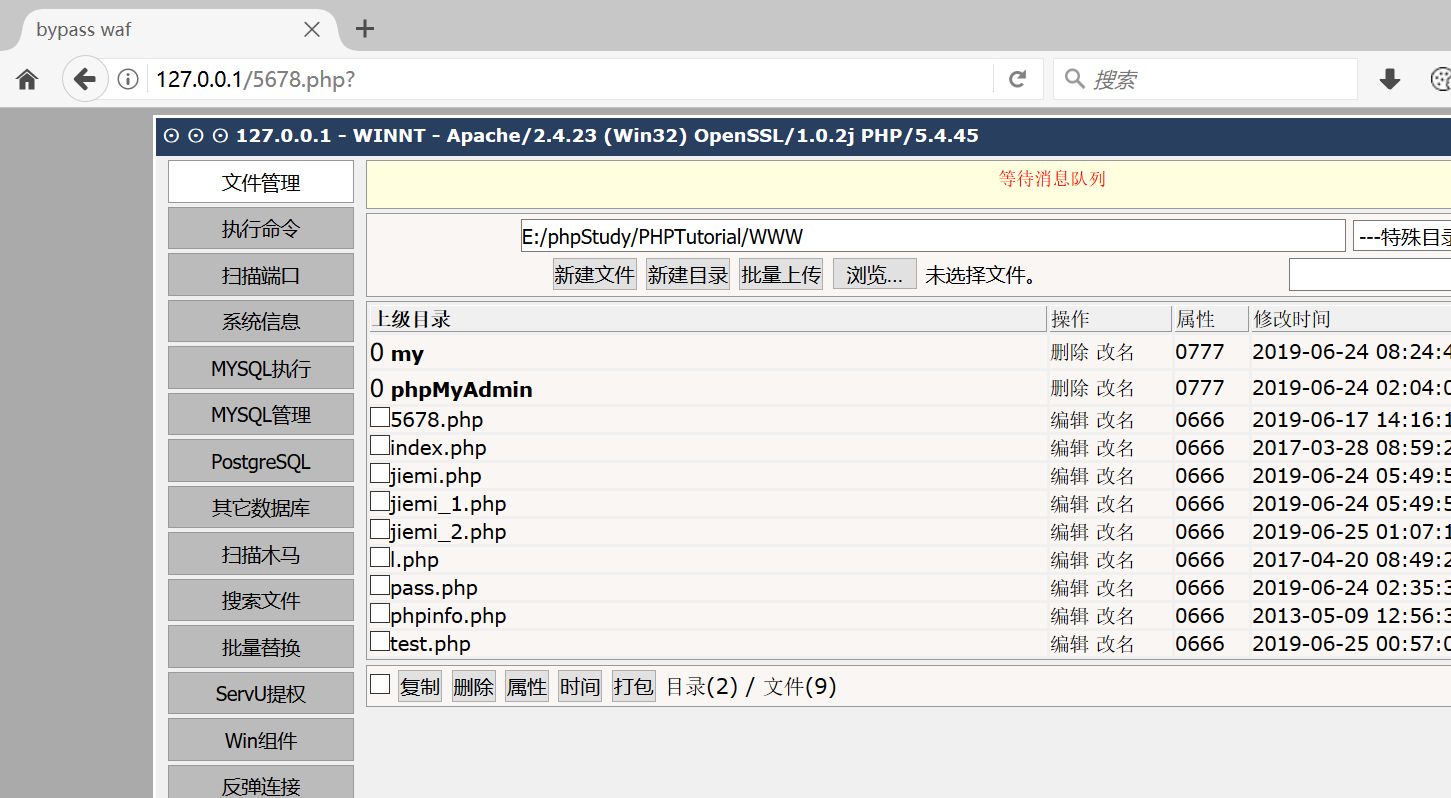
结果输出如下：



此时在将eval修改为echo，即可成功输出我们期待已久的结果，密码为hacker567



可成功登录后门



本次应急过程整体比较简单，最大的收货就是捕获的两只后门马，以及对5678.php的分析，最附上两只马的下载地址以及对5678.php的分析脚本：<https://github.com/tide-emergency/php->

# 攻击溯源

从日志中分析可看出最早从19年1月份，就有利用thinkphp命令执行漏洞进行攻击，进行目录枚举，利用织梦注入漏洞、添加后台用账户等通用性漏洞进行攻击尝试，虽然均未成功，但系统处于水深火热之中。

通过日志分析攻击成功的可疑ip地址如下：112.114.103.247、112.114.103.122、112.114.105.17、112.114.101.202、112.114.102.234，其ip归属地均为云南省临沧市，上述地址在5月21日、6月13日均访问过5678.php的后门程序。

# 安全建议

删除相关敏感文件或进行访问控制，防止被恶意攻击者利用。