Home of CTF: https://2023.knightctf.com/
Team: Obi0n3

Info
[+] Your team can submit a maximum of 3 incorrect flags per minute!

[+] Your team will have a maximum of 10 flag submission attempts per challenge.

Basic

Please join our Discord server and read the rules to get your flag.

```
01001011 01000011 01010100 01000110 01111011 01110111
00110011 01001100 01100011 00110000 01001101 00110011
01011111 01010100 00110000 01011111 01001011 01101110
01101001 01100111 01101000 01110100 01000011 01010100
01000110 01111101
```

Converted from Binary

```
KCTF{w3Lc0M3_T0_KnightCTF}
```

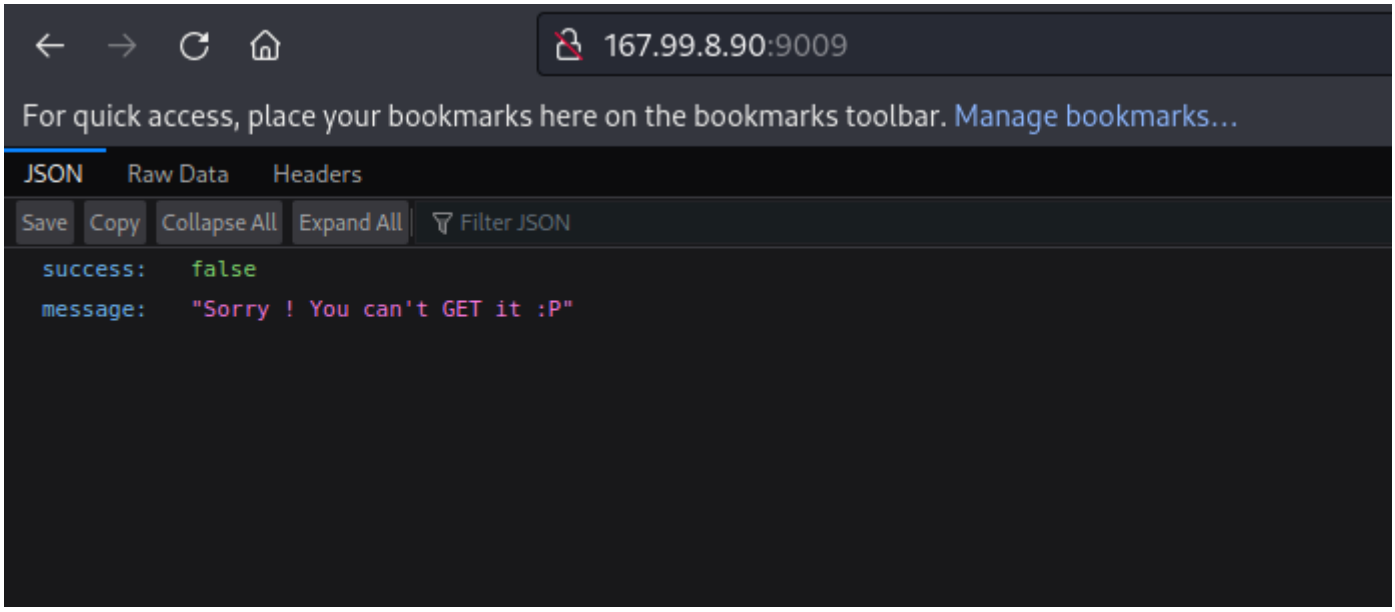
Web/API

#API

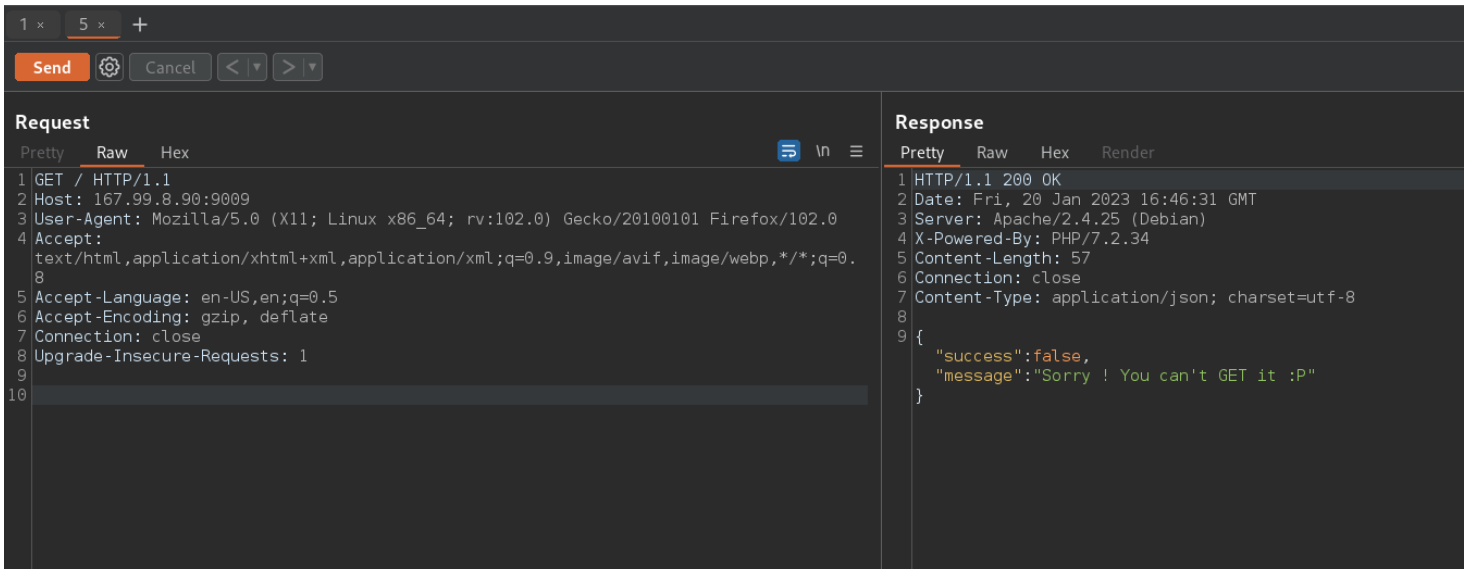
Can you GET the flag from the API ?

```
Link provided: http://167.99.8.90:9009/
```

We would go to the site and get this.



We took it to Repeater in Brup to play around



I tried to changed

OSINT

