

BUUCTF Misc 被嗅探的流量

原创

叶子轻轻摇 于 2022-03-05 10:35:13 发布 105 收藏

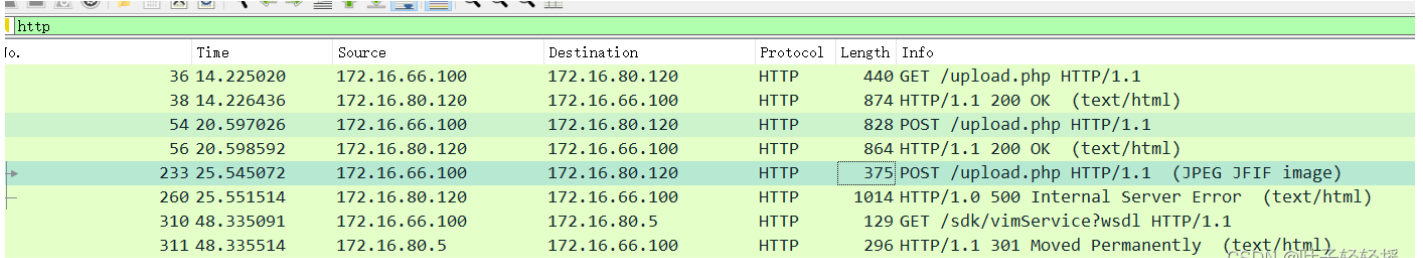
文章标签: [网络安全 tcp/ip](#)

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/qq_20004095/article/details/123290810

版权

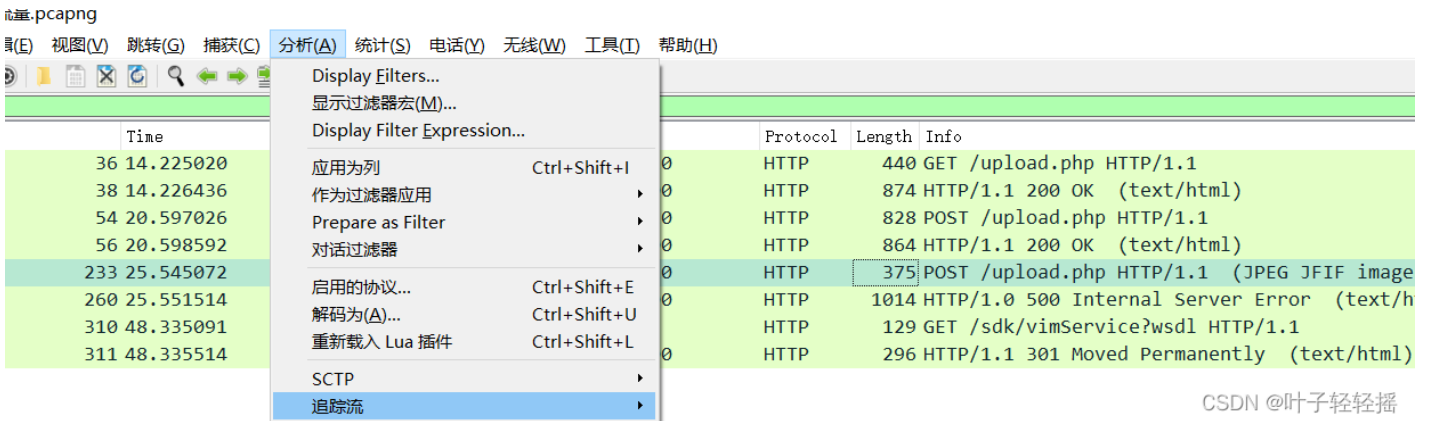
1、使用Wireshark打开文件, 筛选HTTP数据包。仔细观察发现有图片上传。



No.	Time	Source	Destination	Protocol	Length	Info
36	14.225020	172.16.66.100	172.16.80.120	HTTP	440	GET /upload.php HTTP/1.1
38	14.226436	172.16.80.120	172.16.66.100	HTTP	874	HTTP/1.1 200 OK (text/html)
54	20.597026	172.16.66.100	172.16.80.120	HTTP	828	POST /upload.php HTTP/1.1
56	20.598592	172.16.80.120	172.16.66.100	HTTP	864	HTTP/1.1 200 OK (text/html)
233	25.545072	172.16.66.100	172.16.80.120	HTTP	375	POST /upload.php HTTP/1.1 (JPEG JFIF image)
260	25.551514	172.16.80.120	172.16.66.100	HTTP	1014	HTTP/1.0 500 Internal Server Error (text/html)
310	48.335091	172.16.66.100	172.16.80.5	HTTP	129	GET /sdk/vimService?wsdl HTTP/1.1
311	48.335514	172.16.80.5	172.16.66.100	HTTP	296	HTTP/1.1 301 Moved Permanently (text/html)

CSDN @叶子轻轻摇

2、对有上传图片的数据包进行HTTP流追踪。



流量.pcapng

分析(A) 统计(S) 电话(Y) 无线(W) 工具(I) 帮助(H)

