

BSidesBOS CTF



Challenge :

Kiddie the Pool (Warmups)

Read the Rules (Warmups)

Baseball (Warmups)

Give Up (Warmups)

Saving The World (Steganography)

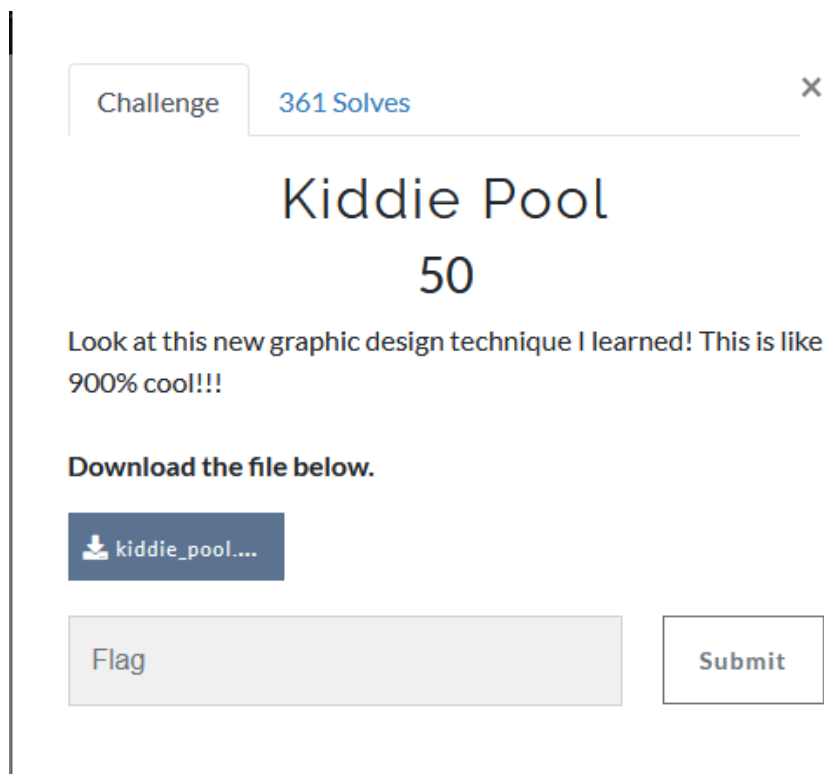
Secret Romance (Steganography)

Creator : MikeD106 (Trio Naga Bonar)

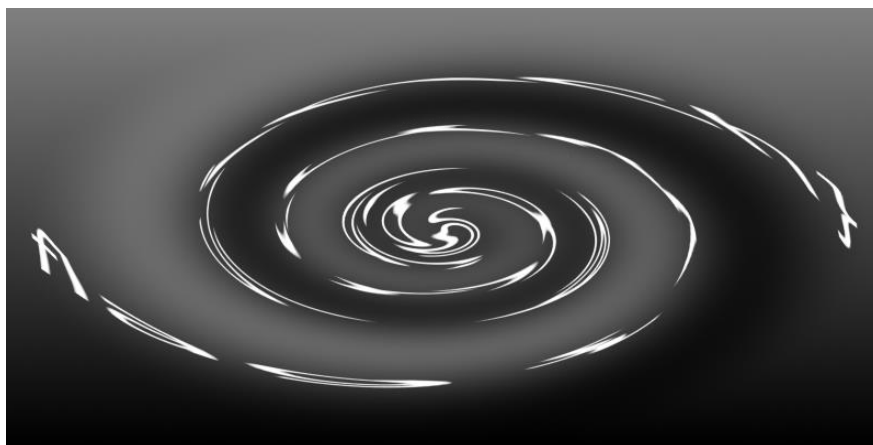
CTF Date : 26 Sept 2020 (09:00 AM EST – 05:00 PM EST)

Kiddie The Pool (Warmups)

Challenge dibuka dengan deskripsi yang berisi seperti berikut :

