【MRCTF2022 writeup】

原创

k_du1t 于 2022-04-26 08:54:05 发布 149 收藏

分类专栏： ctf 文章标签： 后端 安全 web 网络安全

1NDEX

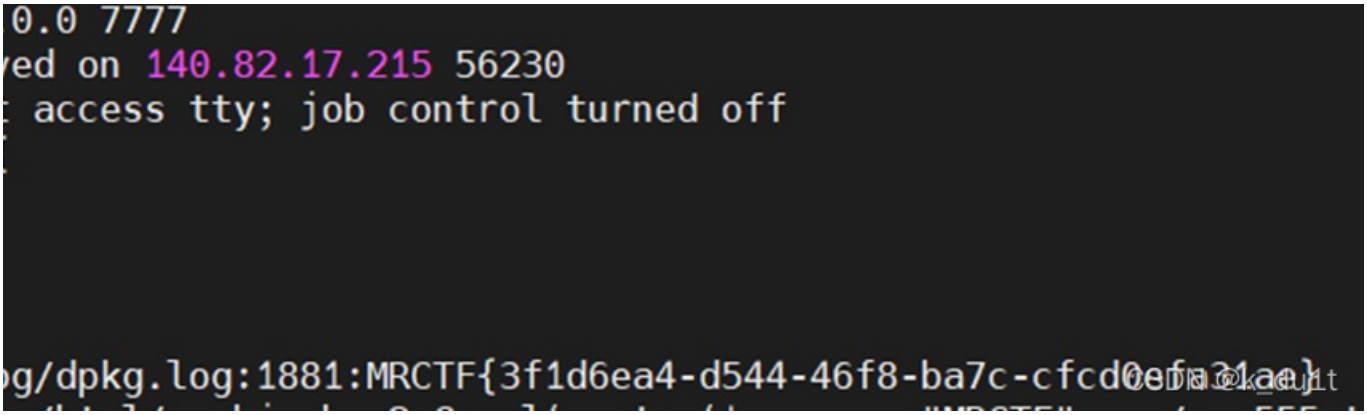
0x00 前言

这把打的太菜了…
没出什么有思考的题目，好好复现吧
贴个团队writeup水一下

Web

WebCheckIn

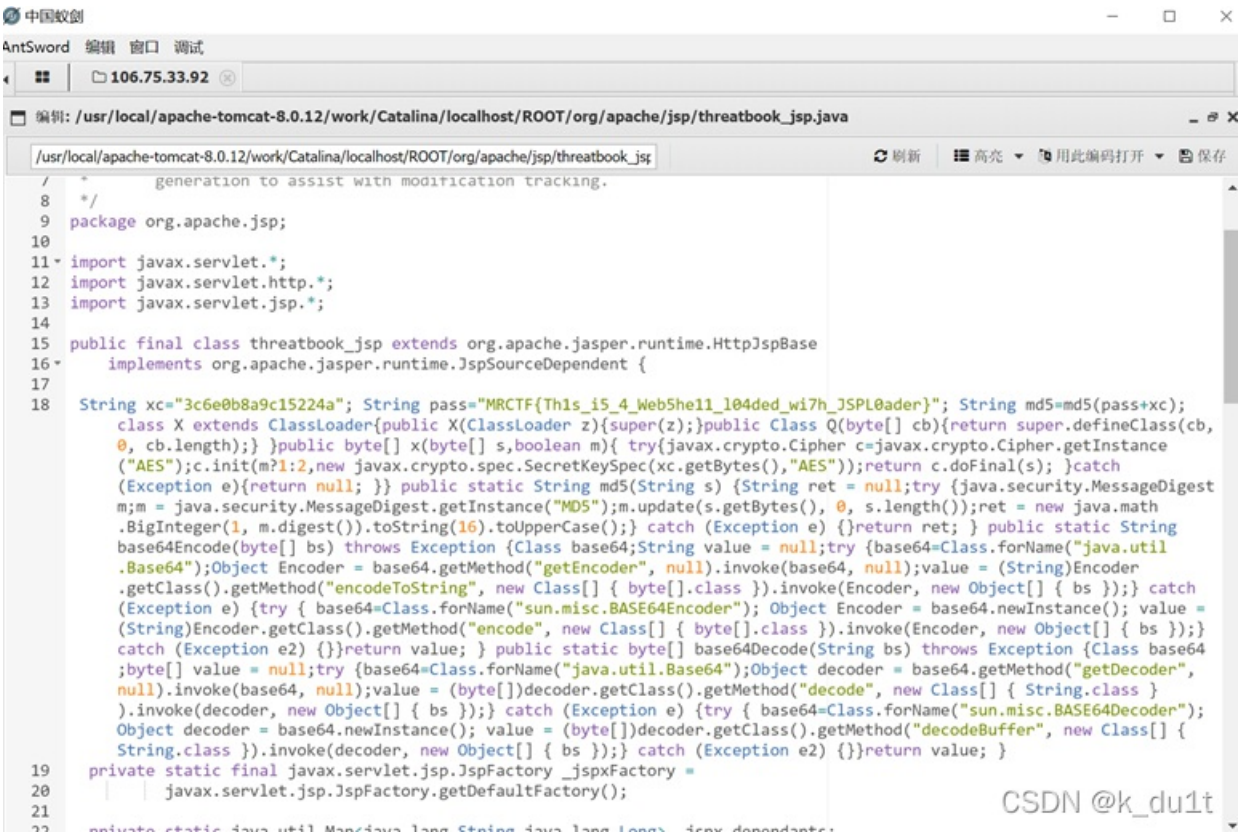
文件上传点会解析php
直接system反弹shell
翻到flag



Bonus

Java_mem_shell_Basic

Tomcat默认密码tomcat/tomcat进manager，在WAR file to deploy处上传压缩为war的jsp木马，连上得到flag

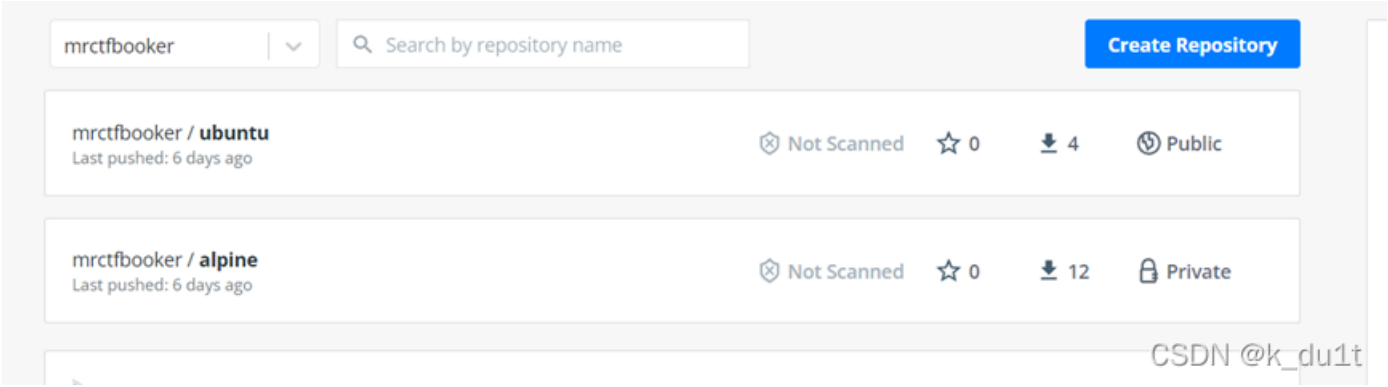


Just Hacking

Msf爆口令foobared
主从rce打 getshell
/root/.docker目录下发现docker hub

```
cat: .docker: Is a directory
# cd .docker
# ls
config.json
# cat config.json
{
        "auths": {
