

24 NİSAN 2024



RACONF'24
CTF ÇÖZÜMÜ

Mehmet MERMER
www.turksiberbirligi.com

RaConf'24 Capture The Flag WriteUp

Herkese merhabalar sizlere bu yazıda 18,19,20 Nisan 2024 tarihinde düzenlenen RaConf'24 isimli siber güvenlik zirvesinde icra edilen ve benim en kısa sürede doğru cevapları vererek birincilikle tamamlamış olduđum CTF yarışmasındaki deneyimlerimden bahsederek kendi bakış açımdan çözüm aşamalarını anlatacađım. Keyifli okumalar dilerim.

Yarışmanın başlaması ile birlikte bize bir drive linki ile gönderilen **"RACONF.zip"** dosyasının yer aldığını görüyoruz. Zip dosyasının parola korumalı olmasından dolayı github içerisinde yer alan ve benim tercihim olan **"python-zip-cracker"** aracını kullanarak **"RACONF.zip"** dosyasına **"rockyou.txt"** wordlistini de vererek kaba kuvvet(bruteforce) saldırısı gerçekleştirmeyi deneyeceğiz.

```
[main] {} python-zip-cracker python3 script.py  
[0] Word List Path: /usr/share/wordlists/rockyou.txt
```

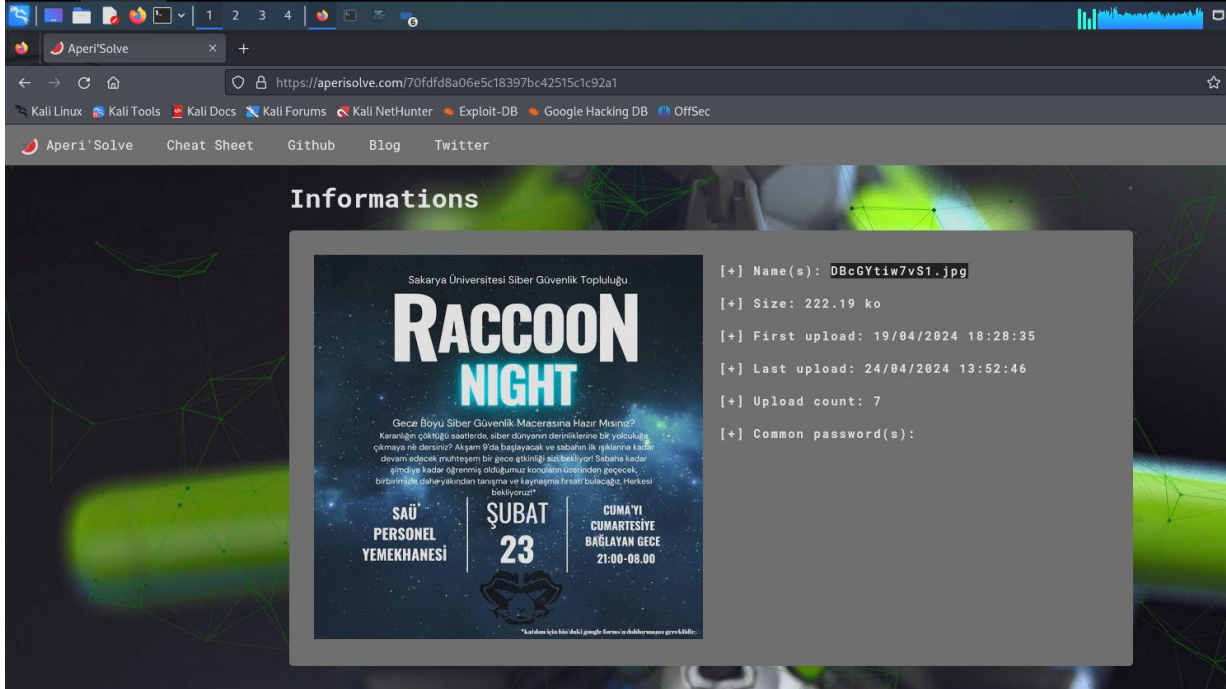
```
83% | 11875061/14344392 [40:15<06:09, 6686.40word/s]  
[+] Password found: 76password92root
```

Yapılan kaba kuvvet saldırısı sonucunda zip dosyasının parolasını **"76password92root"** olduğunu öğreniyoruz. Dosyanın içeriğini **"extract"** ettiğimizde 15 adet resim dosyası ve 1 adet ".txt" uzantılı dosya olduğunu görüyoruz. İlk olarak **"README.txt"** dosyasını okuyalım.

