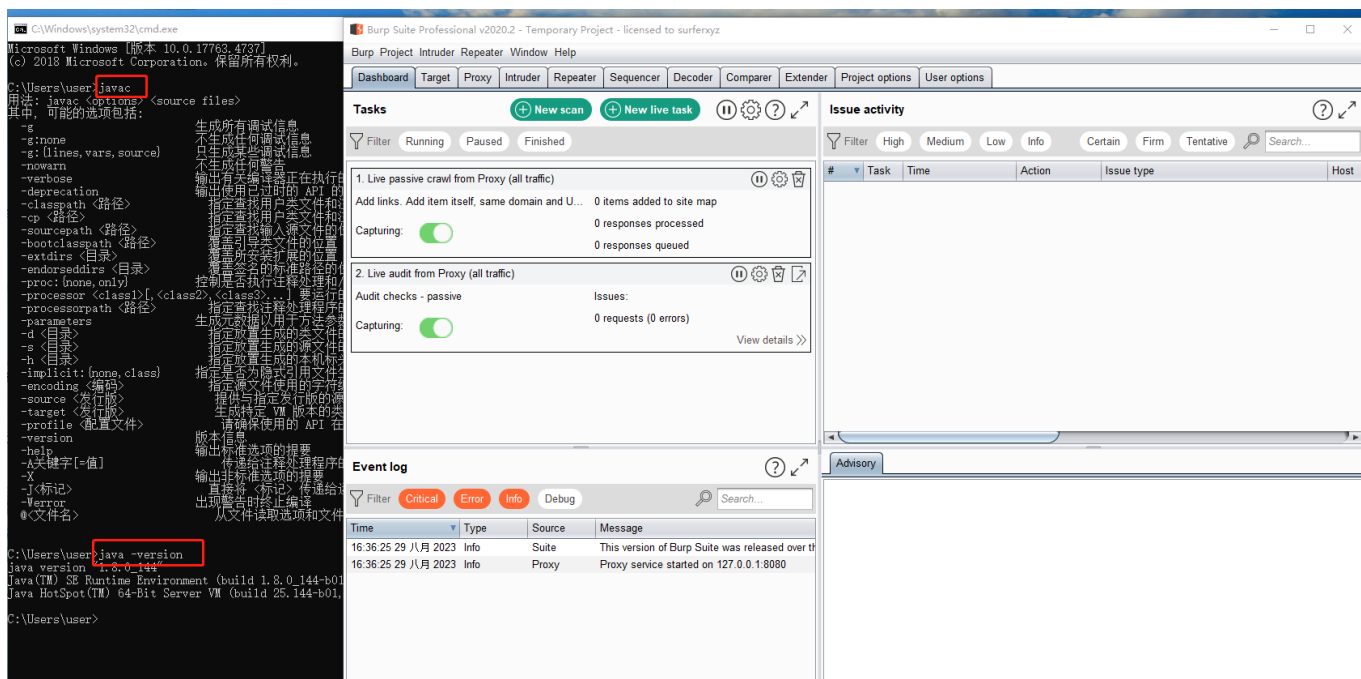
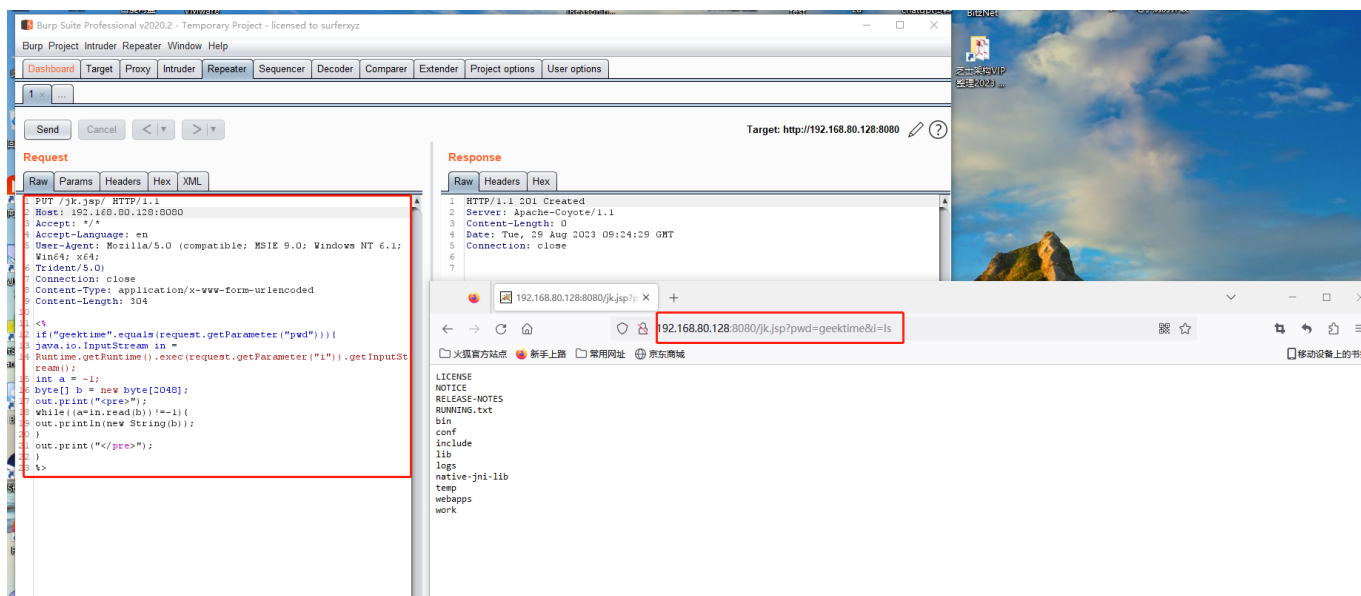


