[2021绿城杯] [Misc] 流量分析 + cobaltstrike 流量解密

原创

shu天 已于 2022-03-17 23:03:16 修改 867 收藏 3

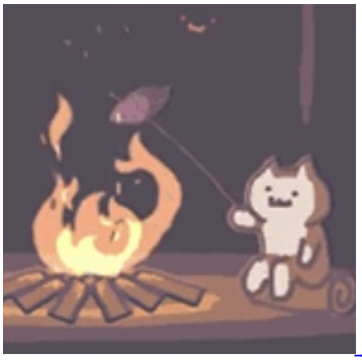
分类专栏： 取证 ctf # misc 文章标签： cobaltstrike 流量分析 misc

于 2022-03-17 22:52:16 首次发布

取证 同时被 3 个专栏收录

49 篇文章 4 订阅

订阅专栏



ctf

81 篇文章 4 订阅

订阅专栏

misc

7 篇文章 0 订阅

订阅专栏

[2021绿城杯] [Misc] 流量分析 + cobaltstrike 流量解密

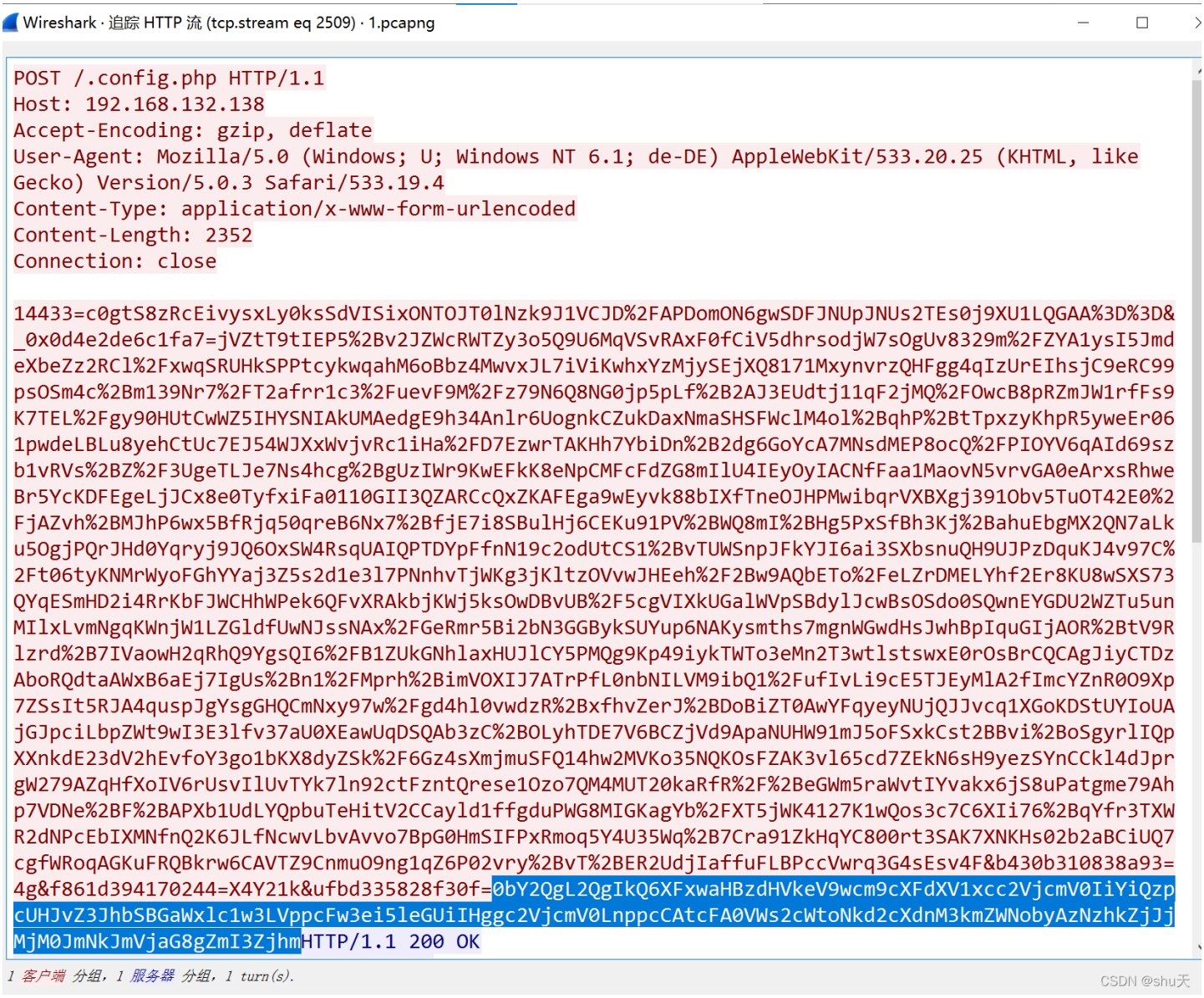
2021年“绿城杯”网络安全大赛-Misc-流量分析

> 本文来自csdn的□□***shu天***□□，平时会记录**ctf、取证和渗透**相关的文章，欢迎大家来我的主页：shu天_CSDN博客-ctf,取证,web领域博主
> 看看ヾ(@ ˇωˇ @)ノ！！

1.webshell分析

框架是Laravel，利用CVE-2021-3129命令执行写马。
分析发现webshell是/.config.php

```
tcp.stream eq 2509
```



去前两位

Y21k&ufbd335828f30f=0bY2QgL2QgIkQ6XFxwaHBzdHVkeV9wcm9cXFdXV1xcc2VjcmV0IiYiQzpcUHJvZ3JhbSBGaWxlc1w3LVppcFw3ei5leGUiIHggc2VjcmV0LnppcCAtcFA0VWs2cWtoNkd2cXdnM3kmZWNobyAzNzhkZjJjMjM0JmNkJmVjaG8gZmI3ZjhmHTTP/1.1 200 OK

