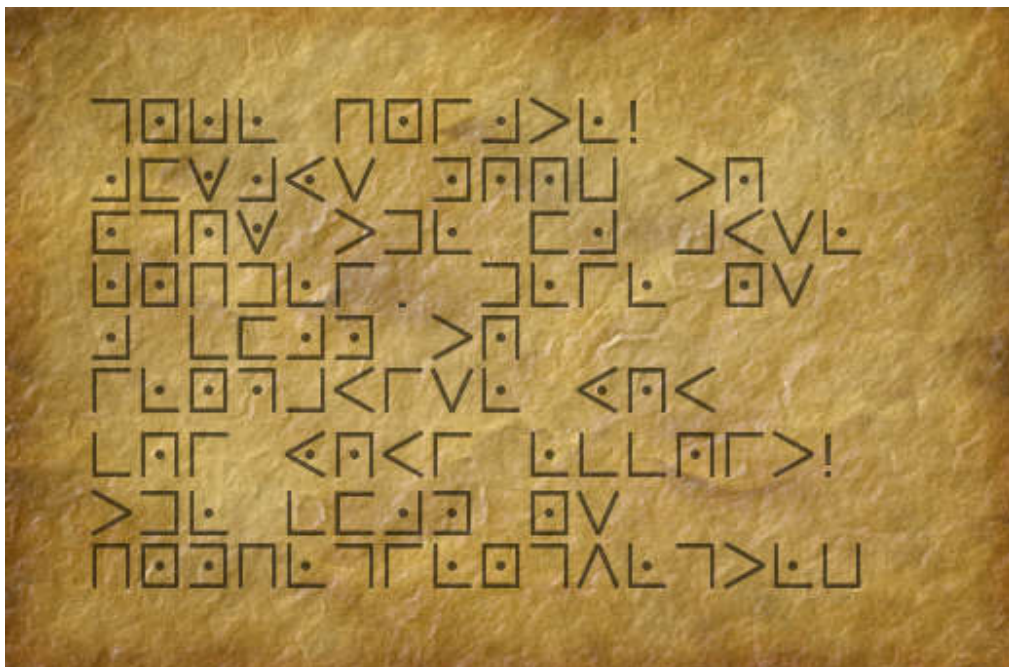


Pork Pen and Paper

Taken directly from the book: "The history of treasure maps" ...The ancient art of treasure map sketching and clue writing is frequently accompanied by a bit of pork meat to keep the writer focussed until his map was complete. There was a small decrease in popularity around 1800 due to difficult distribution of treasure maps when the senile pirate "old buzzard" started writing his cryptic guidance on live piggies...

Attachments

[porkpenpaper.png](#)



Decode met:



Result:

GNKL HNIJTL!
JFWJYS MQQB TQ
OGQW TDL FJ AUSL
KNHDLI DLIL NS
J CFJM TQ
ILNPAUISL YQU
CQI YQUI LCCQIT!
TDL CFJM NS
HNMHLGILNGVLGTLB

Monoalphabetic Substitution Decoder

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	D	F	H	J	L	N	P	R	A	C	E	G	I	P	K	O	X	S	T	U	V	W	Z	Y	Q

⇒ Alphabet Encrypt BDFHJLNPRACEGIPKOXSTUVWZYQ
 ⇒ Alphabet Decrypt JAKBLCMDNEPFGQHOZISTUVWRYX

G	N	K	L	H	N	I	J	T	L	!	J	F	W	J	Y	S	M	Q	Q	B	T
N	I	C	E	P	I	R	A	T	E	!	A	L	W	A	Y	S	G	O	O	D	T
Q	O	G	Q	W	T	D	L	F	J	A	U	S	L	K	N	H	D	L	I		
O	P	N	O	W	T	H	E	L	A	B	U	S	E	C	I	P	H	E	R		
D	L	I	L	N	S	J	C	F	J	M	T	Q	I	L	N	P	A	V	I	S	
H	E	R	E	I	S	A	F	L	A	G	T	O	R	E	I	K	B	U	R	S	
L	Y	Q	U	C	Q	I	Y	Q	U	I	L	C	C	Q	I	T	!	T	D	L	
E	Y	O	U	F	O	R	Y	O	U	R	E	F	F	O	R	T	!	T	H	E	
C	F	J	M	N	S	H	N	M	H	L	G	I	L	N	G	V	L	G	T	L	B
F	L	A	G	I	S	P	I	G	P	E	N	R	E	I	N	V	E	N	T	E	D

