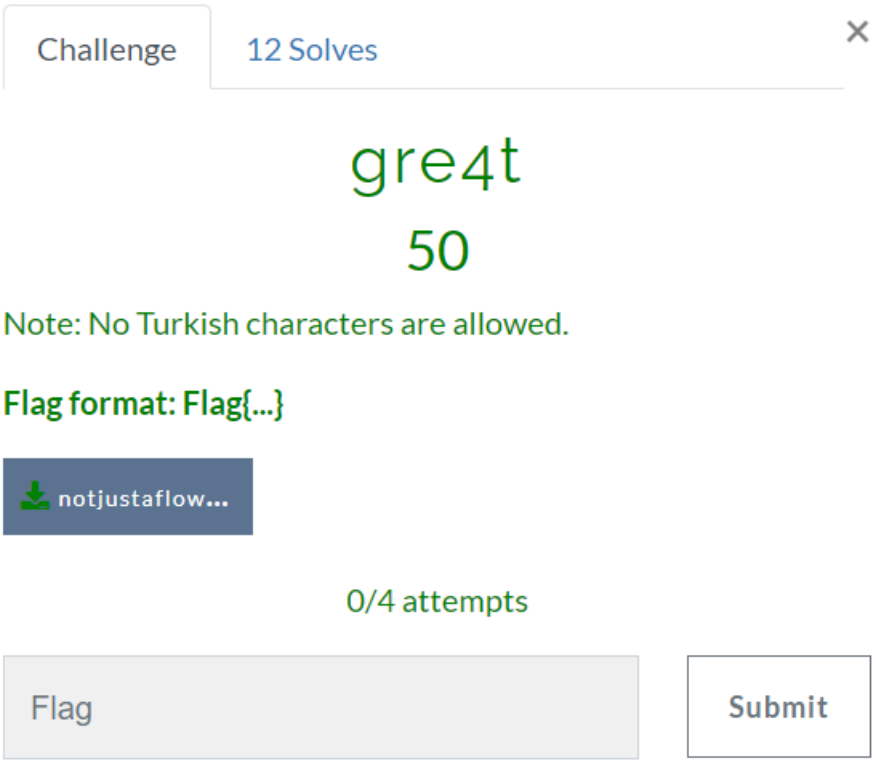
Merhabalar öncelikler kısa soluklu fakat eğlenceli ve bir o kadar da sınayıcı bir CTF olan Battleware yarışmasının ikinci haftasını da geri bırakarak ve çıkan sorulardan OSINT kategorisindeki ilk sorusu olan "**gre4t**" çözümünü paylaşmak isterim sizinle.

OSINT



Bize verilen .png dosyamızı inceliyoruz.

“notjustaflower”

Resim dosyasını indirip, incelemek isterseniz :
https://mega.nz/file/tuJ3jS5T#RFm3rvGs7RXLoIjsLMP4Nx_wYFqPN_dZpY5SUDennNI

Öncelikle resim dosyasının metadatalarına bakarak incelemek için “**Exiftool**” aracıyla resim dosyasının metadatalarını inceliyoruz.

```
File  Actions  Edit  View  Help
kali@kali:~/Desktop$ exif notjustaflower_.jpg
EXIF tags in 'notjustaflower_.jpg' ('Motorola' byte order):
--------------------+------------------------------------------------------
Tag                 |Value
--------------------+------------------------------------------------------
Resolution Unit     |Inch
YCbCr Positioning   |Centered
Copyright           |@1mfl0w3r (Photographer) - [None] (Editor)
X-Resolution        |72
Y-Resolution        |72
Exif Version        |Exif Version 2.1
FlashPixVersion     |FlashPix Version 1.0
Color Space         |Internal error (unknown value 65535)
--------------------+------------------------------------------------------
kali@kali:~/Desktop$
```

Telif hakkı (Copyright) kısmında görüleceği üzere dikkatimizi çeken bir kullanıcı adı buluyoruz.

Nickname: @1mfl0w3r

Bu kullanıcı adıyla açılmış bazı sosyal medya hesaplarının olma olasılığı üzerine araştırmaya başlıyoruz.

