Apache Axis2的两个利用方式

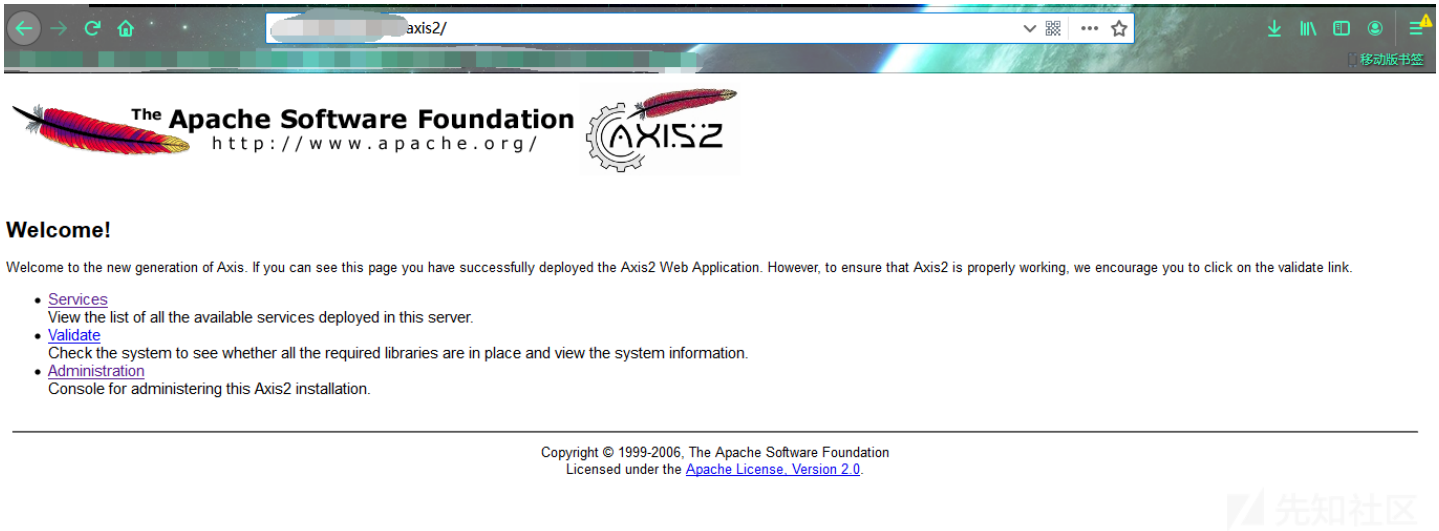
李香兰老师 / 2019-09-04 09:12:00 / 浏览数 3722 安全技术 漏洞分析 顶(0) 踩(0)

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，在一次偶然的机会下，第一次遇见了安装有Apache Axis2服务的tomcat。

确定目标是否存在axis2

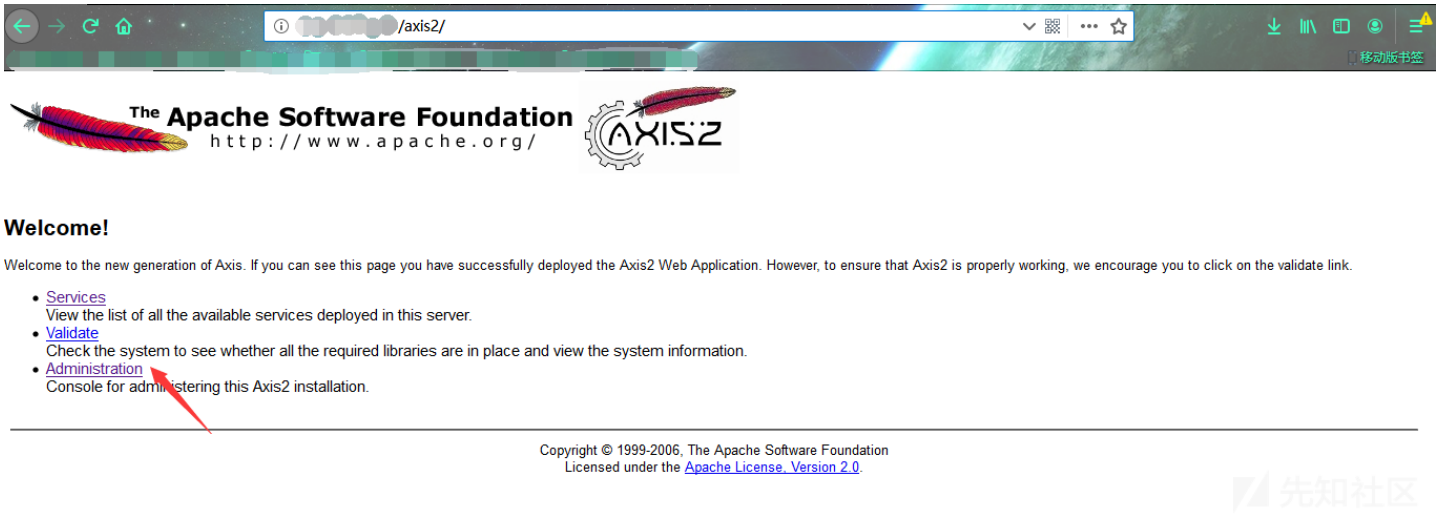