★ PLAINTEXT LANGUAGE

The flag is

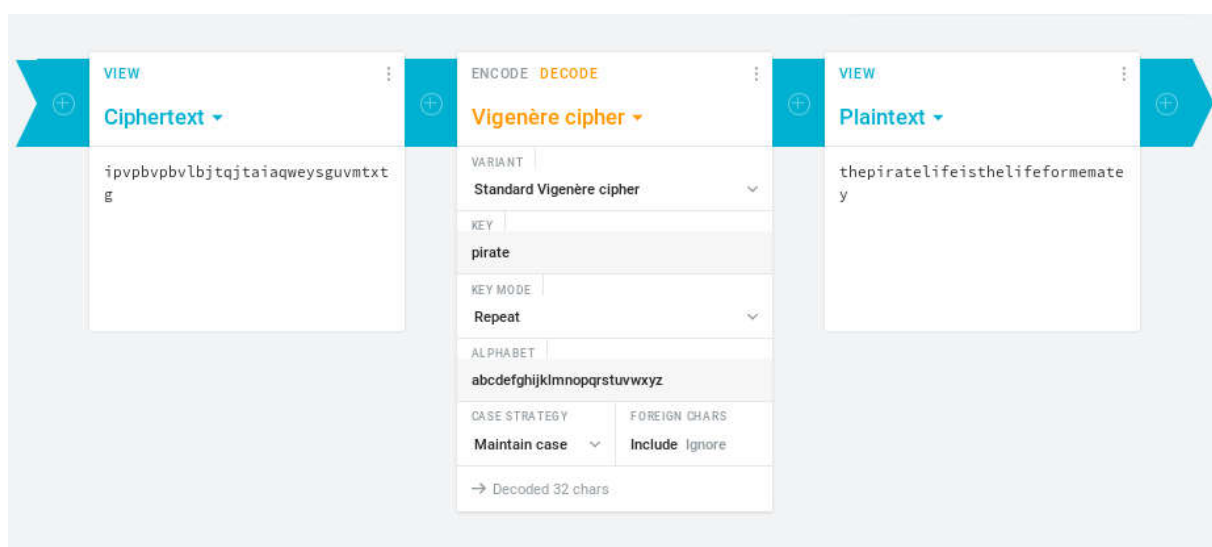
Pigpenreinvented

French Vinaigrette

A French pirate gave us the following message: `ipvpbvpbvblbjtqjtaiaqweysgumtxtg`. We asked him what to do with it and he said that we had to decode it with vinaigrette! Alas, we threw the paper in vinaigrette and nothing happened! Such a shame to throw away good food!

Points: 30

Category: CRYPTO



The screenshot shows a web interface for decoding a Vigenère cipher. It consists of three main panels:

- Ciphertext:** Contains the input message `ipvpbvpbvblbjtqjtaiaqweysgumtxtg`.
- Vigenère cipher:** The central configuration panel with the following settings:
 - Variant: Standard Vigenère cipher
 - Key: pirate
 - Key Mode: Repeat
 - Alphabet: abcdefghijklmnopqrstuvwxyz
 - Case Strategy: Maintain case
 - Foreign Chars: Include Ignore
 - Decoded 32 chars
- Plaintext:** Contains the decoded message `thepiratelifeisthelifeformematey`.

Flag: `thepiratelifeisthelifeformematey`

ICBM

Yarr me Matey, some fellow buccanneers have left us a chest. Inside is a Nuclear launch administration panel, however we can't seem to be able to login to obtain the Nuclear Launch code. Make us proud, ye landlubbber!