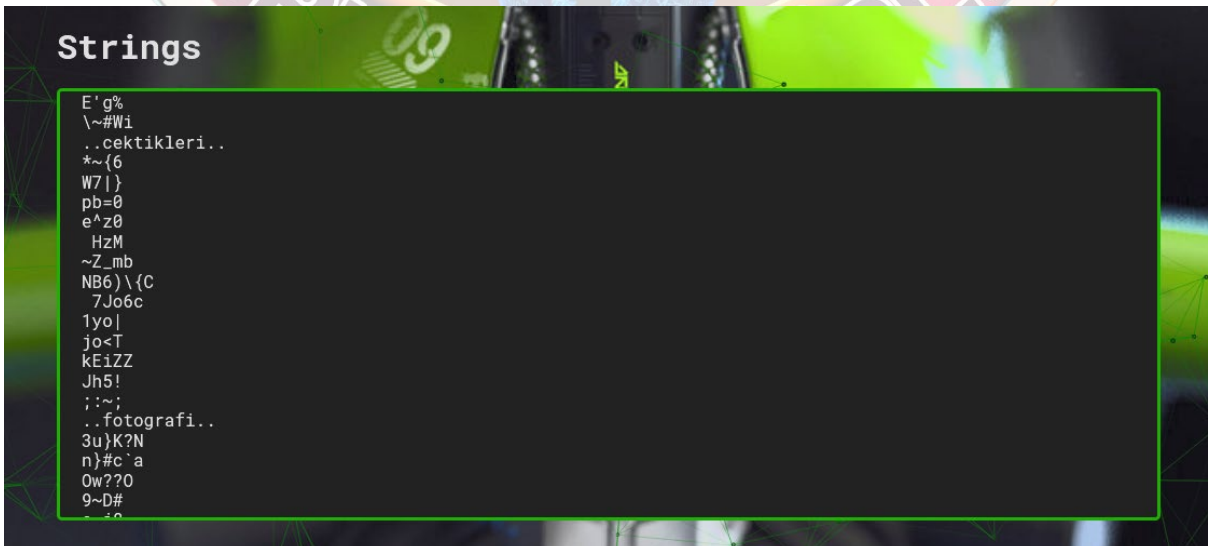
```
~/mermer/RACONF/RACONF/README.txt - Mousepad  
File Edit Search View Document Help  
1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11 Rakunların kalbinde, yılın en büyüğü günü yaklaşırken, bir heyecan fırtınası esiyordu. 25 Ekim, sadece yaprakların dans ettiđi bir sonbahar günü değil, aynı zamanda sakinlerinin kaderlerini değiştirecek olan  
Gölge Festivali için bir araya geldikleri gündü.  
12  
13 Bu özel gün, rakunların yeni rakunlara gizemli hediyeler verdiđi ve bu hediyelerle birlikte, birbirlerinin ruhlarını keşfetme yolculuđuna çıktıkları bir gündü. Hediyeler, sadece birer nesne değil, aynı  
zamanda birer anahtardı; alıcının iç dünyasının kapılarını aralayan ve onları daha yakından tanıma fırsatı sunan birer anahtardı.  
14  
15 Festivalin bu yılki teması, 'Birlikte Keşfetmek' idi. Herkes, bir çember oluşturarak, kendileri hakkında bilimemeyen bir şeyi paylaştı. Bu paylaşımlar, her bir rakunun hayatındaki 25 Ekim'in, sadece bir tarih  
olmadığını, aynı zamanda bir dönüm noktası olduğunu gösteriyordu.  
16  
17 Gün boyunca, Rakunlar birbirlerinin yeteneklerini ve hobilerini keşfettiler, birlikte sohbet ettiler ve eğlendiler. Her etkinlik, onların birbirleriyle olan bağlarını güçlendirdi ve yeni arkadaşlıkların  
tohumlarını attı.  
18  
19 Gölge Festivali'nin sonunda, herkes birbirine daha yakın hissetti ve rakun sakinleri, bir sonraki festivali sabırsızlıkla beklemeye başladılar. Çünkü artık biliyorlardı ki, 25 Ekim sadece eğlenceli bir gün  
değil, aynı zamanda birbirlerini daha iyi tanıma ve anlama şansıydı. Bu tarih, Rakunlar için birlik ve dostluđun sembolü haline gelmişti.  
20  
21 Ancak, dikkatli gözlerle bakıldığında, festivalin gölgesinde saklı kalmış izlerin derinliđi fark edilebilirdi. Belki de o gözden kaçırılan detaylar, gerçek hikayenin ötesindeki gerçeđi anlatıyordu. Kim bilir,  
belki de en büyük sırlar, en küçük izlerde saklıydı.  
22
```


