**BSidesBOS CTF**



**Challenge :**

**Kiddie the Pool (Warmups)**

**Read the Rules (Warmups)**

**Baseball (Warmups)**

**Give Up (Warmups)**

**Saving The World (Steganography)**

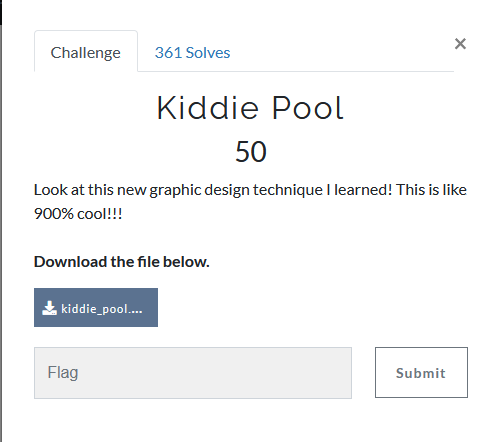
**Secret Romance (Steganography)**

**Creator : MikeD106 (Trio Naga Bonar)**

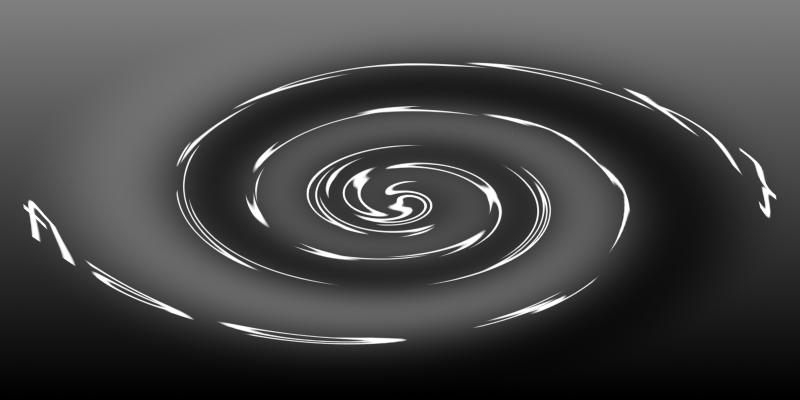
**CTF Date : 26 Sept 2020 (09:00 AM EST – 05:00 PM EST)**

**Kiddie The Pool (Warmups)**

Challenge dibuka dengan deskripsi yang berisi seperti berikut :

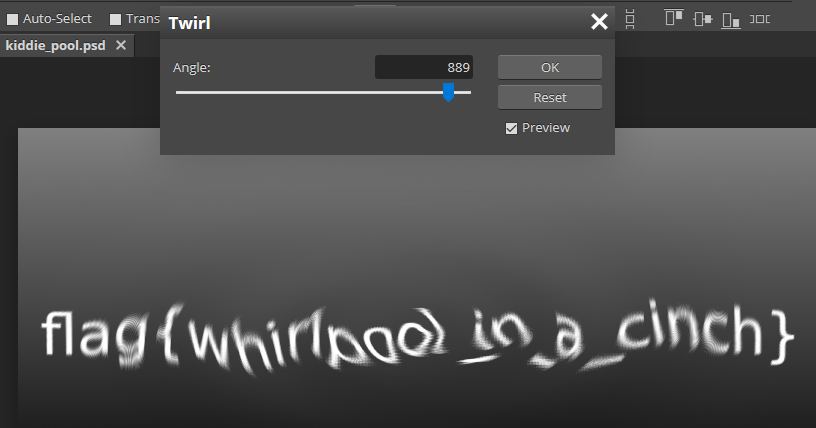


Dari deskripsi yang diberikan, dapat dipastikan bahwa challenge ini berhubungan dengan suatu **effect** pada **teknik design**. Dan dari file image yang di download kita dapat melihat bahwa file tersebut berisikan flag namun diatur dengan suatu effect sehingga sulit dilihat.



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/>

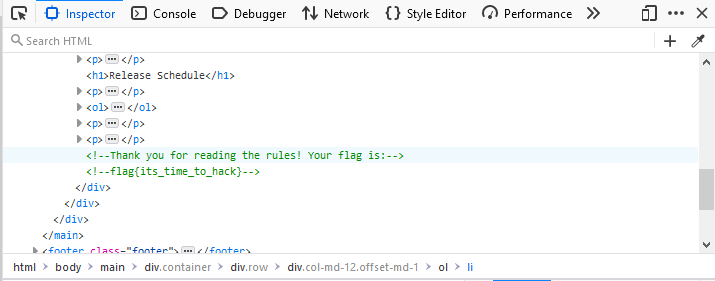
dari hasil reverse editing, saya mendapatkan flagnya