“https://www.instagram.com/@1mfl0w3r“

“https://twitter.com/1mfl0w3r”

“https://www.facebook.com/1mfl0w3r”

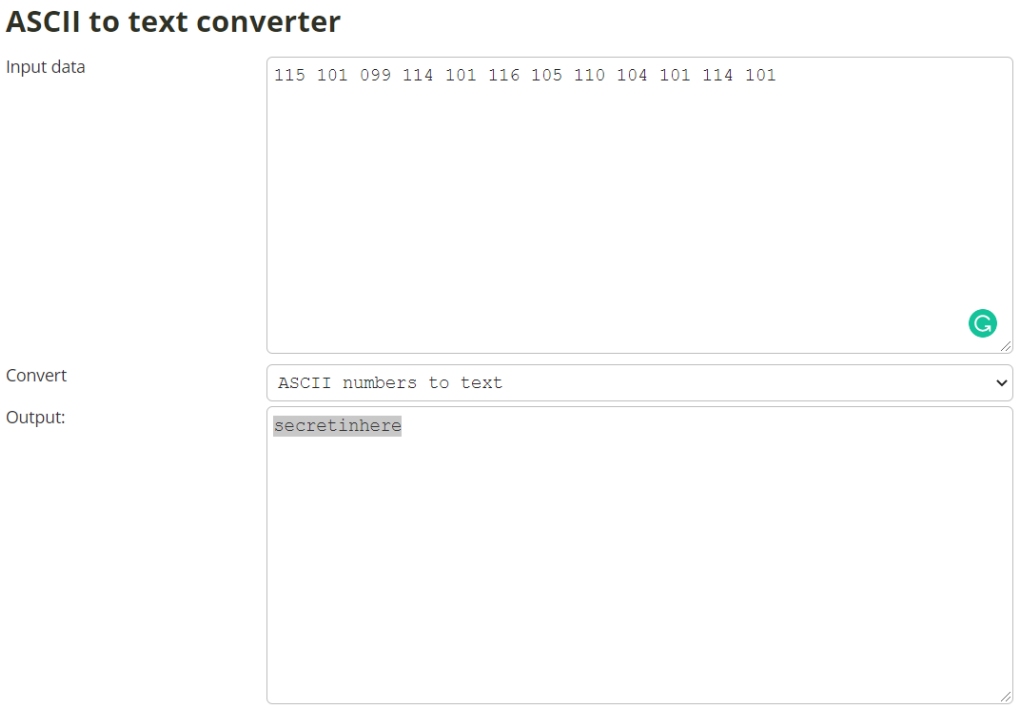
Yukarıdaki gibi örneklerle sosyal medya üzerinden resmin paylaşıldığı platformun “Twitter” olduğunu buluyoruz. Twitter’da aynı kullanıcı adı ve resimle oluşturulmuş bir hesap olduğunu görüyoruz.

Kullanıcının tweetlerini incelediğimizde ise bizim için oluşturulmuş birkaç ipucu olabileceğini görebiliyoruz.

Son tweetine dikkat edersek bize ASCII ile kodlanmış bir tweet attığını görüyoruz. İkinci tweetinde ise *"did hacker created a repository?"* diye bir soru ile karşılaşıyoruz. Bize bilgisayar korsanının bir depo oluşturduğu hakkında bir bilgi vererek aklımıza hemen GitHub üzerinden repository oluşturmuş olma ihtimalini getiriyor. Fakat fazla bilgi vermediği için ASCII ile kodlanmış yazıyı deşifre ederek devam ediyoruz.

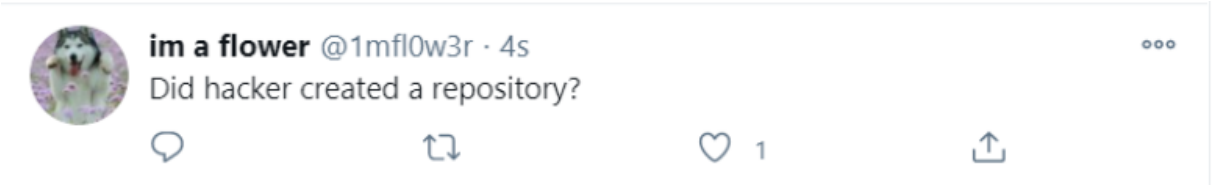
Tweet : 115 101 099 114 101 116 105 110 104 101 114 101

Şifrelenmiş yazıyı deşifre etmek için http://www.unit-conversion.info/texttools/ascii/ sitesinden yardım alıyoruz.

