

# 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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[CTF 专栏收录该内容](#)

49 篇文章 0 订阅

订阅专栏

## 题目链接

<https://buuoj.cn/challenges#greatescape>

题目 [解题快手榜](#)

# greatescape

## 1

注意: 得到的 flag 请包上 flag{} 提交

[7a556a41-8c...](#)

Flag

CSDN @wangjin7356

## 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。

gatescape.pcap

文件(F) 编辑(E) 视图(V) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器 \* \* \* <ctrl-f>

No.	Time	Source	Destination	Protocol	Length	Leftover Capture Data	Info
2218	75.151015	172.31.36.141	52.214.142.175	TCP	68		51398 → 443 [ACK] Seq=518 Ack=153 Win=28032 Len=0 TSval=17432412 TSecr=17432412
2219	75.151250	52.214.142.175	172.31.36.141	TCP	68		51398 → 443 [ACK] Seq=518 Ack=153 Win=28032 Len=0 TSval=17432412 TSecr=17432412
2220	75.151259	52.214.142.175	172.17.0.1	TCP	68		51398 → 443 [ACK] Seq=518 Ack=153 Win=28032 Len=0 TSval=17432412 TSecr=17432412
2221	75.151261	52.214.142.175	172.17.0.1	TCP	68		[TCP Dup ACK 2220#1] 51398 → 443 [ACK] Seq=518 Ack=153 Win=28032 Len=0 TSval=17432412 TSecr=17432412
2222	75.153298	172.31.36.141	52.214.142.175	TLSv1	119		Change Cipher Spec, Finished
2223	75.153542	52.214.142.175	172.31.36.141	TLSv1	119		Change Cipher Spec, Finished
2224	75.153552	52.214.142.175	172.17.0.1	TLSv1	119		Change Cipher Spec, Finished
2225	75.153554	52.214.142.175	172.17.0.1	TCP	119		[TCP Retransmission] 51398 → 443 [PSH, ACK] Seq=518 Ack=153 Win=28032 Len=51 TSval=17432412 TSecr=17432412
2226	75.189765	172.17.0.1	52.214.142.175	TCP	68		443 → 51398 [ACK] Seq=153 Ack=569 Win=28032 Len=0 TSval=17432422 TSecr=17432412
2227	75.189765	172.17.0.1	52.214.142.175	TCP	68		[TCP Dup ACK 2226#1] 443 → 51398 [ACK] Seq=153 Ack=569 Win=28032 Len=0 TSval=17432422 TSecr=17432412
2228	75.189781	172.31.36.141	52.214.142.175	TCP	68		443 → 51398 [ACK] Seq=153 Ack=569 Win=28032 Len=0 TSval=17432422 TSecr=17432412
2229	75.190018	52.214.142.175	172.31.36.141	TCP	68		443 → 51398 [ACK] Seq=153 Ack=569 Win=28032 Len=0 TSval=17432422 TSecr=17432412
2230	75.207120	93.184.220.29	172.31.36.141	TCP	68		80 → 38868 [FIN, ACK] Seq=797 Ack=440 Win=145920 Len=0 TSval=2495252476 TSecr=17428545
2231	75.207190	172.31.36.141	93.184.220.29	TCP	68		38868 → 80 [FIN, ACK] Seq=440 Ack=798 Win=28544 Len=0 TSval=17432426 TSecr=2495252476
2232	75.217043	93.184.220.29	172.31.36.141	TCP	68		80 → 38869 [FIN, ACK] Seq=797 Ack=440 Win=145920 Len=0 TSval=968764786 TSecr=17428545
2233	75.217094	172.31.36.141	93.184.220.29	TCP	68		38869 → 80 [FIN, ACK] Seq=440 Ack=798 Win=28544 Len=0 TSval=17432428 TSecr=968764786
2234	75.224298	93.184.220.29	172.31.36.141	TCP	68		80 → 38868 [ACK] Seq=798 Ack=441 Win=145920 Len=0 TSval=2495252481 TSecr=17432426
2235	75.234192	93.184.220.29	172.31.36.141	TCP	68		80 → 38869 [ACK] Seq=798 Ack=441 Win=145920 Len=0 TSval=968764790 TSecr=17432428
2236	79.793118	172.31.36.141	52.214.142.175	HTTP	646		POST /api/user.php HTTP/1.1 (application/x-www-form-urlencoded)