                "https://index.docker.io/v1/": {
                        "auth": "bXJjdGZib29rZXI6V1o4bnBTSzRUY0M="
                }
        }
```


mrctfbooker:WZ8npSK4TcC
pull私人镜像

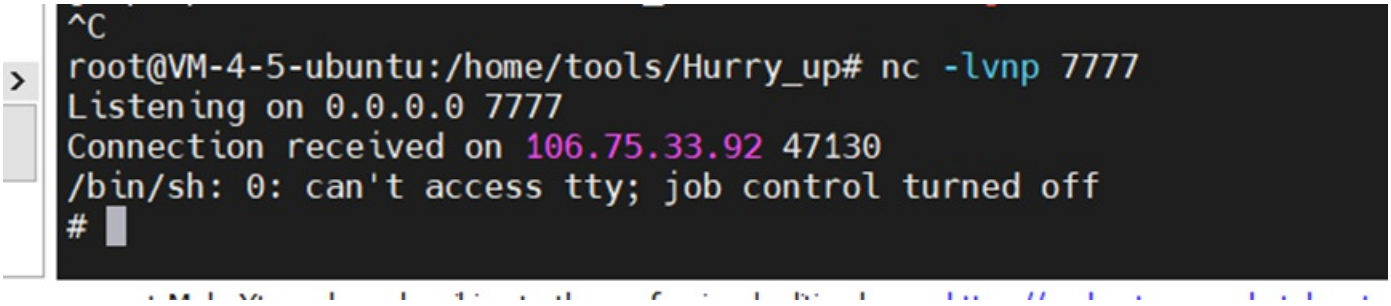



```
^C
/ # ls
bin    dev    etc    home   lib    media  mnt    opt    proc   root   run    sbin   srv    sys
/ # ls -a
.           .dockerenv  dev         home        media       opt         root        sbin
..          bin         etc         lib         mnt         proc        run         srv
/ # cd /root
~ # ls
flag.txt
~ # cat flag.txt
mrctf{0e8692f3-dbdb-4ca9-a16b-b2f5406809c0}
~ #
~ #
~ # whoami
```


