Solution CTF

version 2.0.1



Titre : Message Digest

Le participant doit utiliser un MD5 decrypter pour ce hash.

e4e3f56f18319e998fdee74b98509aec

Lien : <https://md5decrypt.net/#answer>

Password : C0br4

Pays : Canada

Titre : Ave

Le participant doit utiliser la méthode de décalage +17 de César.

Alcvj Tvjri rmrzk vl lev sfeev zuvv ! Cv dfk uv grjjv vjk Rcvr artkr vjk.

Lien : <https://www.dcode.fr/chiffre-cesar>

Password : Alea jacta est.

Pays : Italy

Titre : Tout pareil, c’était évident !

Le participant doit utiliser un Base64 decrypter pour ce hash.

QmFzZTY0IGVzdCBjYXJhY3TDqXJpc8OpIHBhciBsZSDDqWdhbCDDoCBsYSBmaW4gISBMZSBtb3QgZGUgcGFzc2UgZXN0IEYzbDFjMXQ0dDEwbg==

Lien : <https://www.base64decode.org/>

Password : F3l1c1t4t10n

Pays : Romania

Titre : Des nombres partout, aled !

Le participant doit convertir l’ascii en caractère ou ascii to text.

76 101 32 109 111 116 32 100 101 32 112 97 115 115 101 32 100 101 32 99 101 32 99 104 97 108 108 101 110 103 101 32 101 115 116 32 65 115 99 49 49 32 105 115 32 99 48 48 108

Lien : <https://www.dcode.fr/code-ascii>

Password : Asc11 is c00l

Pays : South Sudan

Titre : J’adore les cigares de ce pays !

Le participant doit utiliser %10(modulo) et la clé.

Hash : 12743 09231 66 36204 52026

Clé : 86456

Exemple : 12743 – 86456 = 36395 (36 = G, 39 = I etc)

Lien : <http://www.cryptage.org/chiffre-che-guevara.html>

Password : Gilbert Vernam

Pays : Cuba

Titre : Le programme a un bug ?

Le participant doit convertir la séquence binaire en texte.

01100010 00110001 01101110 00110100 00110001 01110010 00110011 01011111 00110001 01110011 01011111 01000110 01110101 01101110

Lien : <https://www.rapidtables.com/convert/number/binary-to-ascii.html>

Password : b1n41r3\_1s\_Cool

Pays : Zimbabwe

Titre : tu tuututu tuuuuuuu tuutu

Le participant doit utiliser un Morse Decrypter.

.-.. . / -- --- - / -.. . / .--. .- ... ... . / . ... - / -- --- .-. ... . / ... .- -- ..- . .-..

Lien : [https://www.dcode.fr/code-morse#q2](https://www.dcode.fr/code-morse%23q2)

Password : Morse Samuel

Pays : Greenland

Titre : Alphabet Trifide

Le participant doit utiliser un Trilitère Decrypter.

BABABC BAABCBCAC ABBABC BCAAABCCBCCBABC ABCCCBCAC

CACCCABBABABBBACACABCCCAABC

Lien : <https://www.dcode.fr/chiffre-trilitere>

Password : TRILITERE

Pays : Niger

Titre : Trithème

Le participant doit utiliser la technique Ave Maria de Trithème.

Un monde sans fin pour toujours

En une infinité irrévocablement

Au paradis durablement

Un monde sans fin dans la gloire

Dans la béatitude à tout jamais

Lien : <https://www.dcode.fr/ave-maria-tritheme>

Password : CODINGCLUB

Pays : China

Titre : Secret message

Le participant doit utiliser la technique du Steg of the Dump.

J＇aｉｍe bieｎ lａ ｃybeｒséϲｕrｉｔé ! #HackerSisiLaFamille

Lien : <https://holloway.nz/steg/> (Attention, des espaces sont cachés dans la description et doivent être utilisé pour trouver le flag)

Password : stegdump

Pays : Japan

Titre : Secret message v2

Le participant doit uniquement se concentrer sur les premiers mots de chaque phrase.

C’est ici que se cache le mot de passe.

