



WRITE UP « TailleCrayon »

FIC 2K18

ENSIBS CYBERDEFENSE

par @y0r3l



| Date | Acteur | Mail de contact | Version |
|------------|--------|----------------------|---------|
| 21/11/2017 | @y0r3l | y0r3l@protonmail.com | 1.0 |

INTRODUCTION

Ce challenge a été réalisé dans le cadre du Forum International de la Cybersécurité (FIC) 2018 se tenant à Lille le 23 et 24 janvier 2018. L'ENSIBS (Ecole Nationale Supérieur d'Ingénieurs de Bretagne Sud), et plus précisément les étudiants de la formation Cyberdéfense, a été chargée de préparer un événement de type Capture The Flag (CTF).

C'est dans le but d'alimenter cet événement en épreuves que j'ai créé le challenge « TailleCrayon », sujet de ce Write Up.

Ce document a pour but de vous présenter la démarche afin de résoudre le challenge.

Catégorie

OSINT (Open Source INTeelligence)

Niveau de difficulté

Moyen

Énoncé

Le but de ce challenge est de récupérer l'adresse mail et le mot de passe de l'administrateur à l'origine de ce petit site.

Cependant, le challenger ne devra pas utiliser une vulnérabilité d'un des langages de programmation utilisés.

En effet, il devra tout d'abord trouver quelle particularité du site lui permettra de donner des indices sur le mot de passe de l'administrateur.

Puis il devra trouver, sur des sites externes, l'adresse mail et les différents éléments du mot de passe de l'administrateur en utilisant les renseignements d'origine source ouverte (OSINT).

Matériel nécessaire pour le résoudre

Accès à Internet

Matériel nécessaire pour le rejouer

Docker

Indices

Les indices peuvent être donnés tout au long du challenge à intervalle espacé.

1. « Encore un site dont j'ai perdu le mot de passe... »
2. « Que sont-ils devenus ? »
3. « Merci maman... »

Explication détaillée du challenge :

Tout d'abord, nous nous retrouvons face un site portant sur les tailles crayons réalisé par un molubdotémophile, nom donné aux personnes passionnés par les tailles crayons.

Ce site possède, à première vue, quatre pages:

1. une page « Accueil » ;
2. une page « S'inscrire » ;
3. une page « Se connecter » ; et
4. une page « A propos ».

La première page, « Accueil », contient seulement du texte informant le visiteur que le site est en construction et qu'il a pour but de regrouper les différents passionnés de taille crayon français :

Mon amour pour les tailles crayons!

Bienvenue sur le site de "Mon amour pour les tailles crayons".

Ce site est en cours de construction et a pour but de regrouper tous les fans de taille crayon.

Copyright © Harold Malcuit

figue 1 – page « Accueil »

La seconde page, « S'inscrire », contient un formulaire dont les champs sont les suivants :

- Nom ;
- Prénom ;
- Mail ;
- Mot de passe; et
- Indice pour le mot de passe.

Veuillez remplir tous les champs obligatoires (*) !

Inscription

Nom *:

Prénom*:

Mail* :

Mot de passe* :

Indice pour le mot de passe* :

figue 2 – page « S'inscrire »

Ce formulaire paraît plutôt banal malgré le dernier champ qui généralement se traduit plus par une question secrète et une réponse secrète. De plus, en mettant le pointeur de notre souris sur le point d'interrogation se trouvant à la suite de « Indice pour le mot de passe », on découvre l'utilité de ce champ : « Ce champ vous permet de renseigner une ou plusieurs informations afin de vous souvenir de votre mot de passe. Veuillez à ne pas mettre directement votre mot de passe »

A noter que tous les champs sont obligatoires.

La troisième page, « Se connecter », contient aussi un formulaire. Ce dernier demande au visiteur de fournir une adresse mail et un mot de passe afin de s'identifier.

Veuillez remplir tous les champs obligatoires (*) !

Connexion

Mail* :

Mot de passe* :

[Mot de passe oublié : obtenir son indice](#)

figue 3 – page « Se connecter»

Cependant, en dessous du champ « Mot de passe », on retrouve un lien vers une cinquième page dédiée aux personnes ayant oublié leur mot de passe.

En cliquant dessus, on se retrouve sur une page, dont le titre est « Obtenir son indice », nous demandant de renseigner une adresse mail afin d'obtenir l'indice lié à cette dernière.

