

xctf攻防世界 MISC高手进阶区 心仪的公司

原创

18947943 于 2022-01-25 21:56:30 发布 10770 收藏

分类专栏: [攻防世界misc之路](#) 文章标签: [安全 misc](#)

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/18947943/article/details/122692571>

版权



[攻防世界misc之路](#) 专栏收录该内容

68 篇文章 2 订阅

订阅专栏

1. 进入环境, 下载附件

给的是一个rar压缩包, 里面是个抓包流量文件, 使用wireshark打开, 如图:

webshell.pcapng

应用显示过滤器: <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
2408	10.214453	192.168.1.111	202.108.23.152	TCP	54	58174 → 80 [ACK] Seq=6648 Ack=102
2409	10.220380	192.168.1.1	192.168.1.111	DNS	90	Standard query response 0xb934 A
2410	10.220411	192.168.1.1	192.168.1.111	DNS	150	Standard query response 0xe28e A
2411	10.220415	192.168.1.1	192.168.1.111	DNS	90	Standard query response 0xe81d0 A
2412	10.220422	101.201.170.241	192.168.1.111	TCP	74	80 → 43385 [SYN, ACK] Seq=0 Ack=1
2413	10.220453	192.168.1.111	101.201.170.241	TCP	66	43385 → 80 [ACK] Seq=1 Ack=1 Win=
2414	10.220739	192.168.1.111	101.201.170.241	HTTP	1409	GET /psearch/psearch/query?x-acl-
2415	10.220910	192.168.1.111	101.201.170.241	TCP	74	60720 → 80 [SYN] Seq=0 Win=20700

Request URI Path: /psearch/psearch/query

- Request URI Query [truncated]: x-acl-token=kU0m7x6dCaKGFa8RxxLQ5Hm75ioK&index_name=pro_course_v2&pro_id=369
- Request URI Query Parameter: x-acl-token=kU0m7x6dCaKGFa8RxxLQ5Hm75ioK
- Request URI Query Parameter: index_name=pro_course_v2
- Request URI Query Parameter: pro_id=3699123
- Request URI Query Parameter: callback=jQuery203005047280433171697_1477704425321
- Request URI Query Parameter: _client_rcommend_course
- Request URI Query Parameter: fields=id%2Ctitle%2Cpic%2Cstu_count%2Cgood_ratio%2Crc_flag%2Csource_type

0130 66 6c 61 67 25 32 43 73 6f 75 72 63 65 5f 74 79 flag%2Csource_ty

0140 70 65 26 70 72 6f 5f 74 79 70 65 3d 64 6f 77 6e pe&pro_type=down

0150 6c 6f 61 64 26 73 69 7a 65 3d 31 30 26 5f 3d 31 load&size=10&_1

0160 34 37 37 37 30 34 34 32 35 33 32 32 20 48 54 54 47770442 5322 HTT

0170 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 69 6e 74 P/1.1 Host: int

0180 65 72 6e 61 6c 61 70 69 2e 63 73 64 6e 2e 6e 65 ernalapi.csdn.ne

0190 74 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d t>User-Agent: M

01a0 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b ozilla/5.0 (X11;

01b0 20 4c 69 6e 75 78 20 78 38 36 5f 36 34 3b 20 72 Linux x86_64; r

01c0 76 3a 34 35 2e 30 29 20 47 65 63 6b 6f 2f 32 30 v:45.0) Gecko/20

01d0 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 34 100101 Firefox/4

01e0 35 2e 30 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 5.0 Accept: /*/*

01f0 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 Accept-Language

0200 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e e: en-US,en;q=0.

0210 35 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 5 Accept-Encoding

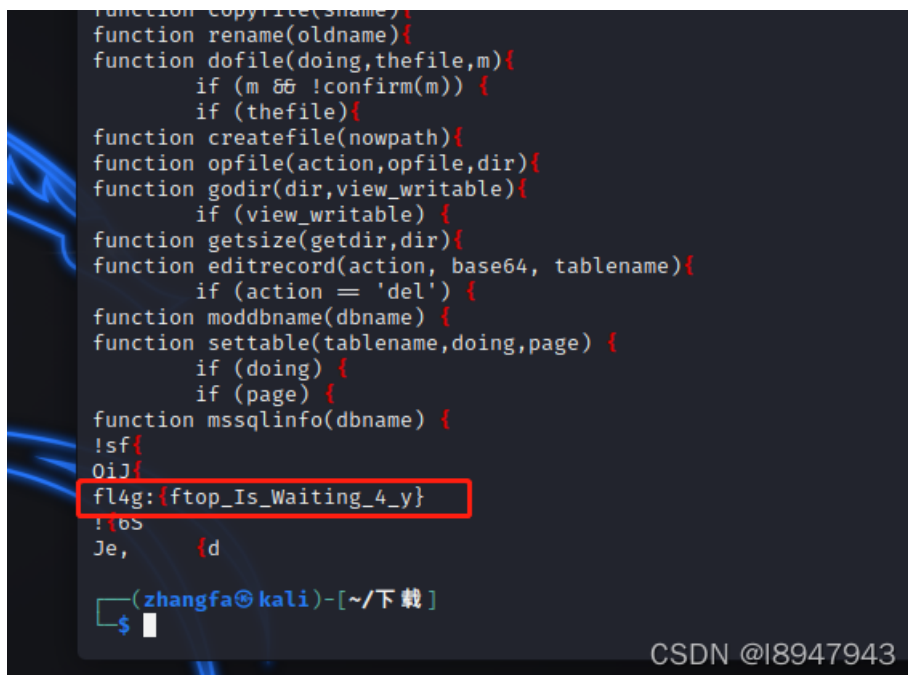
HTTP Request-URI Query Parameter (http.request.uri.query.parameter), 72 byte(s) | 分组: 13498 · 已显示: 13498 (100%) | 配置: 18947943

