

Mu Cyber CTF 2017 Write Ups

Mu Cyber ekibinin 25-26 Kasım 2017 tarihinde yapmış olduğu Capture The Flag yarışmasının sorularının çözümleridir.

Flag Form

Flag - 10

Bu soru flag formatını gösteriyordu.Yani cevap mucyb3r_{FLAG} olucaktı.

Theory

EXE - 100

<http://bfy.tw/FB8q>

flag: mucyb3r_{elf}

GNU - 100

<http://bfy.tw/FB95>

flag: mucyb3r_{gdb}

Sub - 100

<http://bfy.tw/FB9a>

flag: mucyb3r_{26}

Wi-Fi - 100

<http://bfy.tw/FBA5>

flag: mucyb3r_{iwconfig}

Arch - 150

https://wiki.archlinux.org/index.php/Arch-based_distributions

flag: mucyb3r_{blackarch}

Crypto

MD5 - 50

Verilen hash i MD5 ile decode ettiğimizde flage ulaşıyoruz.

flag: mucyb3r_{h4ck3r}

Tekrar Tekrar Dene - 100

Verilen hash i Base64 ile tekrar tekrar decode ettiğimizde flage ulaşıyoruz.

flag: mucyb3r_{RECURSIVE}

NTLM - 100

Verilen hash i NTLM decrypt kullanarak decode ettiğimizde flage ulaşıyoruz.

flag: mucyb3r_{yeni_basliyoruz}

Zor Değil - 150

Klasik bir şifreleme yöntemi olan Vigenère ile şifrelenmiş veriyi verilen key sayesinde decrypt ederek flag e ulaşıyoruz.

<https://www.dcode.fr/vigenere-cipher>

flag: mucyb3r_{blaise_de_vigenere}

ZOR - 200

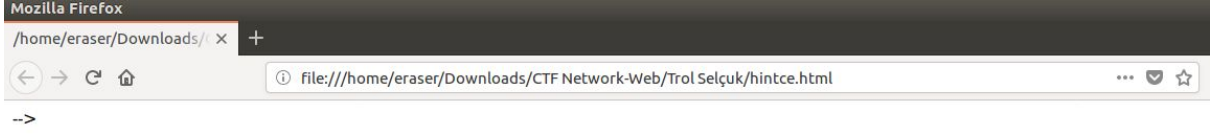
Bu soruda erilen değeri XOR ile decrypt etmemiz gerekiyordu. Bunun için <http://strelitzia.net/wasXORdecoder/wasXORdecoder.html> ı kullandık.

flag: mucyb3r_{hosgeldiniz}

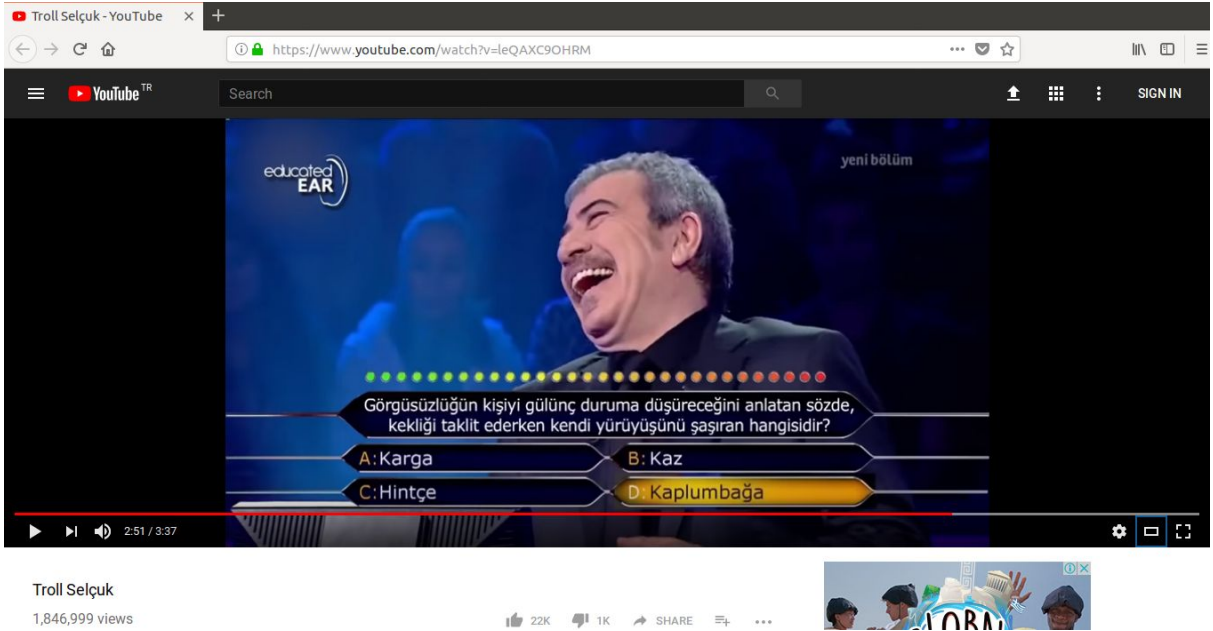
Web - Network

Troll Selçuk - 100

100 Puanlık Troll Selçuk sorusu. Öncelikle sorumuzu açtığımızda hiçbir açıklama olmaksızın bir drive linki veriliyordu. Drive linkinden hintce.tar.xz isimli dosyayı bilgisayarımıza indiriyoruz. İçerisinde sadece hintce.html dosyası var. Html dosyasını çalıştırdığımızda bizi öncelikli olarak boş bir sayfadan youtube linkine yönlendiriyor.



Tabiki can alıcı nokta burası. Bunu farketmemiz gerekiyor. Sayfa yüklendiğinde karşımıza eğlenceli bir video çıkıyor.



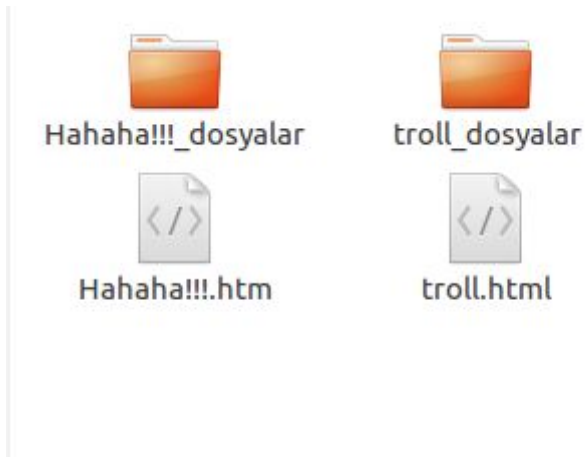
Videoyu keyifle izliyoruz ve bitiyor :) Burda flag yok. Sonra yapmamız gereken şey hintce.html dosyasının kaynak kodlarına bakmalıyız. Sayfanın kaynak kodlarına bakabilmek için html dosyasını bir text editör yardımıyla açıyoruz. Karşımıza 14 satır kısa bi kod bloğu çıkıyor ve dikkatlice baktığımızda burda div etiketi içerisinde flag'in tanımlı olduğunu görüyoruz.

```
<script>
  function hipnoz(){
    window.location.href="https://www.youtube.com/watch?v=leQAXC90HRM"
  }
</script>
<html>
<head>
</head>
<body onload="hipnoz()">
--
>
<div style="display:none;">mucyb3r_(activex)</div>
</body>
</html>
```

