

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：

```
7296E995B3C18C7904429CF380F78060.....LCN.....000.....Jm1100.....
CAB155F4D27F205953F903D797480D7B.....CC.....867.....Jm1167.....
EDE7E2B6D13A41DD9F9480EF84FDC737.....WM.....698.....Jm1172.....
68EFF22D7CC1F7C7FE323276900847D90.....ZQF.....845.....Jm1149.....
B86E8D03FE992D1B0E19656875EE557C.....XJ.....842.....
FC3CF452D3D484028EBB765225C8C0E.....CYLCA.....841.....
02A32AD26696FE298E607FE7CC0E1A0.....CYZYF.....839.....2101.....
8F7D807E1F53EFF5F9FE85CB81090F8.....CYDCM.....848.....Jm2011.....
362E8004DF43803AE6D3F85480CD63626.....CYZYF.....849.....Jm2012.....
FEB815FED5F808006CE95ED087366E35.....CYLCA.....858.....Jm2013.....
1FA399CAEC6F3900149160693694536.....CYDCM.....865.....Jm1165.....
3B3D8AF6850798ACD6A5A5254A8D07B.....ZSP.....868.....Jm1168.....
DD45045F8C68D09F54E70C7648D32E8.....CTT.....869.....Jm1169.....
11163A18CA04879C86326B2815C27D5A.....PYJ.....870.....Jm1170.....
897AB024229C476EB032CFAFC57272AA.....TH.....856.....Jm1156.....
7DE72EC5F45067095EE3F1A00E42A88.....WY.....860.....Jm1160.....
1A12385000351DE9E28008144.....05403068.....FL.....8.....Jm1171.....
AEB31358436AA55373822C010763D054.....ZGJ.....872.....Jm1172.....
43FEAEECD7B2FE2AE2E26D917B6477D.....ZZ.....000003.....CY6762.....
F7A5C99C58183F6865C451EFD08F1826.....JDC.....696.....CY7684.....
KC8929EAE7A4995E8248A3A78F7AC7C7.....SY.....846.....Jm1149.....
84F766969D6A924D550B7FC1F9579A.....LGL.....847.....Jm1158.....
D6753C7BDE4C59A47C4AA2AA324AF85.....LMF.....873.....Jm1173.....
F18F2ABE8DDC2F88113402580F66AFC3.....XCY.....874.....Jm1174.....
2A33A6AC44ECB9D0185AEAD3FF8DA2A2.....ZJ.....875.....Jm1175.....
48B0A590DF11C58E7446C90F0DA5A1A84.....DR.....876.....Jm1176.....
50C18078967844871380F4343191FA8.....XJY.....877.....Jm1177.....
352407221AF8776E3143E8A1A0577885.....YF.....878.....Jm1178.....
80952614B788432C624C094584AC9E0A.....GJ.....879.....Jm1179.....
756086C85E98E1A77F1E38C822F4EF.....WJY.....880.....Jm1180.....
4D46F9CEE770C5AB86117B3EE21F515.....YJ.....881.....Jm1181.....
7584AD08B896320EB3AF0D40F6E1F68.....ZL.....725.....Jm1012.....
23928E3547CF390040AF4D803441583A.....LMS.....1.....726.....Jm1013.....
8D03180672E08B4C5312DCDAFDF6EF36.....LNF.....727.....Jm1114.....
8D4D29872CAF72F9D0A73280EDEF4D.....THL.....837.....Jm1144.....
70A4562F2C970881297087827519E38.....JCM.....855.....Jm1155.....
DE2985F032C6184F67D48D609FC4C55.....XQH.....1.....858.....Jm1158.....
A67F096809415CA1C9F112D96D276898.....XOM.....861.....Jm1161.....
7B50F9F29F8FAF384724F4E25D08FC5.....XL.....862.....Jm1162.....
1238A970F7F65A2FC3C965D27603884E.....XJ.....1.....863.....Jm1163.....
8738351F0A8CC91E3B4C76DC7888BF.....WY.....864.....Jm1164.....
121E431008A938F802928D1568788FE7.....YSQ.....857.....Jm1157.....
8854C5A45C21F08E1E9C9A0800A0.....ZY.....780.....Jm1005.....
1D88625A245E0C306F05DAFEFC374F0.....JSH.....1.....CY6872.....
CACAA238A0B923820DC509A6F758498.....JY.....697.....CY7765.....
1C280E54C157EF973DAD67751C0A525D.....QH.....701.....Jm1006.....
84A528955884F584974E92D025A75D1F.....LXK.....702.....Jm1007.....
8980D90257F8EA6DC6F37C37A50A110.....XL.....703.....Jm1009.....
CD0AC80DC37C8E609843F58CE566282C.....WC.....704.....Jm1010.....
BE1150E1D0A08F4BAE8391D51B431835.....LP.....705.....Jm1011.....
```

