BUUCTF greatescape

原创

wangjin7356 于 2022-01-05 09:47:37 发布 573 收藏

分类专栏： CTF 文章标签： 安全

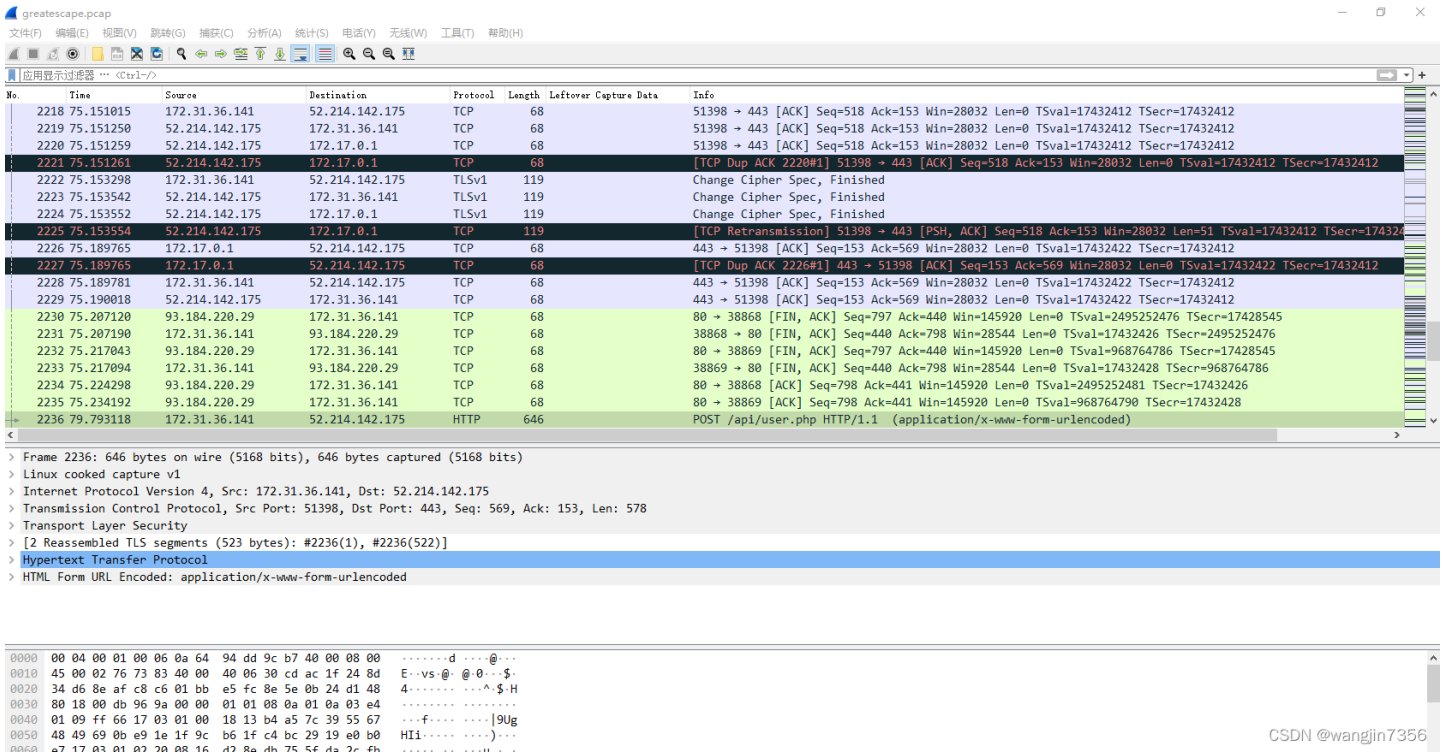
本文链接：https://blog.csdn.net/wangjin7356/article/details/122316562

