0CTF/TCTF2019 Ghost Pepper Writeup

原创

郁离歌 于 2019-03-25 16:00:19 发布 1203 收藏

分类专栏： CTF-WRITE-UP WEB学习 文章标签： 0ctf2019

本文链接：https://blog.csdn.net/like98k/article/details/88797218

0CTF/TCTF2019 Ghost Pepper Writeup

签到成功，告辞。首先发现401一个登陆框，弱口令什么的都试试发现不行。抓包发现返回包里面有karaf的字样。谷歌搜索一波搜到了相关资料：https://karaf.apache.org/manual/latest/webconsole

里面说到：

> The Apache Karaf WebConsole uses the WebContainer port number (see the [WebContainer section|webcontainer] for details) with the /system/console context.
> By default, the Apache Karaf WebContainer port number is 8181.
> It means that the Apache Karaf WebConsole is accessible on the following URL: http://localhost:8181/system/console
> As the Apache Karaf WebConsole uses the security framework, an username and password will be prompted.
> You have to enter an username/password from the karaf realm. By default, you can use karaf/karaf.

随即使用karaf/karaf登陆进去。然鹅发现怎么都是404.提示是`Powered by Jetty:// 9.3.24.v20180605`搜了一下发现这个是java的服务器，类似于tomcat。测试了几个常用feature，发现有`jolokia`！rr师傅前几星期才挖的0day。先知安全客搜了一些文章：

https://xz.aliyun.com/t/4258

https://www.anquanke.com/post/id/173262

https://www.anquanke.com/post/id/87031

按照上面的分析，访问`/jolokia/list`发现并没有相关类导致漏洞。那复现肯定是gg了。

想了半天也没思路，后来猛然想到，为啥入口要弄一个karaf?看看上面的资料https://karaf.apache.org/manual/latest/webconsole
访问`/system/console`可以进入终端控制台。但是直接访问是404，说明没安装。
那么是不是要利用karaf的类执行安装webconsole的命令，然后进控制台拿flag？这个思路太骚了，感觉不是非预期。试着搜了一下。

果然有，好像还是root权限，那么参考着上面那些文章的打法，exec调用feature安装webconsole应该是可行的！
说做就做：

因为没学过javaweb，看语法看了半天，调了好久终于返回200的状态码。注意一些content-type要改一下。
然后访问`/system/console`点`Main->goto`进入终端，执行命令拿到flag，由于没用过karaf的原因，找了半天怎么进终端orz...