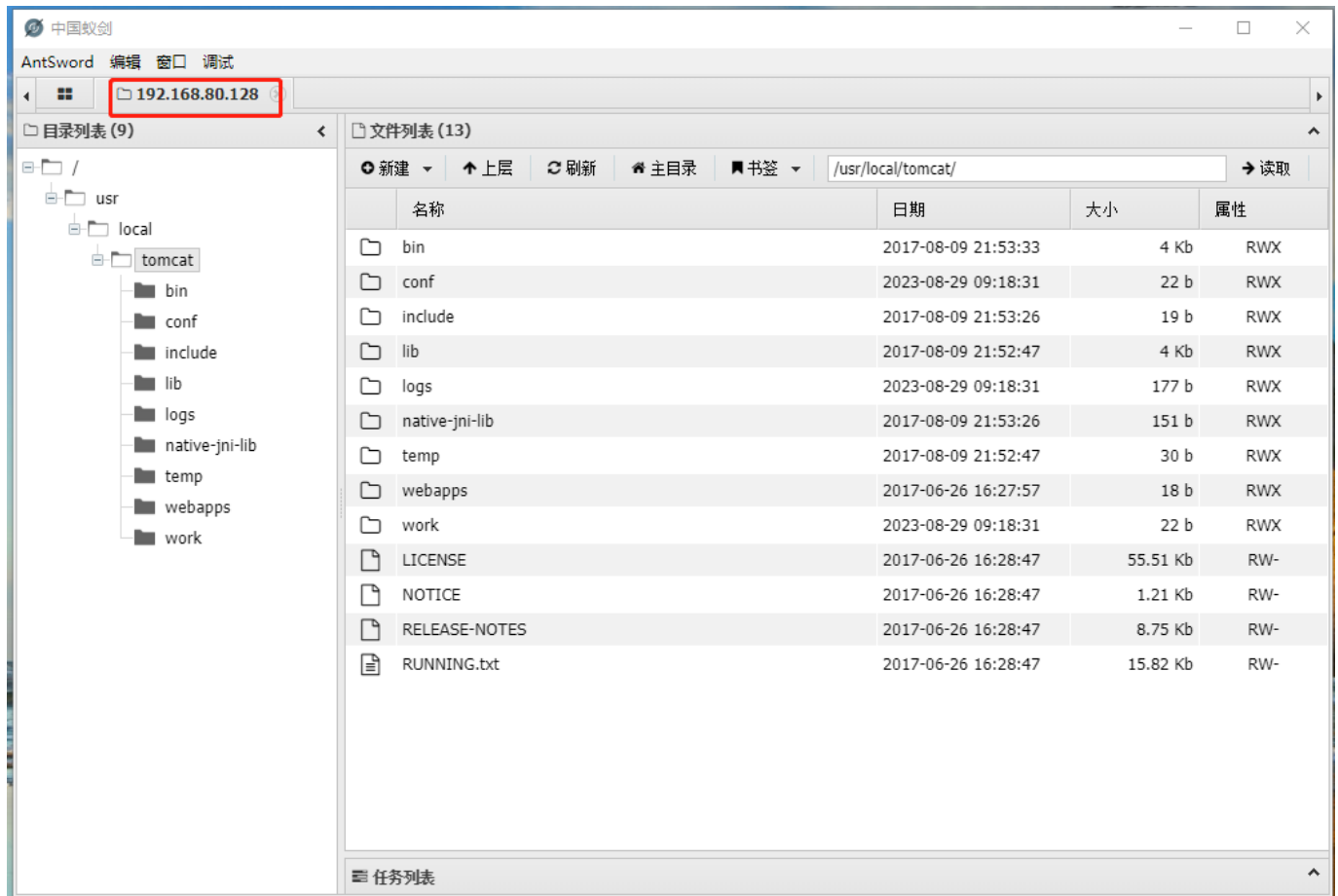
1.安装Java环境并激活Burp



2. 练习 Tomcat PUT 方法任意写文件漏洞（CVE-2017-12615），提供命令执行截图。