题目链接

```
https://buuoj.cn/challenges#greatescape
```

解题过程

打开流量包，传统步骤：追踪流、导出HTTP对象、查找特定字符串。

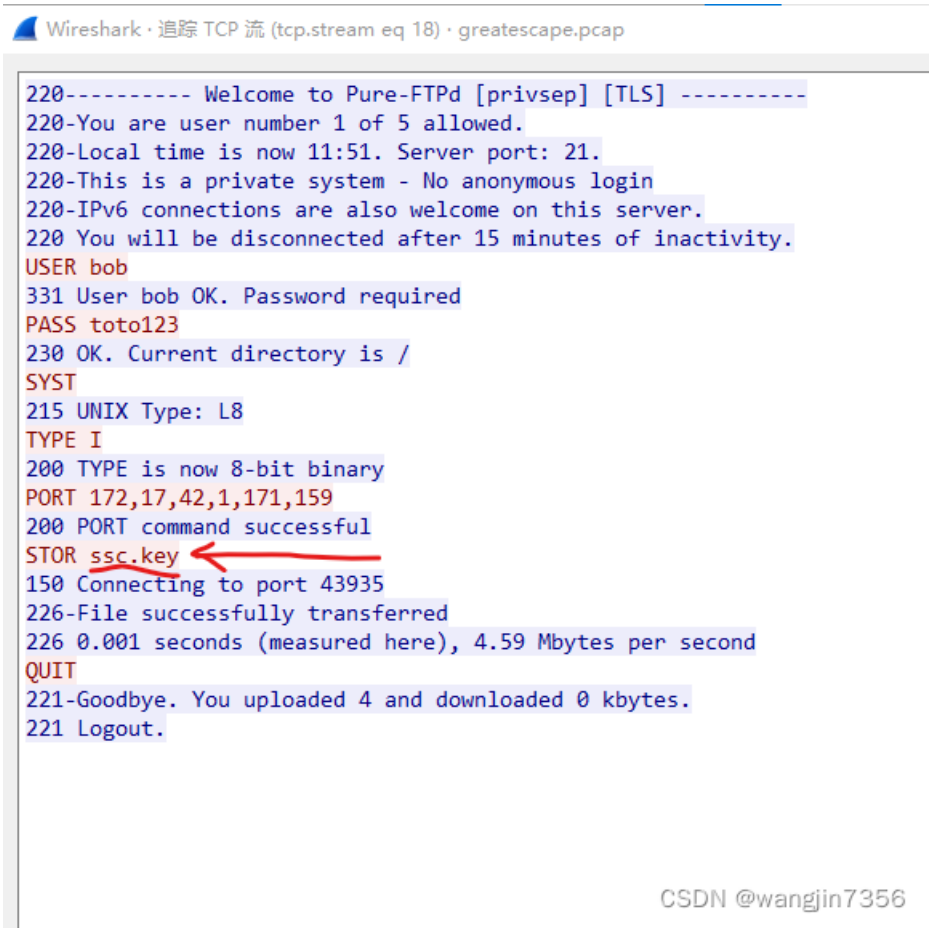


追踪到TCP Stream eq 19时发现了密钥

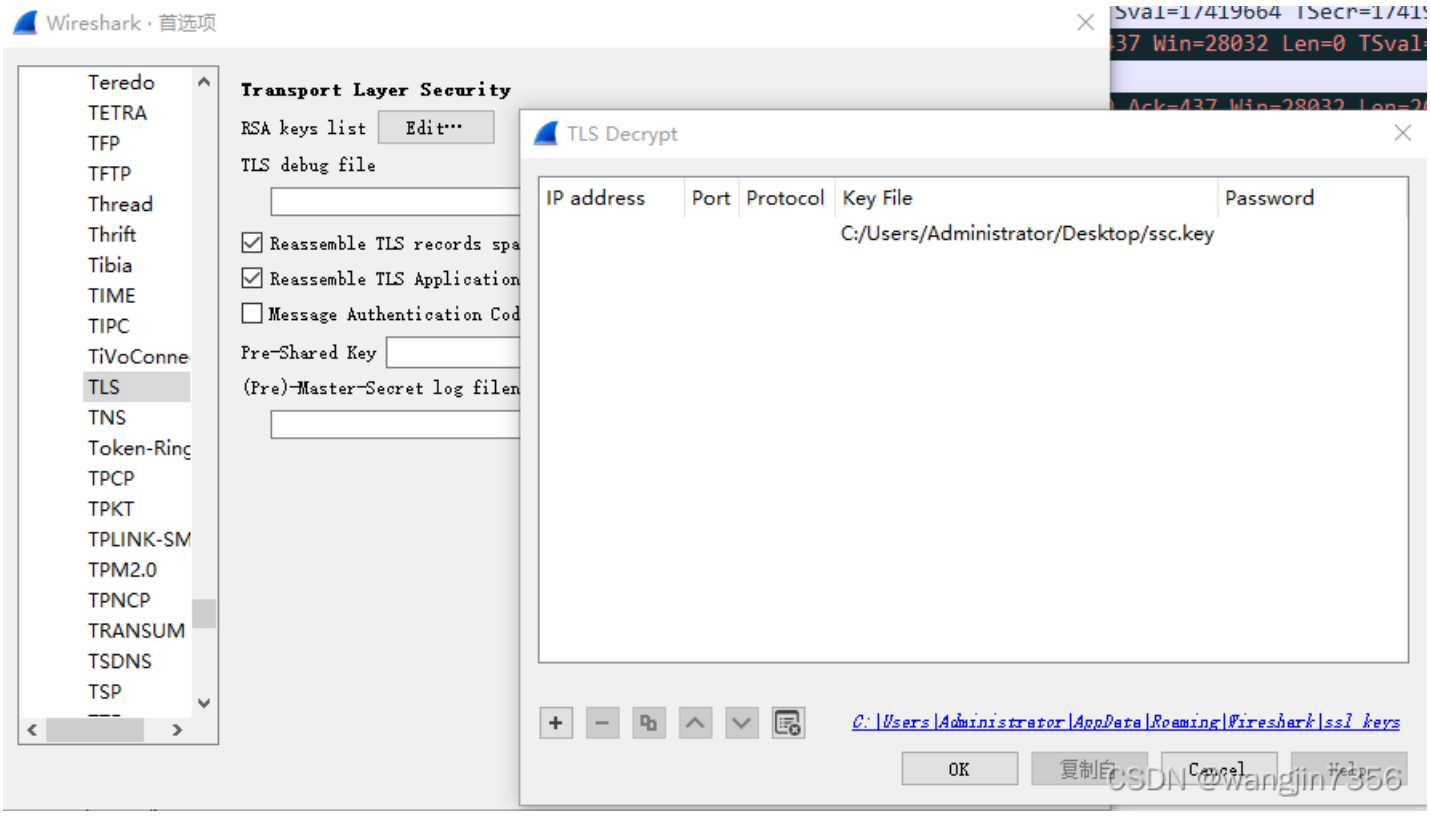
Wireshark · 追踪 TCP 流 (tcp.stream eq 19) · greatescape.pcap

```
-----BEGIN PRIVATE KEY-----
MIIJQwIBADANBgkqhkiG9w0BAQEFAASCCS0wggkpAgEAAoICAQC5twyPH+2U6X0Q
uxOKPTHSR6MkXGSvAz+Ax+G9DKEiBLuTTfl7dNv4oswdmT9nWlSY1kxZatNwlUF8
WAuGLntO5xTEmOJlMtBFrWGD+DVpCE9KORGvyif8e4xxi6vh4mkW78IxV03VxHM0
mk/cq5kkERfWQW81pVeYm9UAm4dj+LcCwQ9aGd/vfTtcACqS5OGtELFbsHJuFVyn
srpp4K6tLtRk2ensSnmXUXNEjqpodfdb/wqGT86NYg7i6d/4Rqa440a6BD7RKrgp
YPaX17pQusemHQPd248fxsuEfEwhPNDJhIb8fDX9BWv2xTfBLhGwOh7euzSh2C4o
KSuBAO+bIkL+pGY1z7DFtuJYfTOSJyQ5zQzToxS+jE+2x9/3GpD2LUD0xkA8bWhv
eecq0v6ZWBVYNX54V5ME3s2qxYc6CSQhi6Moy8xWlcSpTSAa7voNQNa9RvQ4/3KF
3gCbKtFvdd7IHvxfn8vcCrCZ37eVkq0Fl1y5UNeJU/Y0Tt8m7UDn3uKNpB841BQa
hiGayCSjsHuTS8B+MnpnzWCrzD+rAzCB37B599iBK4t/mwSIZZUZaqxTWNoFS2Lz
7m0LumZ4Yk8DpDEuWhNs8OUD8FsgAvWFVAvivaaAciF3kMs8pkmNTs2LFBowOshz
SXfONsHupgXEwwFrKOOZXNhb+O/WKQIDAQABAoICAAT6mFaZ94efft/c9BgnrddC