Şifrelenmiş metni çözdüğümüzde bize okunabilir halini vermiş oldu, metinde **“Gece etkinliğinden”** bahsediliyor, fotoğraflara bakarken bir çok etkinlik, toplu çekilmiş fotoğraf, afiş vb. gibi konulara ait görseller görmüştük, bunun için gece etkinliğinin gerçekleşmiş olduğu fotoğraf dosyası içerisine bakabiliriz.

Fotoğraf dosyasını daha detaylı incelemek adına adli bilişim analizleri de yapılabilen (farklı renk kombinasyonları ve ışık filtreleri ile resim analizi yapan, gizli metinleri gösteren, strings, zsteg, vb. bilgileri getiren) **“AperiSolve”** adlı online aracından yardım alabiliriz.



Fotoğraf dosyamızı online araca yükledikten sonra verdiği çıktıları tek tek incelemeye başlıyoruz. Dosyanın “strings” verilerine baktığımız zaman karmaşanın içerisinde düzenli kelimeler dikkatimizi çekiyor 😊 Bu anlamlı kelimeleri bir araya getiriyoruz. O yarışma heyecanı içerisinde tek tek okudum 😊



“Strings” kısmında yer alan kelimeler şu bilgiyi veriyordu :

“Rakunlar, **etkinlik sonrası çektikleri fotoğrafı incelemeye başladıklarında, sıradan bir fotoğraftan çok daha fazlası olduğunu fark ettiler. Fotoğrafta detaylıca incelediklerinde, derinlerde gizlenmiş bir mesaj olduğunu sezdiler. Ancak dosyanın içeriğini açmak için bir "anahtar"a ihtiyaçları olduğunu anladılar. İşte bu noktada, bir fikir bulmaya çalıştılar ve birden Rakunların kendi web sitesine gönderme yapabileceğini düşündüler. Belki de anahtar, web sitesinde gizli bir yerdeydi ve onları gizli mesajı bulmaya yönlendirecekti.”**

Bu alanda edindiğimiz bilgiye Rakunlar etkinlik sonrası bir fotoğraf çektiler buna göre **Ekip Fotoğrafı'nın “vCmj7CmRFDX8.jpg”** dosyası olduğunu anlıyoruz.

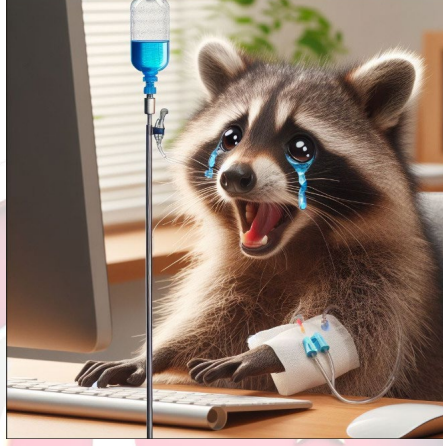


Yukarıdaki ipucuna göre fotoğraf dosyası içeriğinde gizli dosya ve şifre olduğunu öğrendik, bunlara ulaşabilmek için “Stegcracker” ve “Steghide” aracını kullanabiliriz.