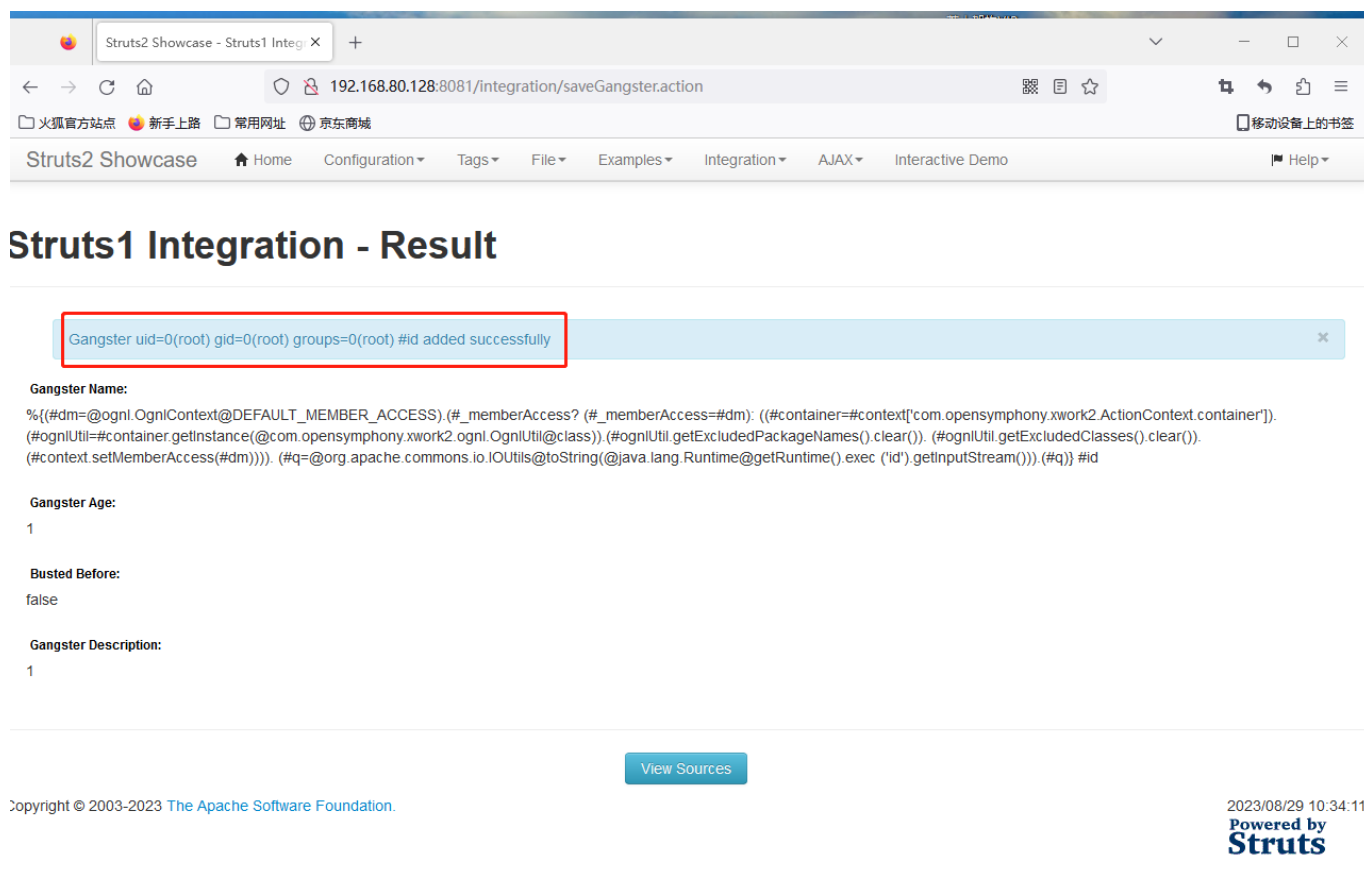
docker run -d -p 8080:8080 cved/cve-2017-12615