XmhSJczfXGt6cF3eIc/Eqra3R3H83wzaaHh+rEl8DXqPfDqFd6e0CK5pud1eD6Y8
4bynkKI/63+Ct3OPSvdG5sFJqGS7GblWIpzErtX+eOzJfr5N5eNOQfxuCqgS3acu
4iG3XWDlzuRjgSFkCgwvFdD4Fg5HVU6ZX+cGhh2sDzTRlr+rilXTMsm4K/E8udIg
yEbv5KqWEI5y+5Eh9gWY7AnGW6TgLNxzfYyt0nhYhI2+Yh4IkRqQd6F8XQARbEhP
yZx1eK4Q/dRPQxOJNY1KkRpl+Cx6tAPVimByRx1hu82qsTstb6rLHemruOPbf5Dw
aqgSFdp7it3uqjJHCwJ2hAZoijAcvlhn1sa1hr/qFFlY/WeDAi8OyvGdCSh3OvS6
yazkah85GOnY85rz+s98F9cvIqcRdGJrAeNbUHHnj6+X9qFVtwDpF0V1vlvn2Ggp
7m8hiZ0Y+8T+7qfnS9WsdPh7MkoIEoZ0CPryYvX+YPLYWqzxtCvrRWF8tAScI6H+
XBz3NlCAUaOk+ZOkKlZ8ZYMSn/g5EV2jj/mwZVdtYoeQjLaCDuLq8E1Hswnpgq7F
54hHU7vOeJ1/TQ1tLCNfJFQRaUD+tPz9R6jVpbqBiXxIC2eiGTo1rP4Ii7hsQRFC
W0KKqu+bV69HJAmi06yBAoIBAQDvz+c+3z9njQFFaeUUqyzl31HOzRHmWhJEoriR
nRhWTLzqMyn+RLGrD3DJQj/dGH6tyxHJ7PdI7gtJ3qaF4lCc2dKR3uQW3CBKI9Ys
wzjBWOTijafbttXHanXEwXR3vnPk+sH52BqTXZQVA5vzPwIPJnz3H6E9hL66b/uM
DS9owYRBmykXlV9Gt91Vl5cpg3yxPixaeLMhqDD2Ebq6OFyuacExQHfGUeP0Va/A
IdM9+H5DE13qR2INX+N0kAFyFzW7k8AvY37KGZdoACUrDzmmGoilfs/pFAC0kZaZ
tKXoR9iLNxWSBtlI2Fr3qz4gc5nItYb7JSQsdu6Lc92+9z4xAoIBAQDGQFDXVQyk
Q5tsWicru5v2c9VoFpLUtBg4Dx3uXOMEVl/S5hZ8jYbUH4dcwKyLCYQLtNSc9aei