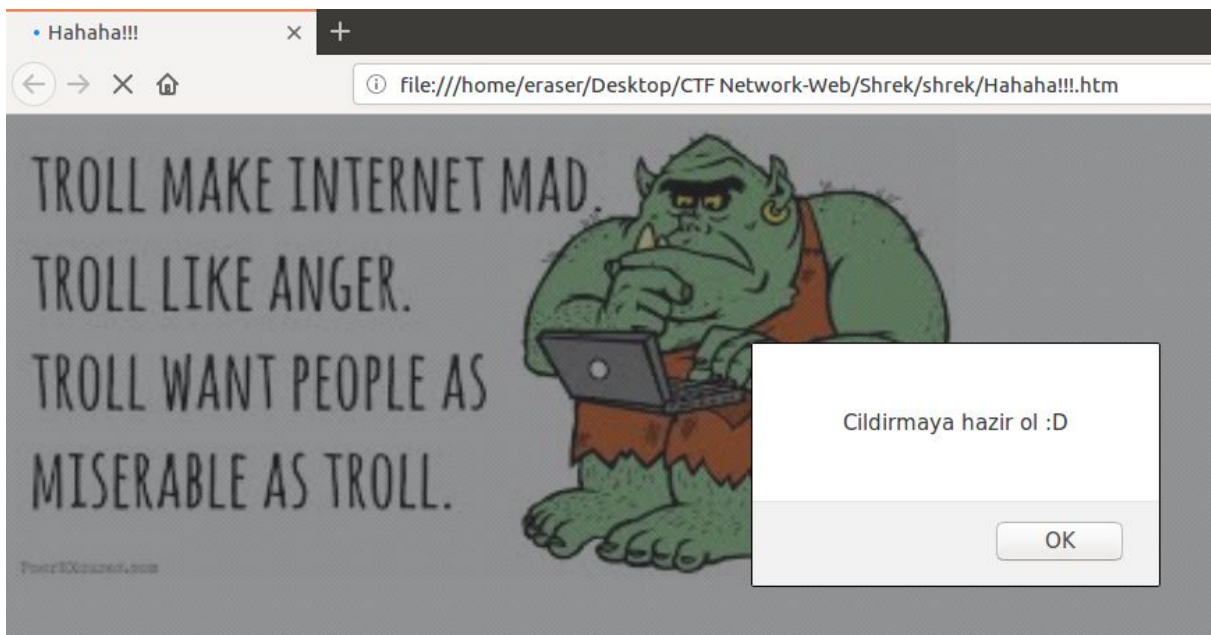
flag : mucyb3r_(activex)

Shrek - 200

200 Puanlık Shrek sorusu. Öncelikle sorumuzu açtığımızda hiçbir açıklama olmaksızın bir drive linki veriliyordu. Drive linkinden troll.rar isimli dosyayı indiriyoruz. İçeriğine bakıyoruz 2 klasör ve 2 dosya var.



Bu dosyalara göz gezdiriyoruz ve Hahaha!!!.html dosyasını açıyoruz içeriğinde çıldırmaya hazır mısın diye bir mesaj var



OK butonuna bastıktan sonra ekrandaki sayfa değişiyor. Dosyalara göz gezdiriyoruz. Json ile yazılmış dosyalar görüyoruz.

Hook.js dosyasının kaynak kodunu incelediğimizde şifreli kod bloğu görünüyor. Fonksiyon

içerisindeki encode edilmiş kodları kopyalayıp "https://www.unphp.net" web adresi veya herhangi Php Decoder sayfasında decode ettiğimizde karşımıza flag is here diye tanımlı flag'imiz çıkıyor.

```
<? function javascript()  
{  
var _0x945d=["SayHello","GetCount","Message : ","flag is oh_beee"];function NewObject(_0x5352x2){var _0x5352x3=0;  
this[_0x945d[0]]= function(_0x5352x4){_0x5352x3++;alert(_0x5352x2+_0x5352x4)};this[_0x945d[1]]= function(){return  
_0x5352x3}}var obj= new NewObject(_0x945d[2]);obj.SayHello(_0x945d[3])  
}  
?>
```

flag: mucyb3r_{oh_beee}

Uptime - 250

Soruda SSID si Meryem olan kullanıcının Uptime süresini bulabilir misin? diyordu. Bu sorunun benzeri SDUCTF'de kullanıldı. Alıntıdır Bize bir adet .pcap(analiz edilmiş ağ dosyası) verilmiş. Ve uptime süresini bulmamız isteniyor. Komut satırından airodump-ng aracıyla uptime süresini bulabiliyoruz. airodump aracını kullanabilmemiz için aircrack-ng'nin yüklü olması gerekiyor alt text Bilgisayarınızda aircrack-ng yok ise "sudo apt-get install aircrack-ng" komutu ile ekliyoruz. Komut satırına airodump-ng -r (dosya konumu) --uptime (-r parametresi dosyayı belirtmek için kullanılıyor, --uptime parametresi ise uptime süresini kolon olarak eklemeyi sağlar) Bu komutu verdiğimizde meryem isimli kullanıcın uptime süresinin "00:10:54" olduğunu görüyoruz.

flag: mucyb3r_{00:10:54}

Handshake - 300

300 Puanlık Handshake Sorusu; Galatasaraylı Emel'in kablosuz ağını ele geçirmek isteyen saldırgan, bir handshake yakaladı. Parolayı bulmasına yardım eder misiniz? NOT: Parola 8 karakterlidir. Bize verilen ipuçları: Galatasaray,Emel,8 Karakter Drive dosyasından indirdiğimiz .cap(yakalanmış paket dosyası)'nı analiz etmek için kullanacak olduğumuz 2 araç var 1)aircrack-ng 2)crunch. Bu 2 araç sayesinde parolayı elde edebiliriz. Crunch:verilen karakter uzunluğunda ve belirtilen kriterlere göre şifreler üretiyor ve bu şifreleri belirttiğimiz dosya üzerinde brute-force tekniğini kullanarak deniyor. kullanım şekli için "crunch (min-max karakter sayısı) (ipuçları) -r (output.file)" -r parametresi dosyaya kaydetmek için belirtiliyor. Üretmiş olduğumuz şifreleri bir txt dosyasına kaydettik, bu işlem biraz zaman alabiliyor tüm karakterlerin kombinasyonlarını deniyor. Ardından aircrack-ng komutuyla kaydetmiş olduğumuz şifre dosyasını ve .cap dosyasını brute-force işlemine tabii tutuyoruz. Kısa süre sonra şifreyi buluyoruz.

```
eraser@eraser-pc: ~  
  
[00:01:30] 160116 keys tested (1763.69 k/s)  
  
KEY FOUND! [ 1905emel ]  
  
Master Key      : A5 20 01 4A BD FF 47 18 C5 B7 21 93 16 3E 91 F5  
                  4F A7 82 6A D7 79 1F 6D DA E7 9B 38 8A 28 F4 DD  
  
Transient Key   : D1 13 C6 83 22 DB BE 81 89 AE 20 9F 8D 2A 4F 4B  
                  57 C6 A4 81 40 49 56 19 55 F5 48 DB 2A CC C6 7F  
                  3B C1 C1 11 6C BC CF 05 05 7C 9D 00 72 41 C8 76  
                  79 C3 3F 38 29 DE 81 2E 11 D8 B7 42 0C E4 5B 5A  
  
EAPOL HMAC      : 8F FF 19 6B 21 7C 9C 02 2E 39 13 31 44 A8 86 19  
eraser@eraser-pc:~$ aircrack-ng cimbom.cap -w keylist.txt -0
```

flag: mucyb3r_{1905emel}

Mr.Robot - 400

400 Puanlık MrRobot sorusu. Karşımızda sadece .pcapng formatında bir dosya var. Öncelikli olarak bu dosyayı wireshark ile pcap dosya formatına çeviriyoruz. Sonrasında komut satırına "tcpflow -d2 -r mrrobot.pcap" (-r dosya belirtme, -d hata ayıklama çıktıları) yazdığımızda ekrana gelen çıktı; tcpflow: retrying_open
::open(fn=004.005.006.007.12345-008.009.010.011.02355,oflag=xc2,mask:x1b6)=5 tcpflow:
Open FDs at end of processing: 1 tcpflow: demux.max_open_flows: 1 tcpflow: Flow map
size at end of processing: 1 tcpflow: Flows seen: 1 tcpflow: Total flows processed: 1 tcpflow:
Total packets processed: 1821

Böyle bir geri dönüt vermekte.004.005.006.007.12345-008.009.010.011.02355 isimli dosyayı
\$ file 004.005.006.007.12345-008.009.010.011.02355 yazdığımızda ise
004.005.006.007.12345-008.009.010.011.02355: JPEG image data, JFIF standard 1.01,
resolution (DPI), density 72x72, segment length 16, progressive, precision 8, 564x572,
frames 3 dönütünü vermekte.Yani pcap bir resim dosyası.Resim dosyası açıldığında
bayrağımızı resmin üzerinde görmekteyiz.

flag: mucyb3r_{unshattered.jpg}

Stegano

Hack İşlemi Başlatılmıştır - 100

Soruyu açtığımızda resimde saklanmış bir mesaj vardı. Steganography ile saklanmış mesajı açığa çıkartabiliriz. Bunun için <http://incoherency.co.uk/image-steganography/#unhide> aracını kullanarak cevabı mucyb3r_(Turkey) olarak buluyoruz.

Image Steganography

[How it works](#)[How to defeat it](#)

Hide images inside other images.

This is a client-side Javascript tool to steganographically hide images inside the lower "bits" of other images.

Select either "Hide image" or "Unhide image". Play with the **example** images (all 200x200 px) to get a feel for it.