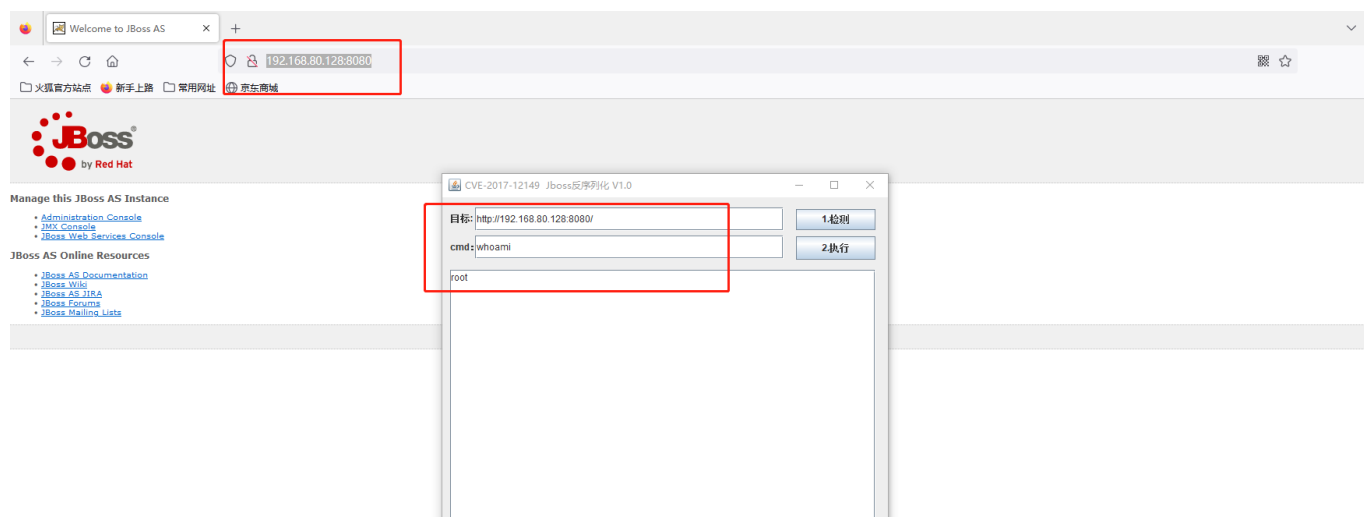
3.练习 S2-048 远程代码执行漏洞 (CVE-2017-9791) , 提供命令执行截图。

```
docker run -d -p 8081:8080 piesecurity/apache-struts2-cve-2017-5638
```