Veuillez remplir tous les champs obligatoires (*) !

Obtenir son indice

Mail* :

figue 4 – page « Obtenir son indice »

On comprend mieux alors l'utilité du champ « Indice pour le mot de passe » dans la page « S'inscrire ».

Enfin, la quatrième page, « A propos », est une page donnant un peu plus d'informations sur le site et son auteur :

A propos !

Bienvenue sur un site dédié à la molubdotémophilie.

Bonjour,
Je m'appelle Harold et je suis passionné depuis mon enfance par les tailles crayons.
Cette passion s'appelle la molubdotémophilie! Je suis donc un molubdotémophile !
Le but de ce site est de permettre aux différents passionnés de présenter leur collection.
Le site en est encore à son début, soyez donc indulgent ;-).

figue 5 – page « A propos »

On peut alors décider de se créer un compte utilisateur pour voir ce qu'il se passe :

Inscription

Nom *:

Prénom*:

Mail* :

Mot de passe* :

Indice pour le mot de passe* :

figue 6 – création d'un compte

Le site nous informe que l'inscription a été effectuée.

Nous essayons donc ensuite de se connecter avec ce compte. La connexion est un succès et nous sommes dirigés vers une nouvelle page :

Connexion réussie en tant qu'utilisateur !

Un peu de patience, le site est loin d'être fini ;-).

figue 7 – page utilisateur

Sur cette page, nous n'avons pas d'autre choix que de retourner sur la page d'accueil, et au vu du message, la connexion en tant qu'utilisateur s'avère être une impasse.

Cependant, comme le mentionne le message, nous nous sommes identifiés en tant qu'utilisateur. On en déduit donc qu'il existe aussi une telle page pour un ou des administrateurs. Certainement une page dédiée à la gestion de ce site et de son contenu.

Il va donc falloir essayer d'accéder à cette page administrateur. Pour cela, penchons-nous sur le seul administrateur dont nous connaissons l'existence : l'auteur de ce site. Ce dernier a précisé son nom dans tous les footers des différentes pages : « Harold Malcuit ».

On peut alors décider de taper ce nom et ce prénom sur Google :

Environ 14 200 résultats (0,28 secondes)

Harold MALCUIT, 33 ans (LILLE) - Copains d'avant
copainsdavant.linternaute.com/p/harold-malcuit-19911061 ▾
 18 nov. 2017 - MALCUIT Harold : Harold MALCUIT, né en 1984 et habite LILLE. Aux dernières nouvelles il était à Lille III :langues étrangères à LILLE entre 2002 et 2005.

Lille Harold Profiles | Facebook
<https://www.facebook.com/public/Lille-Harold> ▾ [Traduire cette page](#)
 People named Lille Harold. Find your friends on Facebook. Log in or sign up for Facebook to connect with friends, family and people you know. Log In. or, Sign Up · Harold GD. See Photos · Harold GD. Sciences Po Lille, ESJ Lille. Académie ESJ Lille. Harold Malcuit. See Photos · Harold Malcuit. Lille, France.

Profils Harold France | Facebook
<https://fr-fr.facebook.com/public/Harold-France?page=3> ▾
 Leader, à Artiste musicien, chanteur, rappeur, compositeur et poète. Habite à Pointe-Noire. Administrateur en Chef, à FRANCE 24. A étudié à ENMA '08. Harold Munoz · Voir les photos · Harold Munoz · Artiste, à Harold Muñoz. Habite à Paris · Harold Malcuit. Voir les photos · Harold Malcuit · Université Lille 3. Habite à Lille.

My Bic pen - Accueil | Facebook
<https://fr-fr.facebook.com/mybicpen/> ▾
 My Bic pen. 575 K j'aime. Welcome to the official BIC pen page! Here you will find news, events and curiosities about the mythical BIC pen.

figue 8 – Recherche « Harold Malcuit » sur google

Le créateur de ce site a l'air d'être référencé sur ce moteur de recherche.