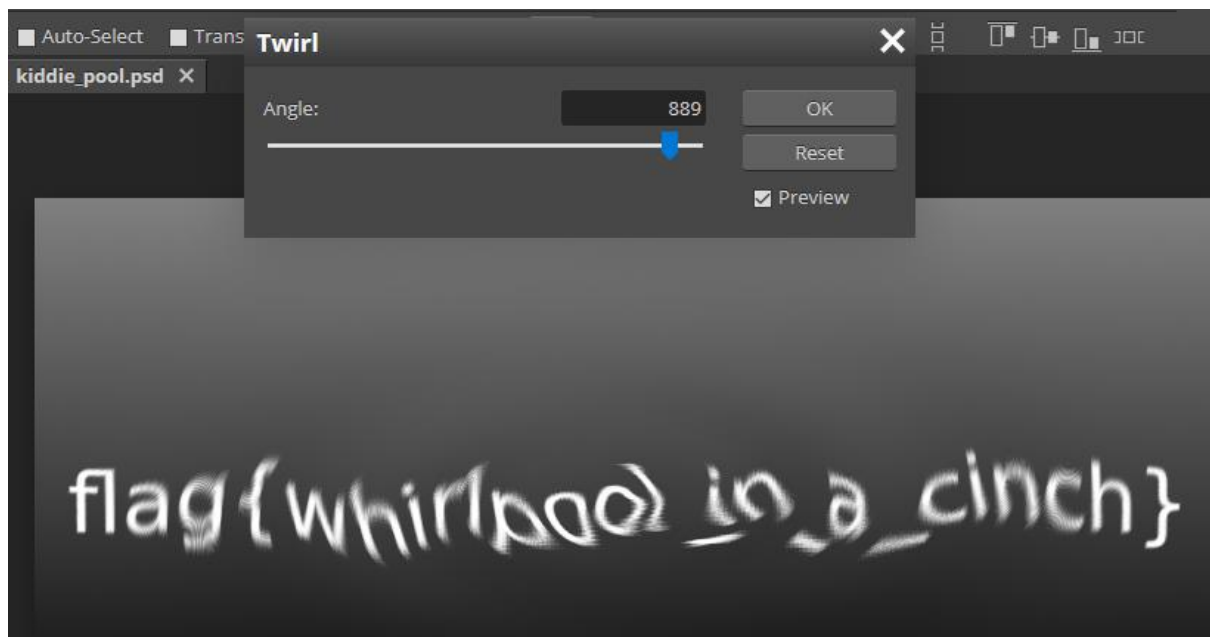


Dari deskripsi yang diberikan, dapat dipastikan bahwa challenge ini berhubungan dengan suatu **effect** pada **teknik design**. Dan dari file image yang di download kita dapat melihat bahwa file tersebut berisikan flag namun diatur dengan suatu effect sehingga sulit dilihat.



setelah mencari mengenai nama effect yang digunakan pada foto tersebut, akhirnya saya mendapatkan bahwa effect tersebut bernama **Twirl**. Saatnya melakukan reverse image effect namun karna saya tidak mempunyai Photoshop sehingga saya menggunakan <https://www.photopea.com/>

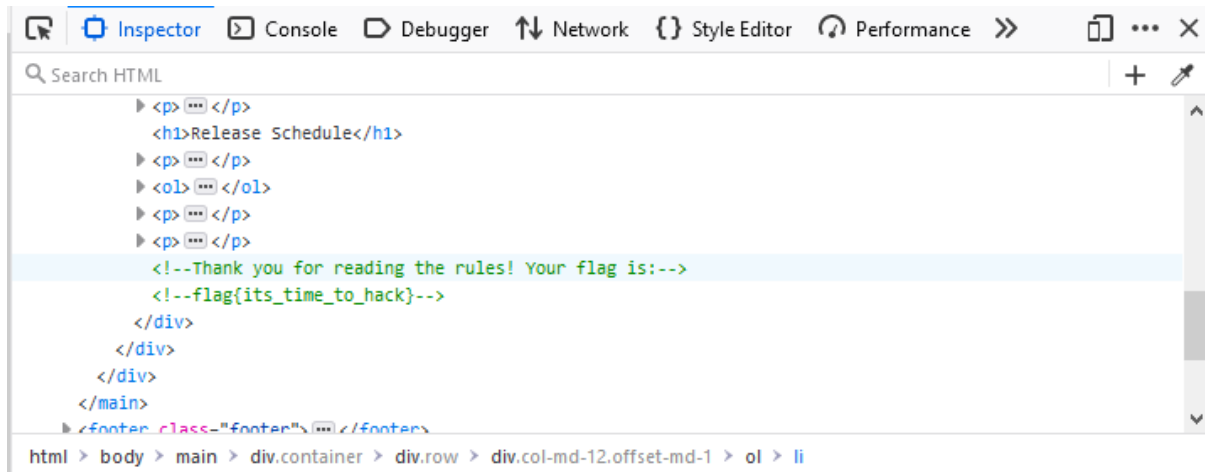
dari hasil reverse editing, saya mendapatkan flagnya