分块 416B, 262 客户端分块, 1,039 服务器分块, 755 turn(s), 灰色选择.

Entire conversation (919 kB)

显示数据为 ASCII

查找: j=1005

```
0057797310DF74D32D0E0400E00E1290A.....CJ.....703.....Jm1039.....
6D4352F10577968A8A8803D0543E7F8.....DY.....G.....784.....Jm1060.....
C8908777F9010A9E8CFAF10F4A29F0.....THP.....785.....Jm1061.....
480A468680AD13DCE35FA99FA4161C65.....YVR.....786.....Jm1062.....
A5A9978C8DAE55F45C9A48188724535.....CL.....787.....Jm1063.....
3621F1454CACF995530EA53652D0F8F8.....HSY.....788.....Jm1069.....
C15DA1F2B5E5ED6E6837A3802F001593.....JZX.....789.....Jm1070.....
7518DAEBCCADE63CE7D08E67E62CF9034.....YZH.....790.....Jm1071.....
2D4C7E8FB98C92E6D749342072048E.....BDX.....791.....Jm1072.....
DF7728AC8CA378F1A8284C6184FE1CC.....JY.....792.....Jm1073.....
96AE4F43A1AA2FD08C72FAACF0C8BAC9.....SY.....793.....Jm1074.....
5E9187F1FC5CCAD1179921D086D847.....YJZ.....794.....Jm1075.....
82489C9737C245530C7A6E8EF3753EC.....WCY.....795.....Jm1076.....
7143503E6D11521E05A880C23CE0591.....DR.....796.....Jm1077.....
744F7A2D28E088D1AA21370FA3EEDDE.....ZSS.....797.....Jm1078.....
44F08F4947E952908A9AD14788815CB8.....LSJ.....798.....Jm1079.....
0396F89D04C7E0EA2C79C5A50AD4D2A1.....QY.....799.....Jm1080.....
28267AB8488CF80782ED53C3A8F8FC8A.....CHJ.....800.....Jm1081.....
9924E67D2A8217E11860755D905F030.....GQX.....801.....Jm1082.....
9168C55AF9D0AD367F8ACECA8F013FAF8.....LX.....1.....802.....Jm1083.....
6AE03FA1BF66576E74BF3C21F8308211.....JK.....3.....803.....Jm1089.....
91DC1E98175380CE77B7F507A6356AA7.....LJ.....804.....Jm1090.....
A021AA2887FE3BD480F170738EC0897F.....XL.....805.....Jm1091.....
56AE697E25B0F2F4621B6968364F00.....LQJ.....1.....806.....Jm1092.....
1F145C2A1FA9EFC618827891E90821FC.....CQ.....807.....Jm1093.....
66EDED4900D3DFF226828255A04D3.....PY.....808.....Jm1094.....
.....B150F524CD5063E51F48A4FAAD8D0D2.....ALJ.....1.....809.....Jm1100.....
AAD074AE508970166A8508883CF3FC2D.....CYN.....810.....Jm1101.....
633158D0E96667C1E273508848E18A429.....YXM.....843.....Jm1147.....
308E28CAF9013134974CE8C7D326A7E5.....ZL.....859.....Jm1159.....
89208340C918B8F69561F0182A783ECC.....JPI.....699.....Jm1081.....
AFD4836712C5E77550897E2571E1D096.....LJS.....691.....Jm1116.....
45028FAF4308C87979A080762D21A5F.....LZL.....811.....Jm1115.....
670E8AA3246801CA1EAC9783E19189.....ZJ.....812.....Jm1117.....
9FFD39D2A6C515CC7ACD39E806F3B10.....LYC.....G.....813.....Jm1118.....
300D802F24E57181E7B4E1D0285A1572.....WSQ.....814.....Jm1119.....
07871537EBF4F8C5DEC25AC3E5098C91.....YXY.....815.....Jm1120.....
8F3A38D3E907CC7673F686FE4613D6.....ZR.....816.....Jm1122.....
471040818F68DCFDCAF03CF81009882.....ZJ.....817.....Jm1123.....
4EDF984CC0E95552F8B469D056F7D66F.....XJM.....818.....Jm1124.....
FC7AD4CE0A4E4321F9C79E8FC032E4.....HJ.....6.....827.....Jm1129.....
71129F912B8CA86282383D2984876C6F.....JYL.....831.....Jm1008.....
FA3AC407F82377F55C19C5D403335C7.....JLZ.....1.....833.....Jm1003.....
54A9585A7575F1D0B2F883D0C00336C9E6.....CDG.....1.....835.....Jm1125.....
80E7C2C7E5B95A3A9374D759DA1B425.....WQC.....836.....Jm1126.....
2812329F700D05E908A6643B9F3801B.....MCM.....838.....Jm1145.....
AB88B1573F543179858600245108D08.....LJ.....@.....851.....Jm1151.....
83D06F4114F5844E7970715C78193890.....ZQ.....729.....Jm1097.....
5F45222603AE1D2AA61759E84A271A84.....MD.....832.....Jm1002.....
6F21C1B58B36C91A1D1F600D006C1D598.....
```