> Frame 2236: 646 bytes on wire (5168 bits), 646 bytes captured (5168 bits)  
 > Linux cooked capture v1  
 > Internet Protocol Version 4, Src: 172.31.36.141, Dst: 52.214.142.175  
 > Transmission Control Protocol, Src Port: 51398, Dst Port: 443, Seq: 569, Ack: 153, Len: 578  
 > Transport Layer Security  
 > [2 Reassembled TLS segments (523 bytes): #2236(1), #2236(522)]  
 > Hypertext Transfer Protocol  
 > HTML Form URL Encoded: application/x-www-form-urlencoded

```

0000  00 04 00 01 00 06 0a 64 94 dd 9c b7 40 00 08 00  ....d...@...
0010  45 00 02 76 73 83 40 00 40 06 30 cd ac 1f 24 8d  E...vs.@...$.
0020  34 d6 8e af c8 c6 01 bb e5 fc 8e 5e 0b 24 d1 48  4.....^$.H
0030  80 18 00 db 96 9a 00 00 01 01 08 0a 01 0a 03 e4  .....
0040  01 09 ff 66 17 03 01 00 18 13 b4 a5 7c 39 55 67  ...f.....[9Ug
0050  48 49 69 0b e9 1e 1f 9c b6 1f c4 bc 29 19 e0 b0  HI.....)...
0060  a7 17 03 01 02 20 08 16 d3 9a db 75 ff da 2c f6  .....u...