`flag{whirlpool_in_a_cinch}`

Read the Rules (Warmups)

Dari deskripsi yang diberikan, kita diarahkan untuk mengikuti aturan CTF yang berlaku di link : <https://bsidesbos.ctf.games/rules> , setelah membaca hingga selesai saya tidak melihat sesuatu yang mencurigakan sehingga saya berpikir ini merupakan warmups web simple, karna itu saya menggunakan inspect element



flag{its_time_to_hack}

Baseball (Warmups)

Pertama kita perlu mendownload file yang disediakan bernama baseball, saatnya mengecek isi tersebut menggunakan command “**cat**”

```
root@opacite:~/Downloads# ls -l
total 28
-rwxr-xr-x  1 root root 8480 Aug 31 23:38 all_enabled
-rw-r--r--  1 root root  172 Sep 28 03:18 baseball
drwxr-xr-x 19 root root 4096 Sep 19 11:29 HTB
drwx----- 2 root root 4096 Jun 19 01:20 php-reverse-shell-master
drwx----- 2 root root 4096 Sep  2 22:09 Web-Shells-master
root@opacite:~/Downloads# cat baseball
TzRaVUNVMlRNRTRIQTZMSFBGwkdTNVpTSzVZVU1ZSlllQk5ER00zREdKtkhBVTJWSkJHVkNWMllPRlVF
SzMyRE9GTUVNMkNaR0Y1RU1VUlpNUlNHS1JSWE9CQ1VVU1pZSk4ySEFWVFPVTJGQzJDV000WlUyUVNH
SlpBVFNNUT0=root@opacite:~/Downloads#
```

Dari **hasil** command “**cat**” tersebut saya mendapatkan string mencurigakan

Kemudian saya mencoba mengecek strings tersebut menggunakan enkripsi apa

Recipe

Magic

Depth 3

Intensive mode

Extensive language support

Crib (known plaintext string or regex)

Input

length: 171
lines: 1

TzRaVUNVMlRNRTRIQTZMSFBGwkdTNVpTSzVZVU1ZSlllQk5ER00zREdKtkhBVTJWSkJHVkNWMllPRlVFSzMyRE9GTUVNMkNaR0Y1RU1VUlpNUlNHS1JSWE9CQ1VVU1pZSk4ySEFWVFPVTJGQzJDV000WlUyUVNHSlpBVFNNUT0

Output

time: 182ms
length: 48472
lines: 1802

| Recipe (click to load) | Result snippet | Properties |
|---|---|---|
| From_Base64('A-Za-z0-9-_', true) From_Base32('A-Z2-7=', false) | w3ASSa8pygyriw2WqFa88 Z33c2ZpSUHMQWxqhEoCqX FhY1zFR9ddeF7pEJK8Ktp Vtu4QhVg3MBFNA92 | Matching ops: From Base58, From Base64 Valid UTF8 Entropy: 5.21 |

Sehingga dari hasil tersebut saya mengetahui bahwa strings tersebut dari base64, kemudian ke base 32 dan terakhir ke base 58, hal ini saya coba berulang kali karna saya mengalami kendala dari dekripsi **base64** ke base selanjutnya sehingga mendapat titik terang bahwa **base32** adalah langkah tersebutnya.

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

From Base32

Alphabet
A-Z2-7=





☒ Remove non-alphabet chars

From Base58

TzRaVUNVMlRNRTRIQTZMSFBGwkdTNVpTSzVZVU1ZS1lIQk5ER00zREdKThBVTJWSkJHVk
NWM1lPRlVFSzMyRE9GTUVNMkNaR0Y1RU1VUlpNUlNHS1JSWE9CQ1VVU1pZSk4ySEFWFVP
VTJGQzJDV000WlUyUVNHS1pBVFNNUT0

Output

start: 58time: 14ms
end: 58length: 58
length: 0lines: 1



flag{wow_you_hit_a_homerun_and_really_ran_the_bases_there}

Fflag{wow_you_hit_a_homerun_and_really_ran_the_bases_there}

Give Up (Warmups)