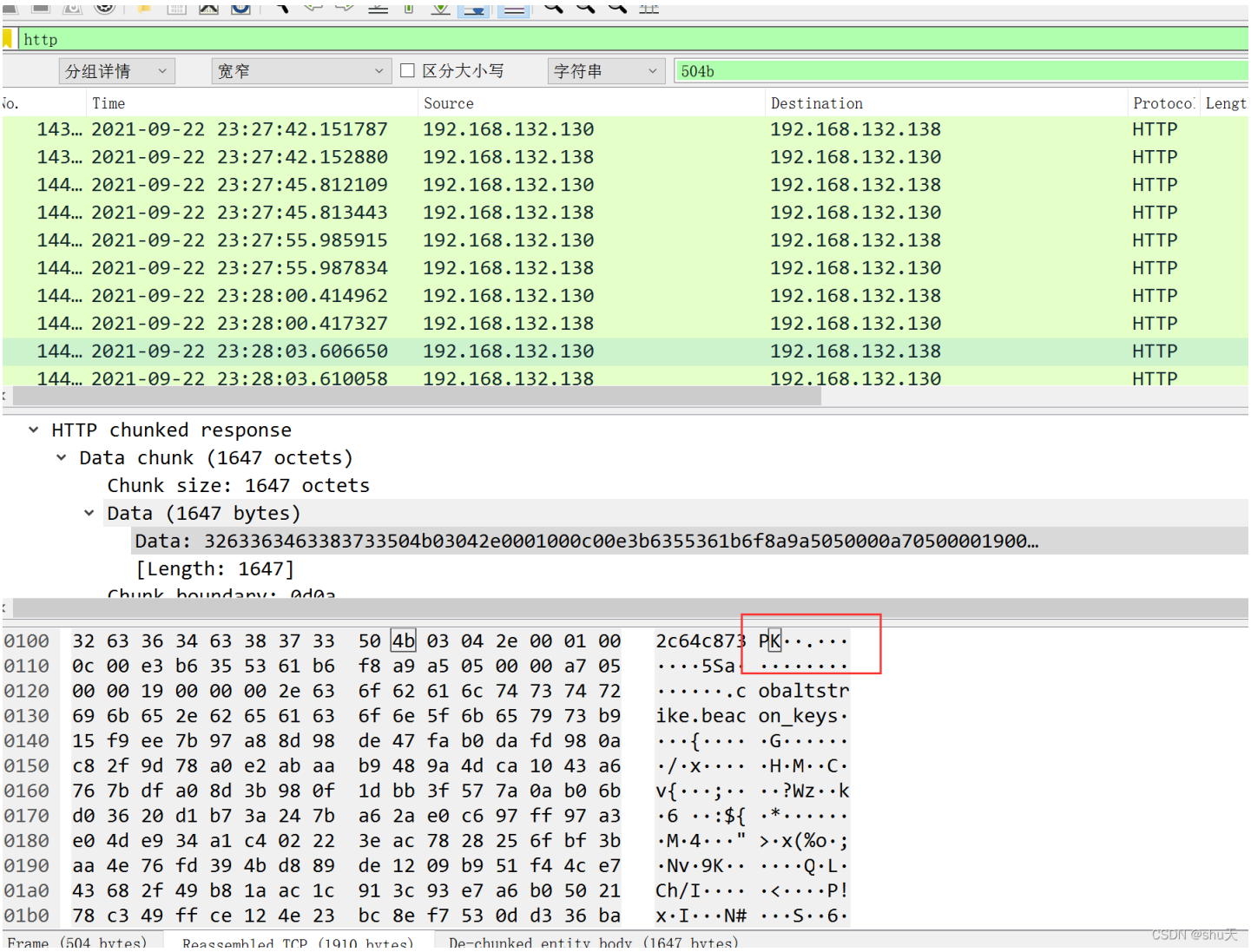
↓

base64解密

↓

cmd����~|�����cd /d "D:\\phpstudy_pro\\WWW\\secret"&"C:\Program Files\7-Zip\7z.exe" x secret.zip -pP4Uk6qkh6Gvqwg3y&echo 378df2c234&cd&echo fb7f8f

secret没找到，搜504b找zip文件头，导出，密码`P4Uk6qkh6Gvqwg3y`解压



2.解密 cobaltstrike 流量

（1）分析`.cobaltstrike.beacon_keys`得到私钥

使用脚本：github.com/Skactor/cs-scripts

```
-----BEGIN PRIVATE KEY-----
MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwggJdAgEAAoGBAIqpewO+lqNYuxQhQwq7pMdM7CP9
2uer5FkUA41vPaelrbpqr1ujH95Q7Rfqt7E7Vc+Xx5dYQCoRaysjNm+UfuRcFocLHG2ugf4+/NEX
/NFE+gI279wXfC+zZ0MGFMQIAC1TClaiMvALwMB9nBuXK/CErC754co9cIbaIkCl/sRXAgMBAAEC
gYBqlSFYXHwfrMmIDJUiv99FzovIko1b/FV2Xxrn8TS8E265Vt3Zm0aYtS25b5Ko6YnpGqqxW4Ve
kKsGqndiRwtNSbIilU1EqWqfdBmucptnISgDdx+ofWbInTRl+leBzDW4Zsl2sMvMmmyhsc/X35pG
bH2lRXXEegPzradtyBwhUQJBANt2IC4p5CQW2UxXVjmrTbA+CuJLfnZE+97HCjzZPi/gUiF4akFQ
x46x0vT1RmcalqUg1Prl7OoKb05Lmwm0XukCQQChv4blpfqVcdz9X6MGJqeaiC22EPZn+2dhm4Pb
ZIhurs57M7+dqlYxoG6LneU0H1N8ieeH9fb9ixG/8+F7iIE/AkEAzyzYfDv3r0oSoMriD1bz5Cjt
xWtXWvcMfuaPd5nt5uxxHD+8ryQ+/ypH6A+UAslK5V/1L1XXLankIZmmJqcr4QJAGUAkF//EUcY3
wJpIgfJQ4e/2auDVBsCZkAROHlbgcZ76fwNCG6P21sJ733Hj0TI+v0dsDK6aQ1SNjdDN15Ik0wJB
AK7C5l0QF8NRlIw2+tPUSDVy/PRUVmpRRd4cD4HXNtVMg0Dr3L7vx9PeyJH0EFuaVWItdBDILP0H
zUR1/wk5ZFY=
-----END PRIVATE KEY-----
```

```
┌──(root💀kali)-[~/Desktop/qz/cs-scripts-master]