分块 416B, 262 客户端分块, 1,039 服务器分块, 755 turn(s), 灰色选择.

Entire conversation (919 kB)

显示数据为 ASCII

查找: j=1005

一本用漫画写的算法书小白也能看得懂！

关闭

VIP

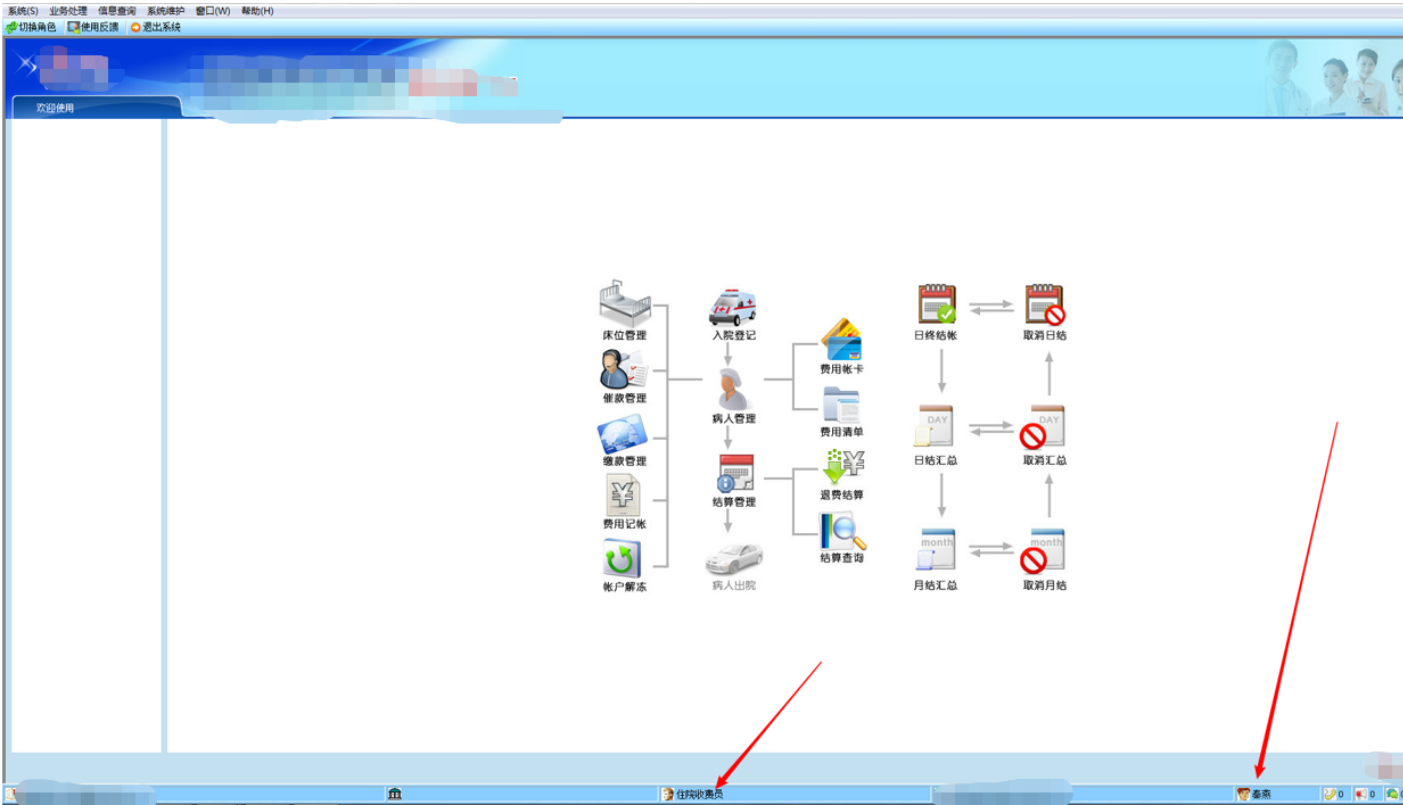
扫一扫

消息

通知

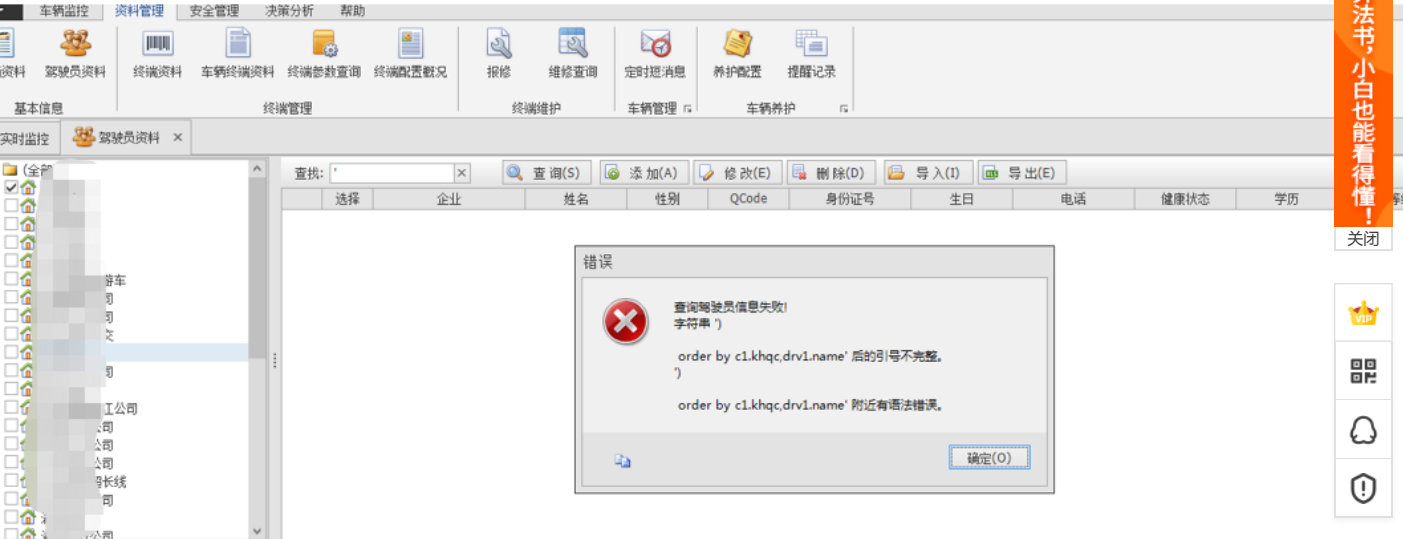