**flag{whirlpool\_in\_a\_cinch}**

**Read the Rules (Warmups)**

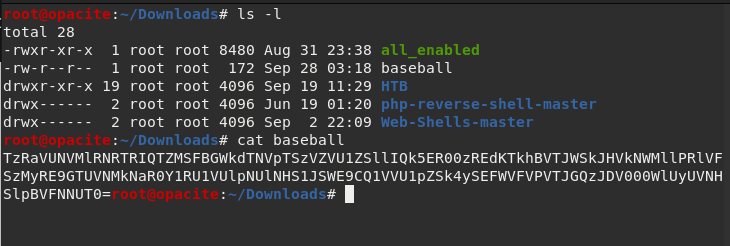
Dari deskripsi yang diberikan, kita diarahkan untuk mengikuti aturan CTF yang berlaku di link : <https://bsidesbos.ctf.games/rules> , setelah membaca hingga selesai saya tidak melihat sesuatu yang mencurigakan sehingga saya berpikir ini merupakan warmups web simple, karna itu saya menggunakan inspect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



**flag{its\_time\_to\_hack}**

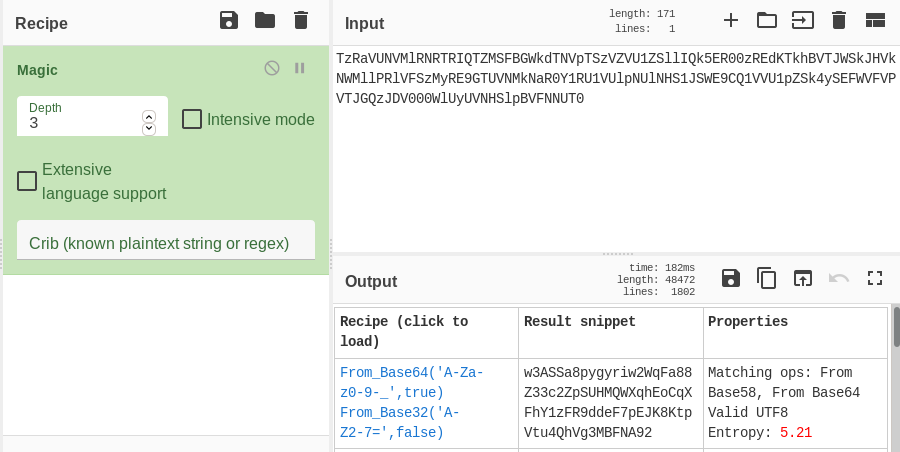
**Baseball (Warmups)**

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

****

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

Kemudian saya mencoba mengecek strings tersebut menggunakan enkripsi apa

****

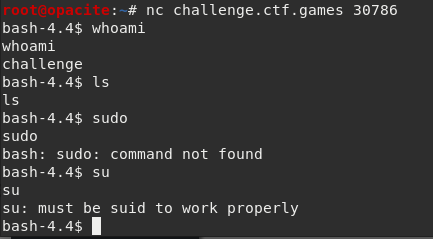
Sehingga dari hasil tersebut saya mengetahui bahwa strings tersebut dari base64, kemudian ke base 32 dan terakhir ke base 58, hal ini saya coba berulang kali karna saya mengalami kendala dari dekripsi **base64** ke base selanjutnya sehingga mendapat titik terang bahwa **base32** adalah langkah tersebutnya.

****

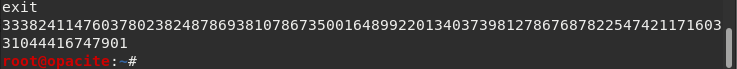
**Fflag{wow\_you\_hit\_a\_homerun\_and\_really\_ran\_the\_bases\_there}**

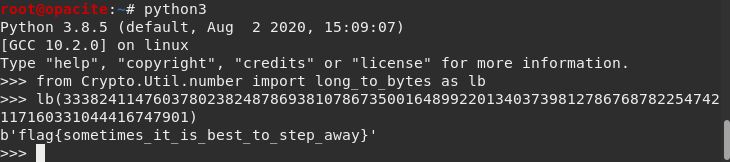
**Give Up (Warmups)**

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

****

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.

****

****

Dan saya mendapatkan flag dari challenge ini

**flag{sometimes\_it\_is\_best\_to\_step\_away}**

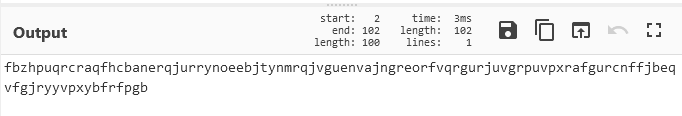
**Saving The World (Steganography)**

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

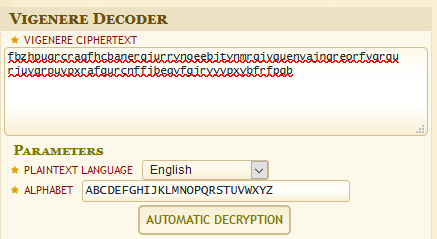


Dari image di atas, terdapat angka yang mencurigakan setelah diteliti lebih lanjut, angka tersebut memiliki angka tertinggi yaitu **26** sehingga ada kemungkinan ini adalah **A1Z26** **enconding** sehingga ketika didecrypt kita dapat menemukan suatu string