└─# python3 /root/Desktop/qz/cs-scripts-master/parse_beacon_keys.py
-----BEGIN PRIVATE KEY-----
MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwggJdAgEAAoGBAIqpewO+lqNYuxQhQwq7pMdM7CP9
2uer5FkUA41vPaelrbpqr1ujH95Q7Rfqt7E7Vc+Xx5dYQCoRaysjNm+UfuRcFocLHG2ugf4+/NEX
/NFE+gI279wXfC+zZ0MGFMQIAC1TClaiMvALwMB9nBuXK/CErC754co9cIbaIkCl/sRXAgMBAAEC
gYBqlSFYXHwfrMmIDJUiv99FzovIko1b/FV2Xxrn8TS8E265Vt3Zm0aYtS25b5Ko6YnpGqqxW4Ve
kKsGqndiRwtNSbIilU1EqWqfdBmucptnISgDdx+ofWbInTRl+leBzDW4Zsl2sMvMmmyhsc/X35pG
bH2lRXXEegPzradtyBwhUQJBANt2IC4p5CQW2UxXVjmrTbA+CuJLfnZE+97HCjzZPi/gUiF4akFQ
x46x0vT1RmcalqUg1Prl7OoKb05Lmwm0XukCQQChv4blpfqVcdz9X6MGJqeaiC22EPZn+2dhm4Pb
ZIhurs57M7+dqlYxoG6LneU0H1N8ieeH9fb9ixG/8+F7iIE/AkEAzyzYfDv3r0oSoMriD1bz5Cjt
xWtXWvcMfuaPd5nt5uxxHD+8ryQ+/ypH6A+UAslK5V/1L1XXLankIZmmJqcr4QJAGUAkF//EUcY3
wJpIgfJQ4e/2auDVBsCZkAROHlbgcZ76fwNCG6P21sJ733Hj0TI+v0dsDK6aQ1SNjdDN15Ik0wJB
AK7C5l0QF8NRlIw2+tPUSDVy/PRUVmpRRd4cD4HXNtVMg0Dr3L7vx9PeyJH0EFuaVWItdBDILP0H
zUR1/wk5ZFY=
-----END PRIVATE KEY-----
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCKqXsDvpajWLsUIUMKu6THTOwj/drnq+RZFAON
bz2npa26aq9box/eUO0X6rexO1XPl8eXWEAqEWsrIzZvlH7kXBaHCxxtroH+PvzRF/zRRPoCNu/c
F3wvs2dDBhTECAAtUwpWojLwC8DAfZwblyvwhKwu+eHKPXCG2iJApf7EVwIDAQAB
-----END PUBLIC KEY-----

┌──(root💀kali)-[~/Desktop/qz/cs-scripts-master]
└─#
```