Image:

 hack.png

Example:

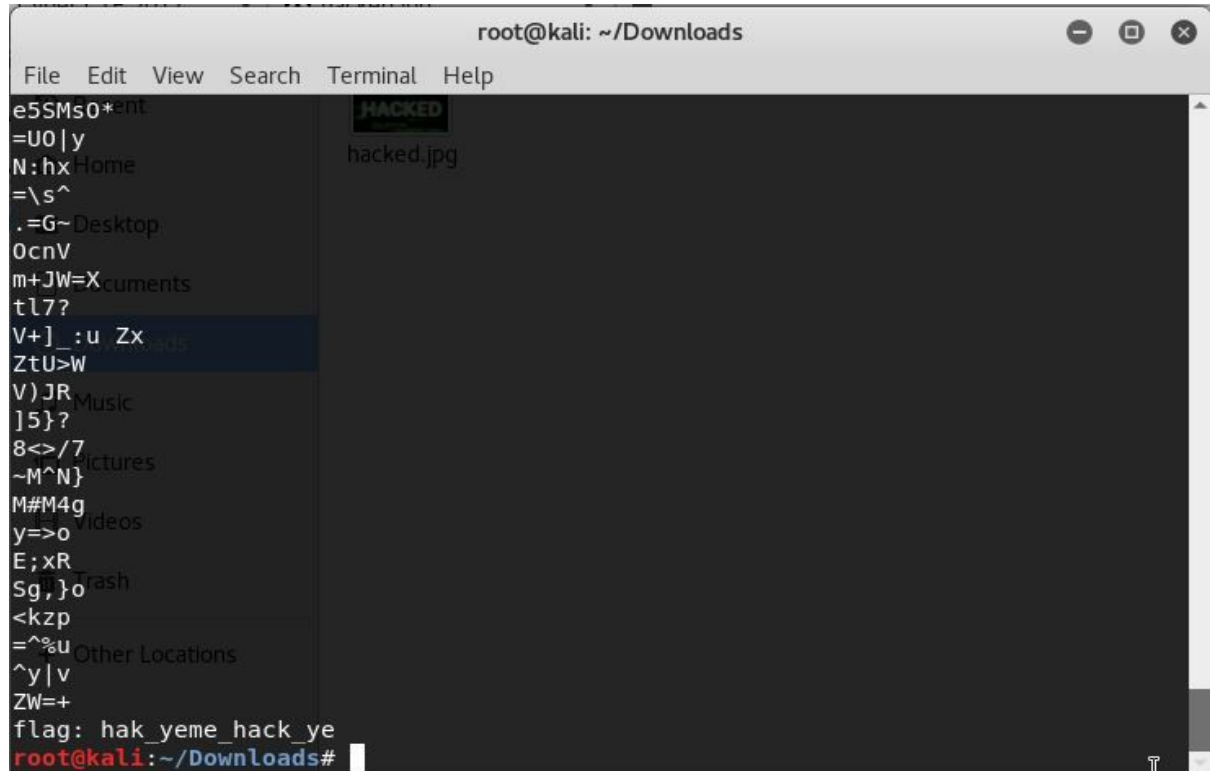
Hidden bits: 1



Kul Hakkı - 200

Bu soruda "strings" komutunu kullanarak flag e ulaşıyoruz.

```
root@kali: ~/Downloads
File Edit View Search Terminal Help
root@kali:~/Downloads# strings hacked.jpg
bExif
Adobe Photoshop CS6 (Windows)
2017:02:21 23:04:36
Adobe_CMop
Adobe
b34rDocuments
7GWgw
AQaq"
dEU6te
'7GWgw
^APs
|kvp
a"5Zc
hM!i
990uu
gMPG
#U8#
pswz[]z
ZqGA
ewmq
t.<9
K* Eb
qh70:
```


flag: mucyb3r_{hak_yeme_hack_ye}

ScreenShot - 250

mucyb3rctf i Snapchat adlı sosyal medya uygulamasında ekleyip son attığı story e bakınca karşımıza bir karekod çıkıyor.



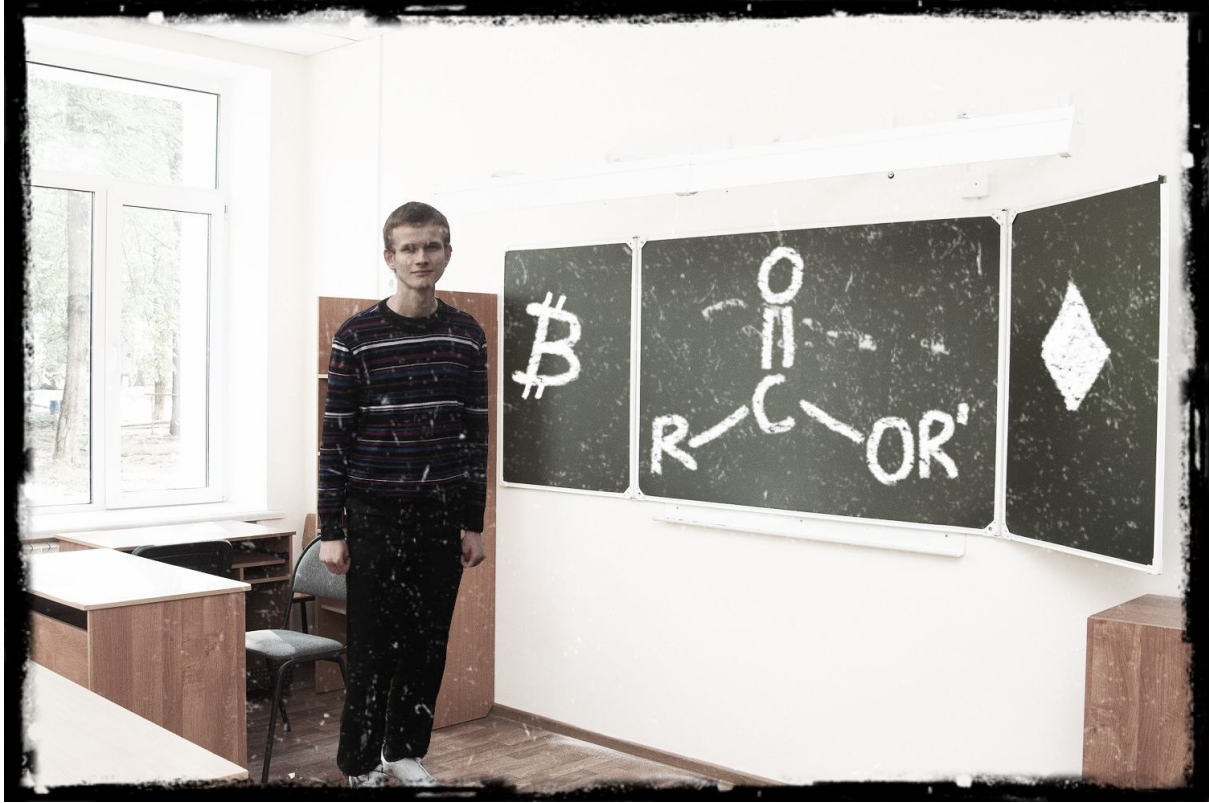
Bu karekodu herhangi bir karekod okuyucu ile okutunca flag e ulaşıyoruz.

 Decode Succeeded	
Raw text	mucyb3r_{do_you_like_me}
Raw bytes	41 86 d7 56 37 96 23 37 25 f7 b6 46 f5 f7 96 f7 55 f6 c6 96 b6 55 f6 d6 57 d0 ec 11 ec 11 ec 11 ec 11
Barcode format	QR_CODE
Parsed Result Type	TEXT
Parsed Result	mucyb3r_{do_you_like_me}