8zm18TdOGm0nCLOo7OPMeet+JHyx8uz11/Sx4ucI/Jq3yVSTqdtXYakxzijTldNQ
M7YnjpBcs0yDk806R7J3xvxZNMbE1QH1bP947Ej0sv40cBcA0hdpjuuNI5C2Ot4P
fUZXfqR34L7aPZPuP82W2WqFgkTyMY8FO235qR+Sy5xrcHSS4L1FdF+PhS5ZjiPN
sUdXRvfNFQlKZRUyqB147XY7EDnx6BZW2aoM7AiYPiGhxZeV4NHy1ChdBO2CSmOA
03FvucMEmUF5AoIBAD2xorAOBuXA5L7Sy1hR4S8SEJ2/LAeyzFhT9F+hpo0tGLy3
hOohCgQT6NQd8wgSMSTMxTrJd6SPeN/8I6L14f84Gm/kg5FN+BCav5KsdoFnORr/
jlt74et3e+yuSCQ2HuKdkCGScuPOgzYUw54Ea6cyI5v/yx9kcxzLik8xZSzx+/BU
1nF2wBgVXR+T7BOF/CIs+IQd4RebiV0EmqElttI36rec+jNPBfHpyVkIWqvqrbDb
3qFS0+rU7FMkaPrM9cnX7O1ED242vzjGMMmvFQmicd0BjsNLnhLWEYRhcP0c3pyS
Az6Z/HQ9FMn6h/UZSErWSG970p6NyjieCkICoUECggEBALdyXhvTPD5nvNL3XRWv
pXLY3plRgg7Gkz6UZmrhksO5tTOu6xHX1/JDNntSYpbJeGFos/CFs9gp3rYH/dgM
xgH/oFdo1KWqD4oK80OqeTAMq0VLo+OB8xyrdNKqsydZXDmU/dxD4GRvZVeXKOhO
lTePtbD/FRqWi310Q5U2GLjkYkWfxyZ+1pDpQ6/jt/xaXoacaVTmhgKpNkTSEBhJ
Y/EIV/F3IqM6jcH6uBewWhpKUspZf7jTJeuZBJXA1gMF20MvxqLhzymPqGcPaU9g
7tbjUEkunQ8AFI40xpmc28cD5MHOS2ms3GwYLdtnTH65aJwiajBM62QSw/3RU67W
rWkCggEBAOtMBi9ko4ZR96BCFcuyPsiMcoDBQBEFgH/drT3hMlwmmVt5dcInw3Zk
DQb3gIWHP1Ul//Ma8qwSeuIua0+6wkQ3NcsDywlJ2cqfZUe7kVJTCl8fuudTAYqT
```