An orchestra was held where this product was mined.What is the name of the organization the conductor of the orchestra leads as a president?

Demo Flag: KCTF{Flag_HeRe}

*File Provided

INfo: http://philharmonic.lg.ua/en/

Crypto

Factorie

Have you ever heard of prime factors? The file `challenge.txt` contains a number that has two prime factors. Can you find them?

```
n: 217409621103282308493223903656649609320628 0423
```

Demo Flag: KCTF{small-number_big-number}

Resource: https://www.thecalculator.co/math/Factoring-Calculator-39.html
Resource: https://www.random-science-tools.com/maths/prime-factors.htm

```
KCTF{2-19}
KCTF{2-491}
```

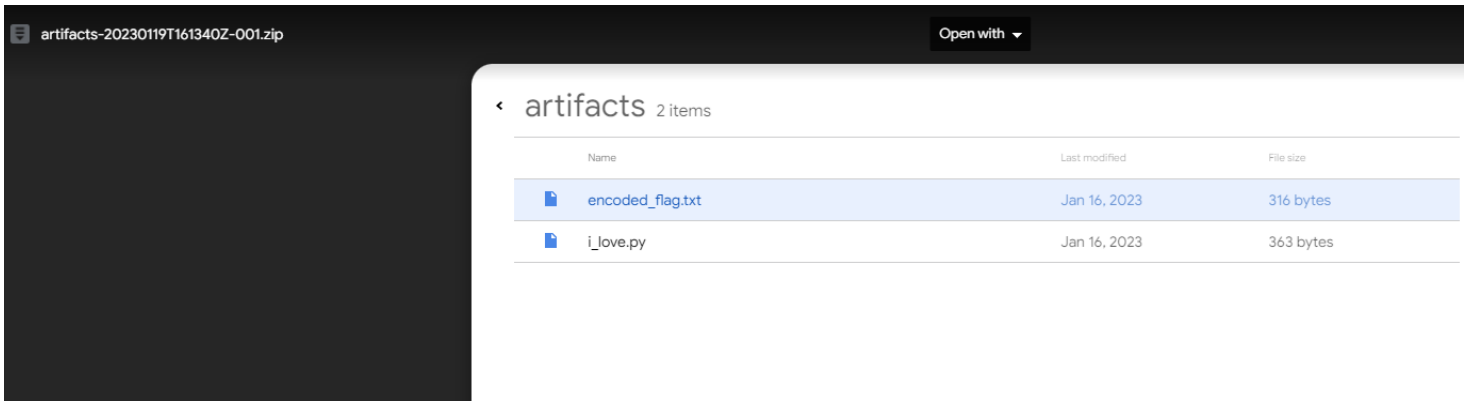
```
KCTF{2-19}
KCTF{2-1879}
KCTF{7-23}
KCTF{7-37875710256959}
KCTF{2-3}
KCTF{2-23}
KCTF{2-37875710256959}
```

I Love Pi

Isaac Newton left me this piece of code and a message. Can you help me decode this...