```

CSDN @wangjin7356

追踪到TCP Stream eq 19时发现了密钥

```
-----BEGIN PRIVATE KEY-----
MIIJQwIBADANBgkqhkiG9w0BAQEFAASCCS0wgGkpAgEAAoICAQC5twyPH+2U6X0Q
uxOKPThSR6MkXG5vAz+Ax+G9DKEiBLuTTF17dNv4oswdmT9nW1SY1kxZatNw1UF8
WAuGLnt05xTEm0J1MtBFRWGD+DVpCE9K0RGvyif8e4xxi6vh4mkW78IXv03VxHM0
mk/cq5kkERfWQW81pVeYm9UAm4dj+LcCwQ9aGd/vfTtCACqS50GtELFbsHJuFVyn
srpp4K6tLlRk2ensSnmXUXNEjqpodfdb/wqGT86NYg7i6d/4Rqa440a6BD7RKrgp
YPaX17pQusemHQpd248fxsuEfEwhPNDJhIb8fDX9Bwv2xTfBlhGwOh7euzSh2C4o
KSuBA0+bIkL+pGY1z7DFtuJYfTOSJyQ5zQzToxS+jE+2x9/3GpD2LUD0xkA8bWhv
eecq0v6ZWBVYNX54V5ME3s2qYc6CSQhi6Moy8xwLcSpTSAa7voNQNa9RvQ4/3KF
3gCbKtFvdd7IHvxfn8vcCrCZ37eVkkq0F11y5UNeJU/Y0Tt8m7UDn3uKNpB841BQa
hiGayCSjsHuTS8B+MnpnzWCrzd+rAzCB37B599iBK4t/mwSIZZUzZaqxTWNoFS2Lz
7m0LumZ4Yk8DpDEuWhNs80UD8FsgAvWfVAvivaaAcif3kMs8pkmNTs2LFBow0shz
SXfONsHupgXEWwFrK00ZXNhb+0/WKQIDAQABoICAAT6mFaZ94efft/c9BgnrddC
Xmh5JczfXGt6cF3eTc/Eqra3R3H83wzaaHh+rE18DXqPFdQfD6e0CK5pud1eD6Y8
4bynkKI/63+Ct30PSvdG5sFJqGS7G6lWIPzErtX+e0zJfr5N5eNOQfxuqCgS3acu
4iG3XWd1zuRjgSfKcGwvFdD4Fg5HVU6ZX+cGhh2sDzTR1r+r1lXTMsm4K/E8udIg
yEbv5KqWEI5y+5Eh9gWY7AnGw6TgLNxzFYyt0nhYhI2+Yh4IkRqQd6F8XQARbEhP
yZx1eK4Q/dRPQx0JNY1KkRp1+Cx6tAPVimByRx1hu82qsTstb6rLHemruOPbf5Dw
aaq5Fdp7it3uqjJHCwJ2hAZoijAcv1hn1sa1hr/qFF1Y/WeDAi80yvGdCSH30vS6
yazkah85G0nY85rz+s98F9cvIqcRdGJrAeNbUHHnj6+X9qFVtwDpF0V1v1vn2Ggp
7m8hiZ0Y+8T+7qfnS9WsdPh7MkoIEoZ0CPryYvX+YPLWqzxtCvrRWF8tAscI6H+
XBz3N1CAUa0k+Z0k1Z8ZYMSn/g5EV2jj/mwZVdtYoeQjLaCDuLq8E1Hswngp7F
54hHU7v0eJ1/TQ1tLCNfJFQRaUD+tPz9R6jVpbqBiXxIC2eiGT01rP4Ii7hsQRFC
W0KKqu+bV69HJAmi06yBAoIBAQDvz+c+3z9njQFFaeUUqyz131H0zRHmWhJEoriR
nRhWTLzqMyn+RLGrD3DJQ/dGH6tyxHJ7PdI7gtJ3qaF41Cc2dKR3uQW3CBKI9Ys
wzjBW0TijaftbtXHanXEWXR3vnpk+sH52BqTXZQVA5vzPwIPJnz3H6E9hL66b/uM
DS9owYRBmykX1V9Gt91V15cpg3yxPixaELMhQDD2Ebq60FyuacExQHfGUEP0Va/A
IdM9+H5DE13qR2INX+N0kAFyFzW7k8AvY37KGZdoACUrDzmmGoi1fs/pFAC0kZaZ
tKXoR9iLlxWSBt1I2Fr3qz4gc5nItYb7J5Qsdu6Lc92+9z4xAoIBAQQDQGFQDXVQyK
Q5tsWicru5v2c9VofPLUtBg4Dx3uXOMEV1/S5hZ8jYbUH4dcwKyLCYQLtNSc9aei
8zm18Td0Gm0nCLo070PMeet+JHyx8uz11/Sx4ucI/Jq3yVSTqdtXYakxziJTldNQ
M7YnjpbCs0yDk806R7J3xvxZNMbE1QH1bP947Ej0sv40cBcA0hdpjuuNI5C20t4P
fUZXFqR34L7aPZPuP82W2WqFgkTyMY8F0235qR+S5y5xrcHSS4L1FdF+PhS5ZjiPN
sUdXRvfNFQ1KZRUYqB147XY7EDnx6BZw2aoM7AiYPiGhxZev4NHy1ChdBO2CSmOA
03FvucMEuUF5AoIBAD2xorA0BuXA5L7Sy1hR4S8SEJ2/LAeyzFhT9F+hpo0tGLy3
h0ohCgQT6NQd8wgSMSTmxTrJd6SPeN/8I6L14f84Gm/kg5FN+BCav5KsdoFnORr/
j1t74et3e+yuSCQ2HuKdkCGSscuP0gzYUw54Ea6cyI5v/yx9kcxzLk8xZSzx+/BU
1nF2wBgVXR+T7B0F/CIs+IQd4RebiV0EmqE1ttI36rec+jNPBFHpyVkiWqvqrDb
3qF50+rU7FMkaPrM9cnX701ED242vzjGMMmvFQmicd0BjsNLnhLWEYRhcP0c3pyS
Az6Z/HQ9FMn6h/UZSErWSG970p6NyjjeCkICoUECgEBALdyXhvTPD5nvNL3XRWv
pXLY3p1Rgg7Gkz6UZmrhks05tT0u6xHX1/JDNntSYpbJEGFos/CFs9gp3rYH/dgM
xgH/ofdo1KwQd4oK800qeTAMq0VLo+OB8xyrdNKqsydZXDmU/dx04GRvZVeXKOh0
1TePtbd/FRqWi310Q5U2LjkYkWfxyZ+1pDpQ6/jt/xaxoacaVTmhgKpNkTSEBhJ
Y/EIV/F3IqM6jcH6uBewWhpKUSpZf7jTJeuZBJXA1gMF20MvxqLhzymPqGcPaU9g
7tbjUEkunQ8AFI40xpmc28cD5MHOS2ms3GwYLDtnTH65aJwiajBM62QSw/3RU67W
rWkCggEBA0tMBi9ko4ZR96BCfcuyPsiMcoDBQBEFGH/drT3hM1wmmVt5dcInw3Zk
DQb3gIWHp1U1//Ma8qwSeuIua0+6wkQ3NcsDywlJ2c2fZUe7kVJTC18fuudTAYqT
P...
```