Pass est la version anglaise de passe.

Le plus drôle dans tous ça, c’est que tu ne comprends pas le but de ces phrases.

Mot de passe très facile à trouver… toujours pas ? Un effort !

Passe ton chemin si tu n’y arrives pas mwouahhahahah.

Ceci est hilarant, je me délecte de vos réactions !

Est-ce que tu as enfin trouvé le mot de passe ?

Inutile de continuer plus loin, c’est la fin du texte :)

Password : Pass

Pays : Germany

Titre : C’est un peu comme le binaire et le décimal mais c’est aucun des deux

Le participant doit convertir le code hexa en texte.

48 65 78 61 5f 70 6f 77 65 72 5f 66 65 61 74 5f 45 70 69 74 65 63 68

Lien : <http://www.unit-conversion.info/texttools/hexadecimal/>

Password : Hexa\_power\_feat\_Epitech

Pays : Bangladesh

Titre : Code Talker

Le participant doit utiliser la technique de navajo decrypt.

DIBEH-YAZZIE AH-JAH BE-TAS-TNI NE-AHS-JAH THAN-ZIE BE AH-NAH CLA-GI-AIH BE-LA-SANA DIBEH DIBEH DZEH DZEH DIBEH A-WOH TSAH TSE-NILL A-KEH-DI-GLINI TSE-NILL YIL-DOI A-KHA

Lien : <https://www.dcode.fr/code-navajo>

Password : NAVAJO

Pays : Guyana

Titre : C’est comme l'hexadécimal mais sans l'hexa

Le participant doit convertir le code décimal en texte.

76 101 32 109 111 116 32 100 101 32 112 97 115 115 101 32 101 115 116 32 121 117 105 111 52 50

Lien : <https://cryptii.com/pipes/decimal-text>

Password : yuio42

Pays : North Korea

Titre : UU code

Le participant doit utiliser un UU decoder. Cependant il ne doit pas mettre les lignes begin et end pour le decoder.

begin 644 dcode\_uuencode

G3&4@;6]T(&1E('!A<W-E(&5S="!555]E;F,P9&5?:7-N=%]H-')D

`

end

Lien : <https://www.dcode.fr/encodage-uu>

Password : UU\_enc0de\_isnt\_h4rd

Pays : Spain

Titre : Sah quel plaisir !

Le participant doit tout simple chiffrer « quel plaisir ! » en sha-256.

Lien : [https://md5decrypt.net/Sha256/#answer](https://md5decrypt.net/Sha256/%23answer)

Password : 40cdfb86e29a00e99f95b804868a733115d5a6a216e1051d2b238db8fd31cb0c

Pays : Uzbekistan

Titre : Rozier

Le participant doit utiliser un Rozier Decrypter sur ce hash.

WXXZRIBATDDCJPEVZOGSDNEFM

Lien : <https://www.dcode.fr/chiffre-rozier>

Password : CODINGCLUB

Pays : Saudi Arabia

Titre : Ils ont tué Kenny !

Le participant doit traduire les pmff de Kenny et effectuer une recherche par la suite sur le nombre de mort de Kenny en 20 saisons.

Fpmppffmm mfmpffmmmpppmpmfmmppmmpppffmppfmm pmfmppfmm mmfmfpmmmfmffpmmppfmm pmmmpp fpmppffmffmm mpmmppfmpmppfmmfmpmpp fmpppffmffmm Pmfmpp ppmppffmp mpmmpp pfmmmmfmmfmmmpp mppfmmfmp ppmppfppp pppppfppmmmppffmpp mpmmpp ppmppfpfffmp ppmppfmffpppfmm 42

Lien : <https://www.dcode.fr/code-kenny-southpark>

Password : 55

Pays : Papua New Guinea

Titre : Primary

Le participant doit utiliser la substitution par nombre premier ou prime decrypter.