直接在URL后面添加/axis2即可。



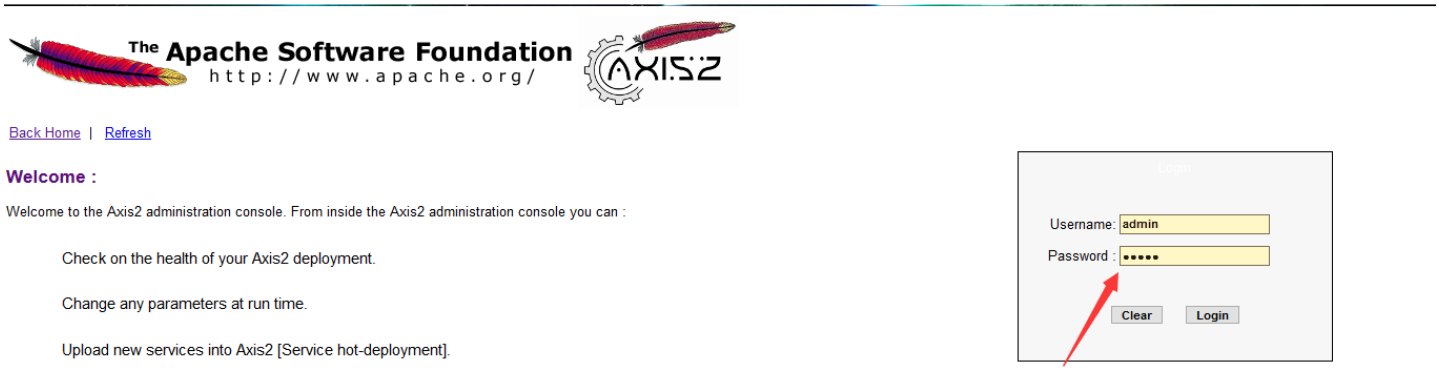
出现上图即可证明此tomcat安装了axis2服务。

方式1 文件上传漏洞

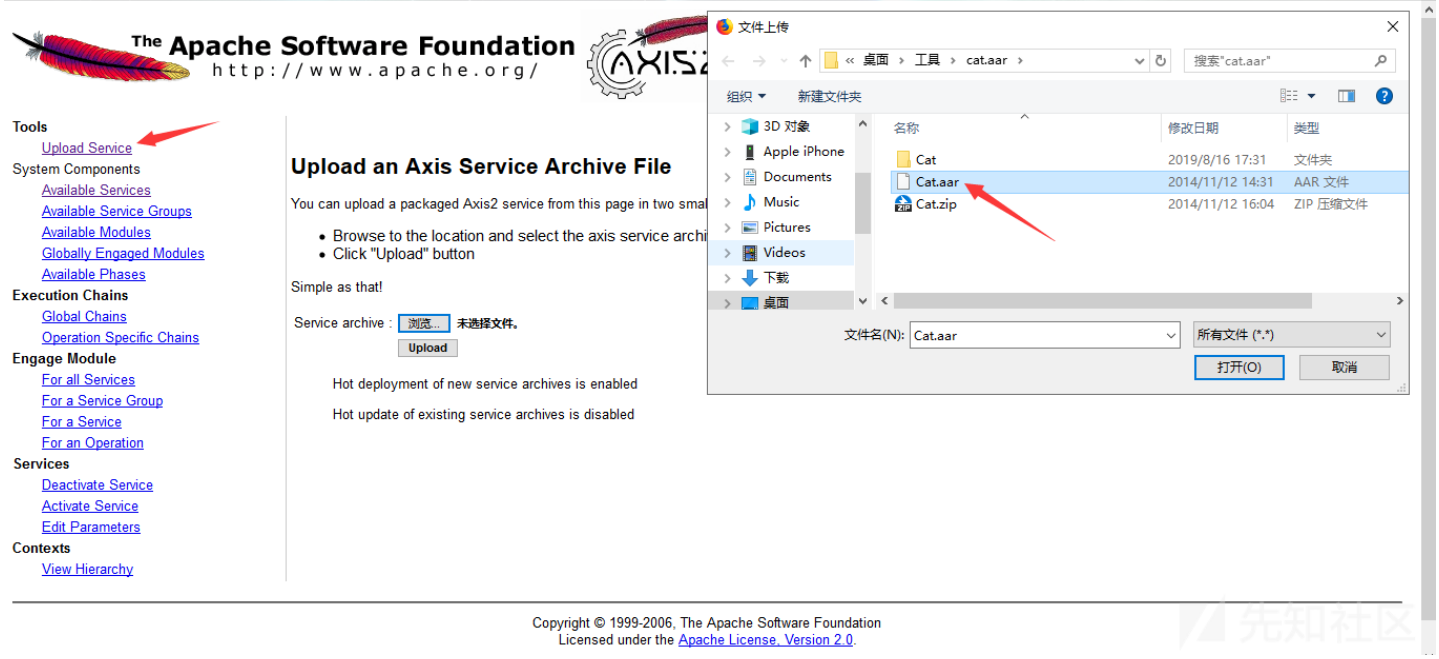
访问axis2的管理员界面



利用默认密码登录（此为前提条件 admin/axis2 ）



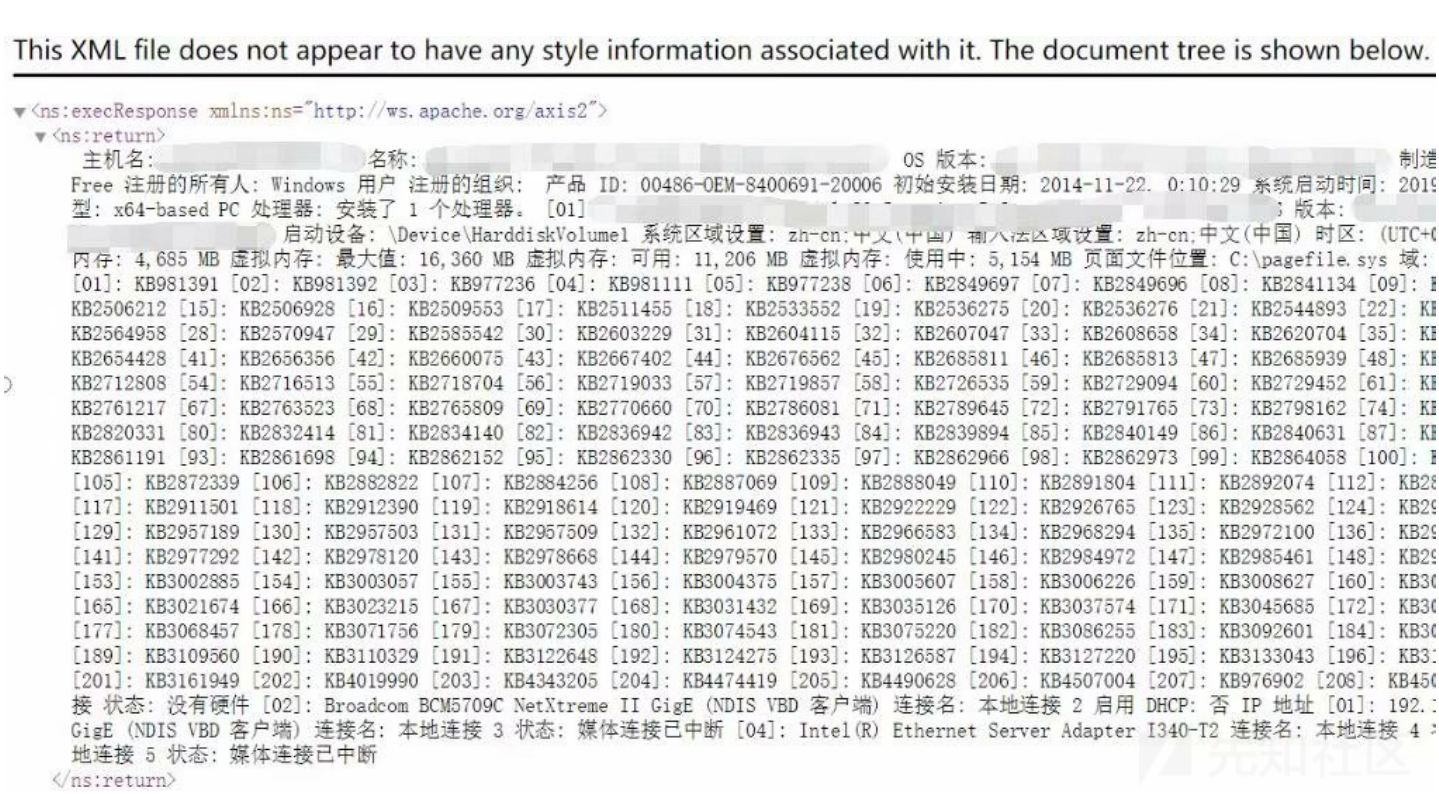
通过上传点，上传Cat.aar，下载见参考文章处