Setelah menyalakan deployment pada challenge, saya mendapatkan akses ke dalam terminal challenge tersebut menggunakan command “**nc challenge.ctf.games 30786**”

```
root@opacite:~# nc challenge.ctf.games 30786
bash-4.4$ whoami
whoami
challenge
bash-4.4$ ls
ls
bash-4.4$ sudo
sudo
bash: sudo: command not found
bash-4.4$ su
su
su: must be suid to work properly
bash-4.4$
```

Setelah mencoba mencari tahu apa yang bisa dilakukan pada **terminal** tersebut, hingga akhirnya mengingat **hint** pada challenge tersebut adalah **give up**, dan setelah berdiskusi dengan salah satu tim yang menyelesaikan, akhirnya saya diberi tahu bahwa dengan menggunakan command “**quit**” kita akan mendapatkan sesuatu.

```
exit
33382411476037802382487869381078673500164899220134037398127867687822547421171603
31044416747901
root@opacite:~#
```

```
root@opacite:~# python3
Python 3.8.5 (default, Aug 2 2020, 15:09:07)
[GCC 10.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> from Crypto.Util.number import long_to_bytes as lb
>>> lb(3338241147603780238248786938107867350016489922013403739812786768782254742
117160331044416747901)
b'flag{sometimes_it_is_best_to_step_away}'
>>>
```

Dan saya mendapatkan flag dari challenge ini

flag{sometimes_it_is_best_to_step_away}

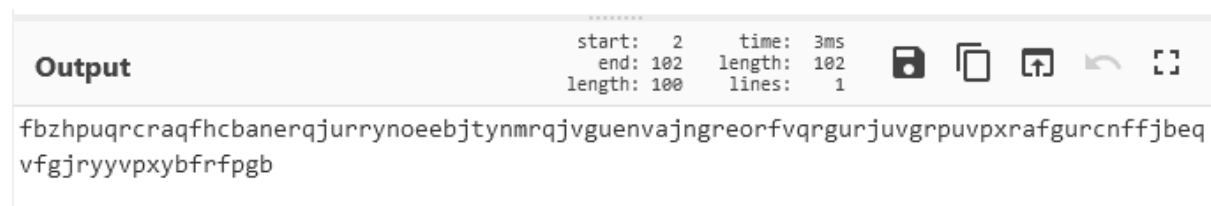
Saving The World (Steganography)

Dari deskripsi challenge yang diberikan, saya diberikan **file image** yang dapat didownload



Dari image di atas, terdapat angka yang mencurigakan setelah diteliti lebih lanjut, angka tersebut memiliki angka tertinggi yaitu **26** sehingga ada kemungkinan ini adalah **A1Z26 encoding** sehingga ketika didecrypt kita dapat menemukan suatu string

6 2 26 8 16 21 17 18 3 18 1 17 6 8 3 2 1 14 5 18 17 10 21 18 18 25 14 15 5 5 2 10 20 25 14 13
18 17 10 22 7 21 5 14 22 1 10 14 7 18 5 15 18 6 22 17 18 7 21 18 10 21 22 7 18 16 21 22 16 24
18 1 6 7 21 18 3 14 6 6 10 2 5 17 22 6 7 10 18 25 25 22 16 24 25 2 6 18 6 16 7 2



Setelah berpikir sekian lama, akhirnya saya mencoba melakukan **dekripsi vigenere** dari :
<https://www.dcode.fr/vigenere-cipher>

VIGENERE DECODER

★ VIGENERE CIPHERTEXT

fbzhpuurcraafhcbanerqjurrvnoeehitvnmraivquenvaingreorfvargu
rjuvgrpuvpxrafgurcnffibegvfqirvvyvpxybfrrfpgb

PARAMETERS

★ PLAINTEXT LANGUAGE

★ ALPHABET

AUTOMATIC DECRYPTION

Dan mendapatkan hasilnya di mana string tersebut merupakan **vigenere** dengan **key "NN"**

| ↑↓ | ↑↓ |
|----|--|
| | somuchdependsuponaredwheelabrowglazed |
| NN | withrainwaterbesidethewhitechickensthe |
| | passwordistwellicklosescto |