一通过关键词搜索后无果

2. 问题分析

扔到kali中，使用strings命令，进行过滤尝试

```
strings webshell.pcapng | grep {
```



```
function copyfile(sname){
function rename(oldname){
function dofile(doing,thefile,m){
    if (m && !confirm(m)) {
        if (thefile){
function createfile(nowpath){
function opfile(action,opfile,dir){
function godir(dir,view_writable){
    if (view_writable) {
function getsize(getdir,dir){
function editrecord(action, base64, tablename){
    if (action = 'del') {
function moddbname(dbname) {
function settable(tablename,doing,page) {
    if (doing) {
        if (page) {
function mssqlinfo(dbname) {
!sf{
0iJ{
fl4g: {ftop_Is_Waiting_4_y}
!{bs
Je,      {d

(zhangfa@kali)-[~/下载]
└─$
```

或者使用正则过滤:

```
# 贪婪模式，前置几个字符，{}中字符长度在1到20之间，并且以}符号结尾
strings webshell.pcapng | grep -E '^.*?:{.[1,20]}$'
```

结果如图:

```
zhangfa@kali: ~/下载
文件 动作 编辑 查看 帮助
(zhangfa@kali)-[~/下载]
└─$ strings webshell.pcapng | grep -E '^.*?:{.1,20}$'
m-input-wrap":[],".bdcs-search-form-input-notspan":{"margin-left":"0px","font-family":"Arial,SimSun,sans-serif","color":"#000000","font-size":"14px"},".bdcs-search-form-input .icon-nofocus":{"left":"","right":"","top":"","height":"","width":"","bdcs-search":{"width":"541px","height":"28px","overflow":"hidden","border-color":"#00AA00","border-radius":"0px","border-width":"1px","box-shadow":"none","background-color":"#00AA00"},".bdcs-search-form-input":{"border-color":"#00AA00","margin-right":"0px","width":"478px","height":"26px","line-height":"26px","font-family":"Arial,SimSun,sans-serif","color":"#000000","font-size":"14px","border-radius":"0px","background-color":"#FFFFFF"},".bdcs-search-form-input:focus":{"border-color":"#f79646"},".bdcs-search-form-submit-wrap":[],".bdcs-search-form-submit":{"border-color":"#00AA00","height":"26px","width":"60px","background-color":"#00AA00","color":"#ffffff","font-family":"Arial,SimSun,sans-serif","font-size":"14px","border-radius":"0px"},".bdcs-search-sug-list":{"width":"px"},".bdcs-search-sug-list-item":{"height":"28px","line-height":"28px","font-family":"Arial,SimSun,sans-serif","font-size":"14px"},".bdcs-search-sug-list-item-value":{"color":"#1f497d"},".bdcs-hot":{"width":"600px","height":"21px","line-height":"21px"},".bdcs-hot-item":{"color":"#494429","font-family":"Arial,SimSun,sans-serif","font-size":"12px"},".div#default-searchbox .default-channel-meun":{"width":"75px"}
,"container" : {"anchoredType":3,"closeType":1,"floated":{"blockType":1,"clientw":0,"contw":1024,"dockType":1,"follow":1},"height":270,"location":6,"sizeType":1,"slide":{"width":120}
,"fillstyle" : {"cloudTheme":{},"elements":[1,2],"layout":[1],"lu":{"search":{},"styleType":2,"txt":{"number":1},"video":{}}
,"container" : {"anchoredType":1,"floated":{"height":60,"sizeType":1,"slide":{"width":468}
,"fillstyle" : {"backgroundColor":"#FFFFFF","cloudTheme":{},"elements":[0,1,2],"flush":0,"layout":[1,2],"lu":{"search":{},"styleType":2,"txt":{"cbackground":"#FFFFFF","cborder":"#FFFFFF","cdesc":"#444444","cflush":"#e10900","ctitle":"#0000FF","curl":"#008000","number":2},"video":{}}
,"container" : {"anchoredType":1,"floated":{"height":250,"sizeType":1,"slide":{"width":300}
,"fillstyle" : {"backgroundColor":"#ffffff","cloudTheme":{},"elements":[0,1,2,4,5],"flush":0,"layout":[1,2],"lu":{"search":{},"styleType":2,"txt":{"cbackground":"#ffffff","cborder":"#ffffff","cdesc":"#333333","cflush":"#e10900","ctitle":"#006699","curl":"#333333","number":3},"video":{}}
f14g:{ftop_Is_Waiting_4_y}
└─(zhangfa@kali)-[~/下载]
CSDN @I8947943
```

最终答案为: f14g:{ftop_Is_Waiting_4_y}