转 几个有意思的客户端漏洞

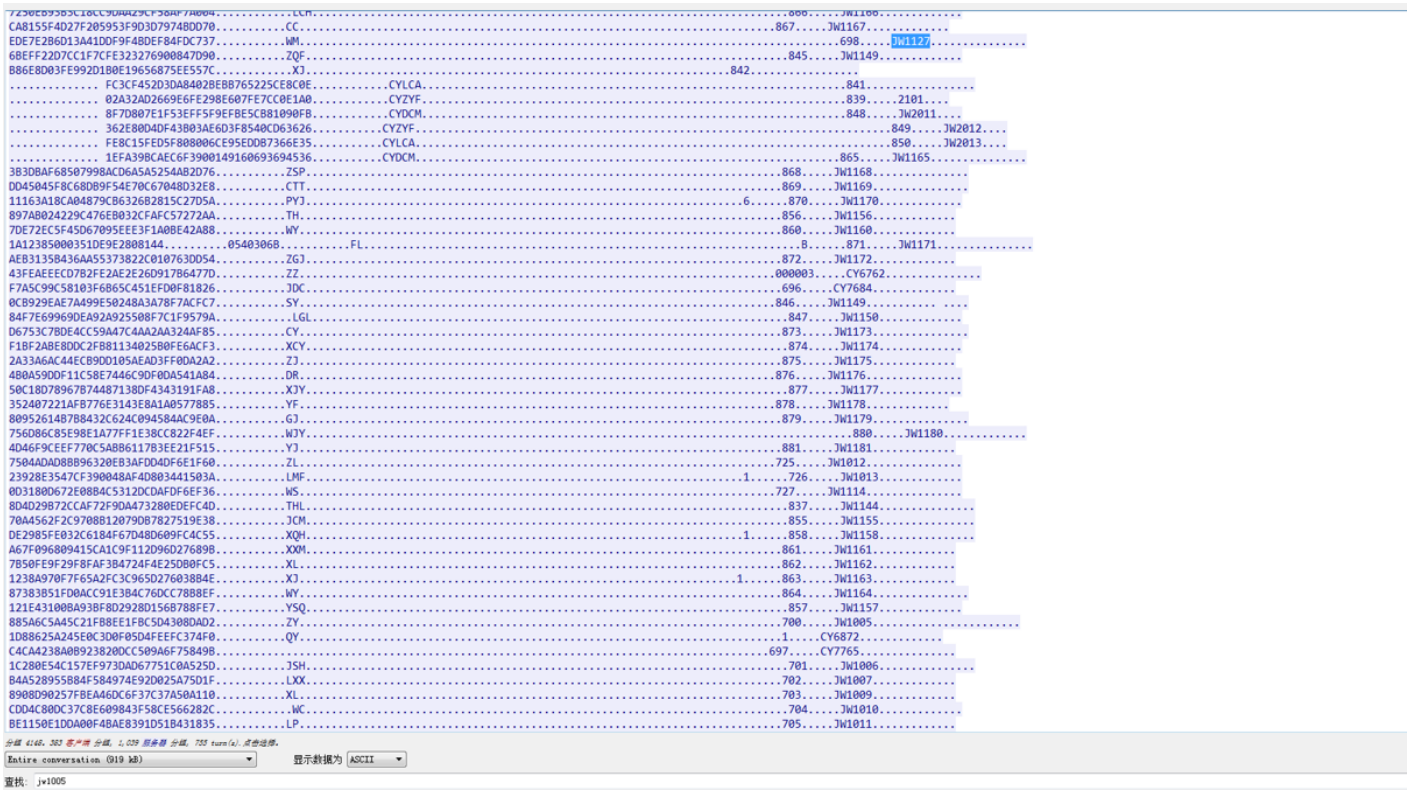
2019年03月30日 20:17:00 weixin_30685047 阅读数 5