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
```

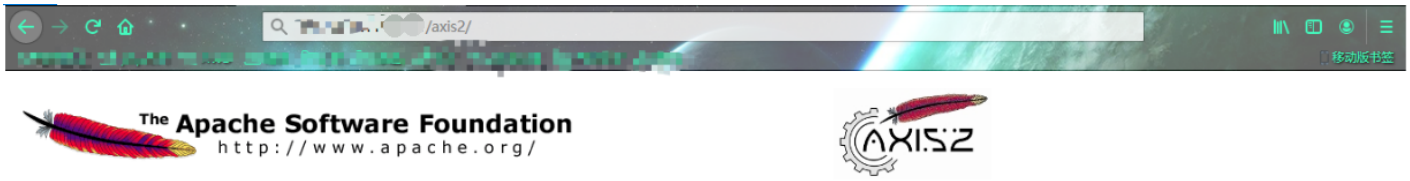


参考文章

- [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



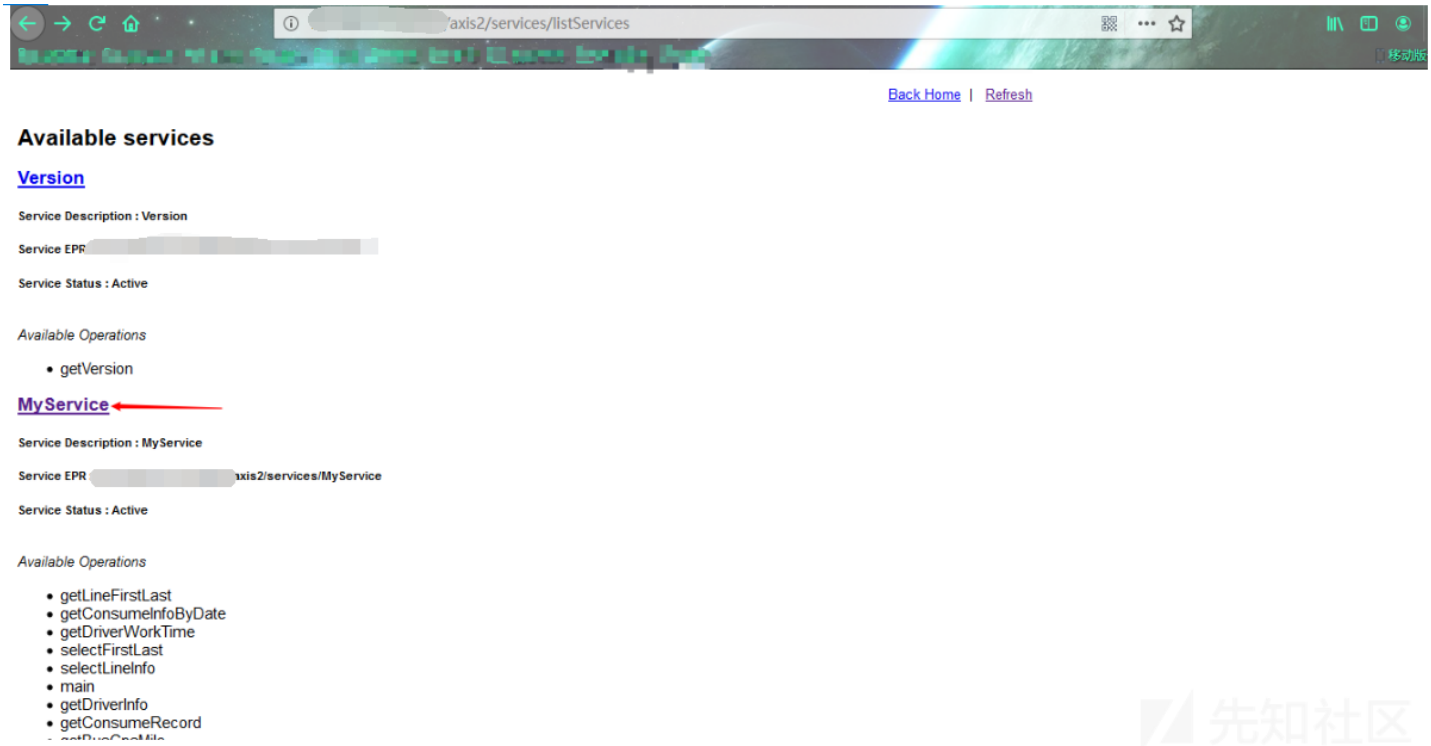
Welcome!

Welcome to the new generation of Axis. If you can see this page you have