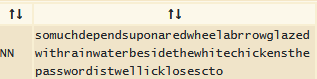
6 2 26 8 16 21 17 18 3 18 1 17 6 8 3 2 1 14 5 18 17 10 21 18 18 25 14 15 5 5 2 10 20 25 14 13 18 17 10 22 7 21 5 14 22 1 10 14 7 18 5 15 18 6 22 17 18 7 21 18 10 21 22 7 18 16 21 22 16 24 18 1 6 7 21 18 3 14 6 6 10 2 5 17 22 6 7 10 18 25 25 22 16 24 25 2 6 18 6 16 7 2



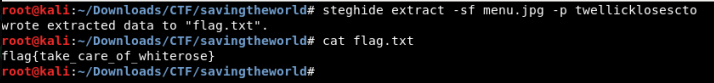
Setelah berpikir sekian lama, akhirnya saya mecoba melakukan **dekripsi vigenere** dari : <https://www.dcode.fr/vigenere-cipher>



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



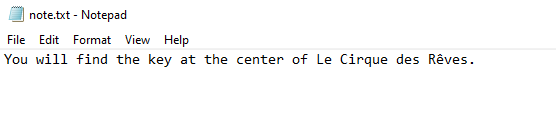
Daari hasil dekripsi, kita dapat melihat string password yang berupa “**twellicklosescto**”, awalnya saya tidak tahu password tersebut digunakan di mana, sehingga mencoba satu satu hingga akhirnya menggunakan **Steghide**



**flag{take\_care\_of\_whiterose}**

**Secret Romance (Steganography)**

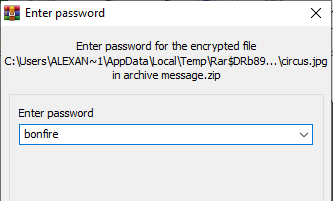
Challenge ini diawali dengan mendownload **file zip**, dan dalam file tersebut terdapat 2 file lagi yaitu **1 file txt, 1 file zip** bernama **message.zip**, mari kita cek 1 file txt nya bernama note.txt



Dengan mencari kata “Le Cirque des Rêves” saya mendapatkan bahwa itu merupakan buku [Erin Morgenstern](https://en.wikipedia.org/wiki/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**”

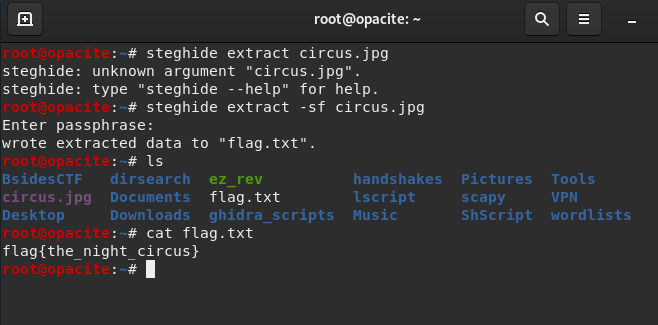


Dan saatnya mencoba memasukkan kata “bonfire” ke message.zip dulu

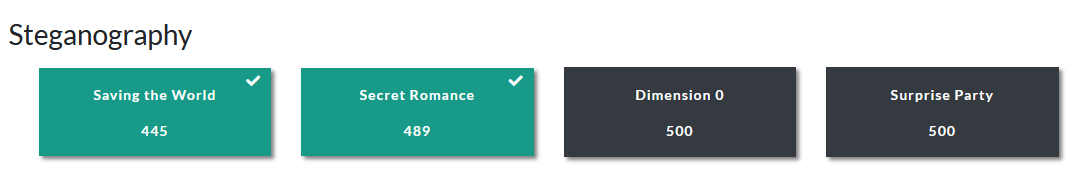


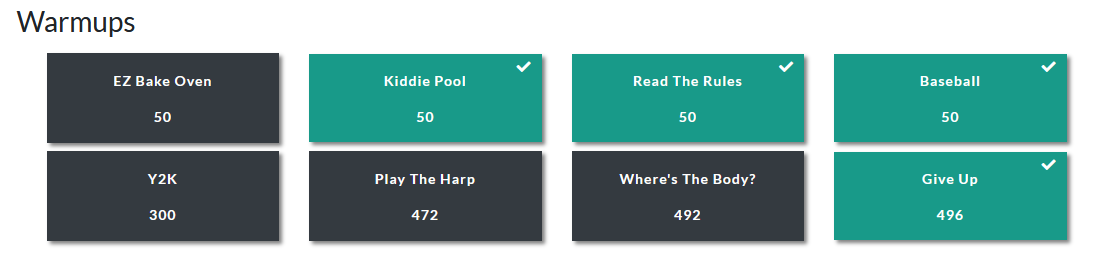
Dari hasil zip folder tersebut, terdapat **2 file, 1 file txt** dan **1 file jpg**, dari file txt tersebut kita dapat melihat suatu pesan yang ditulis oleh penulis buku tersebut, erinmorgenstern

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



**flag{the\_night\_circus}**

****

****