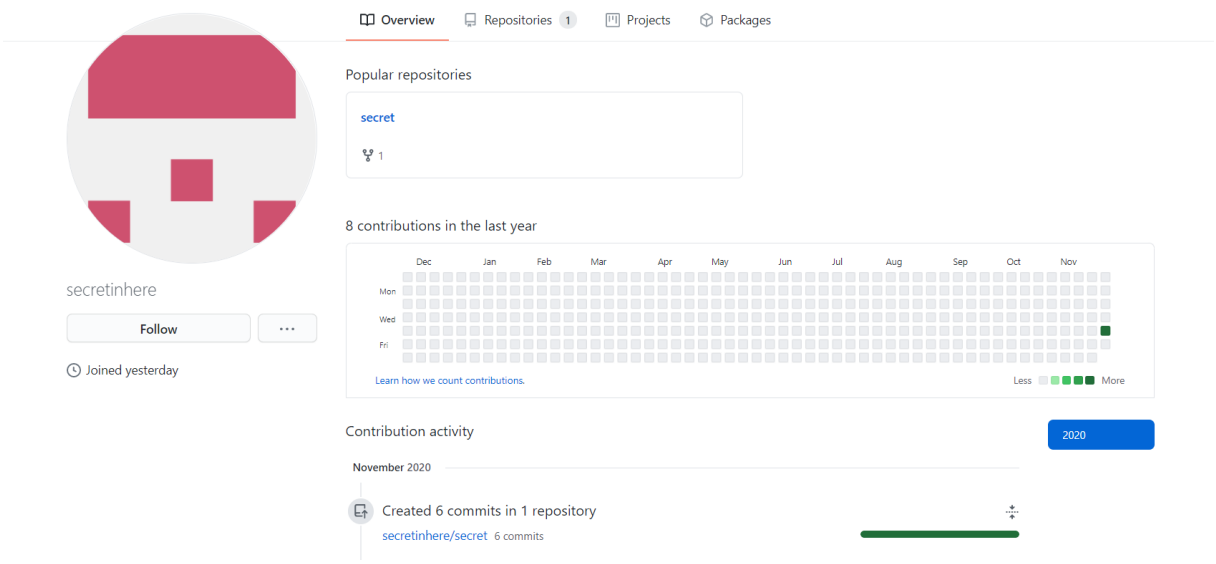


Deşire edilen metin : secretinhere

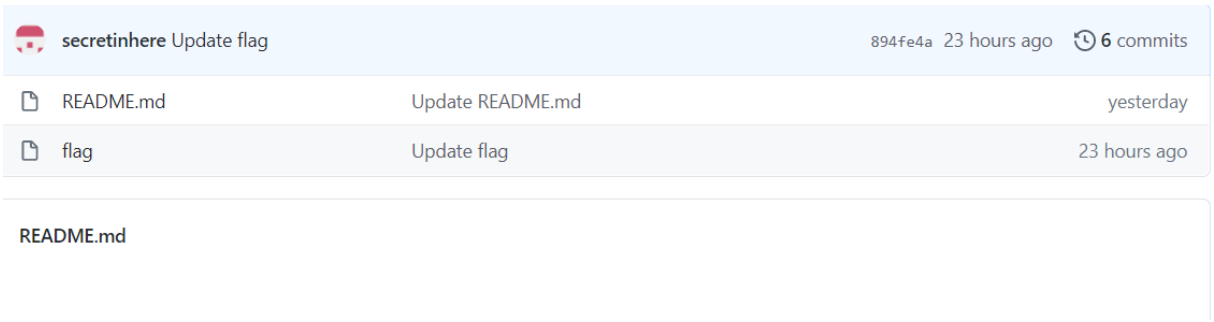
Deşifre edilen metin bize ikinci tweette verilen ipucunu tekrar hatırlatıyor.



Deşifre edilen metnin bir kullanıcı adına uygun olabileceğini düşündürüyor ve tweette bize verdiği ipucu bize GitHub üzerinde böyle bir kullanıcı olduğunu düşüyor. Ve tam da düşündüğümüz gibi "https://github.com/secretinhere/" adresi bizi kullanıcıya yani tweette bahsedilen bilgisayar korsanına ulaştırıyor.



Kullanıcının oluşturduğu repsitory'i incelediğimizde ise karşımıza *"secret"* isimli bir repository'nin mevcut olduğunu görüyoruz.