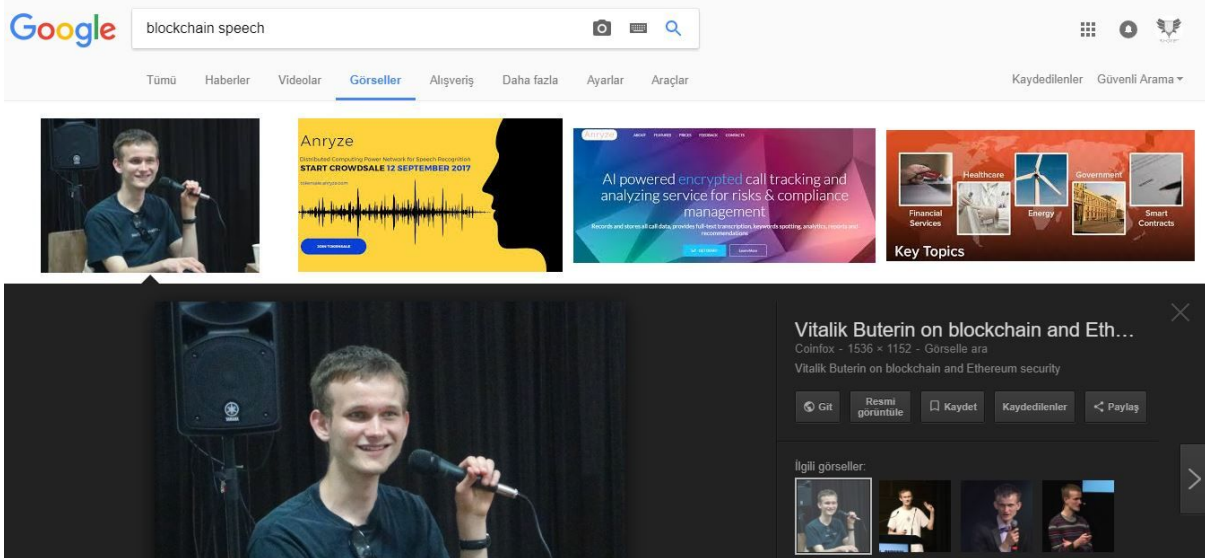
flag: mucyb3r_{do_you_like_me}

Who is this guy? - 300

Verilen fotoğraftaki dosyanın adı blockchain speech ile alakalıydı.



Google Görseller' de blockchain speech diye arattığımızda ilk fotoğraftaki adamın bizim adamımızla aynı adam olduğunu görüyoruz.



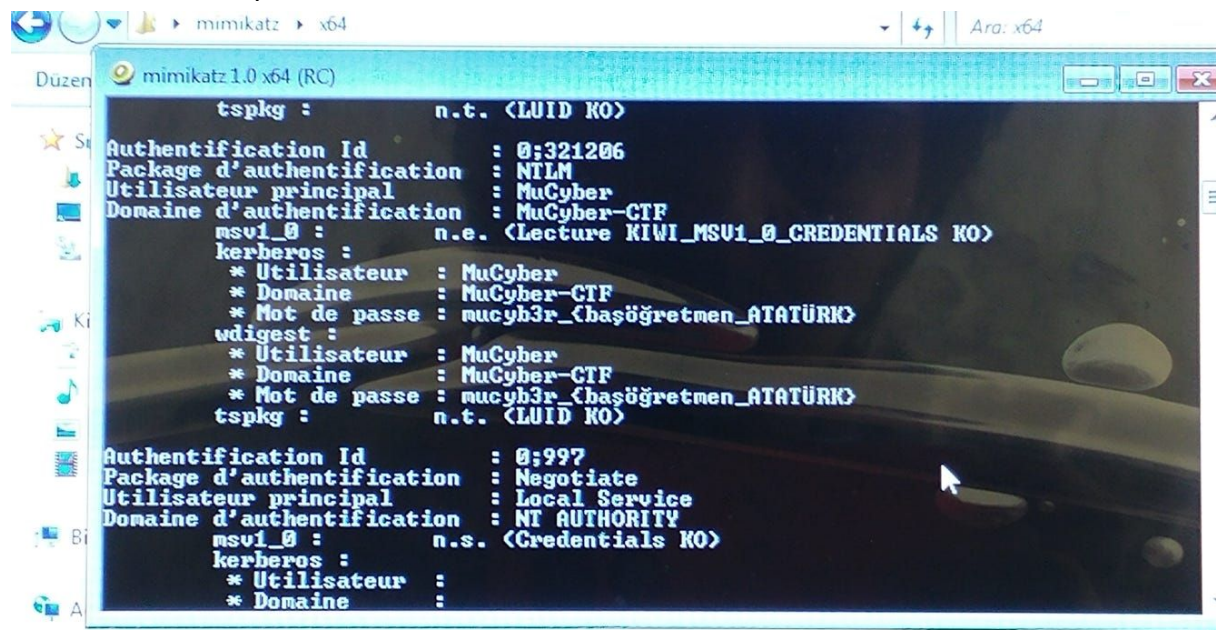
Bu adamın adı ise Vitalik Buterin.

flag: mucyb3r_{vitalik_buterin}

24 Kasım - 400

Bu soruyu çözmek için mimikatz aracından faydalanacağız. Mimikatz i indirdikten sonra verilen dosyayı mimikatz'in klasörüne kopyalıyor ve mimikatz i çalıştırıyoruz. Sırasıyla komutları giriyoruz:
"privilege::debug"

"sekurlsa::minidump lsass.DMP"



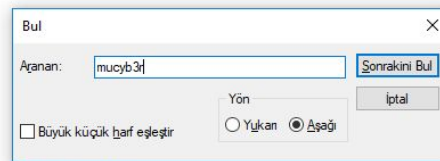
flag: mucyb3r_{bařuęretmen_ATATÜRK}

Forensic

Log - 100

Dosyamızı indirdikten sonra note pad ile açıyoruz. CTRL+F yaparak "mucyb3r" şeklinde arama yapıyoruz flag karşımıza çıkıyor.

_analytics_video_tutoria_1.htm www.mysite.com 200 0 0 3508 844 549

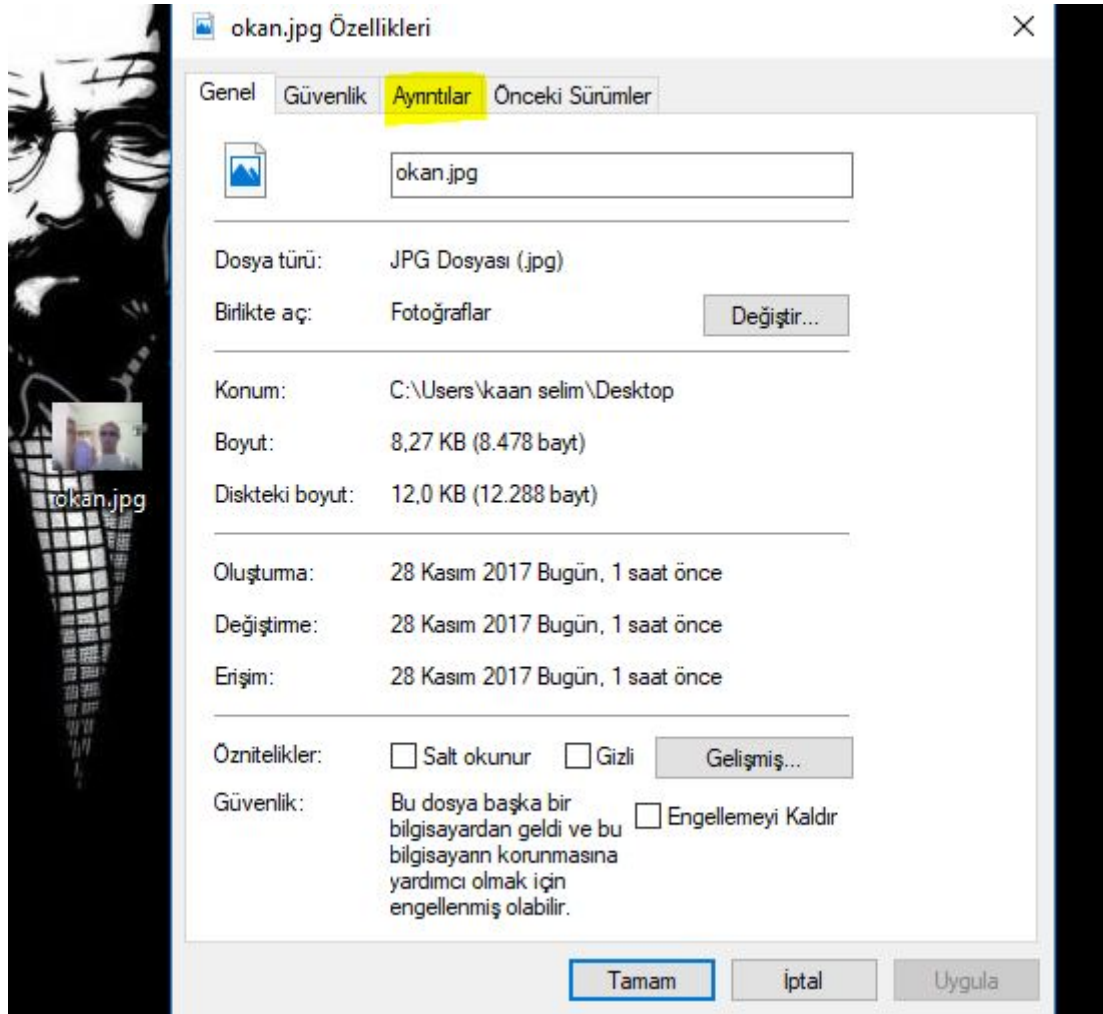


849 140
gle_analytics_video_tutoria_1.htm www.mysite.com 200 0 0 1519 832 343
39414400 http://www.mysite.com/2007/02/google_analytics_video_tutoria_1.htm www.mysite.com 200 0 0 2094 904 218
http://www.mysite.com/2007/02/google_analytics_video_tutoria_1.htm www.mysite.com 200 0 0 12025 894 1015 mucyb3r_{learn_searching}