37 11 41 47 71 7 11 53 2 67 67 11 11 67 71 53 61 11 41 23 11 61

Lien : <https://www.dcode.fr/substitution-nombres-premiers>

Password : premier

Pays : Thailand

Titre : Pourrir

Le participant doit utiliser le chiffre de ROT avec une rotation de +42.

v19;@01<-??11?@m->-<A/1

Lien : <https://www.dcode.fr/chiffre-rot>

Password : Carapuce

Pays : Mozambique

Titre : C֤ÉTAUTOMATIX

Le participant devra utiliser un Blowfish Decrypter, attention seul le lien fourni permet de décrypter le hash avec la clé (CÉTAUTOMATIX). Attention de ne pas copier/coller celui du titre, un caractère supplémentaire s’y est glissé !

BTB1o18ViJWdPB7bWQGe6/TLrGcpirGEWuQz9hczu3c4LJ6LMTYIJpVvnNvJIVzY

Lien : <https://encode-decode.com/blowfish-encrypt-online/>

Password : Il\_3st\_frais\_mon\_pO1s50n

Pays : France

Titre : Detroit

Le participant devra utiliser un D3 Decrypter.

21/2/ /20/18/13/ /3/2/ /17/6/14/14/2/ /2/14/13/ /21/2/ /4/18/3/24/19/26/ /4/21/12/5/ /2/14/13/ /24/19/4/15/18/8/6/5/21/2

Lien : <https://www.dcode.fr/code-d3-detroit>

Password : le coding club est incroyable

Pays : Ukraine

Titre : Malespin

Le participant doit utiliser un Malespin Decrypter.

La pib da messa asb ringlax

Lien : <https://www.dcode.fr/argot-malespin>

Password : goinfrex

Pays : Morocco

Titre : Leet speak

Le participant doit utiliser un LSPK90 horaire Decrypter.

\_|W E[]|-- ¯¯ULL| ^-<(V\[/]W LL|(/)|-- [--{}()|UU<{v^)--|LL()^<|]

Lien : <https://www.dcode.fr/lspk90-h-leet-speak-90-degres-horaire>

Password : T0O\_EASY\_FOR\_U

Pays : Brazil

Titre : Javanais

Le participant doit enlever la syllabe « PAT » dans ce hash ou utiliser un Javanais Decrypter

LPATEMPATOTDPATEPPATASSPATEESTSPATALPATAMPATECHE

Lien : <https://www.dcode.fr/javanais-slang>

Password : salameche

Pays : Chili

Titre : Il fait beau non ?

Le participant doit utiliser un Meteo Decrypter de Wetterkurzschlussel.

+17°C +24°C +16°C +14°C +9°C +25°C +24°C +13°C +28°C +10°C +10°C +24°C +24°C +10°C +9°C +9°C +24°C +16°C +13°C +24°C +11°C +28°C +9°C +8°C +11°C +24°C +10°C

Lien : <https://www.dcode.fr/codes-meteo-wetterkurzschlussel>

Password : temperatures

Pays : Croatia

Titre : Wolseley

Le participant doit utiliser un Wolseley Decrypter en utilisant la clé (67000).

PVOMGWVLZHHVVHGHGIZHYMFIT

Lien : <https://www.dcode.fr/chiffre-wolseley>

Password : Strasbourg

Pays : United-States

Titre : THIS IS SPARTA

Le participant doit utiliser un Scytale Decrypter. Il doit conserver la ponctuation et les espaces.

Ldsaoeeeoumpeuhoash·tsta·

Lien : <https://www.dcode.fr/chiffre-scytale>

Password : aouhaouh

Pays : Sweden

Titre : J’ai mal au crâne

Le participant doit utiliser le langage « Brainfuck » pour décrypter.

++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>>----.>++++++++++++++.-----------------.++++++++.+++++.<++++.+++++++++++++++.------------------.++++++++.

Lien : <https://www.dcode.fr/langage-brainfuck>

Password : Br41nFuck

Pays : Tanzania

Titre : Scarabée

Le participant doit utiliser Scarabée d’or Decrypter. Il doit cocher «  UTILISER LA VARIANTE DE 'A FEW WORD ON SECRET WRITING » pour trouver

&. 0†[ \*. ‡(]]. .][ ;†&\*]:☞?‘.