POC

We get some files and they look to be dealing in python.



I take it over to Geany to see what the py file does

```python
import base64

lengths = [--REDACTED--]
flag = "KCTF{*******************************}"

# len(lengths) = 10
# len(flag) = 39

s = 0
encoded_flag = ""
for l in lengths:
    seg = flag[s:s+l]
    for _ in range(len(seg)):
        seg = base64.b64encode(seg.encode('ascii')).decode('ascii')
    s+=l
    encoded_flag += seg

print(encoded_flag)
```

I can see that it take a file and it decodes the base64 to ASCII, looks to be encoded in a way. Lets run it and see what it says

```
┌──(kali㉿kali)-[~/Desktop/artifacts]
└─$ python ./i_love.py encoded_flag.txt
  File "/home/kali/Desktop/artifacts/./i_love.py", line 3
    lengths = [--REDACTED--]
                           ^
SyntaxError: invalid syntax

┌──(kali㉿kali)-[~/Desktop/artifacts]
└─$
```

From the output there is an issue with line 3. Lets look again.

```python
1  import base64
2
3  lengths = [--REDACTED--]
4  flag = "KCTF{*******************************}"
5
6  # len(lengths) = 10
7  # len(flag) = 39
```

From what I can tell there is variables that are commented out. In the lengths variable I changed it from Redacted to 10.

```python
import base64

lengths = [10]
flag = "KCTF{******************************}"

# len(lengths) = 10
# len(flag) = 39
```

Lets run it again

```
┌──(root㉿kali)-[/home/kali/Desktop/artifacts]
└─# python ./i_love.py encoded_flag.txt
Vm0wd2QyVkZOVWhUV0d4V1YwZG9WRll3Wkc5V01WbDNXa2M1V0ZadGVIbFhhMXBQVmpGYWRHVkVRbUZXVjFKSVdWZDRZV014VG5OWGJGcFhaV3RhU1Z
adGVHRlpWMUpJVm10a2FGSnRhRmxWTUZaTFYxWmtXR1JIUmxSTmF6VjVWRlphVjFZeVNraGhSbXhXVFVaYVRGUnRlR0ZqTVdSMFVteGtUbFp1UWxoV1
JscFhWakpHU0ZadVJsSldSM001

┌──(root㉿kali)-[/home/kali/Desktop/artifacts]
└─# echo "Vm0wd2QyVkZOVWhUV0d4V1YwZG9WRll3Wkc5V01WbDNXa2M1V0ZadGVIbFhhMXBQVmpGYWRHVkVRbUZXVjFKSVdWZDRZV014VG5OWGJGc
FhaV3RhU1ZadGVHRlpWMUpJVm10a2FGSnRhRmxWTUZaTFYxWmtXR1JIUmxSTmF6VjVWRlphVjFZeVNraGhSbXhXVFVaYVRGUnRlR0ZqTVdSMFVteGtU
bFp1UWxoV1JscFhWakpHU0ZadVJsSldSM001" | base64 -d
Vm0wd2VFNUhTWGxWV0doVFYwZG9WMVl3Wkc5WFZteHlXa1pPVjFadGVEQmFWV1JIWVd4YWMxTnNXbFpXZWtaSVZteGFZV1JIVmtkaFJtaFlVMFZLV1Z
kWGRHRlRNazV5VFZaV1YySkhhRmxWTUZaTFRteGFjMWR0UmxkTlZuQlhWRlpXVjJGSFZuRlJWR3M5

┌──(root㉿kali)-[/home/kali/Desktop/artifacts]
└─# echo "Vm0wd2VFNUhTWGxWV0doVFYwZG9WMVl3Wkc5WFZteHlXa1pPVjFadGVEQmFWV1JIWVd4YWMxTnNXbFpXZWtaSVZteGFZV1JIVmtkaFJta
FlVMFZLV1ZkWGRHRlRNazV5VFZaV1YySkhhRmxWTUZaTFRteGFjMWR0UmxkTlZuQlhWRlpXVjJGSFZuRlJWR3M5" | base64 -d
Vm0weE5HSXlVWGhTV0doV1YwZG9XVmxyWkZOV1ZteDBaVWRHYWxac1NsWlZWekZIVmxaYWRHVkdhRmhYU0VKWVdXdGFTMk5yTVZWV2JHaFlVMFZLTmx
ac1dtRldNVnBXVFZWV2FHVnFRVGs9

┌──(root㉿kali)-[/home/kali/Desktop/artifacts]
└─# echo "Vm0weE5HSXlVWGhTV0doV1YwZG9XVmxyWkZOV1ZteDBaVWRHYWxac1NsWlZWekZIVmxaYWRHVkdhRmhYU0VKWVdXdGFTMk5yTVZWV2JHa
FlVMFZLTmxac1dtRldNVnBXVFZWV2FHVnFRVGs9" | base64 -d
Vm0xNGIyUXhSWGhWV0doWVlrZFNWVmx0ZUdGalZsSlZVVzFHVlZadGVGaFhXSEJYWWtaS2NrMVVWbGhYU0VKNlZsWmFWMVpWTVVWaGVqQTk=

┌──(root㉿kali)-[/home/kali/Desktop/artifacts]
└─# echo "Vm0xNGIyUXhSWGhWV0doWVlrZFNWVmx0ZUdGalZsSlZVVzFHVlZadGVGaFhXSEJYWWtaS2NrMVVWbGhYU0VKNlZsWmFWMVpWTVVWaGVqQ
Tk=" | base64 -d
Vm14b2QxRXhVWGhYYkdSVVlteGFjVlJVUW1GVVZteFhXWHBXYkZKck1UVlhXSEJ6VlZaV1ZVMUVhejA9

┌──(root㉿kali)-[/home/kali/Desktop/artifacts]
└─# echo "Vm14b2QxRXhVWGhYYkdSVVlteGFjVlJVUW1GVVZteFhXWHBXYkZKck1UVlhXSEJ6VlZaV1ZVMUVhejA9" | base64 -d
Vmxod1ExUXhXbGRUYmxacVRUQmFUVmxXWXpWbFJrMTVXWHBzVVZWVU1Eaz0=

┌──(root㉿kali)-[/home/kali/Desktop/artifacts]
└─# echo "Vmxod1ExUXhXbGRUYmxacVRUQmFUVmxXWXpWbFJrMTVXWHBzVVZWVU1Eaz0=" | base64 -d
VlhwQ1QxWldTblZqTTBaTVlWYzVlRk15WXpsUVVUMDk=

┌──(root㉿kali)-[/home/kali/Desktop/artifacts]
└─# echo "VlhwQ1QxWldTblZqTTBaTVlWYzVlRk15WXpsUVVUMDk=" | base64 -d
VXpCT1ZWSnVjM0ZMYVc5eFMyYzlQUT09

┌──(root㉿kali)-[/home/kali/Desktop/artifacts]
└─# echo "VXpCT1ZWSnVjM0ZMYVc5eFMyYzlQUT09" | base64 -d
UzBOVVJuc3FLaW9xS2c9PQ==

┌──(root㉿kali)-[/home/kali/Desktop/artifacts]
└─# echo "UzBOVVJuc3FLaW9xS2c9PQ==" | base64 -d
S0NURnsqKioqKg==

┌──(root㉿kali)-[/home/kali/Desktop/artifacts]
└─# echo "S0NURnsqKioqKg==" | base64 -d
KCTF{*****

┌──(root㉿kali)-[/home/kali/Desktop/artifacts]
└─#
```