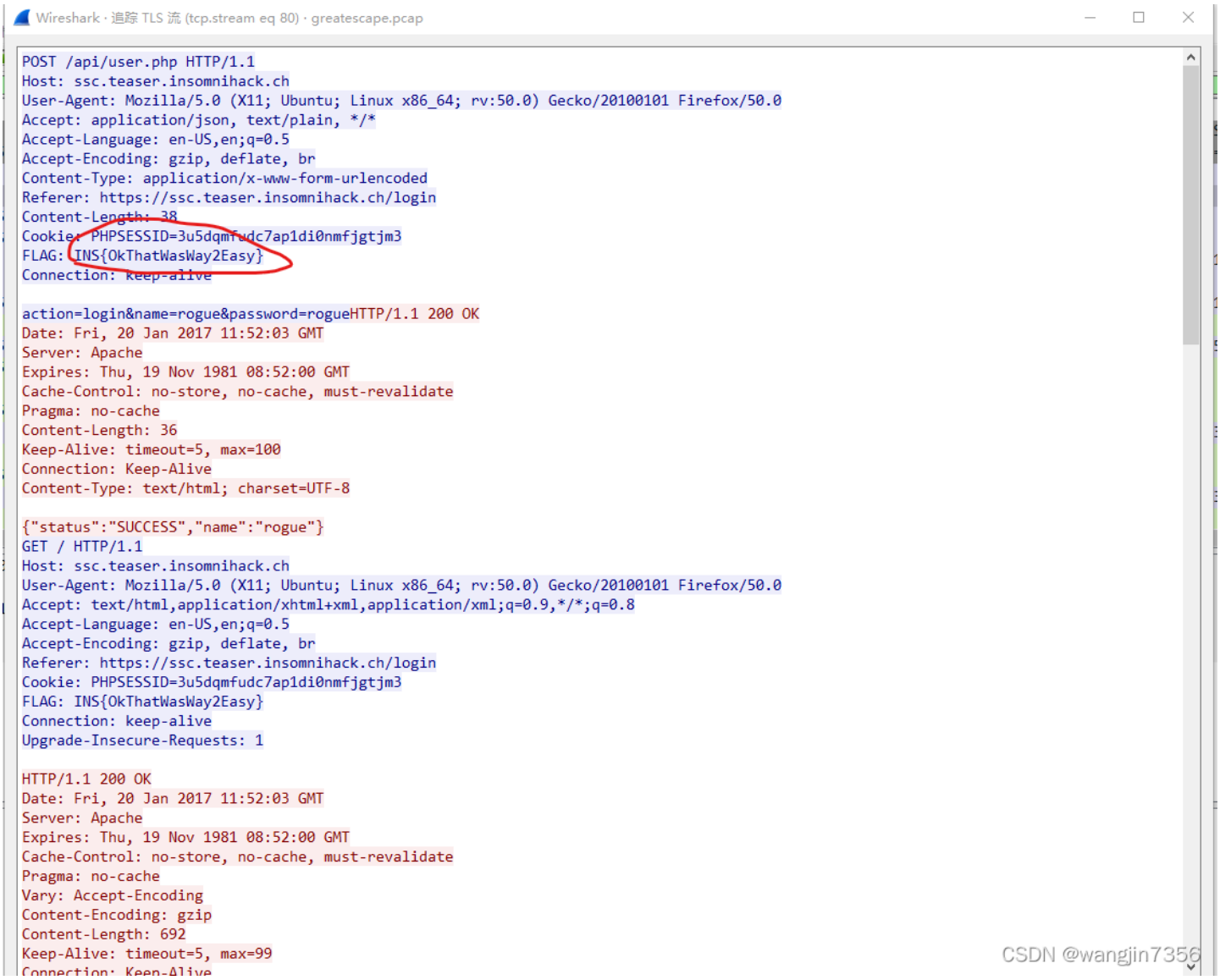

退回到流18，发现传了ssc.key私钥文件



把ssc.key添加到TLS协议了，看看加密数据有什么东西。



在TCP Stream eq 80发现了flag




```
flag{OkThatWasWay2Easy}
```