CSDN @shu天

（2）通过私钥解密元数据、获取 AES KEY

翻一翻http流，可以发现对/en_US/all.js的GET请求

Wireshark · 追踪 HTTP 流 (tcp.stream eq 3937) · 1.pcapng

```
GET /en_US/all.js HTTP/1.1
Accept: */*
Cookie: bGOniQ5nfrSmAW9fgdZSCC+42t5xvQt+B4SVEu6Q8MvC4rPn/
OThepmxP6GjDiP1wCUB1EE3sqeXkwdHHMd9wikZhiQnjT9AB3e2RNacCVF+8v/nj/Rv85fSD2Phfc/
wsaAjld9Fy8ZJJKz1wPwPY6lTxArMGFtX7W+VW/gzujI=
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Host: 192.168.132.128
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Wed, 22 Sep 2021 15:31:10 GMT
Content-Type: application/octet-stream
Content-Length: 0
```

CSDN @shu天

Cookie 是一个 base64 字符串，通过配置文件可知这是 RSA 公钥加密的元数据。

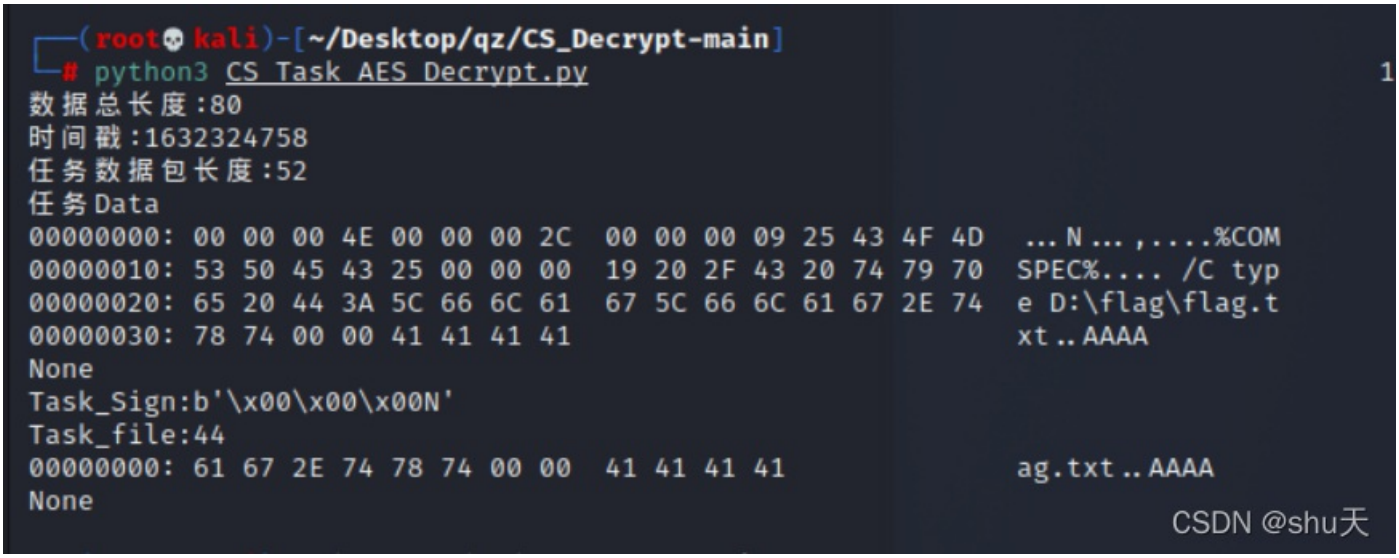
```
Cookie: bGOniQ5nfrSmAW9fgdZSCC+42t5xvQt+B4SVEu6Q8MvC4rPn/OThepmxP6GjDiP1wCUB1EE3sqeXkwdHHMd9wikZhiQnjT9AB3e2RNac
CVF+8v/nj/Rv85fSD2Phfc/wsaAjld9Fy8ZJJKz1wPwPY6lTxArMGFtX7W+VW/gzujI=
```

利用大佬的脚本解密：github.com/WBGlll/CS_Decrypt

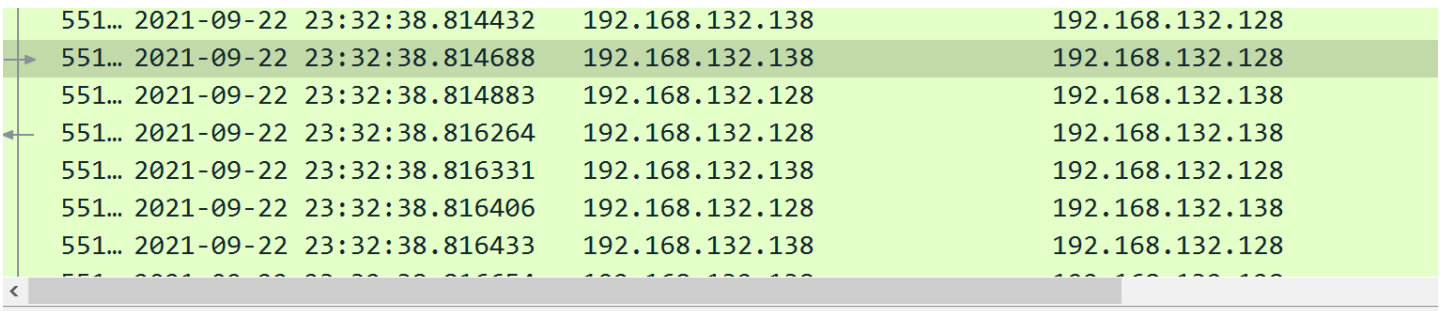

```
AES key:7c83bf30a6ad2dc410040d33e1399cf6
HMAC key:a77945b3a56687a39f90683cb24d00c2
```