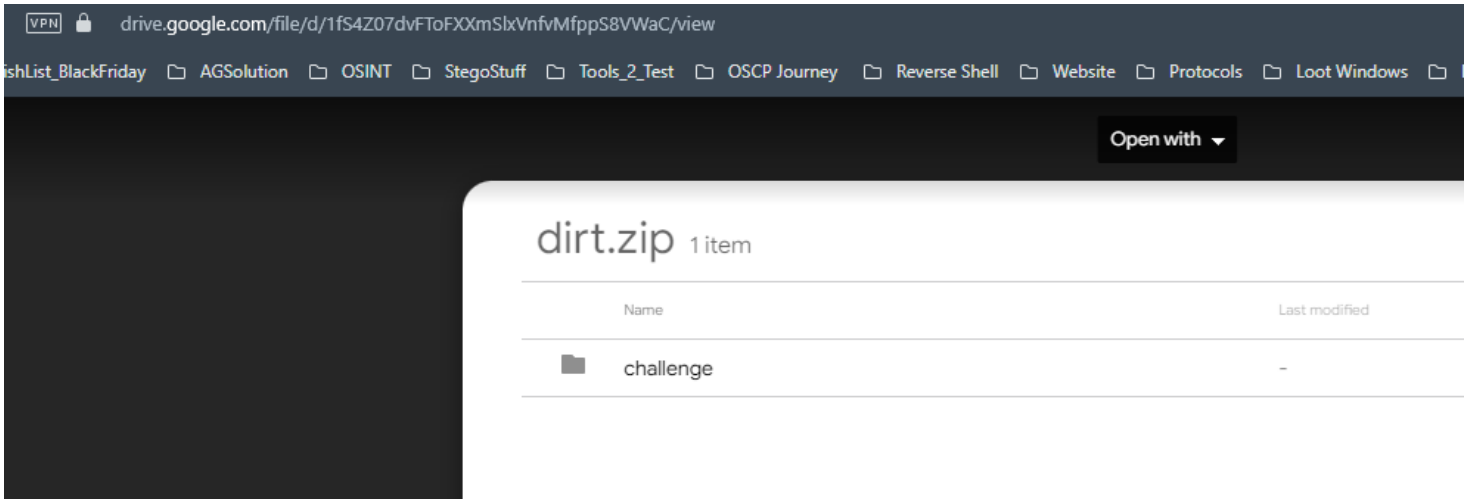
Hmmm. I hit a wall. Let go back and look at the code.

