CHALLENGES CTF

DIVERSITY by EPITECH

Titre : Message Digest

Le participant doit utiliser un MD5 decrypter pour ce hash.

704b037a97fa9b25522b7c014c300f8a

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

Password : 4dm1n

Titre : Ave

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

Alcvj Tvjri rmrzk r vl lev sfeev zuvv ! Cv dfk uv grjjv vjk mvez mzuz mztz

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

Password : veni vidi vici (Les espaces doivent être gardé)

Titre : Tout pareil, c'était évident !

Le participant doit utiliser un Base64 decrypter pour ce hash.
QmFzZTY0IGVzdCBjYXJhY3TDqXJpc8OpIHBhciBsZSDDqWdhbCDDoCBsYSBmaW4gISBMZSBtb3QgZGUgcGFzc2UgZXN0IEJyNHYwIA==

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

Password : Br4v0

Titre : Des nombres partout, aled !

Le participant doit utiliser 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

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

Password : Asc11

Titre : J'adore les cigares de ce pays !

Pour réaliser ce challenge, 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

Titre : Le programme a un bug ?

Le participant doit utiliser binary to text.

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_Fun

Titre : tu tuututu tuuuuuuu tuutu

Le participant doit utiliser un Morse decrypter.

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

Lien : https://www.dcode.fr/code-morse#q2

Password : SamuelMorse

Titre : Alphabet trifide

Le participant doit utiliser Trilitère decrypter.

BABABC BAABCBCAC ABBABC BCAAABCCBCCBABC ABCCCBCAC
ACACCAABCABBABCCCABBAABABBA

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

Password : frederici

Titre : Trithème

Le participant doit utiliser la technique Ave Maria de Trithème.

à perpétuité

dans la divinité

irrévocablement

dans son royaume

à perpétuité

un monde sans fin

sans cesse

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

password : epitech

Titre : Secret message

Le participant doit utiliser la technique du steg of the dump.

J'aime bien la cybersécurité ! #HackerSisiLaFamille

Lien : https://holloway.nz/steg/

Password : aled (Attention, des espaces sont cachés dans la description et doivent être utilisé pour trouver le flag)

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

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

Le participant doit utiliser hexa to text.

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

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

Password : Hexa_feat_Epitech

Titre : Code talker

Le participant doit utiliser la technique de navajo decrypt.

NASH-DOIE-TSO AH-NAH TSIN-TLITI A-KHA D-AH CHINDI AH-JAH CLA-GI-AIH BE-LA-SANA KLESH DIBEH AH-NAH AH-JAH KLESH D-AH A-KHA AH-YA-TSINNE WOL-LA-CHEE A-KEH-DI-GLINI TSE-NILL TSAH

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

Password : ojavan

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

Le participant doit utilser decimal to text.

76 101 32 109 111 116 32 100 101 32 112 97 115 115 101 32 101 115 116 32 121 117 105 111 49 50

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

Password : yuio12

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\S;F,P9&5?,7-N=%]H-')D

`

end

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

Password : UU_3nc0de_1snt_h4rd

Titre : Sah quel plaisir !

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

Lien : https://md5decrypt.net/Sha256/#answer

Password : 40cdfb86e29a00e99f95b804868a733115d5a6a216e1051d2b238db8fd31cb0c

Titre : Rozier

Le participant doit utiliser un Rozier decrypter sur ce hash.

WXXZRIBATDDCJPEXATRJZSLEC

Et utiliser cette clé :

EPITECH

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

Password : EpitechStr

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 mfmpffmmmpppmpmfmm-ppmèpffmppfmm pmfmppfmm mmfmfpmmmfmffpmmppfmm ! pmmmpp fpmppffmffmm mpméfmpmppfmmfmpmpp fmpppffmffmm, pmfmpp ppmppffmp mpmmpp pfmmmmfmmfmmmpp mppfmmfmp ppmppfppp pppppfppmmmppffmpp mpmmpp ppmppfpfffmp

Lien : https://www.dcode.fr/code-kenny-southpark
Password : 97

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 23 41 2 61 97

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

Password : primary

Titre : Pourrir

Le participant doit utiliser le chiffre de ROT avec une rotation de +26.

f!)+0~!,{//!!/0j%'{}$1

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

Password : Pikachu

Titre : CÉTAUTOMATIX

Le participant devra utiliser un blowfish decrypter, attention seul le lien fourni permet de décrypter le hash avec la clé !