4.练习 JBoss 5.x/6.x 反序列化漏洞（CVE-2017-12149），提供命令执行截图。

`docker run -d -p 8080:8080 hackingpub/cve-2017-12149`



5.安装并使用 Nmap 扫描一个地址（本机、VPS、虚拟机环境都可以），提供扫描结果截图。

```
C:\Windows\system32\cmd.exe
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.34 seconds

C:\Users\user>nmap -A -T4 -sT -sV 192.168.80.128/32
Starting Nmap 7.92 ( https://nmap.org ) at 2023-08-29 18:55 ?D1ú±ê×?ê±??
Nmap scan report for 192.168.80.128
Host is up (0.00040s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.0 (protocol 2.0)
  ssh-hostkey:
    3072 ff:8d:c2:5e:ee:a6:67:ae:c9:ca:21:6a:1c:a9:c0:b8 (RSA)
    256  b6:bf:66:6d:6d:84:f1:51:5c:9c:13:79:98:09:38:3a (ECDSA)
    256  77:24:47:43:76:11:65:73:70:83:9a:48:2d:00:17:5f (ED25519)
25/tcp    open  tcpwrapped
  _smtp-commands: Couldn't establish connection on port 25
110/tcp   open  tcpwrapped
  _sslv2: ERROR: Script execution failed (use -d to debug)
  _tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
  _ssl-date: ERROR: Script execution failed (use -d to debug)
  _tls-alpn: ERROR: Script execution failed (use -d to debug)
  _ssl-cert: ERROR: Script execution failed (use -d to debug)
111/tcp   open  rpcbind      2-4 (RPC #100000)
  rpcinfo:
    program version  port/proto  service
    100000  2, 3, 4    111/tcp    rpcbind
    100000  2, 3, 4    111/udp    rpcbind
    100000  3, 4      111/tcp6   rpcbind
    100000  3, 4      111/udp6   rpcbind
3080/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
  _http-title: Welcome to JBoss AS
  http-methods:
    _ Potentially risky methods: PUT DELETE TRACE
  _http-open-proxy: Proxy might be redirecting requests
  _http-server-header: Apache-Coyote/1.1
3081/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
  http-title: Struts2 Showcase
  _Requested resource was showcase.action
  _http-server-header: Apache-Coyote/1.1
MAC Address: 00:0C:29:2F:00:AF (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
```

6.以任一企业为关键词进行信息收集练习并汇总形成报告，禁止进行违规操作。

当前位置: 站长工具 > WHOIS查询

广告

实力产品收量

大秀实力产品无限收量

whois查询

最新注册

邮箱反查

注册人反查

电话反查

域名批量查询

域名注册

历史查询

全球域名后缀

域名注册商

qzhospital.com

查询

域名 qzhospital.com 的信息

求购此域名

以下信息更新时间: 2023-08-11 16:22:32

立即更新

获取API

申请删除隐私

域名	qzhospital.com
注册商	Bizcn.com,Inc.
更新时间	2023年06月02日
创建时间	2004年06月11日
过期时间	2024年06月11日
注册商服务器	whois.bizcn.com
DNS	ns7.cnmsn.net ns8.cnmsn.net
状态	注册商设置禁止删除(clientDeleteProhibited) 注册商设置禁止转移(clientTransferProhibited)

过期域名查询

域名删除时间查询

PR查询

IP地址查询

网站收录查询

Alexa排名查询

友情链接检测

SEO综合查询

网站权重查询



鹰眼舆情监测系统

企查查

全国企业信用查询系统
官方备案企业征信机构

衢州市人民医院

查一下

应用

企业套餐

开通会员

综合 3653

企业 102

人员

风险 247

商标 16

专利 174

招投标 2939

新闻 142

创投库

全球企业

筛选条件

高级搜索

批量查询

查找范围

☐ 企业名

☐ 经营范围

☐ 企业简介

☐ 联系地址

☐ 品牌/产品

☐ 法定代表人

☐ 专利

☐ 商标

☐ 股东

☐ 主要人员

省份地区

浙江省 (102)

成立年限

☐ 3个月内

☐ 半年内

☐ 1年内

☐ 1-3年

☐ 3-5年

☐ 5-10年

☐ 10年以上

☐ 自定义

国际行业与

批发和零售业 (4)

交通运输、仓储和邮政业 (1)

住宿和餐饮业 (1)

居民服务、修理和其他服务业 (1)

卫生和社会工作 (4)

更多筛选

① 注册资本

① 实缴资本

① 企业规模

① 登记状态

投资机构

投资商地区

资本类型

分支机构

经营状况

联系电话

手机号码

固定电话

① 疑似代理记账号码

联系邮箱

实缴资本

参保人数

变更信息

① 小微企业

一般纳税人

为您找到 102 条相关结果

已显示40条, 开通会员查看更多

☐ 空号过滤

☐ 仅看公司

卡片

表格

默认排序

批量操作

导出数据

衢州市人民医院 (衢州中心医院)

正常

事业单位

三甲甲等

被执行人

负责人: 叶金林

注册资本: 95648万元人民币

成立日期: -

统一社会信用代码: 12330800471866062F

电话: -

邮箱: -

官网: http://www.qzhospital.com

地址: 衢州市柯城区衢江大道100号

笔记

关注

chaziyu.com/qzhospital.com/

查子域
chaziyu.com

qzhospital.com X 查子域名 查备案

高配服 gaopeifu.com 大陆高配服务器 66元定制服务费 买卖域名, 网站, 自媒体 上中介网!