<https://drive.google.com/open?id=1x1U9Brl6Js74BxjNKV2UrJ0jN0kHgZzo>

Points: 80

Category: REVERSE

Gdb:

```
gdb-peda$ n
[-----root@hades-kali:~/Desktop/HTF# ./AdminPanel-----]
RAX: 0x555555769280 ("3455441xvc@#453fnwertgh5454414325bsw4564derrr%")
```

./Adminpanel:

```
root@hades-kali:~/Desktop/HTF# ./AdminPanel
Welcome General!

Please enter your password:
3455441xvc@#453fnwertgh5454414325bsw4564derrr%
sh: 1: cls: not found
Please make a choice:
1. Generate nuclear launch code
2. Exit
> 1

Nuclear launch code: BQ=7?K~Yke3o\FDDT^

Press any key to exit
█
```

Flag = BQ=7?K~Yke3o\FDDT^

Nmap -p-:

```
|=====|  
|          UGlyYXRlEdhdGV3YXkgdjAuMQ==          |  
| QWhveSEgc29sdmUgdGgnlGNhcHRjaGEgdCcgY29udGludWUh |  
|=====|  
MzE3MDgrNDQxOTY3
```

WWUgYmUgdG9vIHNSb3cgZmVlHRoaXMhEdldCB5ZXIgc2hpdCB0b2dldGhlciE=

Base 64:

Pirate Gateway v0.1

Ahoy! solve th' captcha t' continue!

....

MzE3MDgrNDQxOTY3

....

Ye be too slow fer this! Get yer shit together!

Sunflower:

- Enigma machine
- Rotoren waren grote letters in duitse tekst

Pirate Net

- Eerst alle dns request naar file (de tekst)

```
H4sIAHkEmlsAA7O2HgvDCXABAB91xi6RAQAA
H4sIAHoEmlsAA7O2HgvDCXABAB91xi6RAQAA
H4sIAHoEmlsAA7O2HgvDCXABAB91xi6RAQAA
H4sIAHsEmlsAA7O2HgvDCXABAB91xi6RAQAA
H4sIAHsEmlsAA7O2HgvDCXABAB91xi6RAQAA
H4sIAHvEmlsAA7O2HgvDCXABAB91xi6RAQAA
H4sIAH0EmlsAA7O2HgvDCXABAB91xi6RAQAA
H4sIAH0EmlsAA7O2HgvDCXABAB91xi6RAQAA
H4sIAH4EmlsAA7O2HgvDCXABAB91xi6RAQAA
H4sIAH4EmlsAA7O2HgvDCXABAB91xi6RAQAA
H4sIAH8EmlsAA7O2HgvDCXABAB91xi6RAQAA
H4sIAH8EmlsAA7O2HpvJAXY8glUB9oN5IFuADyr41nkQEAAA==
H4sIAIAEmlsAA7O2HpvJAT4Eg0BtoN5IFuADXH6P1kQEAAA==
H4sIAIAEmlsAA7O2HpvJAT4Eg0BtoN5IFuADXH6P1kQEAAA==
H4sIAIEEmlsAA7O2HpvJAXQ8BFJAAkrD6QLuRLMAFAIaGQcWRAQAA
H4sIAIEEmlsAA7O2HvJATwE09AbaLRQDLgAFF8UEkQEAAA==
H4sIAIIEmlsAA7O2HvJATwE09AbaLRQDLgAFF8UEkQEAAA==
H4sIAIMEmlsAA7O2HvJATwE09AbaLRQDLgAFF8UEkQEAAA==
H4sIAIMEmlsAA7O2HvJATwE09AbaLRQDLgAFF8UEkQEAAA==
H4sIAIQEmlsAA7O2HvJATwE09AbaLRQDLgAFF8UEkQEAAA==
H4sIAIQEmlsAA7O2HvJATwE09AbaLRQDLgAFF8UEkQEAAA==
H4sIAIUEmIsAA7O2HvJATwE09AbaLRQDLgAFF8UEkQEAAA==
H4sIAIUEmIsAA7O2HvJATwE09AbaLRQDLgAFF8UEkQEAAA==
H4sIAIYEmlsAA7O2HvJATwE09AbaLRQDLgAFF8UEkQEAAA==
H4sIAIYEmlsAA7O2HvJATwE09AbaLRQDLgAFF8UEkQEAAA==
H4sIAIEmlsAA7O2HvJATwE09AbaLRQDLgAFF8UEkQEAAA==
H4sIAIEmlsAA7O2HvJATwE09AbaLRQDLgAFF8UEkQEAAA==
H4sIAIcEmlsAA7O2HvJATwE09AbaLRQDLgAFF8UEkQEAAA==
H4sIAIcEmlsAA7O2HvJATwE09AbaLRQDLgAFF8UEkQEAAA==
H4sIAIkEmlsAA7O2HvJATwE09AbaLRQDLgAFF8UEkQEAAA==
H4sIAIkEmlsAA7O2HvJAXQ801AfaLRQDLgBCrHc5kQEAAA==
H4sIAIoEmlsAA7O2HgvDCXABAB91xi6RAQAA
H4sIAIoEmlsAA7O2HgvDCXABAB91xi6RAQAA
H4sIAIsEmlsAA7O2HgvDCXABAB91xi6RAQAA
H4sIAIsEmlsAA7O2HgvDCXABAB91xi6RAQAA
H4sIAIwEmlsAA7O2HgvDCXABAB91xi6RAQAA
H4sIAI0EmlsAA7O2HgvDCXABAB91xi6RAQAA
H4sIAI0EmlsAA7O2HgvDCXABAB91xi6RAQAA
H4sIAI4EmlsAA7O2HgvDCXABAB91xi6RAQAA
H4sIAI4EmlsAA7O2Hgv0B0rqbBRwAQayZv4IkQEAAA==
```