successfully deployed the Axis2 Web Application. However, to ensure that Axis2 is properly working, we encourage you to click on the validate link.

- Services
  View the list of all the available services deployed in this server.
- Validate
  Check the system to see whether all the required libraries are in place and view the system information.
- Administration
  Console for administering this Axis2 installation.

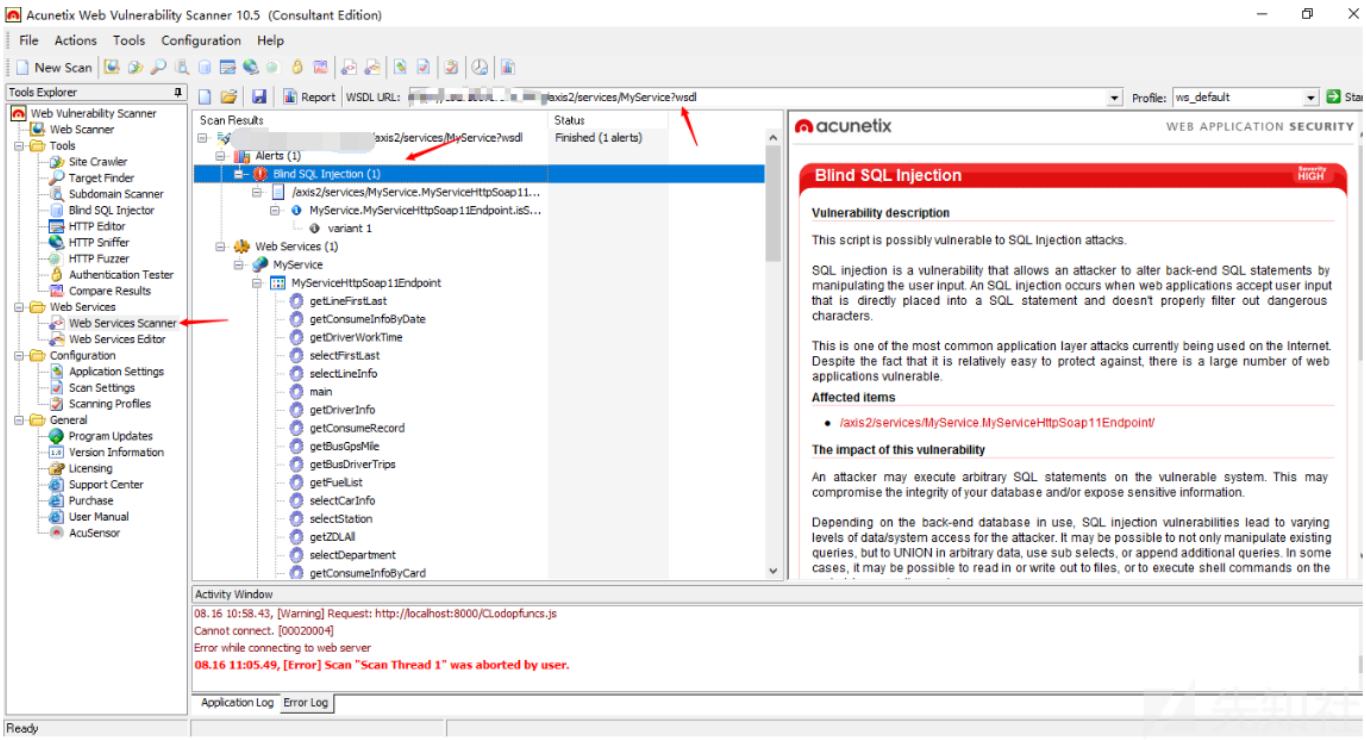
Copyright © 1999-2006, The Apache Software Foundation
Licensed under the Apache License, Version 2.0.