Java_mem_shell_Filter

直接name处输入payload即可

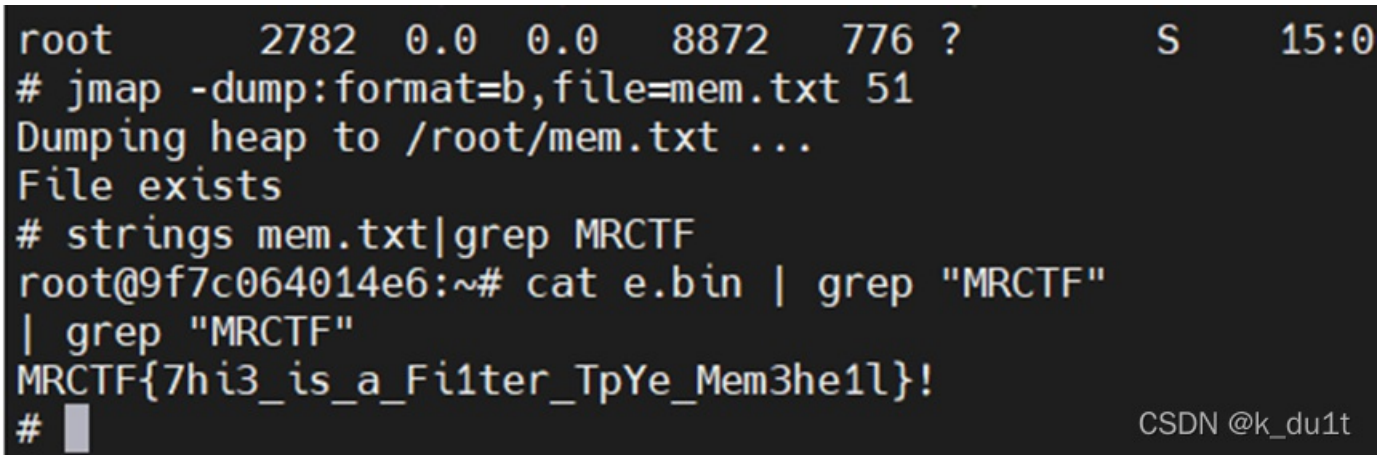
Log4j反弹shell



全局没搜到flag...

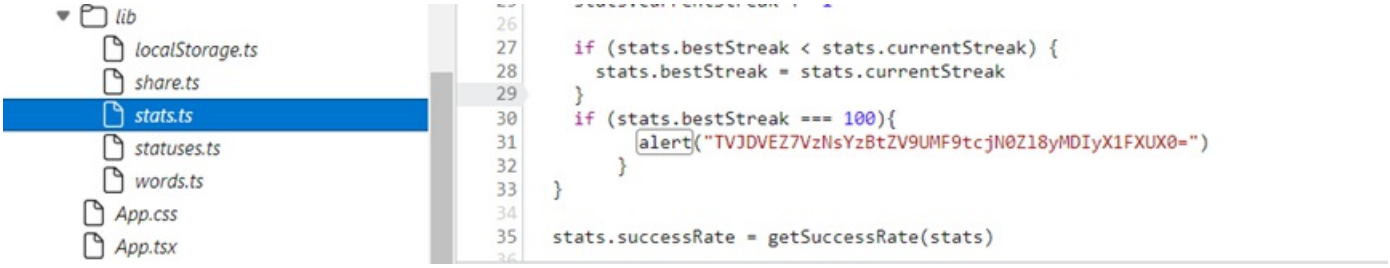
Mem想到打印内存

【JVM】jmap命令详解----查看JVM内存使用详情 - Angel挤一挤 - 博客园 (cnblogs.com)



MISC

Checkin



MRCTF{W3lc0me_T0_mr3tf_2022_QWQ}

PDD

参照*CTF 2021，基本一摸一样，利用分组加密的漏洞构造，主要就是找对哪个字符串加密，用debug试了一下，通过构造username，成功了。使用如下payload
SRMr2xR0uuLsQScgoAegYwlz9tod7K3gLTPTcqOGlyYRlWG6qC652QhE1u1Zw1iFs/5+fMCPNhR4pR+FHJWe3eydb1UtueXoodo3h/v8zo9Gh1Qkg/K6xKRBgVNKHksD

0x01 rethink

破事太多真的影响发挥…
希望每个ctfer都能实现时间自由吧