Misc

Dirt

My friend loves to travel. Can you help him get the flag?

POC
We got a zip file



Then I took it to call to see what is inside of the file

```
tree challenge
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ tree challenge
challenge
└── }
    └── s
        └── r
            └── 3
                └── d
                    └── l
                        └── 0
                            └── f
                                └── _
                                    └── 3
                                        └── d
                                            └── 1
                                                └── 5
                                                    └── n
                                                        └── 1
                                                            └── _
                                                                └── s
                                                                    └── r
                                                                        └── 3
                                                                            └── d
                                                                                └── l
                                                                                    └── 0
                                                                                        └── f
                                                                                            └── {
                                                                                                └── F
                                                                                                    └── T
                                                                                                        └── C
                                                                                                            └── K

29 directories, 0 files

┌──(kali㉿kali)-[~/Desktop]
└─$
```

The flag is backwards.

Flag

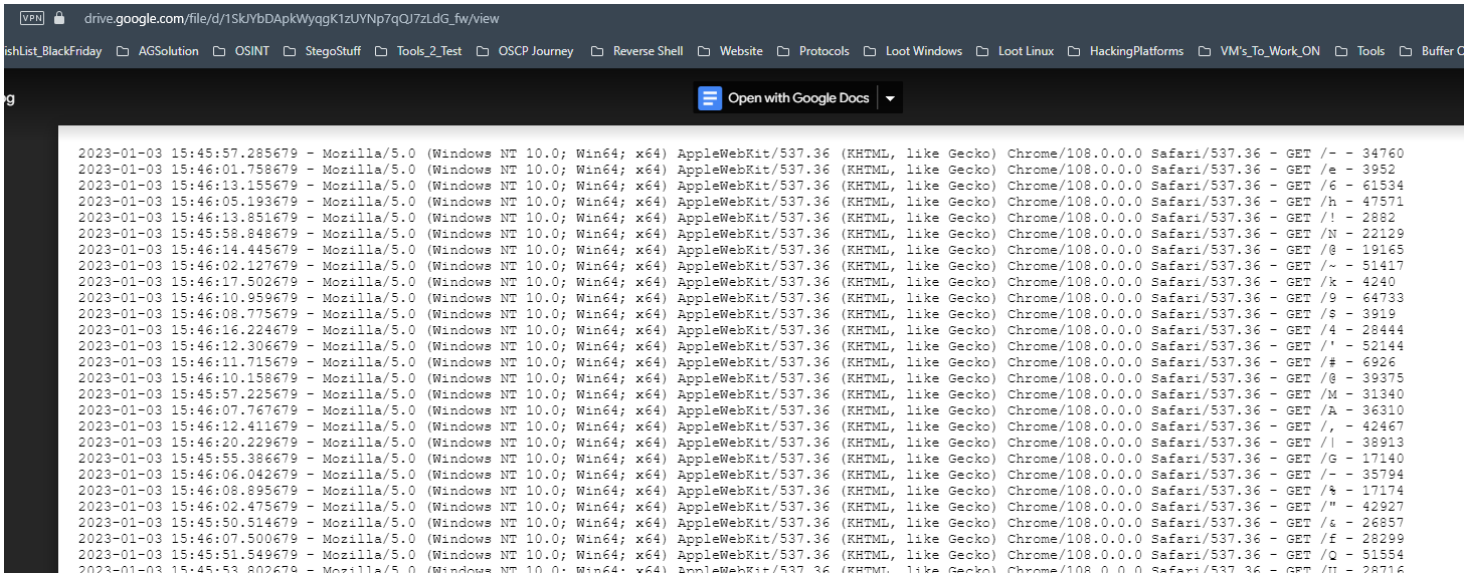
```
KCTF{f0ld3rs_1n51d3_f0ld3rs}
```

Logger

Sysadmin found an access log that contains some requests to weird endpoints. It's said that the flag lies among them. Are you smart enough to find it?

POC

We check out the file that is downloadable



From what we can see and the info about the challenge we have a logg file to sort through. Let take it to Kali and see if we can put it together.