“Anahtar” kelimesinden yola çıkarak anahtarı ele geçirmemiz için kaba kuvvet saldırısında bulmamız gerektiğini de anlıyoruz. Ayrıca “**Belki de anahtar, web sitesinde gizli bir yerdeydi ve onları gizli mesajı bulmaya yönlendirecekti**” ifadesinden rakunların websitesi olan raconf.com üzerinde araştırma yapıyoruz. F12 incele yöntemi ile website kaynak kodunda çok karmaşık ve vakit alacağından bir ipucu elde edemiyoruz. Bu sırada Raconf CTF duyuru grubundan “**Rakun resimlerde gezinirken toplu çekilen \$(ekip fotoğrafına) bakarken göz yaşlarını tutamadı. Duygulanmıştı.**”

İçerisinde gizli dosya olan bu resimde şifreyi web sayfasına koymak çok akıllıcaydı. Neyse ki cewl diye bir araç vardı?

Kaynak kodda okumak zor olabilirdi :)" tüyosu geliyor ☺ O ana kadar önde olduğumu düşünüyorum. Sessiz sedasız bu bilgiyi kullanarak hızımı arttırıyorum.



Böylece **“CEWL”** aracını kullanarak web sitesinin kaynak kodunu sözlük saldırısında kullanabileceğim bir wordlist'e dönüştürmek için **“brute.txt”** isimli dosyaya kaydediyorum. (CeWL (Özel Kelime Listesi oluşturucu), belirli bir URL'yi belirli bir derinliğe kadar tarayan ve daha sonra John the Ripper gibi şifre kırıcılar için kullanılacak bir kelime listesi döndüren bir ruby uygulamasıdır. İsteğe bağlı olarak CeWL harici bağlantıları takip edebilir.)

```
{ } RACONF cewl http://raconf.com/ > brute.txt
```

Ardından ekip fotoğrafı dosyasındaki şifreyi çözmek için fotoğraf dosyasının ismini vererek ve oluşturduğum **“brute.txt.”** wordlist'ini kullanarak **“Stegcracker”** aracı ile kaba kuvvet saldırısını gerçekleştiriyoruz.

```
File Actions Edit View Help
stegcracker x steghide x dirfuzz x
{ } RACONF stegcracker vCmj7CmRFDX8.jpg brute.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2024 - Luke Paris (Paradoxis)
RaConf24
StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.
StegSeek can be found at: https://github.com/RickdeJager/stegseek
Counting lines in wordlist..
Attacking file 'vCmj7CmRFDX8.jpg' with wordlist 'brute.txt'..
Successfully cracked file with password: sAaUuSsIiBbEeRrRrAaCcOoNnFf
Tried 1385 passwords
Your file has been written to: vCmj7CmRFDX8.jpg.out
sAaUuSsIiBbEeRrRrAaCcOoNnFf
{ } RACONF s
```

Tebrikler..

...kullanılan sembollerle doluydu ve onlara anlam veremiyorlardı. Artık yorumları artık bunların hepsi sona erecekti.

Tebrikler...

Rakunlar, web sitesinde keşfettikleri şifreli bir mesajla karşılaştılar. Mesajın içeriği, tuhaf sembollerle doluydu ve onlara anlam veremiyorlardı. Artık yorulmuşlardı ama biliyorlardı artık bunların hepsi sona erecekti.