（3）解密cs流量

`tcp.stream eq 8956`可以看到查看了flag



看下一条submit.php的`tcp.stream eq 8957`



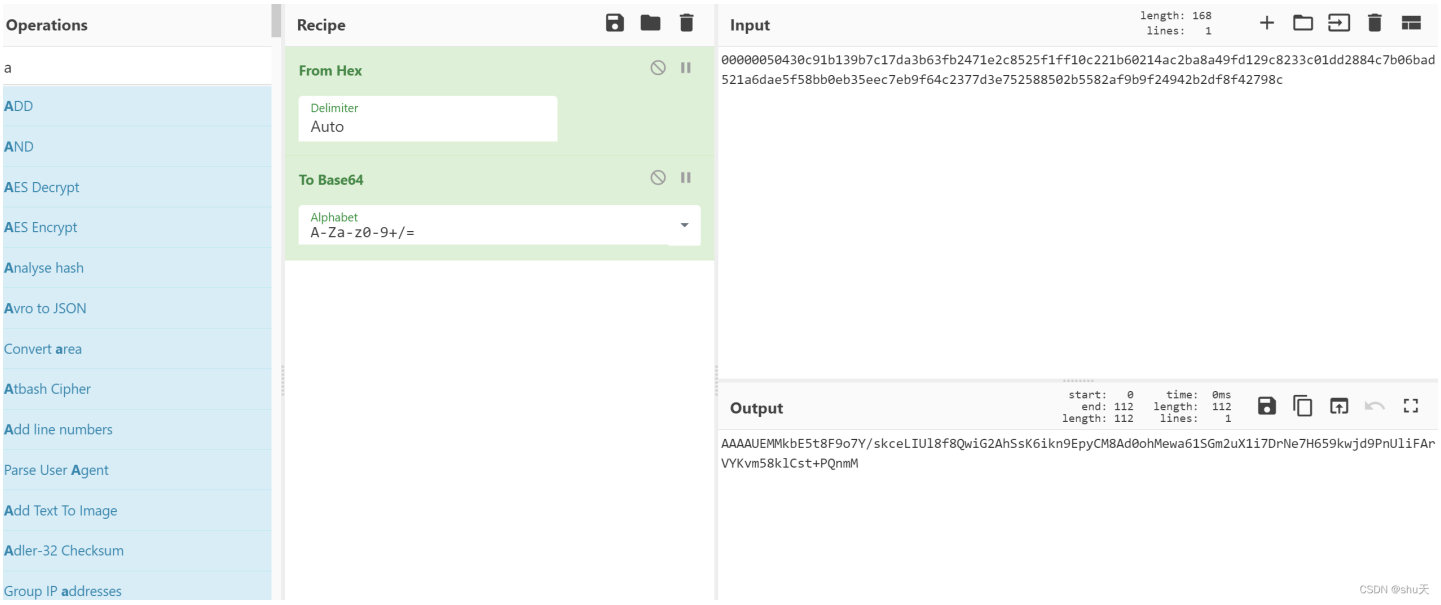

```
    \r\n
    [Full request URI: http://192.168.132.128/submit.php?id=1515569398]
    [HTTP request 1/1]
    [Response in frame: 55170]
    File Data: 84 bytes
Data (84 bytes)
```

Data (84 bytes)