*First thing I want to do is sort it by

Flag

Network

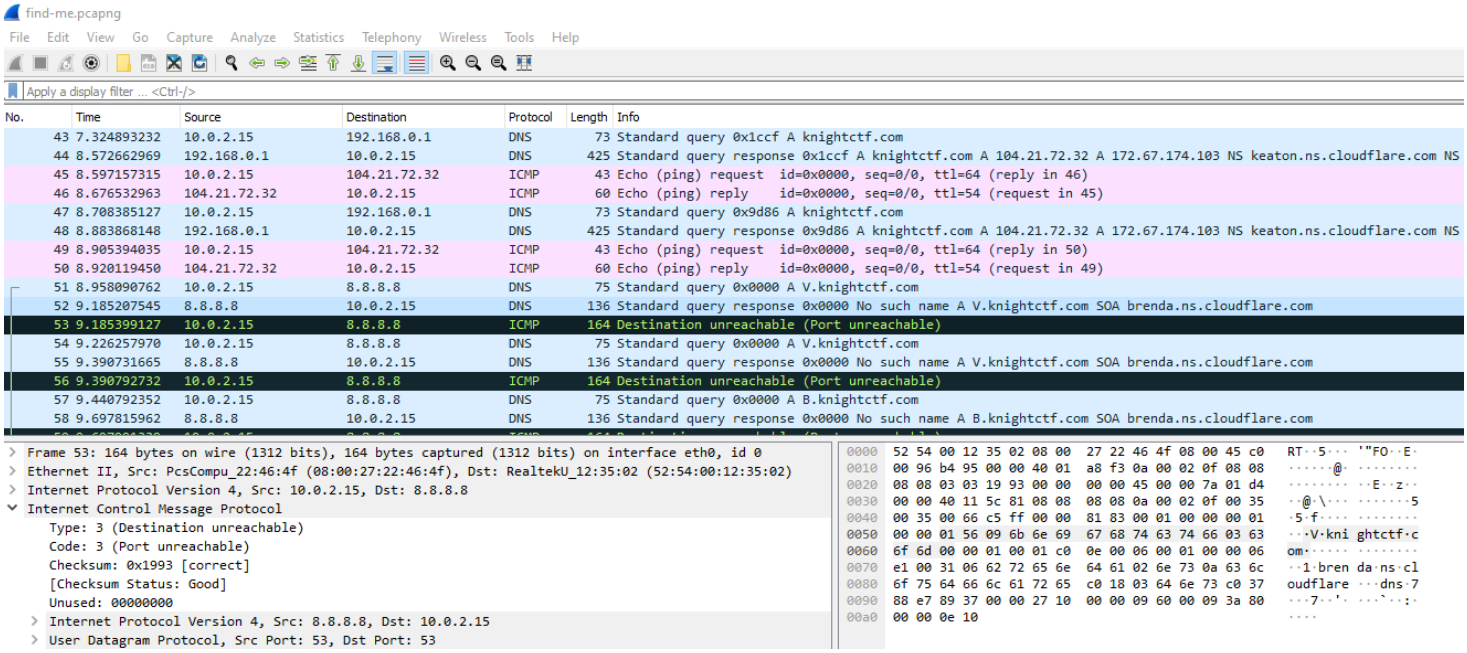
Sir vignere came to my dreams and sent me this packet capture and told me to find the flag from it which is the key to my success. I am a noob in these cases. So I need your help. Please help me find the flag. Will you?