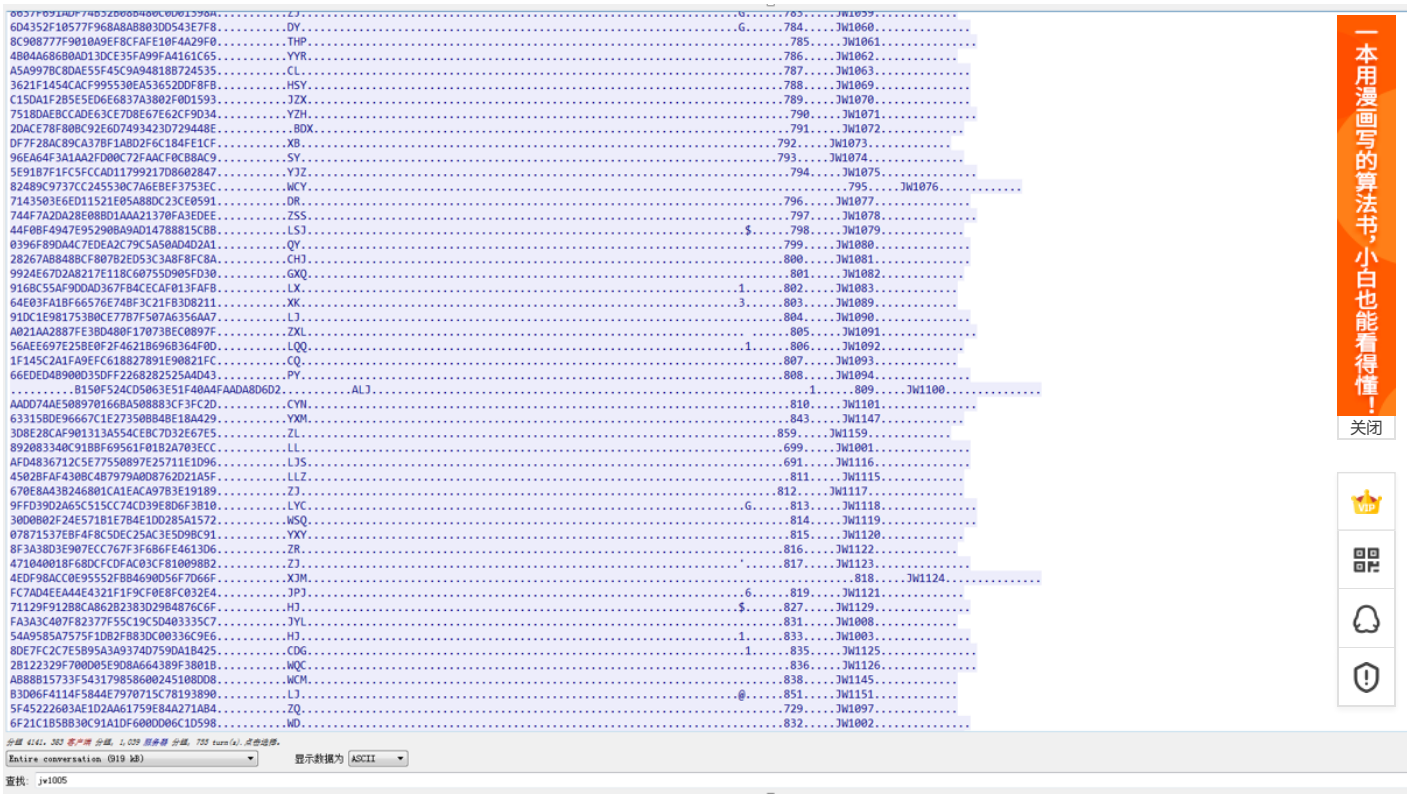
原文链接：http://www.cnblogs.com/Rakjong/p/10628701.html