Lien : <https://www.dcode.fr/scarabee-or-poe>

Password : GOLDSHRINE

Pays : Poland

Titre : JS Keycode

Le participant doit utiliser un code touches javascript decrypter.

76 69 77 79 84 68 69 80 65 83 83 69 69 83 84 81 87 69 82 84 89

Lien : <https://www.dcode.fr/code-touches-javascript>

Password : QWERTY

Pays : New Zealand

Titre : B36

Le participant doit utiliser B36 decrypt.

770 29405 482 42494270 19181 7353563

Lien : <https://www.dcode.fr/chiffre-base-36>

Password : 4DM1N

Pays : Turkmenistan

Titre : Unicode

Le participant doit utiliser un Unicode Decrypter.

76 101 32 109 111 116 32 100 101 32 112 97 115 115 101 32 101 115 116 32 113 119 101 114 116 121 117 105 111 112

Lien : <https://www.dcode.fr/codage-unicode>

Password : qwertyuiop

Pays : Laos

Titre : Casette

Le participant doit utiliser un K7 Decrypter.

6/13/ /5/3/24/ /14/13/ /2/17/25/25/13/ /13/25/24/ /18/17/26/16/9

Lien : <https://www.dcode.fr/code-k7-cassette>

Password : ZARBI

Pays : Kenya

Titre : Quel douce melodie

Le participant doit utiliser un acéré decrypter et copier les notes.

Img : melodie

Lien : <https://www.dcode.fr/chiffre-acere>

Password : Musique

Pays : India

Titre : Templier

Le participant doit utiliser le code des templiers.

Img : templier

Lien : <https://www.dcode.fr/chiffre-templiers>

Password : chevalier

Pays : Egypt

Titre : Mary Stuart

Le participant doit utiliser le code de Mary Stuart.

Img : souris

Lien : <https://www.dcode.fr/code-mary-stuart>

Password : Stuart Little

Pays : Costa Rica

Titre : PigPen

Le participant doit utiliser le code Pig Pen des Francs-Maçons.

Img : souris

Lien : <https://www.dcode.fr/chiffre-pig-pen-francs-macons>

Password : cochon

Pays : Colombia

Titre : Mr Robot

Le participant doit tout d’abord aller dans le fichier.

<http://54.38.232.200:30069/robots.txt>

Il trouvera le liens suivant

<http://54.38.232.200:30069/6c8e5427c0d041fa371ada84a42d917cc15f75b3.html>

En ouvrant le code source, il trouvera le flag.

Password : Robots.txt\_c4n\_k33p\_hid3en\_data

Pays : Paraguay

Titre : QR Code

Le participant doit tout d’abord modifier la couleur background du body, il y trouvera un QR code.

Ce QR code donne un hash en base 64. Le participant n’a plus qu’à décrypter le hash.

Password : W4kand4

Pays : Philippines

Titre : SQL injection

Le participant doit modifier dans l’url suivante le « admin » par « ‘ or ‘’=’ »

<http://54.38.232.200:31006/?username=admin>

Password : Hack3rmAn

Pays : Yemen

Titre : Simple HTML

Le participant doit ouvrir le code source de la page et trouver le flag

Password : read\_s0urce\_c0d3

Pays : Senegal

Titre : SweetHome

Le but de ce challenge est d'accéder à un fichier nommé /server-status.

Pour cela l'utilisateur doit accéder depuis le serveur lui-même.

En se connectant sur le http:/localhost/ on peut voir que cela nous retourne la page web

Et par déduction si on fait http:/localhost/server-status cela nous retourne alors

flag{YøøÅre†øø5trøng}

Password : YøøÅre†øø5trøngPassword

Pays : Indonesia

Titre : Ping access

Le participant doit tout simplement ping 127.0.0.1 comme dans l’exemple, puis utiliser « ; » afin d’exécuter une autre commande.

Or, on ne peut pas écrire « 127.0.0.1;ls params » etc. Les espaces sont supprimés dans ce challenge. Pour pallier à cela, il faut utiliser $IFS (Internal Field Separator). IFS représente un espace.