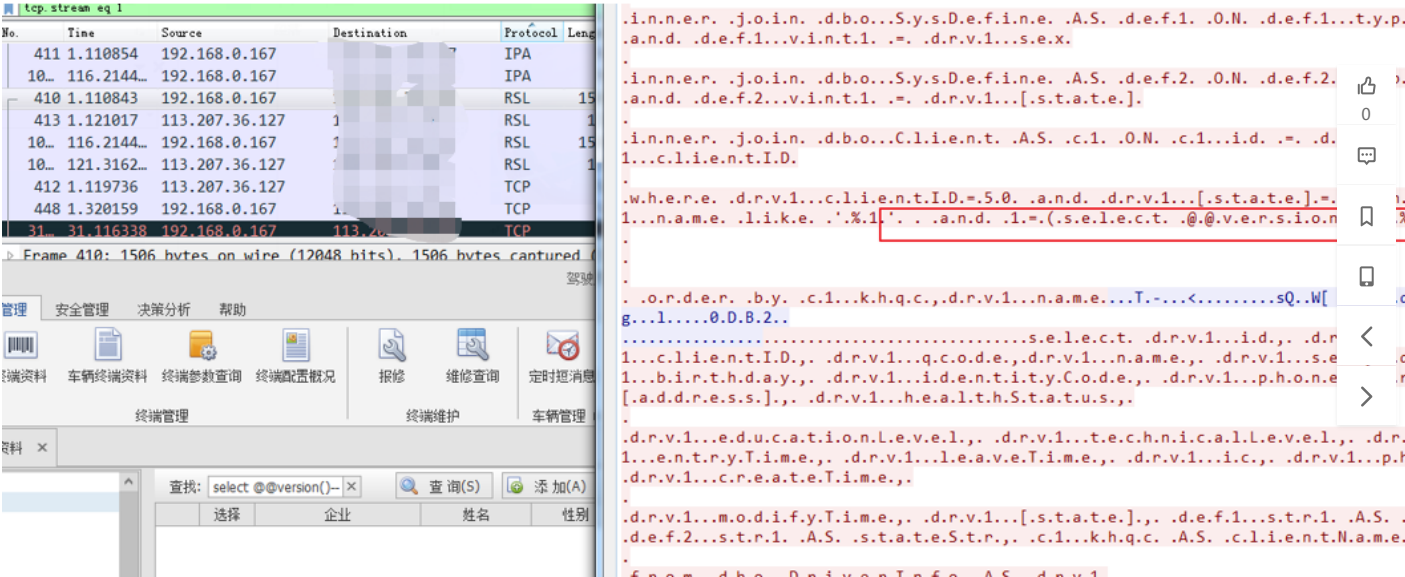
解密以后使用账户密码即可登录任意用户：



• SQL注入

参数未经过滤直接带入数据库查询：



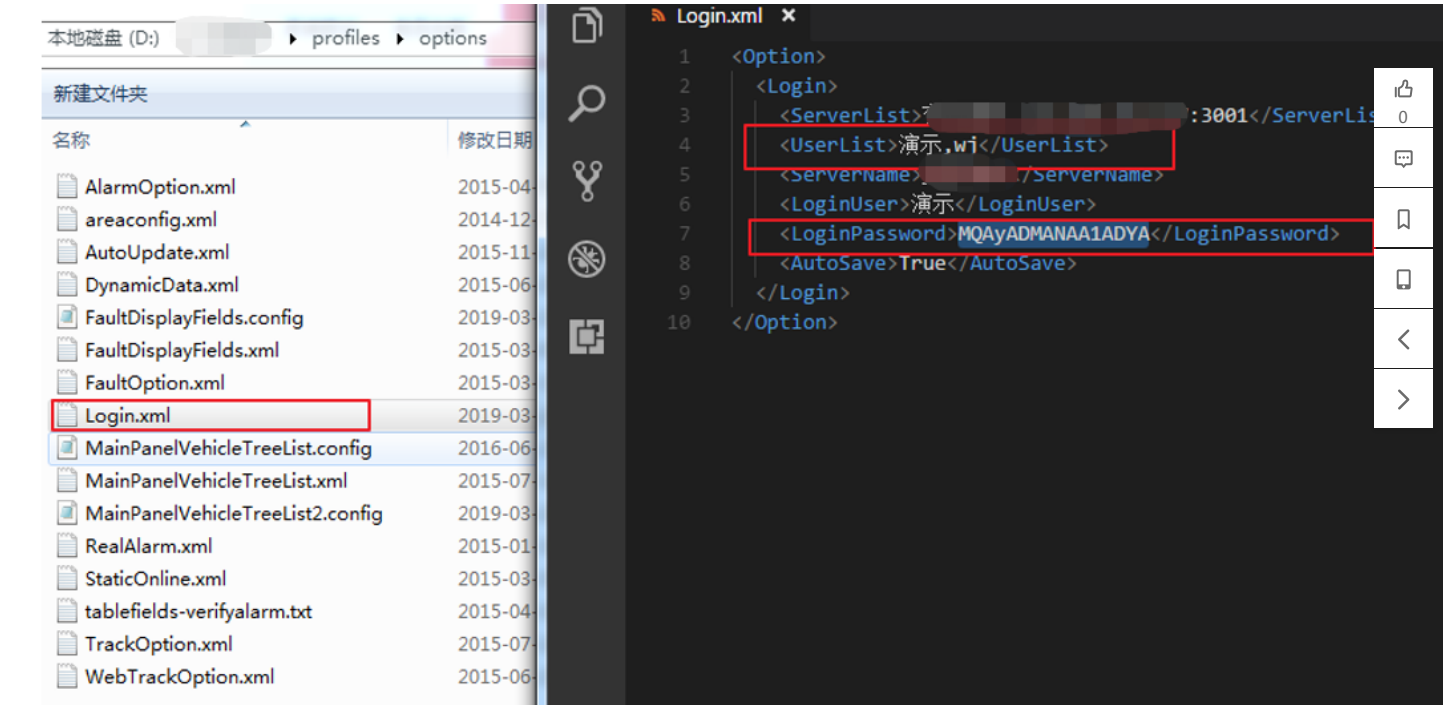


万能密码登录：

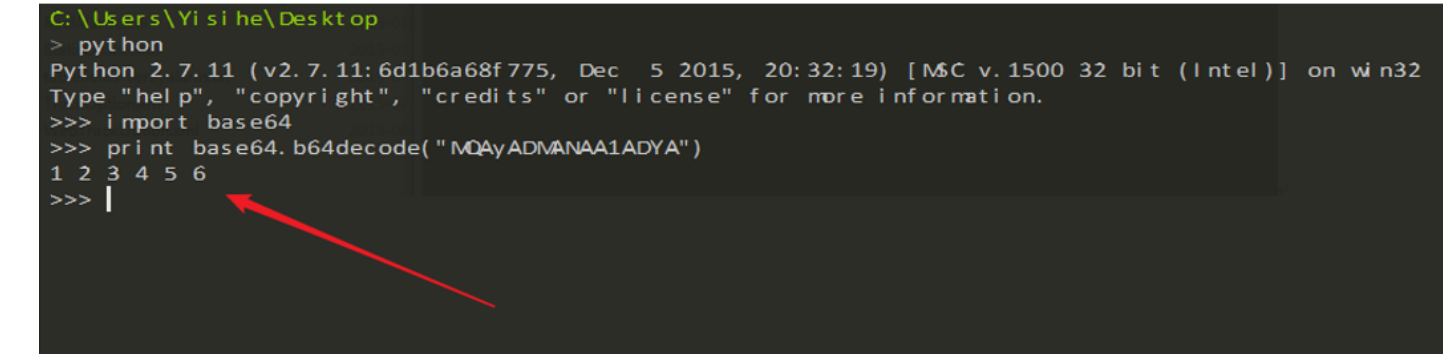


• 本地静态文件信息泄露

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>

中国真正厉害的只有一种人：三不卖七不买，盈利一辈子都不会停止
永盛·顶新

博主设置当前文章不允许评论。

移动客户端安全漏洞等级划分 阅读数 399
移动客户端安全漏洞等级划分移动客户端安全漏洞等级划分我们将漏洞危害程度分为：严重、高危、中... 博文 来自： Leslie_Yu的博客

几个超级有意思的网站 阅读数 39
来自公众号浅黑科技(ID:qianheikeji)Dos游戏博物馆首先贴出网站Dos游戏博物馆里面收录了还是Dos... 博文 来自： weixin_33832...

我常用的几个比较有意思的网站 阅读数 268
###部分手段需要/科/学/上/网上网类Chrome+Google——程序员必备Tor——深层网络(只可意会不... 博文 来自： Dan的博客

几个有趣的AI项目 阅读数 746
没事的时候可以玩一玩。。1. 从零开始造一个“智障”聊天机器人--基于TensorFlow，seq2seq模型2.... 博文 来自： 大羚羊的学习...