POC

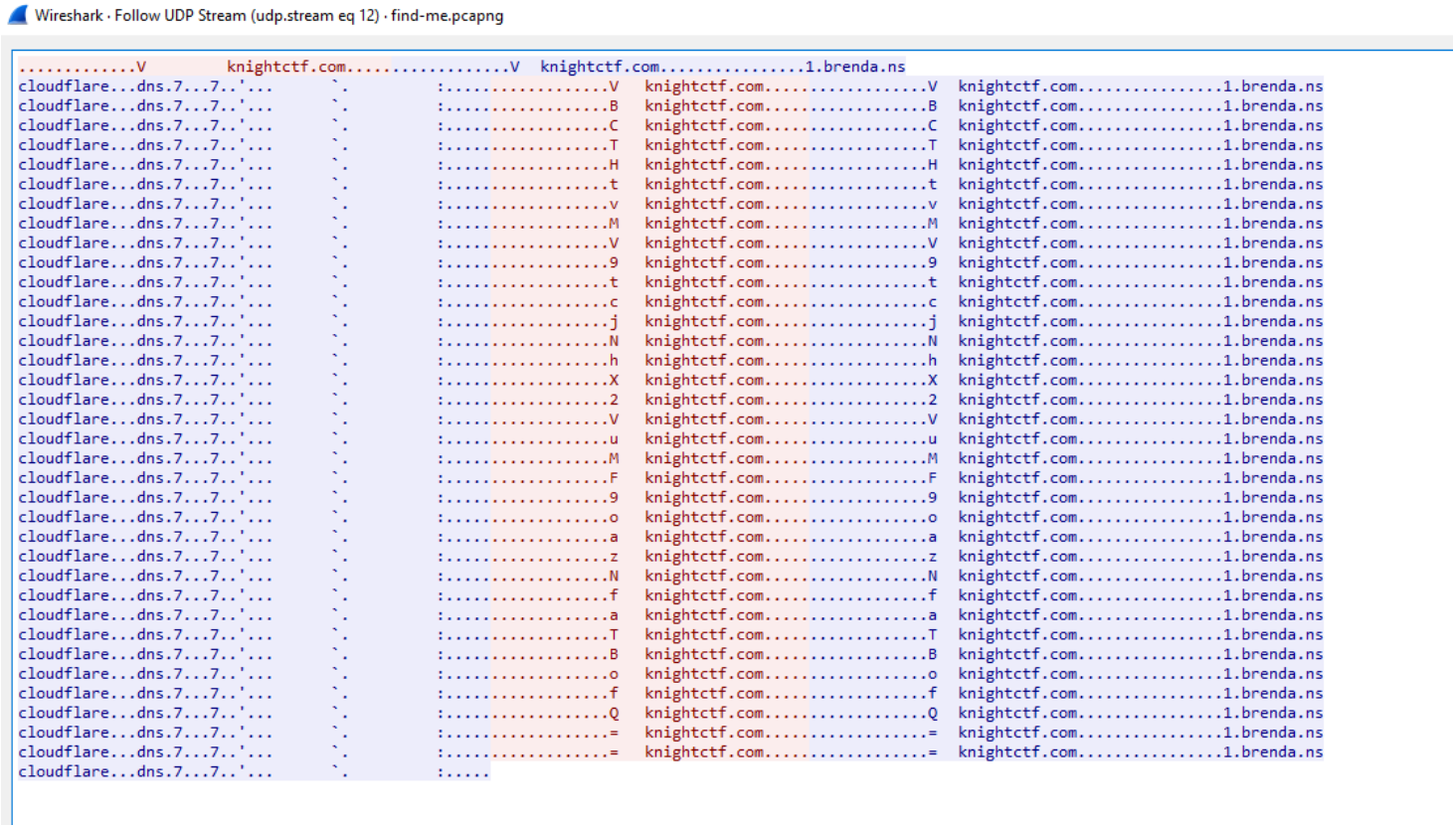
We have a pcap file. I want to see what protocols are being used the most.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	85	100.0	9728	10 k	0	0	0	85
Ethernet	100.0	85	12.2	1190	1235	0	0	0	85
Internet Protocol Version 4	100.0	85	17.5	1700	1765	0	0	0	85
User Datagram Protocol	84.7	72	5.9	576	598	0	0	0	72
Domain Name System	84.7	72	47.0	4572	4747	72	4572	4747	72
Internet Control Message Protocol	15.3	13	17.4	1690	1754	0	0	0	13
Domain Name System	15.3	13	12.6	1222	1268	13	1222	1268	13

I see that DNS and UDP are the most used protocols here. Lets see what is working.