Une fois avoir trouvé le fichier flag à l’aide de ls, il suffit juste de cat le ficher en question.

Command : 127.0.0.1;cat$IFS../../../flag

Password : T00HotForU

Pays : Norway

Titre : Header

Le participant doit créer un script.

Tout d’abord, il doit ouvrir le code source de la page et se rendre dans network.

Une fois dans network, il trouvera dans le header de la page de base [Get-flag]. C’est un hash en base64.

Une fois ce hash décrypté, il peut l’envoyer au formulaire afin de valider le challenge…

Ah non, il faut faire ça rapidement ! Vous trouvez un script en python ci-dessous pour valider le challenge.

#!/usr/bin/env python

#Importing libraries

import base64

import requests

#Initializing request session

req = requests.Session()

res = req.post("http://54.38.232.200:30085/index.php")

#Get 'Get-flag' header

get = res.headers['Get-flag']

#Decode header

header\_byte = base64.b64decode(get)

header = header\_byte.decode('ascii')

#Make new request with ASCII header

res = req.post("http://54.38.232.200:30085/index.php", data={'MasterInput' : header})

print(res.content)

Password : G4rd3\_ton\_P4nn34u

Pays : Kazakhstan

Titre : User-Agent

L’utilisateur doit changer son user-agent par admin. Une technique simple et de créer un son propre émulateur de device.

Lorsque vous accéder au code source de la page, vous pouvez tester le responsive. Lorsque vous créez votre propre device, plusieurs paramètres vous sont demandés. Nom, taille de l’écran en pixel, useragent et le type de l’appareil. Une fois votre device créé et sélectionné, vous n’avez plus qu’à rafraîchir la page afin de voir le mot de passe apparaître !

Password : User\_4gent\_h4cker

Pays : Iran

Titre : Easy Reverse

Une technique pour réaliser ce challenge est de créer un fichier .c et de créer une shared library.

gcc -fPIC – shared nom\_du\_fichier.c -o lib.so

Ensuite il faut utiliser la commande LD\_PRELOAD

LD\_PRELOAD=./lib.so ./cracking\_2 + un argument

Le mot de passe apparaîtra dans la console.

#include <stdio.h>

int strcmp(const char \*s1, const char \*s2)

{

printf("%s\n%s\n", s1, s2);

return (0);

}

Password : EAsy-r3v3rs3

Pays : Turkey

Titre : Easiest things in my life

Le participant doit simplement télécharger le binaire et tester une de ces solutions.

Strings cracking\_1

cat cracking\_1

objdump -s cracking\_1

Password : E4sy1est\_than\_the\_34s1er\_?

Pays : United Kingdom

Titre : Glitched

Lors de la lecture de la vidéo plusieurs symboles. Le premier de ces symboles est différent des autres et constitue un indice. La partie du haut correspond uniquement aux consonnes tandis que la partie basse est liée aux voyelles et ont un numéro par rapport à la lettre voulue.

Tableau des consonnes :

B= 1 ; C= 2 ; D= 3 ; F = 4 ; G= 5 ; H= 6 ; J= 7 ; K= 8 ; L= 9 ; M= 10 ; N= 11 ; P= 12 ; Q=13 ; R= 14 ; S= 15 ;   
T= 16 ; V= 17 ; W= 18 ; X= 19 ; Z= 20

Tableau des voyelles :

A= 1 ; E= 2 ; I = 3 ; O = 4 ; U = 5 ; Y =6

Ce qui nous donne en suivant les symboles de la vidéo le message :

PEUTONVOIRLESSONS  
Peut-on voir les sons?

Il s’agit d’un indice nous demandant de verifier l’audio de la video. À l’aide du logiciel Sonic Visualiser nous pouvons trouver un code caché dans le spectre audio de la vidéo(layer->Add Spectogram).

Le code RmxhZzoge1N5bmVzdGjDqXNpZX0=est en base64 ce qui nous donne le flag pour terminer le défi.

Password : {Synesthésie}

Pays : Bolivia