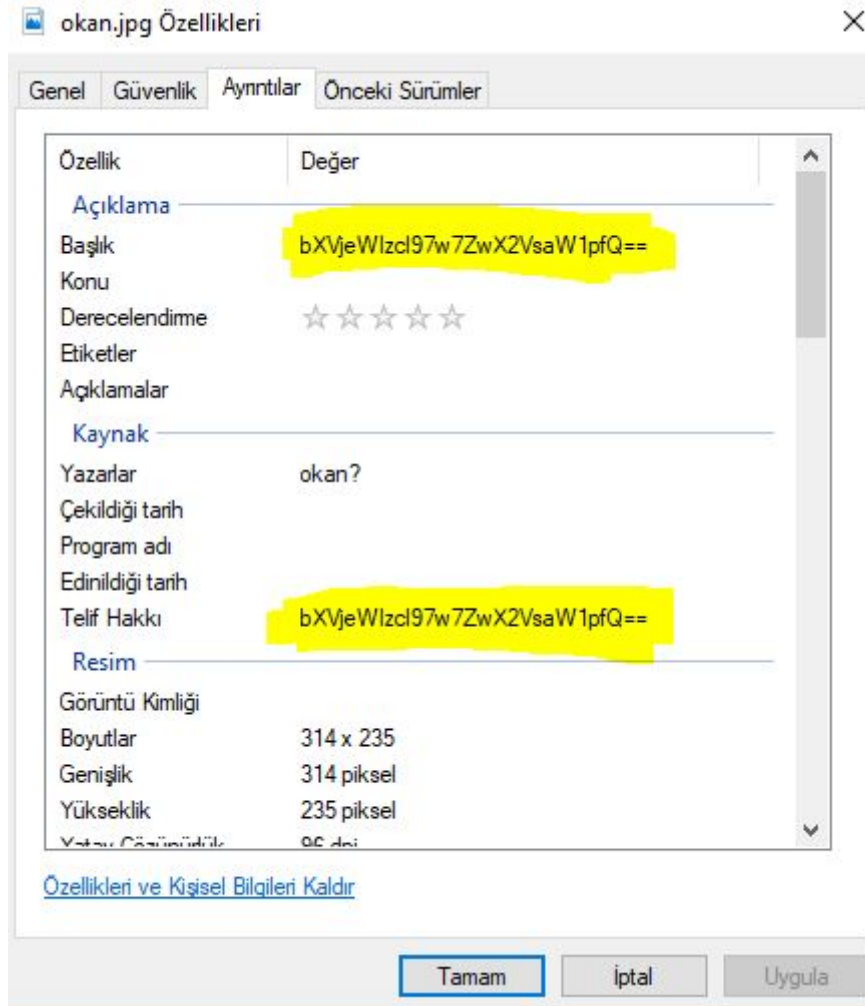
flag: mucyb3r_{learn_searching}

Hacker Okan - 150

jpg dosyamızı indirdikten sonra Hacker Okan'a sağ tıklayıp özelliklerine giriyoruz.



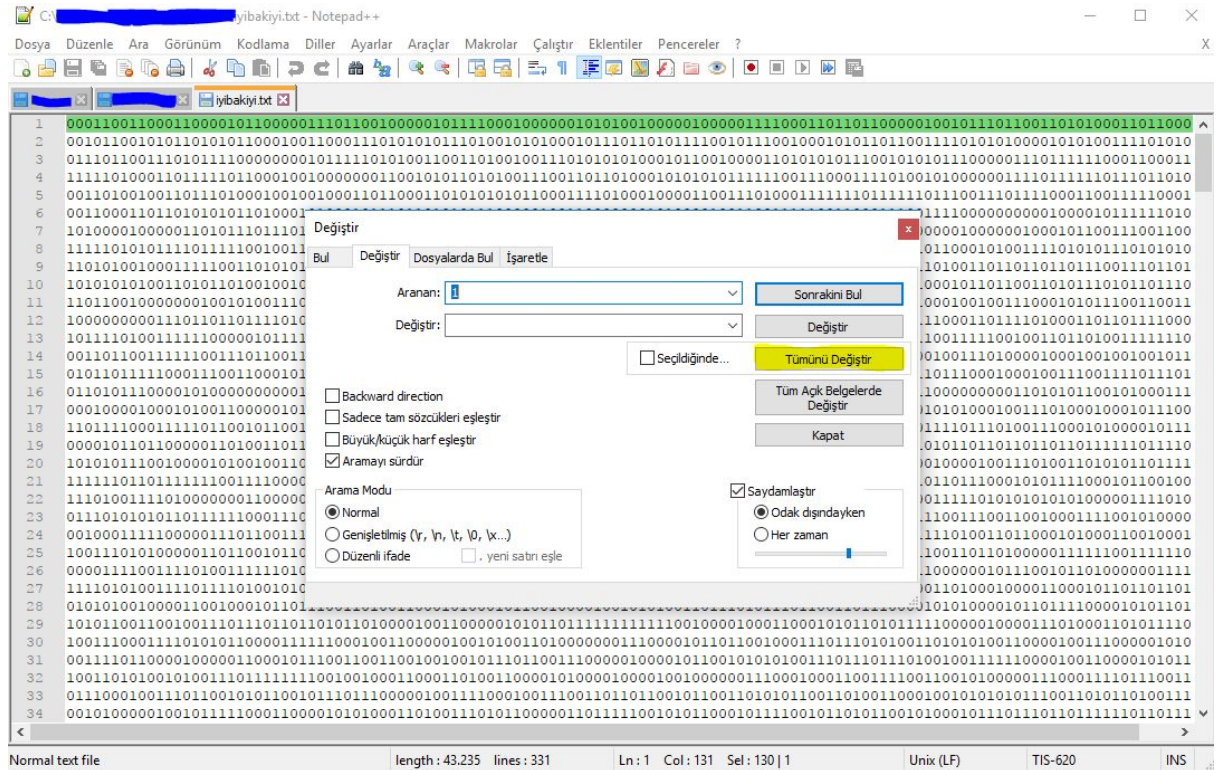
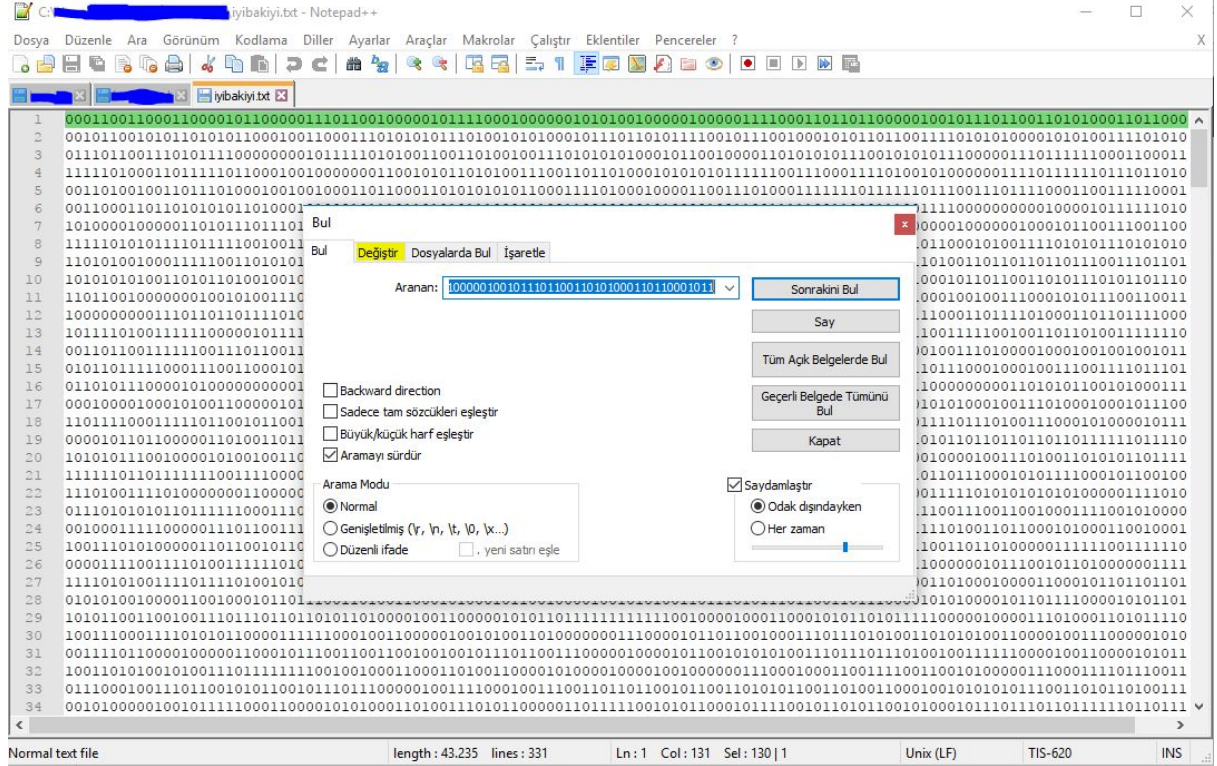
Açılan pencerede ayrıntılara girince karşımıza base64 ile şifrelenmiş bir hash çıkıyor.