Flag'in bulunduğu dizine giderek flag'in içeriğini okuyabiliyoruz.

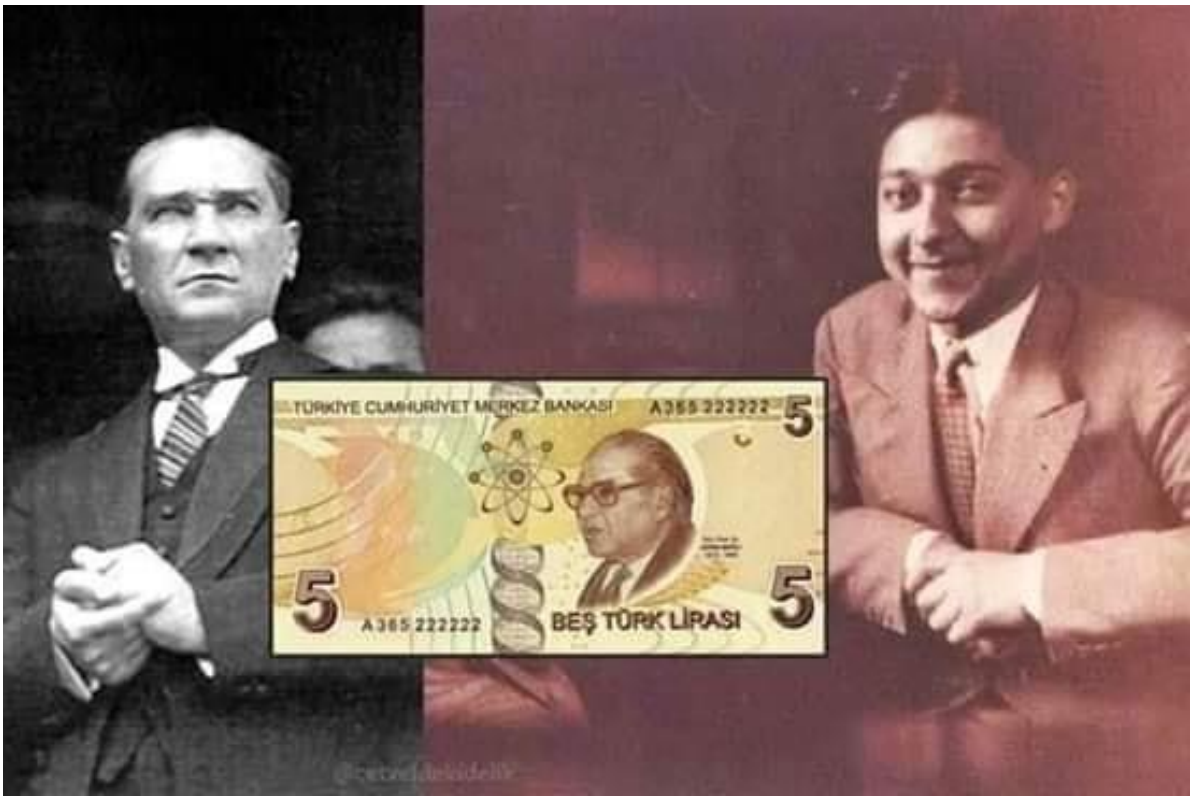
Flag'in içeriğine ulaşmak için: https://github.com/secretinhere/secret/blob/main/flag

```
3 lines (3 sloc)  212 Bytes
1  format of flag = Flag{NameSurname}
2  do not use spaces and Turkish characters
3  Who was the first person that Mustafa Kemal Ataturk sent abroad for education and received the first PhD in the field of world science?
```

Bize flag'i nasıl bulacağımızı ve flag formatının nasıl olduğundan bahsediyor.

Flag için çözmemiz gereken soru : Who was the first person that Mustafa Kemal Ataturk sent abroad for education and received the first PhD in the field of world science?

Soruda Atatürk'ün yurt dışına doktora eğitimi için yolladığı ilk öğrencinin kim olduğunu soruyordu ve biz de araştırarak Aydın Sayılı'nın kim olduğunu öğrenmiş olduk 😊



Türkçe karakter içermediği için flag'imiz;

Flag : **Flag{AydinSayili}**

Okuduğunuz için Teşekkürler 😊