平时测试客户端时发现了几个比较有意思的客户端漏洞，记录一下。

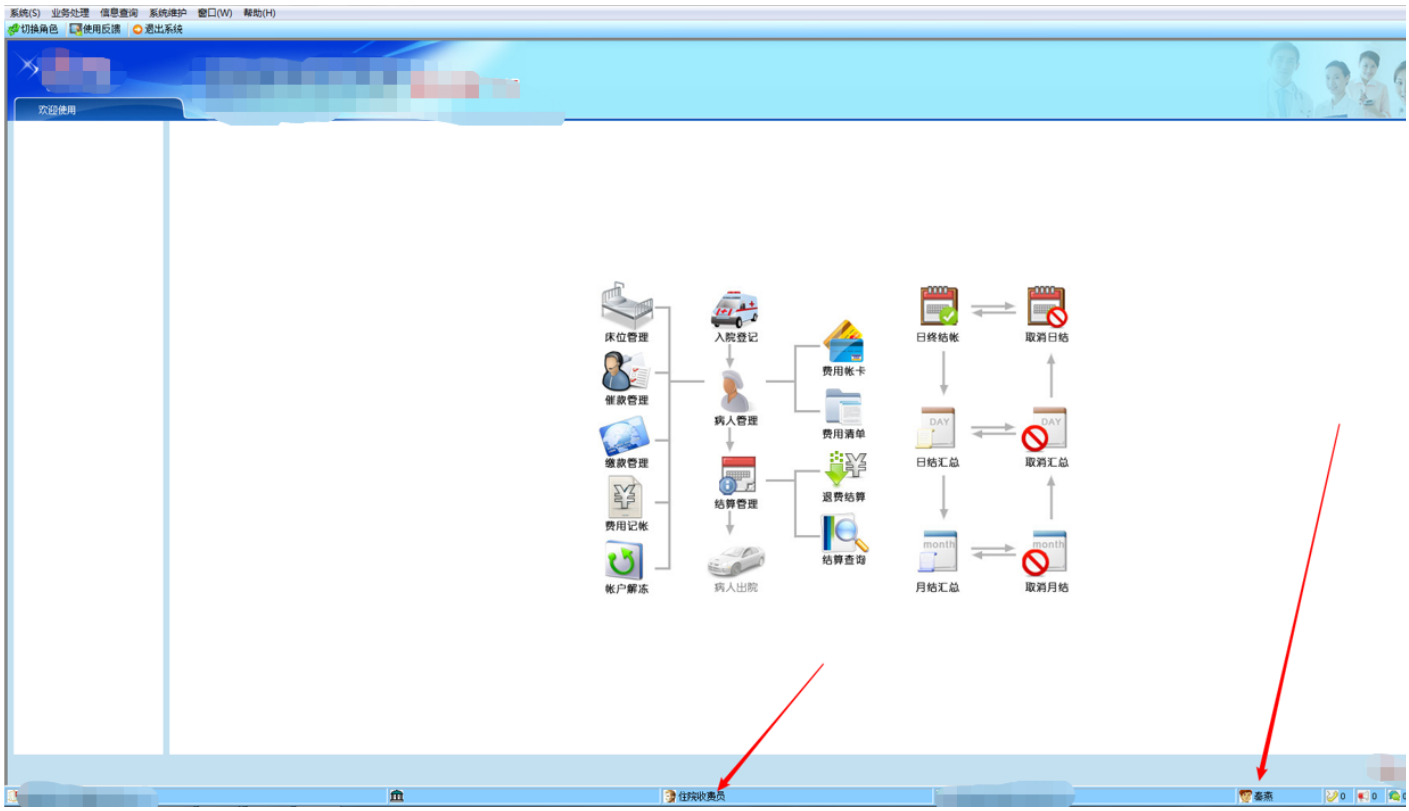
- **非必要的数据传输**

系统登录时，某个数据包会返回系统所有的用户名和加密的MD5密码：



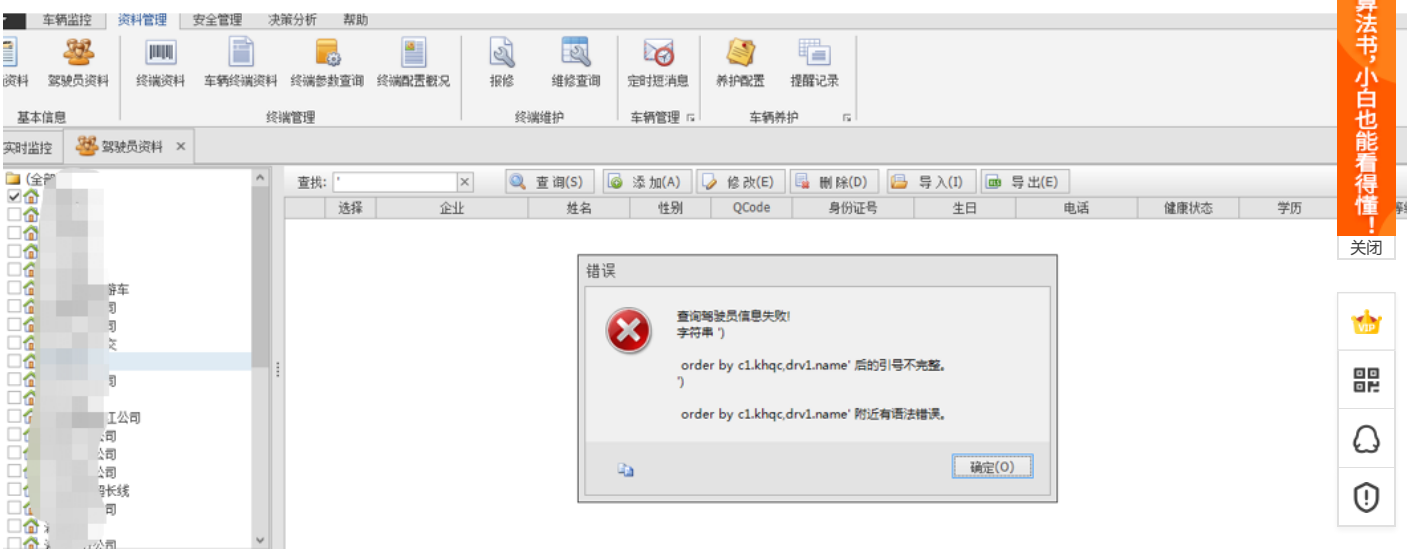