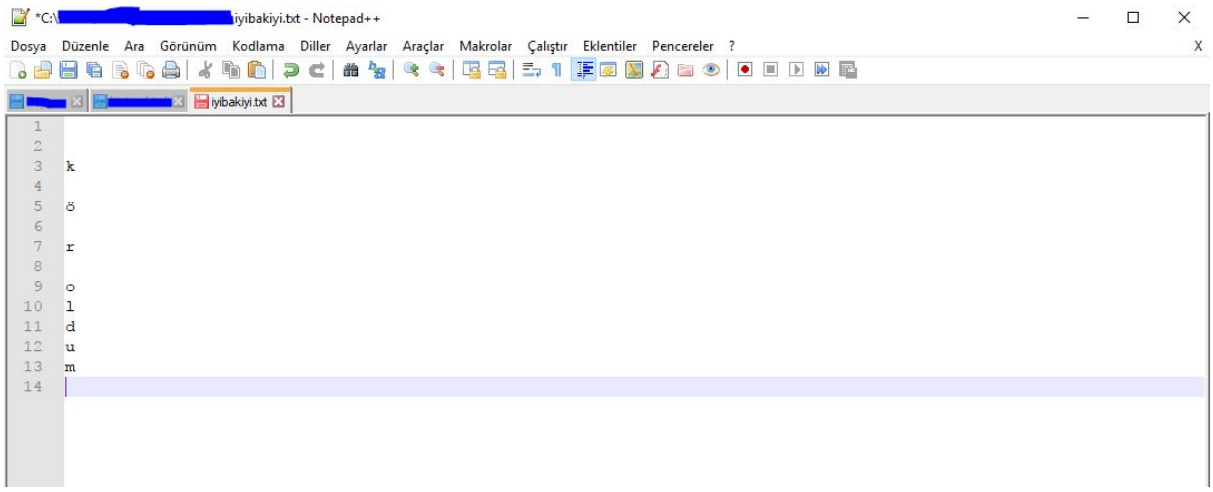
Bunu base64 ile decode edince karşımıza flag çıkıyor.

flag: mucyb3r_{öp_elimi}

Sorumuzda verdiğimiz linke girince karşımıza iyibakiyi.txt adlı bir dosya çıkıyor. Bu dosyayı indirip notepad++ ile açıyoruz. CTRL+F yapıp karşımıza çıkan penceredendeğiştir kısmına giriyoruz.



Buradan aranan kısma 1 yazıp deęiştir kısmını boş bırakarak tümünü deęiştir diyoruz. Ardından aynı işlemi 1 yerine 0 yazıp tekrar ediyoruz. Bu işlemleri yaptıktan sonra dosyamızda sadece flag'ımız kalıyor.



flag: mucyb3r_{köroldum}

Git - 200

Sorumuzda verilen linke giriyoruz.

Challenge

36 Solves

Git
200

<https://github.com/MuCyberLab/CTF>

Key

SUBMIT

Karşımıza çıkan github reposunda commitlere bakıyoruz. Yeterince eski commitlere gidince delete flag adında bir commit ile karşılaşırız. Bu commite girince flag karşımıza çıkıyor.

```
+flag: mucyb3r_{taktigin_ iyi}
```

flag: mucyb3r_{taktigin_ iyi}

Use Calc - 500

Verilen linke girince bir ses dosyası ile karşılaşırız. Bu ses dosyasının içinde ise arama esnasında basılan tuşların sesleri yer alıyor. Bu ses dosyasını <http://dialabc.com/sound/detect/> adresine yüklüyoruz.

← → ↻ dialabc.com/sound/detect/

Uygulamalar Yeni klasör

DialABC

Detect DTMF Tones

Detect DTMF Tones

DialABC lets you find DTMF tones within audio clips. All you have to do is to upload an audio file to the dialabc web site using the form below. Our software then analyzes the audio recording and presents you with some statistics, a graph and a table showing you what DTMF tones are contained in the data and where.

All you need is an short audio sample in one of several standard audio data file formats.

Use this form to run your sound sample through our DTMF detection tool. See disclaimer below.

Sound File Dosya seçilmedi A number of audio file formats are supported including RIFF Microsoft WAV PCM and Sun/NeXt Audio.

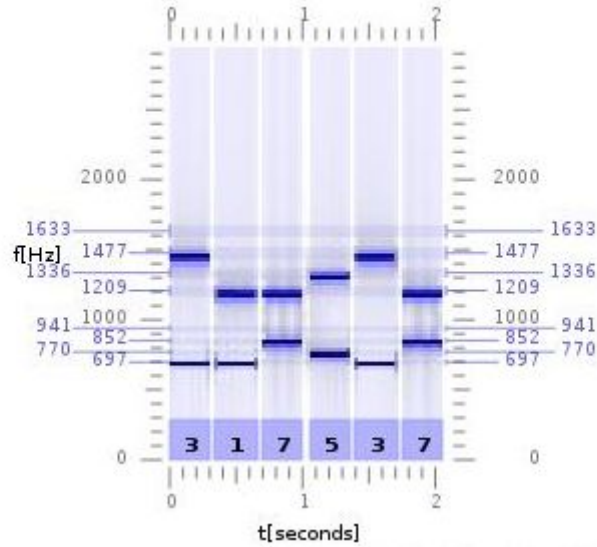
If you have concerns regarding privacy, please read our privacy policy.

Contents

- DialABC
- Words
- Numbers
- Motion
- Sound
- DTMF
- Generate
- Detect
- Explain
- FAQ
- Music
- Anagrams
- Links
- About

Domain Astrophysical Observatory
Help bring back science education to the Center of the Universe

Karşımıza 317537 şeklinde bir sayı çıkıyor.



Sample Format RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, mono 44100

Sample Size 185,260 bytes
approximately 91,839 usable samples
2.1 seconds

Tones Found	Tone	Start Offset [ms]	End Offset [ms]	Length [ms]
	3	0 ± 15	301 ± 15	301 ± 30
	1	331 ± 15	663 ± 15	331 ± 30
	7	694 ± 15	995 ± 15	301 ± 30
	5	1,056 ± 15	1,358 ± 15	301 ± 30
	3	1,388 ± 15	1,720 ± 15	331 ± 30
	7	1,750 ± 15	2,052 ± 15	301 ± 30

Bu sayıyı hesap makine yazıp ters çevirdiğimizde flag karşımıza çıkıyor.