CSDN @wangjin7356

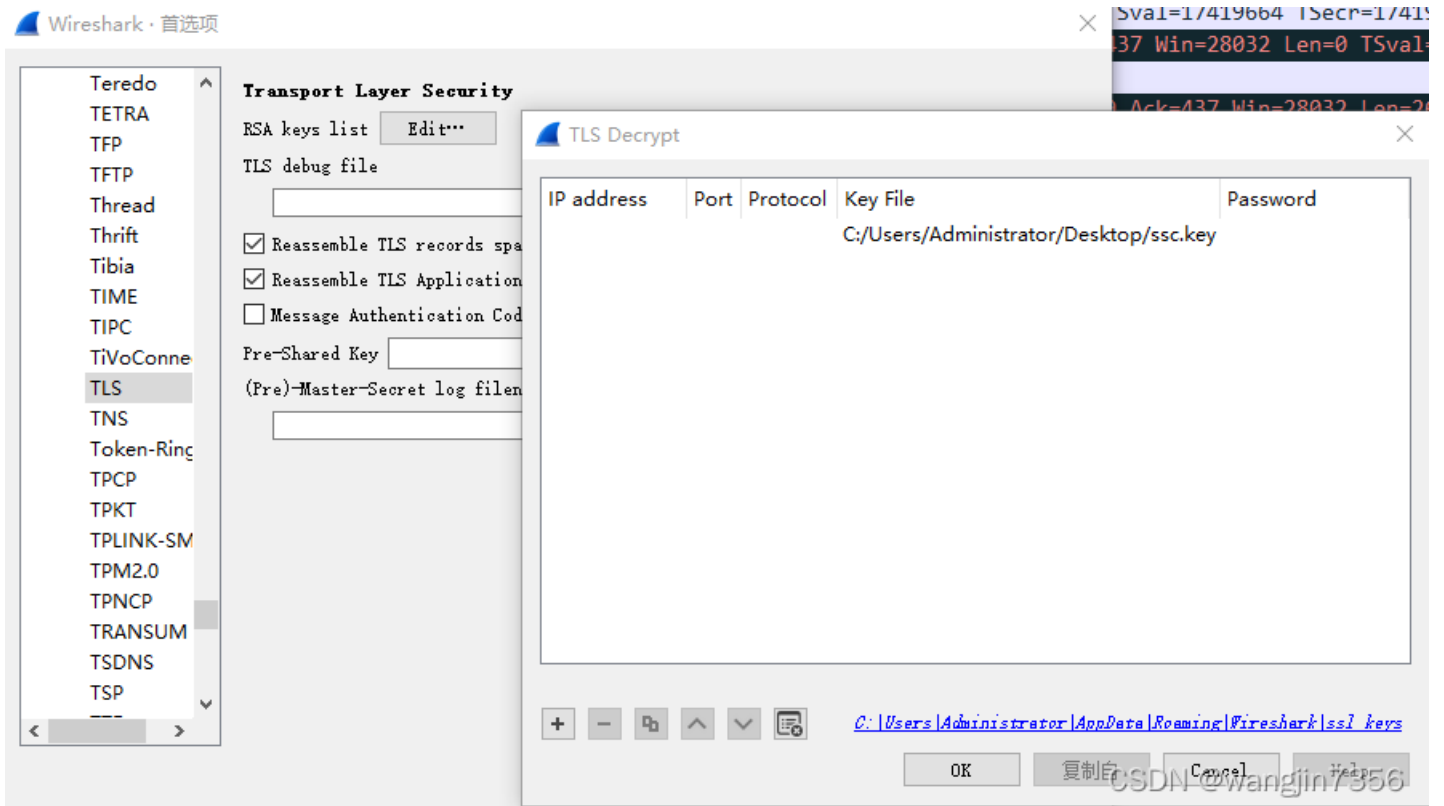
退回到流18，发现传了ssc.key私钥文件

```

220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 5 allowed.
220-Local time is now 11:51. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
USER bob
331 User bob OK. Password required
PASS toto123
230 OK. Current directory is /
SYST
215 UNIX Type: L8
TYPE I
200 TYPE is now 8-bit binary
PORT 172,17,42,1,171,159
200 PORT command successful
STOR ssc.key ←
150 Connecting to port 43935
226-File successfully transferred
226 0.001 seconds (measured here), 4.59 Mbytes per second
QUIT
221-Goodbye. You uploaded 4 and downloaded 0 kbytes.
221 Logout.
    
```

CSDN @wangjin7356

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

```
POST /api/user.php HTTP/1.1
Host: ssc.teaser.insomnihack.ch
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:50.0) Gecko/20100101 Firefox/50.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Referer: https://ssc.teaser.insomnihack.ch/login
Content-Length: 38
Cookie: PHPSESSID=3u5dqmfd7ap1di0nmfjgtjm3
FLAG: INS{OkThatWasWay2Easy}
Connection: keep-alive
```

```
action=login&name=rogue&password=rogueHTTP/1.1 200 OK
Date: Fri, 20 Jan 2017 11:52:03 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 36
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

```
{"status": "SUCCESS", "name": "rogue"}
GET / HTTP/1.1
Host: ssc.teaser.insomnihack.ch
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:50.0) Gecko/20100101 Firefox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://ssc.teaser.insomnihack.ch/login
Cookie: PHPSESSID=3u5dqmfd7ap1di0nmfjgtjm3
FLAG: INS{OkThatWasWay2Easy}
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Fri, 20 Jan 2017 11:52:03 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 692
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
```