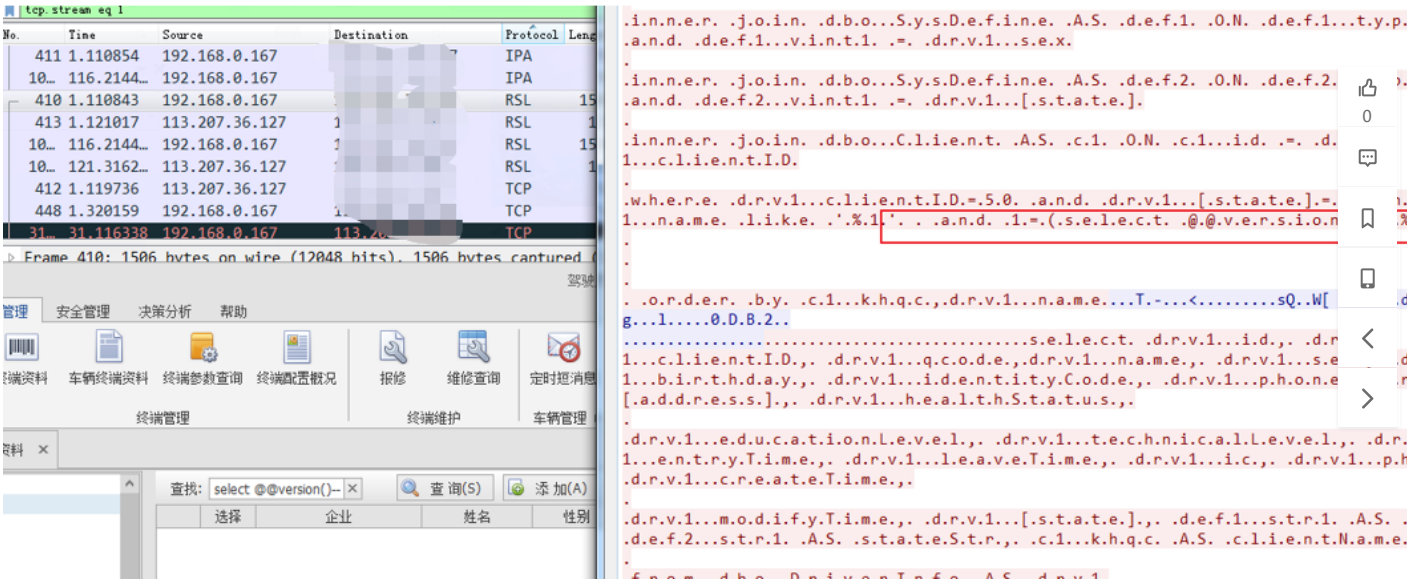
解密以后使用账户密码即可登录任意用户：



- **SQL注入**

参数未经过滤直接带入数据库查询：

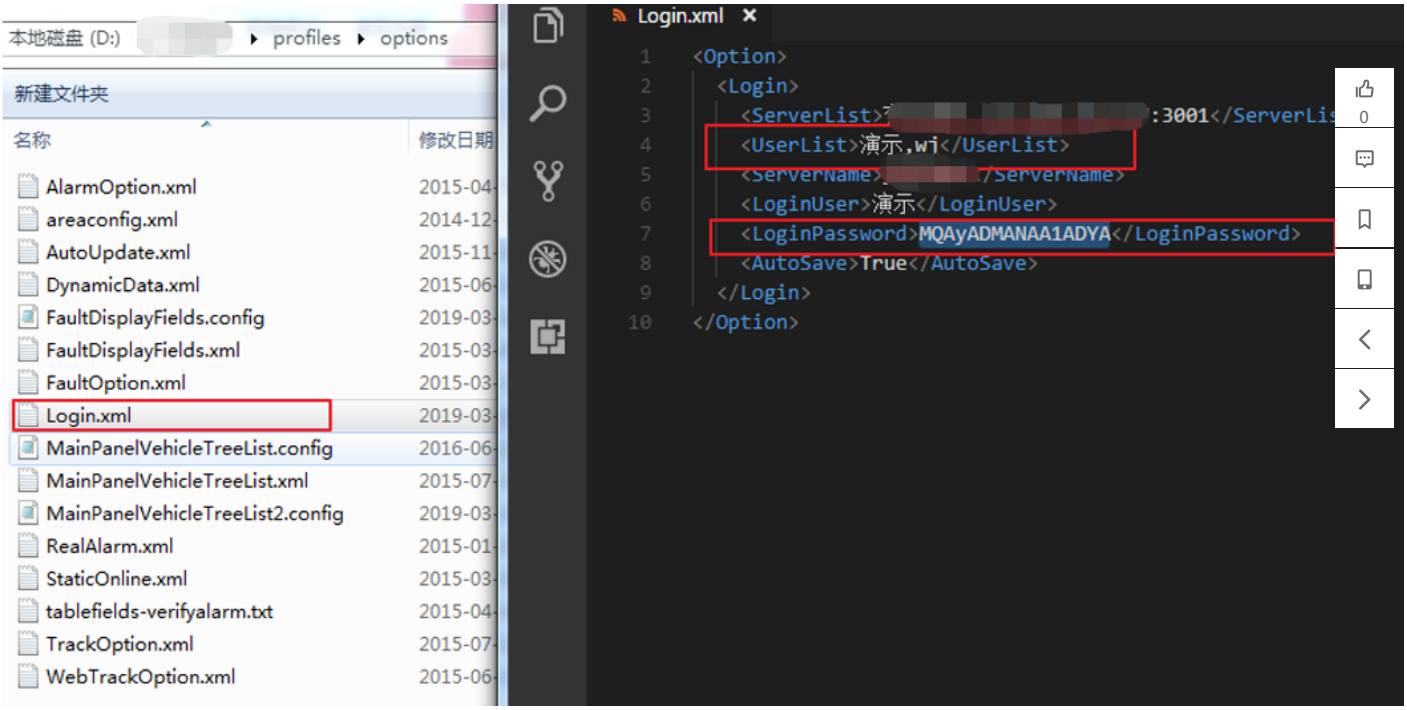