广告QQ: 3083352837

qzhospital.com子域名查询
icp备案: 浙ICP备05015372号-1

ipchaxun.com

序号	子域名
1	yjp.qzhospital.com
2	ipacs.qzhospital.com
3	wechat.qzhospital.com
4	diancan.qzhospital.com
5	www.qzhospital.com

真实IP

```
C:\Users\user>ping www.qzhospital.com

正在 Ping www.qzhospital.com [122.227.65.178] 具有 32 字节的数据:
来自 122.227.65.178 的回复: 字节=32 时间=46ms TTL=254
来自 122.227.65.178 的回复: 字节=32 时间=41ms TTL=254
来自 122.227.65.178 的回复: 字节=32 时间=13ms TTL=254
来自 122.227.65.178 的回复: 字节=32 时间=1ms TTL=254

122.227.65.178 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 46ms, 平均 = 25ms
```

GoogleHack语法

国内版国际版

Microsoft Bing

site:qzhospital.com filetype:xls

196

登录

网页 图片 视频 学术 词典 地图 更多

约 107 个结果 时间不限 自适应缩放

qzhospital.com

https://www.qzhospital.com/UploadFile/file/20210629/... 网页视图

DL:SI 衢州市人民医院

网页 2021年5月11日 · 浙江省医保诊疗编码库变更 (20210701执行) 浙江省医保诊疗编码库变更 (20210630执行) 序号 项目编码 项目名称 项目内涵 收费项目等级 备注 国家医疗服务 ...

qzhospital.com

https://www.qzhospital.com/UploadFile/file/20210629/... 网页视图

DL:SI 衢州市人民医院

网页 2021年6月25日 · 浙江省医保药品编码库变更 (20210705执行) 浙江省医保药品编码库变更一览表 序号 医保编码 分类 医保中文名称 备注2 (省版药品限定使用范围) 医保文件剂型

qzhospital.com

https://www.qzhospital.com/UploadFile/file/20210301/... 网页视图

DL:SI 衢州市人民医院

网页 2021年2月23日 · 浙江省医保药品编码库变更 浙江省医保药品编码库变更一览表 序号 医保编码 分类 医保中文名称 英文名称 医保文件剂型 ...

qzhospital.com

https://www.qzhospital.com/UploadFile/file/20210425/... 网页视图

DL:SI 衢州市人民医院

网页 2021年4月25日 · 药品目录详情 序号 医保编码 分类 医保中文名称 英文名称 医保文件剂型 备注 招标药品号 招标药品通用名 商品名 剂型 规格 ...

qzhospital.com

https://www.qzhospital.com/UploadFile/file/20220223/... 网页视图

DL:SI 衢州市人民医院

NMAP

```
C:\Windows\system32\cmd.exe

C:\Users\user>nmap -A -T4 -sT -sV 122.227.65.178
Starting Nmap 7.92 ( https://nmap.org ) at 2023-08-29 19:41 ?D1ú±ê×?ê±??
Nmap scan report for 122.227.65.178
Host is up (0.0023s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Microsoft ftpd
25/tcp    open  smtp?
|_smtp_commands: Couldn't establish connection on port 25
80/tcp    open  http     nginx
110/tcp   open  pop3?
|_ssl_date: ERROR: Script execution failed (use -d to debug)
|_ssl_cert: ERROR: Script execution failed (use -d to debug)
|_tls_nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_tls_alpn: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
443/tcp   open  ssl/http nginx
|_http_title: Welcome to nginx!
|_ssl_cert: Subject: commonName=MEDIWAY SELF KEY/organizationName=MEDIWAY/stateOrProvinceName=Beijing/countryName=CN
Subject Alternative Name: DNS:ih.mediway
Not valid before: 2020-05-29T10:20:45
Not valid after: 2030-05-27T10:20:45
|_ssl_date: TLS randomness does not represent time
tls_alpn:
  h2
  http/1.1
  http/1.0
  http/0.9
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2003
OS CPE: cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows Server 2003 SP2
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   66.00 ms  192.168.115.1
2   3.00 ms  122.227.65.178

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 285.46 seconds

C:\Users\user>
```