点击MyService

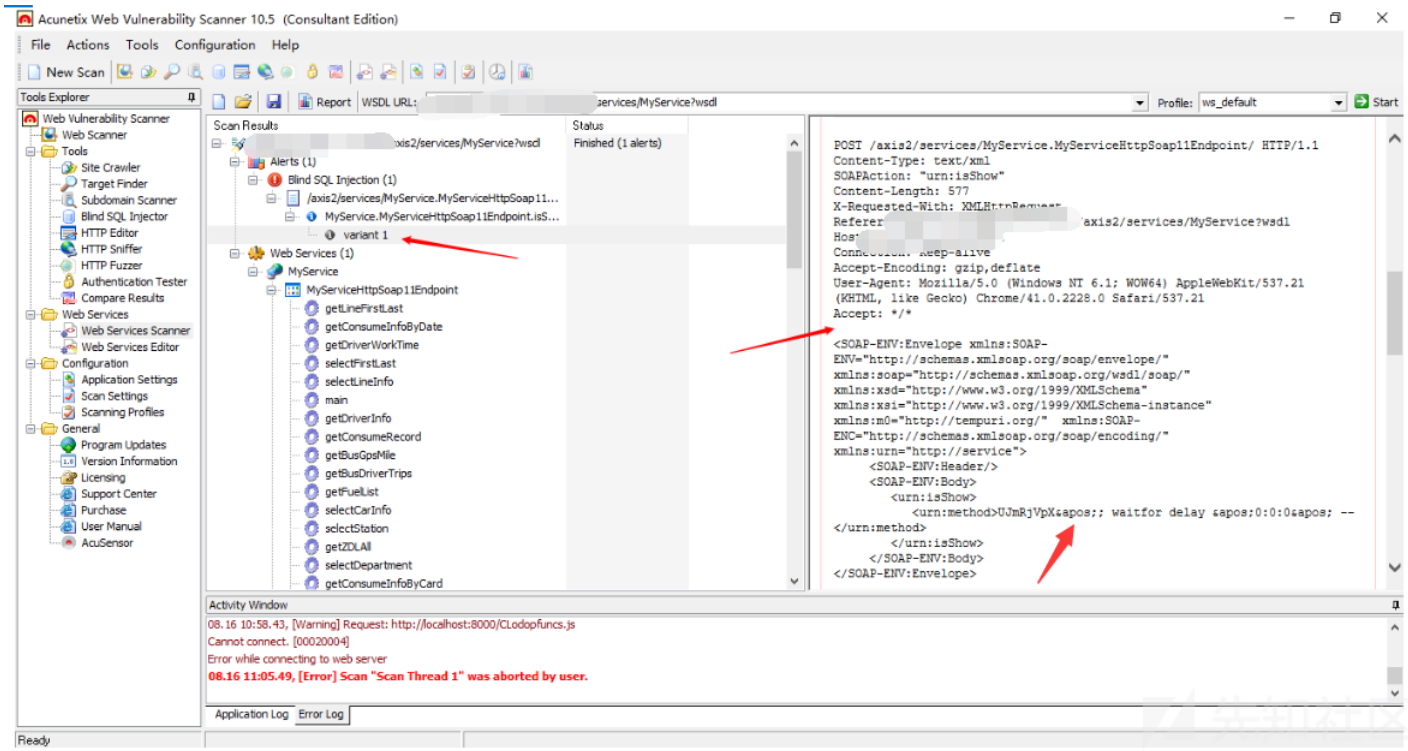


可以看见此页面(利用前提)

使用AVWVS对该页面进行扫描（或者使用burp抓包）

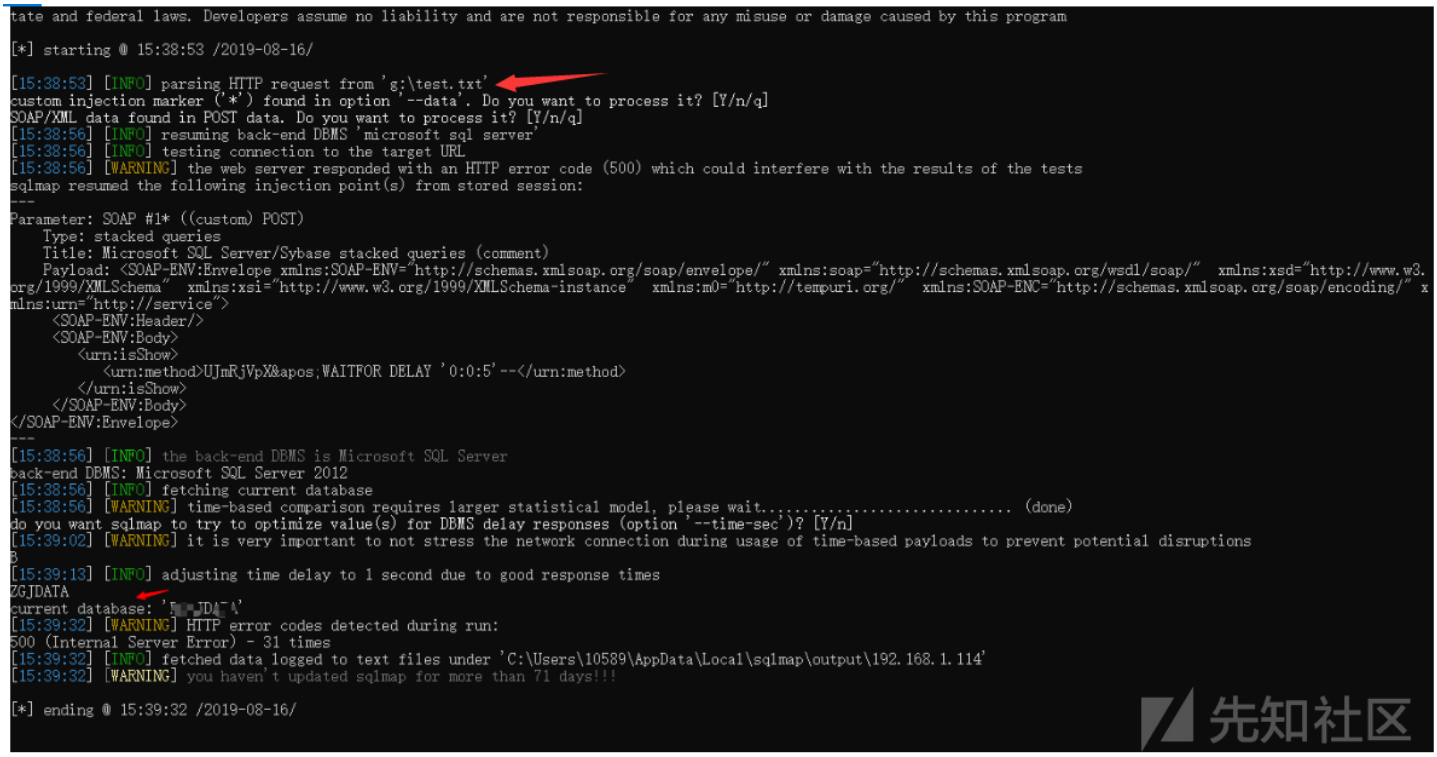


复制POST的数据，保存为test.txt



对如图所示的地方进行修改

放入SQLmap(按回车即可)



本文仅限技术研究与讨论，严禁用于非法用途，否则产生的一切后果自行承担

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！

目录