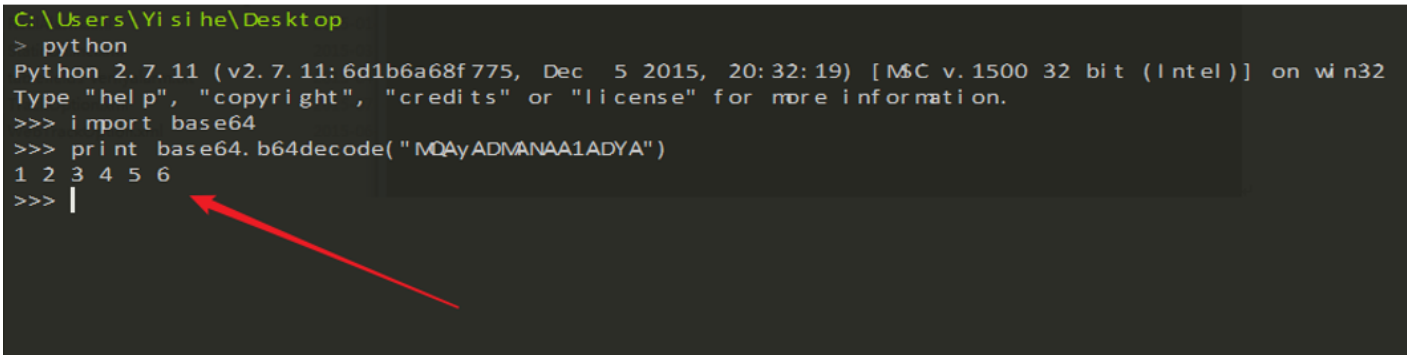
万能密码登录：

- **本地静态文件信息泄露**

登录成功后，登录的用户名密码会保存：



密码是base64加密：



over~

转载于:https://www.cnblogs.com/Rakjong/p/10628701.html