LESLIE

flag: mucyb3r_{leslie}

Mixed

Dosya Analizi - 500

Sorumuzda verilen linki indirince siber.png adında bir dosya karşımıza çıkıyor. Bu dosyayı linux komut satırında "strings" komutu ile açıyoruz.

```
selim@selim-Aspire-E5-571G: ~/Desktop
selim@selim-Aspire-E5-571G:~/Desktop$ strings siber.png
```

Bu işlemden sonra karşımıza bir takım binary kodları çıkıyor.

```
selim@selim-Aspire-E5-571G: ~/Desktop
'!!!
7jjj6n
;>P2m
`0477wvzyy
BQ__o2
gll,(5r
IEND
*****be cool !
*****attention please !
*****what about fucking flag ??????????
*****ya oldugun gibi gorun ya da gorundugun gibi ol ;)
*****be cool !
*****attention please !
*****what about fucking flag ??????????
*****ya oldugun gibi gorun ya da gorundugun gibi ol ;)
>>>01101000 01101000 01101000 01100000 01100011 00111010 00101111 00101111 01100100 01100010 0110100
1 01101110 01100101 00101110 01100111 01101111 01101111 01100111 01101100 01100101 00101110 01100011
01101111 01101101 00101111 01100110 01101001 01101100 01100101 00101111 01100100 00101111 00110001
00111001 01010000 01010110 01111000 00111001 01001000 01010100 01010011 01000111 01101001 01000001 0
1001010 01100010 01011111 01100010 00110110 01101111 01000101 01011010 01010010 01100111 01001011 01
000011 00111000 00101101 01110001 01000001 01001101 01101001 01101001 01110010 01011000 00101111 011
10110 01101001 01100101 01101111 00111111 01110101 01110011 01110000 00111101 01110011 01101000 0110
0001 01110010 01101001 01101110 01100111<<<
selim@selim-Aspire-E5-571G:~/Desktop$
```

Bu kodları binary converter ile karakterlere çevirdiğimizde karşımıza başka bir link çıkıyor. Bu linkte ise bak_da_gör.png adında bir karekod ile karşılaşyoruz. Bu karekodu indirip tekrar "strings" komutu ile açınca karşımıza başka bir link daha çıkıyor :)

```
selim@selim-Aspire-E5-571G: ~/Desktop
selim@selim-Aspire-E5-571G:~/Desktop$ strings bak_da_gor.png

IEND
https://drive.google.com/file/d/10hywt38RdTc5pkLh0mBXvVSaPM5pLFyq/view?usp=shari
ng
selim@selim-Aspire-E5-571G:~/Desktop$
```

Bu linkten ise fiifi.tar adında bir dosya ile karşılaşyoruz. Tar dosyasının içindekileri çıkardığımızda 13.pdf, görmek-önemli.png, ordamısın-değilmisin.pcap adında 3 dosya bizi karşılıyor.



Ordamisin-degilmisin.pcap dosyasını wireshark ile açıyoruz.

```
selim@selin-Aspire-E5-571G:~/Desktop$ wireshark ordamisin-degilmisin.pcap
void DBusMenuExporterPrivate::addAction(QAction*, int): Already tracking action
" under id 190
void DBusMenuExporterPrivate::addAction(QAction*, int): Already tracking action
" under id 191
```

Bu sefer karşımıza çıkan ekranda, ICMP paketlerinin içinde başka bir takım binary kodları ile karşılaşırız.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.1	ICMP	104	Echo (ping) request ...
2	0.003821	192.168.1.1	192.168.1.102	ICMP	104	Echo (ping) reply ...
3	2.329647	192.168.1.102	192.168.1.1	ICMP	104	Echo (ping) request ...
4	2.335023	192.168.1.1	192.168.1.102	ICMP	104	Echo (ping) reply ...
5	3.608174	192.168.1.102	192.168.1.1	ICMP	104	Echo (ping) request ...
6	3.615525	192.168.1.1	192.168.1.102	ICMP	104	Echo (ping) reply ...
7	4.329481	192.168.1.1	192.168.1.255	RIPv2	86	Response
8	5.249814	192.168.1.1	224.0.0.1	IGMPv2	60	Membership Query, ge...
9	20.302881	192.168.1.1	224.0.0.1	IGMPv2	60	Membership Query, ge...
10	34.332732	192.168.1.1	192.168.1.255	RIPv2	86	Response

Frame 1: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
Ethernet II, Src: IntelCor_8f:7c:cb (00:db:df:8f:7c:cb), Dst: Tp-LinkT_6f:bd:ce (e8:de:27:6f:bd:ce)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.1
Internet Control Message Protocol

Offset	Hex	ASCII
0000	e8 de 27 6f bd ce 00 db df 8f 7c cb 08 00 45 00	..o....E.
0010	00 5a 00 01 00 00 40 01 f6 ea c0 a8 01 66 c0 a8	.Z....@.f..
0020	01 01 08 00 43 4a 00 00 00 00 30 31 31 31 30 30CJ.. ..011100
0030	31 31 20 30 31 31 31 30 31 30 30 20 30 31 31 31	11 01110 100 0111
0040	30 31 30 31 20 30 31 31 31 31 30 30 30 20 30 31	0101 011 11000 01
0050	31 30 31 31 31 30 20 30 31 31 30 30 31 30 31 20	101110 0 1100101
0060	30 31 31 31 30 31 30 30	01110100

bunları da çevirince flagımız çıkıyor.

Convert text to binary

Input data

01110011011101000111010101111000011011100110010101110100

Convert

binary numbers to text

Output:

stuxnet

flag: mucyb3r_{stuxnet}

C Program - 500

Bu sorumuzda verilen [c.cpp](#) adlı dosyamız her ne kadar C dili ile yazılmış gibi görünse de bu dosyamızın yazıldığı dil White Space dilidir.

[Bu linkten](#) verilen kodu yapıştırdığımızda flag değeri gayet ne bir şekilde görülebiliyordu.

```
#include <unistd.h>

int main(){ int run;
run>>=5;run=0;
run&=01; int MUCYBER[10000];
run>>=5;
using namespace std;

char *res[6] = {"Nothing_" ,
" and _no _one _is _perfect. ",
"It_ just _takes_ a_good _eye_",
"to_find_" ,
"those_hidden_" ,
"imperfections. :)" };

int i = 0,j=0;
for( i=0;i < 6 ; i++)for(j=0;j<strlen(res[i]);j++)
{int t=(int)res[i][j];if(t == '_' )MUCYBER[run++]=32;else if((t==32||t==9)&&(j!=27))MUCYBER[run++]=-1;
else MUCYBER[run++]= t ;}
for( i=0; i< run ;i++ )
if(MUCYBER[i+1])printf("%c",(char)MUCYBER[i]); i-=1 ;
printf("\n") ;
return 0;
}

/*END*/
► Footer
► Input
► Arguments
▼ Output
the_flag_is_WpUAItsadmhak
```

flag: mucyb3r_{WpUAItsadmhak}

Joy

Tweety - 300

Bu sorumuzda flag değerini almak için Twitter'da <https://twitter.com/mucyberlab> sayfamızı takip edip #mucyberCTF hashtag altında tweet atmanız gerekiyordu. Ardından Sayfa yöneticilerimiz size bir flag değeri verdi.

Algebra - 300

Bu sorumuzda ilk önce denklemlerdeki x değerlerini tek tek bulmanız gerekiyordu:

$$2x-7=211 \quad x=109$$

$$x-8=109 \quad x=117$$

$$x+2=101 \quad x=99$$

$$x+10=131 \quad x=121$$

$$-x+8=-90 \quad x=98$$

$$-2x+5=-97 \quad x=51$$

$$2x-1=227 \quad x=114$$

$$-x+10=-85 \quad x=95$$

$$x-9=114 \quad x=123$$

$$2x-5=201 \quad x=103$$

-3x+9=-342 x=117
-x+1=-115 x=116
3x+2=155 x=051
-2x+3=-217 x=110
-3x-1=-286 x=095
-x-3=-112 x=109
2x+9=105 x=048
x-4=110 x=114
-3x+10=-299 x=103
4x+1=205 x=051
x-11=99 x=110
-x+3x=250 x=125

Bulduğumuz sayılar ASCII formatında olduğundan herhangi bir online ASCII Decoder sayfasında decode ettiğimizde flag değeri gayet açık bir şekilde görölüyordu.

ASCII to text converter

Input data

```
109 117 099 121 098 051 114 095 123 103 117 116 051 110  
095 109 048 114 103 051 110 125
```