LS4tIC4uLi0gLi0tIC4uLiAuLiAvIC4tLi4gLS4gLi0tIC4tLS4gLS4gLiAvIC4uLS4gLS4uLSAuLS4g
Li0gLi4uLSAuLS4uIC0uLi0gLyAtLi4uIC0uIC0tIC4uIC0uLi4gLS4tLSAuLi4gLS0gLS0uIC0uLi4g
LS0uLiAuLiAvIC0tLSAtLiAuLS0tIC4tLSAuLi0gLi0tIC4uLi4gLyAuLi0uIC4tLS0gLiAuLi4tIC4uLi0
gLi0tLiAuLS0uIC0uIC4uLi4gLi0uIC8gLi0uLi0uIC4tLS4gLi4uLiAtLi0gLi0tLiAuLi4tIC8gLS4tLSA
uLi4uIC0uLSAtLS4gLi0uIC4tLi4tLiAvIC4tIC4tLi4gLS4gLS0gLS4tLSAtLi4uIC4uLSAvIC0uLi4gLS
S0gLiAvIC4uLi0gLi0uLiAuLS4gLi4uLiAuLS4gLyAtLS4tIC0uLi4gLSAtLi0tIC0uLS0gLi0tLSAuLi
4uIC0uLSAtLi4tIC0uIC4tIC4tLS4gLi0uIC4tLi0uLSAvIC0uLiAtLiAuLS0tIC4uLi4gLS4gLyAtLS0g
LS4gLi4uLSAuLiAuIC0uLi0gLS0uLiAtLi4uIC8gLi0uIC0tLSAuLS0gLi0uLS4t


İpucu

İyi şanslar!

#Mr. Rakun!

İPUCU İÇERİĞİ'ne baktığımızda açılır pencerede :

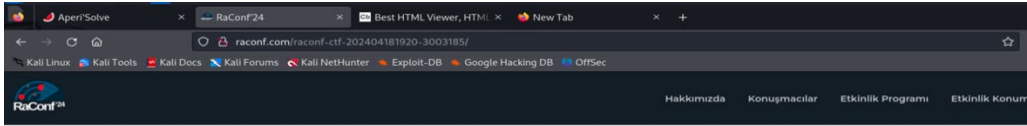
İpucu



Görünenin ötesinde gizlenen gerçekler her zaman vardır. İşte tam da bu noktada, sıradışı olanı keşfetmek bizim uzmanlık alanımızdır. Aradığın cevapları bulmak için **RAKUN**'un kapısını çalabilirsin. Onlar, sıradanını ötesindeki gizemleri çözmek için bekliyorlar.

Kapat

Bilgisine ulaşıyoruz.



Tebrikler...

Rakunlar, web sitesinde keşfettikleri şifreli bir mesajla karşılaştılar. Mesajın içeriği, tuhaf sembollerle doluydu ve onlara anlam veremiyorlardı. Artık yorulmuşlardı ama biliyorlardı artık bunların hepsi sona erecekti.

```
LS4tIC4uLi0gLi0tIC4uLiAuLiAVIC4tL4gLS4gLi0tIC4tLS4gLS4gLiAVIC4uLS4gLS4uLSAuLS4gLi0gLi4uL
SAuLS4uLC0uLi0gLyATLi4uLiC0uLiC0tIC4uLC0uLi4gLS4tLSAuLi4gLS0gLS0uLC0uLi4gLS0uLiAuLiAVIC0tLS
ATLiAuLS0tIC4tLSAuLi0gLi0tIC4uLi4gLyAuLi0tIC4tLS0gLiAuLi4tIC4uLi0gLi0tLiAuLS0uLiC0uLi4gLi
0uLiC0gLi0uLi0tIC4tLS4gLi4uLiATLi0gLi0tLiAuLi4tIC4tLS4tLSAuLi4uLiC0uLSATLi4gLi0tIC4tLi4tLiAVIC4
tIC4tLS4gLS0gLS4tLS4tLS4uLi4uLiC0uLi4gLS0gLiAVIC4uLi0gLi0tLiAuLS4gLi4uLiAuLS4gLyAT
LS4tIC0uLi4gLSATLi0tIC0uLS0gLi0tLSAuLi4uLiC0uLSATLi4tIC0uLiC4tLS4gLi0tLiAuLS4gLyAT
LS4tIC0uLi4gLS4gLyATLi0gLS4gLi4uLSAuLiAuLiC0uLi0gLS0uLiATLi4uLiC8gLi0tLiAuLS0gLi0u
LS4t
```

[İpucu](#)

İyi şanslar!

#Mr. Rakun!