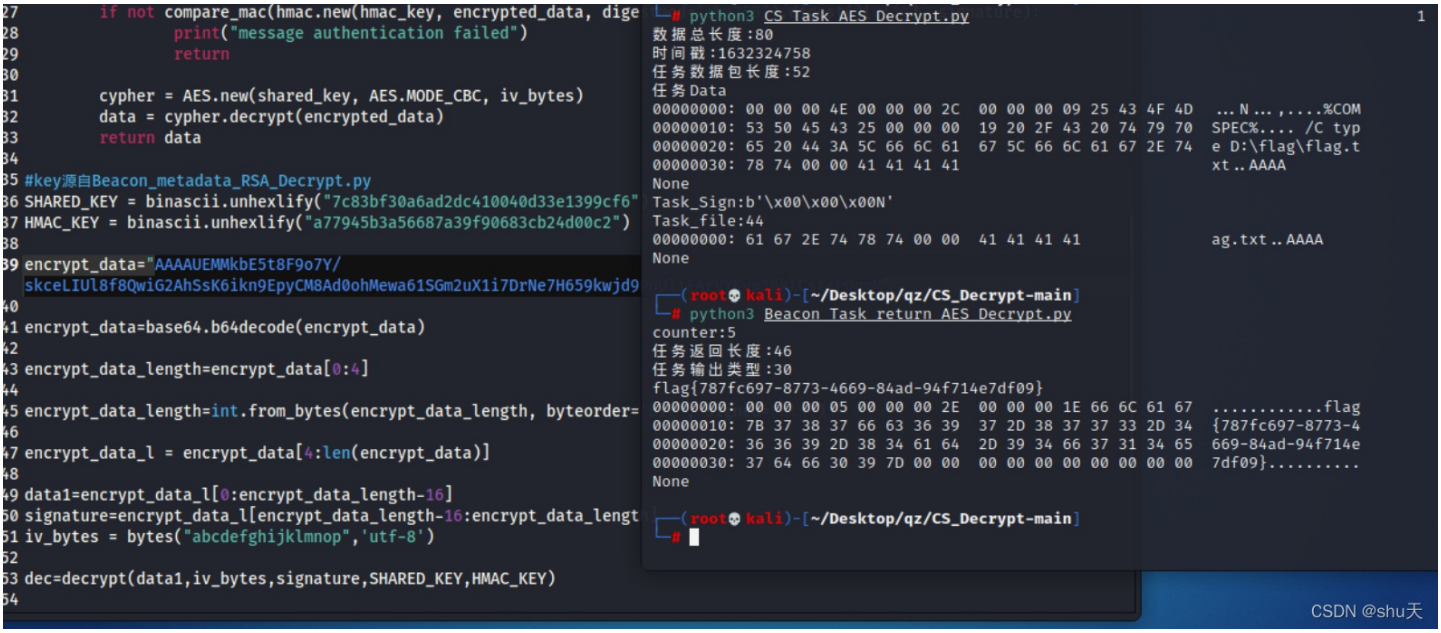
Data: 00000050430c91b139b7c17da3b63fb2471e2c8525f1ff10c221b60214ac2ba8a49fd129…

```
00d0  31 3b 20 57 69 6e 36 34  3b 20 78 36 34 3b 20 54   1; Win64 ; x64; T
00e0  72 69 64 65 6e 74 2f 35  2e 30 29 0d 0a 48 6f 73   rident/5 .0)··Hos
00f0  74 3a 20 31 39 32 2e 31  36 38 2e 31 33 32 2e 31   t: 192.1 68.132.1
0100  32 38 0d 0a 43 6f 6e 74  65 6e 74 2d 4c 65 6e 67   28··Cont ent-Leng
0110  74 68 3a 20 38 34 0d 0a  43 6f 6e 6e 65 63 74 69   th: 84·· Connecti
0120  6f 6e 3a 20 4b 65 65 70  2d 41 6c 69 76 65 0d 0a   on: Keep -Alive··
0130  43 61 63 68 65 2d 43 6f  6e 74 72 6f 6c 3a 20 6e   Cache-Co ntrol: n
0140  6f 2d 63 61 63 68 65 0d  0a 0d 0a 00 00 00 50 43   o-cache· ···PC
0150  0c 91 b1 39 b7 c1 7d a3  b6 3f b2 47 1e 2c 85 25   ···9··}· ·?·G·,·%
0160  f1 ff 10 c2 21 b6 02 14  ac 2b a8 a4 9f d1 29 c8   ····!··· ·+····)·
0170  23 3c 01 dd 28 84 c7 b0  6b ad 52 1a 6d ae 5f 58   #<··(··· k·R·m·_X
0180  bb 0e b3 5e ec 7e b9 f6  4c 23 77 d3 e7 52 58 85   ···^·~·· L#w··RX·
0190  02 b5 58 2a f9 b9 f2 49  42 b2 df 8f 42 79 8c      ··X*···I B···By·
```


base64编码后解密，得到flag



AAAAUEMMkbE5t8F9o7Y/skceLIUl8f8QwiG2AhSsK6ikn9EpyCM8Ad0ohMewa61SGm2uX1i7DrNe7H659kwjd9PnUliFArVYKvm58klCst+PQnmM



参考wp：
wkr.moe/ctf/610.html
blog.nviso.eu/2021/10/27/cobalt-strike-using-known-private-keys-to-decrypt-traffic-part-2/

本文来自csdn的□□***shu天***□□，平时会记录**ctf、取证和渗透**相关的文章，欢迎大家来我的主页：shu天_CSDN博客-ctf,取证,web领域博主
看看ヾ(@ ˇωˇ @)ノ！！