- Deze vanuit base64 vertaald
- De eerste 3bites waren van gzip data

```
00000000: 1f8b 0800 7904 9a5b 0003 b3b6 1e05 8309  ....y..[.....
00000010: 7001 001f 75c6 2e91 0100 00                p...u.....
```

- Script gebruikt om te uncompressen
- File uitgezoemd

Steven seagul;

- Steghide

```
steghide extract -sf steven/steven-seagull.jpg
```

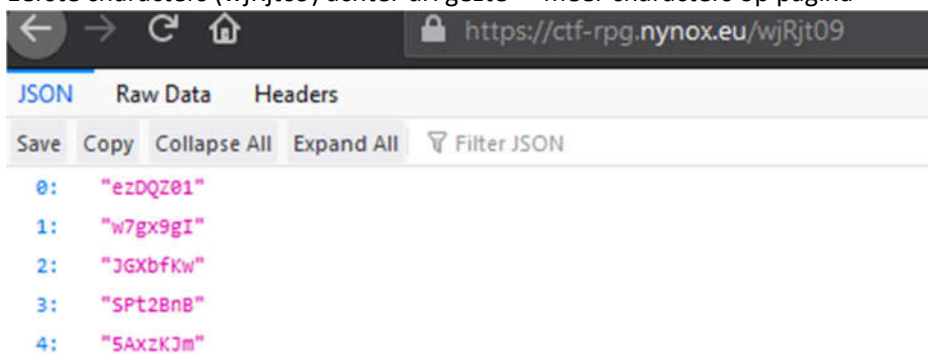
- Dan was er een squashfs
- Die mounten
- Dan de stash openen

```
In case i forgot where me stash was:  
  
https://www.dropbox.com/s/3nezkun9p4vj1bg/StevenSeagullWare.mkv?dl=0  
  
Hope me mateys don't find out i'm not taking care of the ship!
```

- Video downloaden met wget
- Hierin zat een archive met mp4 video
- Daarin zat een flag gevonden met strings

Angry parrot

- Eerst naar site gegaan
- Eerste characters (wjRjt09) achter url gezet -> meer characters op pagina



-
- Andere pogingen werkte soms niet
- Script gevonden om alles te testen om de juiste cookies te vinden:


```

import requests
import urllib

def fetch(suburl):
    print '-----'
    global baseurl
    global cookie
    url = baseurl+suburl
    print url
    r = requests.get(url, cookies=cookie)
    if "This path leads nowhere" in r.text:
        return
    print r.text
    x = r.text.replace('[', '').replace(']', '').replace("'", '')
    suburls = x.split(',')
    if len(suburls) != 5:
        if "cookie" in r.text or "COOKIE" in r.text:
            print r.cookies
            cookie[r.cookies.keys()[0]] = urllib.unquote(r.cookies[r.cookies.keys()
[0]].decode('utf8'))
            for sub in suburls:
                fetch(suburl+"/"+sub)

baseurl = "http://51.68.252.196:8082"
cookie = {}
fetch('')

```

- Die info kwam in een file met daarin de flag

Jack The Swimmer

- Uitgetekend in paint

Very interesting marooned file

- Deze herkende ik als vim -> uitgetypt in vim

Strange bar;

- Stl file -> 3D file
- Geopend in blender
- Naarbinnen gekeken
- De bovenkant eraf gedaan
- String gevonden

Davy Jones Double locker

- 2*sha256 decoded