Web sitesi içerisinde bulunan alandaki şifreyi çözümlenmemiz gerekiyor. Bunun için çeşitli online araçlar, teknikler kullanabiliriz. Öncelikle site içerisinde tespit ettiğimiz şifreli metnin formatını öğrenmek için “Cipher identifier” tekniğini kullanıyoruz.

Burada “www.Dcode.fr” sitesini kullanarak şifrelemede kullanılan potansiyel methodları öğreniyoruz.



Sitenin döndürdüğü cevaplar incelendiğinde metnin “morse code” ve “base64 coding” tekniği ile şifrelendiğini tespit ediyoruz. Olasılıkları değerlendirerek öncelikle “base64” ile Decode ettiğimiz zaman içerisinden “mors koduna” sahip oluyoruz.



BASE64 CODING
Informatics · Character Encoding · Base64 Coding

BASE 64 DECODER

SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'boolean'

BROWSE THE FULL DCODE TOOLS LIST

Results

LS4tIC4uLi0g..S4t

Summary

- Base 64 Decoder
- Base64 Encoder
- What is Base64 encoding? (Definition)
- How to encrypt using Base64 coding?
- How to decrypt Base64 encoding?
- How to recognize a Base64 ciphertext?
- Why using Base64?
- Does Base64 always end with ==?
- Why is data size increasing?
- Why is Base64 named like this?

Mors kod formatındaki şifrelenmiş metni de çözümlendiğimizde yine bir şifrelenmiş metin karşımıza çıkıyor.



MORSE CODE
Communication System · Telecom · Morse Code

MORSE CODE TRANSLATOR

SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'boolean'

BROWSE THE FULL DCODE TOOLS LIST

Results

KVWSI LNPNE FXRAVLX BNMIBYSMGBZI ONJWUWH
FJEVPPNHR "PHKPV YHKGR" ALNMYBU BME VLRHR
QBTTYJHKXNAPR. DNJHN ONVIEZB ROW.

Summary

- Morse Code Translator
- Morse Encoder
- What is Morse Code? (Definition)
- How to encrypt using Morse Code cipher?
- How to decrypt Morse Code cipher?

Ardından tekrardan "cipher identifier" tekniği kullanarak şifreli metni analiz ettiğimizde karşımıza analizler arasında "vigenere" tekniği ile şifrelenmiş bir metin olduğu ortaya çıkıyor.



ENCRYPTED MESSAGE IDENTIFIER

SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'boolean'

BROWSE THE FULL DCODE TOOLS LIST

Results

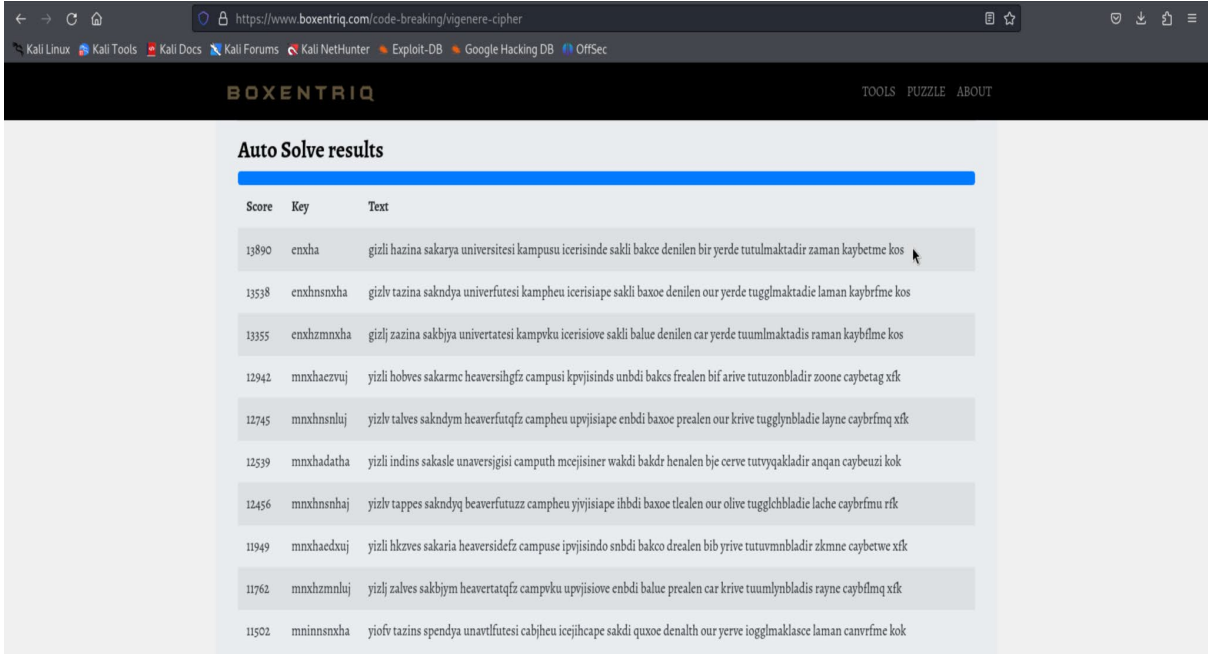
dCode's analyzer suggests to investigate:

	↑↓	↑↓
Vigenere Cipher	██████	██████
Autoclave Cipher	██████	██████
Beaufort Cipher	██████	██████
Rozier Cipher	██████	██████
Vernam Cipher (One Time Pad)	██████	██████
Variant Beaufort Cipher	██████	██████
Gronsfeld Cipher	██████	██████

Summary

- Why does the detector display a warning?
- Why does the analyzer/recognizer not detect my cipher method?
- How does the cipher identifier work?

Sonrasında kullandığım www.boxentriq.com sitesine gelerek “vigenere cipher” içerisinde denemeleri anahtar algoritması yöntemiyle yaptığında şifreleme algoritmasını çözecek anahtarım “enxha” olduğunu ele geçirip şifreyi çözümlüyoruz. Key olarak “enxha” verildiği zaman anlamlı bir metin karşımıza çıkıyor.



Score	Key	Text
13890	enxha	gizli hazina sakarya universitesi kampusu icerisinde sakli bakce denilen bir yerde tutulmaktadır zaman kaybetme kos
13538	enxhnsnxha	gizlv tazina sakndya univerfutesi kampheu icerisiapie sakli baxoe denilen our yerde tugglmaktadie laman kaybrfme kos
13355	enxhzmnxha	gizlv zazina sakbjya univerfutesi kampvku icerisiove sakli balue denilen car yerde tuumlmaktadis raman kayblfme kos
12942	mnhxaezvuj	yizlv hobves sakarmc heaversihgfv campusu kpvjisinds unbdv bakcs frealen bif arive tutuzonbladiv zoone caybetag xfk
12745	mnhxhnsnluj	yizlv talves sakndym heaverfutqfv campheu upvjisiapie enbdv baxoe prealen our krive tugglynbladiv layne caybrfmq xfk
12539	mnhhadatha	yizlv indins sakasle unavrsjgisi camputh mcejisiner wakdiv bakdr henalen bje cerve tutvyqakladiv anqan caybeuzi kok
12456	mnhxhnsnhaj	yizlv tappes sakndyq beaverfutuzz campheu yivjisiapie ihbdi baxoe tealen our olive tugglehbladiv lache caybrfmu rfk
11949	mnhxaezxuj	yizlv hkzves sakaria heaversidefv campuse ipvjisindo snbdi bakco drealen bib yrive tutuvmnbladiv zkmne caybetwe xfk
11762	mnhxhzmnluj	yizlv zalves sakbjym heavertatqfv campvku upvjisiapie enbdv balue prealen car krive tuumlynbladiv rayne caybrfmq xfk
11502	mninnsnxha	yiofv tazins spendya unavrlfutesi caybheu icejihape sakdiv quxoe denalth our yerve iogglmaklasce laman canvrime kok

“Gizli hazine Sakarya Üniversitesi kampüsü içerisinde saklı bahçe denilen bir yerde tutulmaktadır zaman kaybetme koş”

Şimdi zaman kaybetmeden **Gizli Bahçeye** koşma vakti! 😊 @Sausiber @raconf24 ekibine sonsuz saygı ve sevgilerimle....