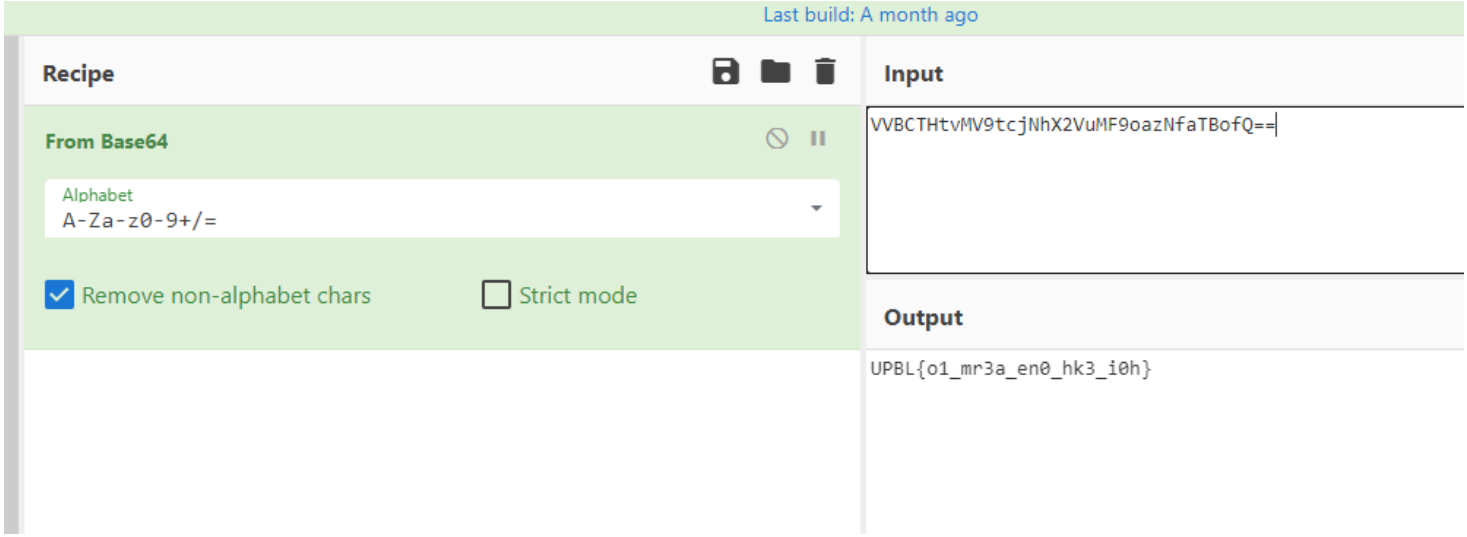


What I am interested is what is .15 sending to the DNS server 8.8.8.8, We can follow the UPD stream



Looking at the format it looks like its bas64

```
VVBCTHtvMV9tcjNhX2VuMF9oazNfaTBofQ==
```



From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

☐ Strict mode

Input

```
VVBCTHtvMV9tcjNhX2VuMF9oazNfaTBofQ==
```

Output

```
UPBL{o1_mr3a_en0_hk3_i0h}
```

We get some what a decoded output. We got a hint that this might be a vignere cihper

Reverse Engineer

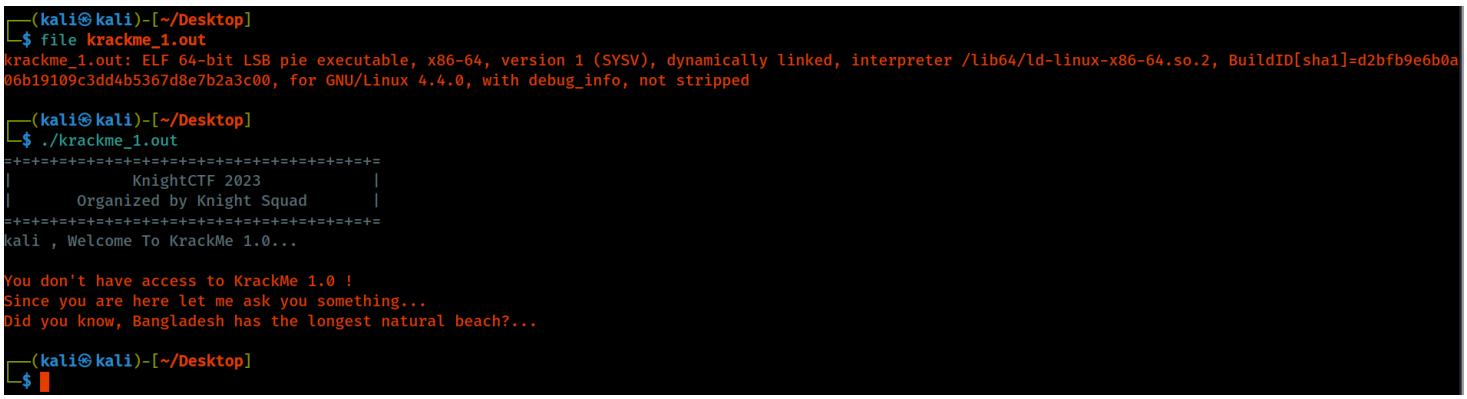
KrackME

Find the right flag from the binary.

Demo Flag: KCTF{Fl4g_H3r3}

POC

We download a file from the site and move it over to kali and check what it is.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ file krackme_1.out
krackme_1.out: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=d2bfb9e6b0a
06b19109c3dd4b5367d8e7b2a3c00, for GNU/Linux 4.4.0, with debug_info, not stripped

┌──(kali㉿kali)-[~/Desktop]
└─$ ./krackme_1.out
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
|             KnightCTF 2023             |
|       Organized by Knight Squad         |
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
kali , Welcome To KrackMe 1.0...

You don't have access to KrackMe 1.0 !
Since you are here let me ask you something...
Did you know, Bangladesh has the longest natural beach?...

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```