Daari hasil dekripsi, kita dapat melihat string password yang berupa **"twellicklosescto"**, awalnya saya tidak tahu password tersebut digunakan di mana, sehingga mencoba satu satu hingga akhirnya menggunakan **Steghide**

```
root@kali:~/Downloads/CTF/savingtheworld# steghide extract -sf menu.jpg -p twellicklosescto
wrote extracted data to "flag.txt".
root@kali:~/Downloads/CTF/savingtheworld# cat flag.txt
flag{take_care_of_whiterose}
root@kali:~/Downloads/CTF/savingtheworld#
```

flag{take_care_of_whiterose}

Secret Romance (Steganography)

Challenge ini diawali dengan mendownload **file zip**, dan dalam file tersebut terdapat 2 file lagi yaitu **1 file txt**, **1 file zip** bernama **message.zip**, mari kita cek 1 file txt nya bernama note.txt

 note.txt - Notepad

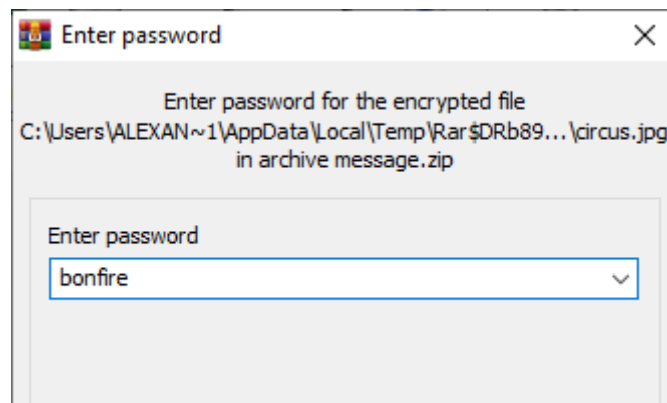
File Edit Format View Help

You will find the key at the center of Le Cirque des Rêves.

Dengan mencari kata “Le Cirque des Rêves” saya mendapatkan bahwa itu merupakan buku [Erin Morgenstern](#) berjudul **Night Circus**, dan mencari dari wikipedia saya mencoba mencari kata kunci “**center**” namun tidak menemukannya, dan ketika saya mencoba mencari **sinonim** dari “**center**” saya melihat ada kata “**central**” dan kata “**bonfire**”

circus via a magical link to the central bonfire,

Dan saatnya mencoba memasukkan kata “bonfire” ke message.zip dulu



Dari hasil zip folder tersebut, terdapat **2 file**, **1 file txt** dan **1 file jpg**, dari file txt tersebut kita dapat melihat suatu pesan yang ditulis oleh penulis buku tersebut, erinmorgenstern

Dan karna hanya memiliki clue dari file gambar tersebut, jadi saya mencoba untuk mencari metadata dari gambar tersebut menggunakan command “**Steghide**”

```
root@opacite: ~
root@opacite:~# steghide extract circus.jpg
steghide: unknown argument "circus.jpg".
steghide: type "steghide --help" for help.
root@opacite:~# steghide extract -sf circus.jpg
Enter passphrase:
wrote extracted data to "flag.txt".
root@opacite:~# ls
BsidesCTF  dirsearch  ez_rev      handshakes  Pictures  Tools
circus.jpg Documents  flag.txt    lscript     scapy     VPN
Desktop    Downloads  ghidra_scripts Music        ShScript  wordlists
root@opacite:~# cat flag.txt
flag{the_night_circus}
root@opacite:~#
```

flag{the_night_circus}

Steganography

| | | | |
|--|--|---------------------------------------|--|
| <div>Saving the World ✓</div> <div>445</div> | <div>Secret Romance ✓</div> <div>489</div> | <div>Dimension 0</div> <div>500</div> | <div>Surprise Party</div> <div>500</div> |
|--|--|---------------------------------------|--|

Warmups

| | | | |
|---------------------------------------|---|---|-------------------------------------|
| <div>EZ Bake Oven</div> <div>50</div> | <div>Kiddie Pool ✓</div> <div>50</div> | <div>Read The Rules ✓</div> <div>50</div> | <div>Baseball ✓</div> <div>50</div> |
| <div>Y2K</div> <div>300</div> | <div>Play The Harp</div> <div>472</div> | <div>Where's The Body?</div> <div>492</div> | <div>Give Up ✓</div> <div>496</div> |