BTB1o18ViJWdPB7bWQGe6/TLrGcpirGEWJcyPVjEFcLI+hH+icbc9B+7Gh9oOzuu

La clé est CÉTAUTOMATIX

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

Password : Il_3st_fr41s_m0n_pO1s50n

Titre : Detroit

Le participant doit utilser 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/ /26/2/19/24/6/21

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

Password : le coding club est genial

Titre : Malespin

Le participant doit utiliser un Malespin decrypter.
La pib da messa asb ringlax

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

Password : ronflex

Titre : Leet speak

Le participant doit utiliser un LSPK90 horaire decrypter.

_|UU E[][-- ¯¯VW /_<{V\[/]\|/ UUv^|-- [--()[]|\|/_+v^>-|L|_()^<|]

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

Password : TOO_E4SY_FOR_U

Titre : Javanais

Le participant doit tout simplement enlever la syllable PAT dans ce hash ou utiliser un javanais decrypter.

LPATEMPATOTDPATEPPATASSPATEESTPATALPATED

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

Password : aled

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 +16°C +24°C +9°C +24°C +14°C

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

Password : meteo

Titre : Wolseley

Le participant doit utiliser un Wolseley decrypter en utilisant la clé.

PVOMGWVLZHHVVHGHGIZHYMFIT

La clé est :

67000

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

Password : Strasbourg

Titre : THIS IS SPARTA

Le participant doit utiliser un scytale decrypter.

Lde0ee·0··e·mps·oat·ts···s3·

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

Password : 300

Titre : J'ai mal au crâne

Le participant doit utiliser le langage brainfuck pour décrypter.

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

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

Password : Br41nFuck

Titre : Scarabée

Le participant doit utiliser un scarabée d'or decrypter.

&. 0†[*. ‡(]]. .][-?[.*†☞

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

Password : CITEDOR

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 65 90 69 82 84 89

Le lien : https://www.dcode.fr/code-touches-javascript

Password : AZERTY

Titre : B36

Le participant doit utiliser B36 decrypt

770 29405 482 42494270 19181 17431871

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

Password : ADMIN

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 97 122 101 114 116 121 117 105 111 112

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

Password : azertyuiop

Titre : Casette

Le participant doit utiliser un K7 decrypter.

6/13/ /5/3/24/ /14/13/ /2/17/25/25/13/ /13/25/24/ /15/17/11/13/24/24/13

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

Password : cagette

Titre : Quel douce melodie

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

Img 2 : melodie

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

Password : Musique

Titre : Templier

Le participant doit utiliser le code des templiers.

Img 2 : templier

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

Password : chevalier

Titre : Mary Stuart

Le participant doit utiliser le code de Mary Stuart.

Img 2 : souris

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

Password : Stuart Little

Titre : Pig Pen

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

Img 2 : souris

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

Password : cochon

Titre : Mr Robot

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

http://54.38.232.200:30069/robots.txt

Puis dans

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

En ouvrant le code source html, il y trouvera le flag.

Password : Robots.txt_c4n_k33p_hid33n_data

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 : W4k4ndA

Titre : SQL injection

Le participant doit tout simplement modifier dans l'url

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

admin par ' or ''='

Password : hackerman

Titre : Simple html

Le participant doit tout simplement ouvrir le code source de la page et trouver le mot de passe.

Password : r34d_s0urc3_c0d3

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.

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

Password : TooHot4U

Titre : Header

Le participant doit créer un script. pour réaliser le challenge.

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

import base64

import requests

r = requests.Session()

reponse = r.post("http://54.38.232.200:30085/index.php")

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

get_byte = bytes(get, 'utf-8')

header_byte = base64.b64decode(get_byte)

header = header_byte.decode('ascii')

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

print(reponse.content)
```

Password : G4rd3_t0n_P4nn34u

Titre : User-Agent

L'utilisateur doit changer son user-agent par admin.

Une technique simple et 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, user-agent et le type de l'appareil. Un 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_3g3nt_h4cker

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 et le mot de passe apparaîtra.

```
#include <stdio.h>

int strcmp(const char *s1, const char *s2)
{
	printf("%s\n%s\n", s1, s2);
	return (0);
}
```

Password : E4sy_r3v3rs3

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_th4n_th3_e4s1er_?