- Display Filters...
- 显示过滤器宏(M)...
- Display Filter Expression...
- 应用为列 Ctrl+Shift+I
- 作为过滤器应用
- Prepare as Filter
- 对话过滤器
- 启用的协议... Ctrl+Shift+E
- 解码为(A)... Ctrl+Shift+U
- 重新载入 Lua 插件 Ctrl+Shift+L
- SCTP
- 追踪流

No.	Time	Source	Destination	Protocol	Length	Info
0				HTTP	440	GET /upload.php HTTP/1.1
0				HTTP	874	HTTP/1.1 200 OK (text/html)
0				HTTP	828	POST /upload.php HTTP/1.1
0				HTTP	864	HTTP/1.1 200 OK (text/html)
0				HTTP	375	POST /upload.php HTTP/1.1 (JPEG JFIF image)
0				HTTP	1014	HTTP/1.0 500 Internal Server Error (text/h
0				HTTP	129	GET /sdk/vimService?wsdl HTTP/1.1
0				HTTP	296	HTTP/1.1 301 Moved Permanently (text/html)

CSDN @叶子轻轻摇

3、追踪HTTP流中发现flag。

Wireshark · 追踪 HTTP 流 (tcp.stream eq 2) · 被嗅探的流量.pcapng

```
5...;.....d...x..B.....g...i"1+'i ..n..... ..M...n.....!?.Bw.::Np=.....!...V/..k..s..?.#.D..E.....
~;.C.R..Vh. u.l.8.
...O..$.~?....._.....~;..E.+S...T.....,5...T../*{=.....R.o_..W{1$.&.k.
W...{.....6dqB.....+.....e.7.f5.K.i.[.....$..\\|C*'0.....Z.Kd..8.e.....c.Js...X)..U.....W..o..T..KE.K.8.../
h.f....16.M.X...
.P...|-i.ZE.
...G.....=.....D.1.n-..V'.....c....C.*.....z...._p.k.iT.f...
.W+.P.}N.X..R...}.}.....$.Ga..|,tq..z.....iNN.....m..$.d.4.X^..M#QQ"..I.0^...q.....\u3\"I.r%.....D0e
*..FG...l.....f.y.c:..G.*.$.....~@.M.....M..).v.yo.....az~.Efi~..D.X$.7...J..)o.....DZ.wJ1.e.%.....7W../.
.. )d...q.B.....Z...K
M...I..Q..g?..+..!..W...../..?.....=..J@...7K...G..Q...G.....G.P...r?..`f....._2..P..>{E...B.../..?..
\\R.....m'.....
?.@j.8..u1.&b.&[.9.....>.*qW(,=.U..).j.e.j... .F..n...{..*.j$.s.....|+n.J66...C.EQ.....[.
$.G.q..w...?.....~...../..V...
..qP.....,y
.....c.....V.jG..4yi ..*.....s..?.....D...X..@.....B..j....P...Y[$.\w...ka.?...._m(.. ....R.
49.r..C...:..tTk.Rl.%.....k..d..x..F...R....QM..h8~:6...vIv...`Z.....U7..-(.*$o.^..B.
3.bc7j.....R.F.....s.....hR.....s.....K..P.....H.?K.[E...7:Q.P
ZbUs.>.[AW.....s..5.V.....:..#.....x...<...QS...L.....W.19i..g.....<+....[AG.....P...M...5.3.lg.l.9<S..
\\j...#c2...b.l..g..Q..6.PP..h.'...I.y.8..dn.....a...s b7..`t...r...R/
o..b]-...j.....z6...*.QM...B...:.....*..i.....oe.vd.r.'...n..b.].7..G...T..^...Q,U.X...@...j.j.m.e...E:...o.F.
9..M..t...e\K_b/:Y'..'w>.B.....L.l..&,a.....C].C5P%.....).t.k.....8.!@-J%I.|b.'..+.
[a.?.#.....=.._!..f....._..0.....s.....+F0...Uv.\*$..}].f.M..e..
...Y\...x.Y+...Q..5gi.Y.0..@w.[ .{...>q'j.....s...N.....Zwi.?.
..M.....S.....A.D?\s..}...
..i7$.I.M..Z..... x.o.c.y...s8.b.gwb.6...?.....V.....KZ.
.....f.[...J...o.V.v...m...As.mp.....+..#.....#.....kx^...|.s.%YQ.{,=.N.*.....1.....!...a.....?
*.q...g.Z...V?.0.".....m$.?.....?.....Y.>.....EZ...7..s..?.....d\..x..A..P...M...'.(.lou.#s>..
C.*.j..E.....?.....z...((o...?Y_00...EW..
Q..9...R3.....M.....V.....x.S_x.Z=..xI.....H/.a.....j<9zu0..T.#OKG..E[...
a.....J.....flag{da73d88936010da1eeeb36e945ec4b97}.
-----WebKitFormBoundaryTeRP7p2QAo2zkT2U-----
HTTP/1.0 500 Internal Server Error
Date: Tue, 18 Aug 2015 10:40:44 GMT
```

CSDN @叶子轻轻摇



[创作打卡挑战赛](#)
[赢取流量/现金/CSDN周边激励大奖](#)