Convert

ASCII numbers to text

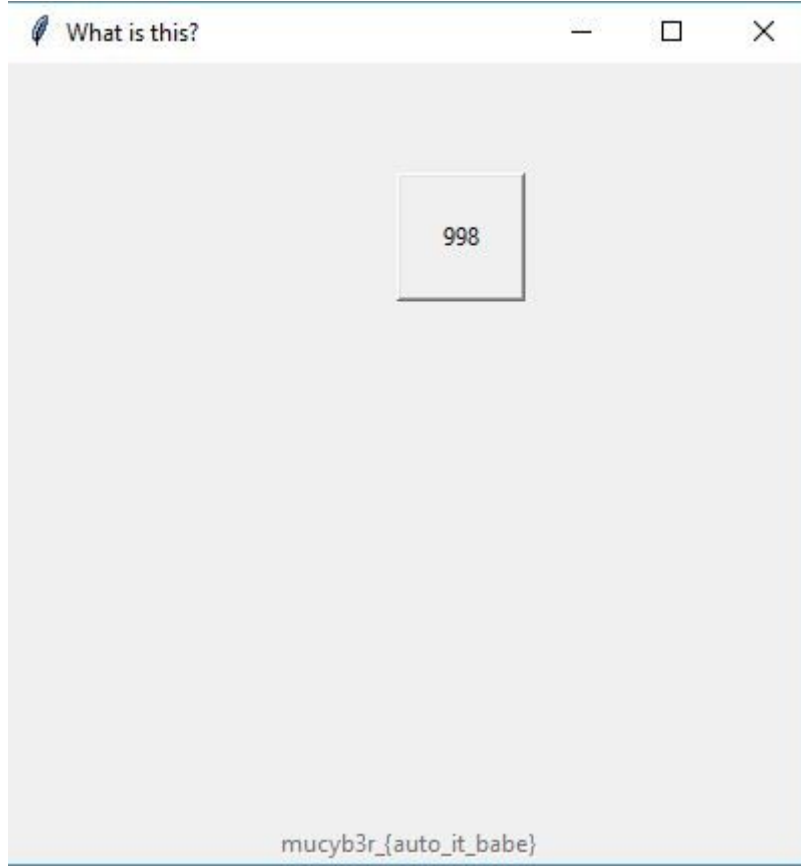
Output:

```
mucyb3r_{gut3n_m0rg3n}
```

flag: mucyb3r_{gut3n_m0rg3n}

998 mi? - 400

Bu sorumuzda karşımıza Mu-Cyber.exe adlı bir dosya geliyordu. Dosyayı açtığımızda fareyi üzerine getirdiğimizde kayan bir buton vardı. Butona tıklayabilmek için TAB+ENTER tuşlarına 998 kez basmamız gerekiyordu. Kısa bir yol olarak basit bir Autoit scripti yazarak kısa sürede flag değerine ulaşmamız mümkündü.



flag: mucyb3r_{auto_it_babe}

Ne Diyo Bu? - 500

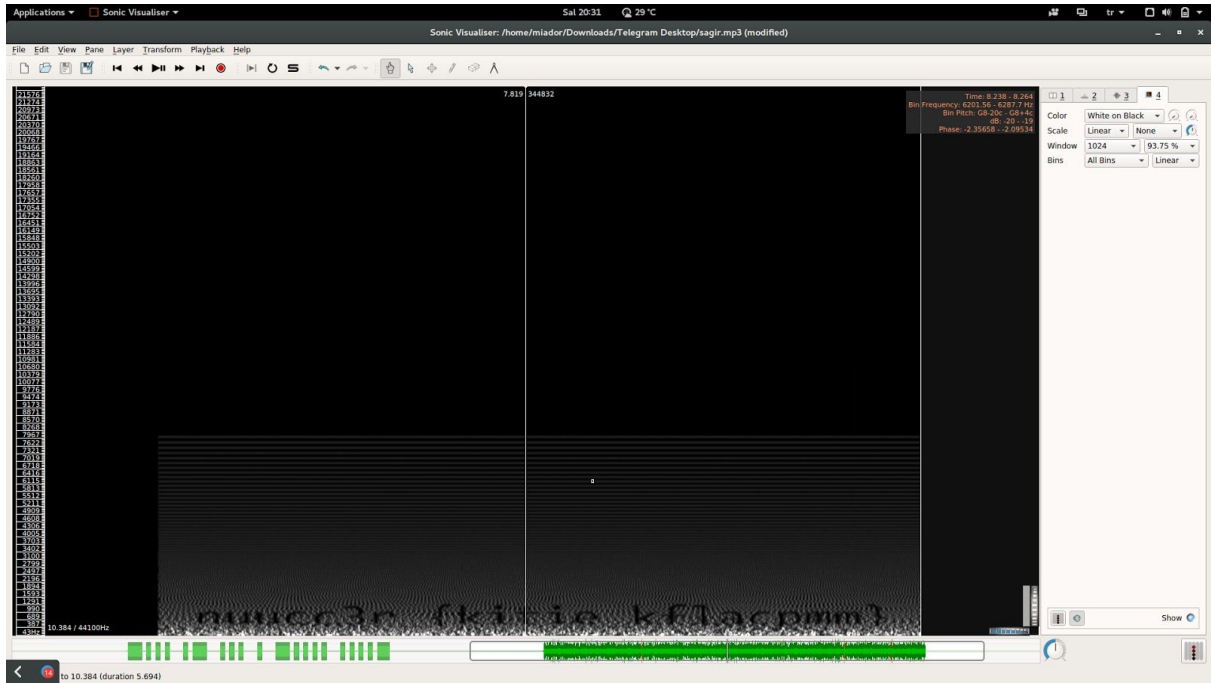
Bu sorumuzda Mors Alfabesi ile kodlanmış bir ses dosyası vardı. Flag değerine ulaşabilmek için dosyayı herhangi bir online Morse Decoder sitesinden decode edip vigenere kodumuz için gerekli olan key değerini buluyorduk.

Or analyse an audio file containing Morse code:



BASE64 ##

Ardından dosyayı Sonic Visualiser adlı ses programı ile açıp özellikleri Spectrogram sekmesinden şekildeki gibi ayarladığımızda karşımıza bir satır yazı geliyordu.



Ardından bu satırda yazanları online bir Vigenere Cipher yardımıyla key değerimizi girerek flag değerine ulaşıyoruz.

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:

GO

Results

mucyb3r_{sesim_geliyomu}

Vigenere Cipher - dCode

Tag(s) : Cryptography, Poly-Alphabetic Cipher

dCode and you

dCode is free and its tools are a valuable help in games, puzzles and problems to solve every day! You have a problem, an idea for a project, a specific need and dCode can not (yet) help you? You need custom development? [Contact-me!](#)

Sponsored ads

Vigenere Decoder

★ VIGENERE CIPHERTEXT

☒ KNOWING THE KEY:

☐ KNOWING THE KEY-LENGTH, SIZE:

☐ KNOWING ONLY A PARTIAL KEY:

☐ KNOWING A PLAINTEXT WORD:

☐ TRY A COMMON-WORDS DICTIONARY ATTACK

☐ TRY TO DECRYPT AUTOMATICALLY (STATISTICAL ANALYSIS)

☒ ALPHABET

DECRYPT VIGENERE


flag: mucyb3r_{sesim_geliyomu}

Nişasta - 1000

Bu sorumuz herhalde bütün yarışmacılarımızı beynini yakmıştır :)

Soruda sonradan [Twitter Adresimizde](#) verilen ipucundan yola çıkarak Google arama motoruna "2011 Erzurum" yazdığımızda ilk çıkan arama sonucunda kış olimpiyatlarını görüyoruz.

Ardından [bu linke](#) tıkladığımızda alt kısımda Dünya Üniversite Oyunları kısmında yaz olimpiyatlarının yapıldığı yıllar yazıyordu.

Yıl	Oyun	Yaz Üniversite Oyunları
1959	I	Torino,  İtalya
1960		—
1961	II	Sofya,  Bulgaristan
1962		—
1963	III	Porto Alegre,  Brezilya
1964		—
1965	IV	Budapeşte,  Macaristan
1966		—
1967	V	Tokyo,  Japonya
1968		—
1970	VI	Torino,  İtalya
1972		—
1973	VII	Moskova,  SSCB
1975	VIII	Roma,  İtalya
1977	IX	Sofya,  Bulgaristan
1978		—
1979	X	Mexico City,  Meksika
1981	XI	Bükreş,  Romanya
1983	XII	Edmonton, Alberta,  Kanada
1985	XIII	Kobe,  Japonya
1987	XIV	Zagreb,  Yugoslavya
1989	XV	Duisburg,  Almanya
1991	XVI	Sheffield,  Birleşik Krallık
1993	XVII	Buffalo, New York,  ABD
1995	XVIII	Fukuoka,  Japonya
1997	XIX	Sicilya,  İtalya
1999	XX	Palma de Mallorca,  İspanya
2001	XXI	Pekin,  Çin
2003	XXII	Daegu,  Güney Kore
2005	XXIII	İzmir,  Türkiye
2007	XXIV	Bangkok,  Tayland
2009	XXV	Belgrad,  Sırbistan
2011	XXVI	Shenzhen,  Çin
2013	XXVII	Kazan,  Rusya
2015	XXVIII	Gwangju,  Güney Kore
2017	XXIX	Taipei,  Tayvan
2019	XXX	Napoli,  İtalya

Yılları verilen sırayla yazdığımızda nişastanın hidroliz edilmesiyle oluşan karbonhidrat grubunun ismi olan DEKSTRİN flag değeri geliyordu.

1989	D	uisburg
1983	E	dmenton
1985	K	obe
1961	S	ofya
2017	T	aipei
1975	R	oma
2005	I	zmir
2019	N	apoli

flag: mucyb3r_{dekstrin}