Allons voir du côté du premier résultat ce que cela peut nous apporter :

Copains d'avant

ACTUALITÉS FINANCE CULTURE SPORT AUTO VOYAGE HIGH-TECH PLUS ▾ [Twitter](#) [f](#) [User icon](#)

S'INSCRIRE SE CONNECTER LYCÉES COLLÈGES PRIMAIRES UNIVERSITÉS ENTREPRISES SERVICE MILITAIRE AVIS DE RECHERCHE [Rechercher](#)

Harold MALCUIT

• Salut, tout le monde. Pour ceux qui me connaissent, hésitez pas à me contacter directement par mail : harold.malcuit@gmail.com
 • LILLE

[Ajouter](#)

PARCOURS

Parcours scolaire

LILLE III :LANGUES ÉTRANGÈRES - Lille
 2002 - 2005

RÉSULTATS des examens 2017

► **BREVET | BAC | BTS**

Retrouvez gratuitement :
 - Le **résultat du bac** à Lille ou à proximité, mais aussi tous les résultats du bac dans l'Académie de

figue 9 – Profil de « Harold Malcuit » sur le site <http://copainsdavant.linternaute.com>

Le premier lien nous emmène vers un profil du célèbre site « Copains d'avant ». Cette page nous donne une adresse mail (harold.malcuit@gmail.com).

Cette adresse mail peut être directement testée. En effet, nous avions vu que la page « Obtenir son indice » demandait simplement une adresse mail. Nous retournons donc sur le site dédié aux molubdotémophiles et nous remplissons l'unique champ de la page « Obtenir son indice » avec l'adresse mail trouvée sur le site « Copains d'avant » :

L'indice pour harold.malcuit@gmail.com est: "Nom de mon premier chien et numero de département"

Obtenir son indice

Mail* :

figue 10 – Résultat de la page « Obtenir son indice » avec comme adresse mail « harold.malcuit@gmail.com »

Comme le souligne, cette adresse mail est belle et bien renseignée dans la base de données du site. De plus, nous obtenons l'indice rempli par le créateur du site : « Nom de mon premier chien et numéro de département »

On en déduit donc que la composition du mot de passe est une simple association d'un nom de chien et d'un numéro de département.

Or, nous disposons certainement déjà de la seconde partie du mot de passe. Sur son profil « Copains d'avant », Harold Malcuit avait renseigné qu'il habitait à Lille, ville du département « Nord » dont le code officiel géographique est 59.

Il nous manque plus qu'à trouver la première partie du mot de passe : un nom de chien. Et rien de mieux que de fouiller sur les réseaux sociaux pour en découvrir plus sur le quotidien des personnes.

Une simple recherche sur Twitter de « Harold Malcuit » nous informe de l'existence d'un compte « @MalcuitHarold » :

Harold Malcuit
@MalcuitHarold
Papa passionné par les tailles crayons !
Lille, France
Inscrit en novembre 2017
[Tweeter](#)

Tweets 1 Abonnements 108 Abonnés 1

Tweets **Tweets & réponses**

Harold Malcuit @MalcuitHarold · 26 nov.
Bonjour Twitter ! #monpremierTweet

1 1 1

figue 11 – Profil de «@MalcuitHarold » sur Twitter

Malheureusement, ce compte s'avère être une impasse vu le peu de contenu.

Allons voir sur le réseau social Facebook si Harold Malcuit s'est créé un compte. Quand on recherche ce nom et ce prénom sur ce réseau, on tombe sur un seul résultat :

Harold Malcuit

Message ...

Journal À propos Amis Photos Plus ▾

VOUS CONNAISSEZ HAROLD ?

Si vous connaissez Harold personnellement, [envoyez-lui un message](#).

Intro

A étudié à Université Lille 3

Habite à Lille

De Lille

Photos

Harold Malcuit a partagé la publication de Paradise Flower.

22 novembre, 11:18 ·

figue 12 – Profil de «Harold Malcuit » sur Facebook

On peut facilement en déduire que ce profil correspond bien au créateur du site sur les tailles crayons car la photo de profil utilisé est la même que celle du profil « Copains d'avant ».

Ce profil est plutôt vide, seulement deux photos (une photo de profil et une photo de couverture) et quelques publications partagées. En cherchant bien on ne trouve aucun nom de chien sur cette page.

Cependant, on remarque qu'une personne a commenté la photo de profil de Harold Malcuit :



figue 13 – Photo de profil de « Harold Malcuit » sur Facebook

Le commentaire est « Qu'il est beau mon fils !!! » et a été posté par une certaine Gisèle Lovier-Malcuit. Il semble que cette personne soit la mère de Harold Malcuit.

Intéressons-nous maintenant au profil de cette mère tout en gardant en tête que l'objectif est de trouver un nom de chien :

A screenshot of a Facebook profile page for 'Gisèle Lovier-Malcuit'. The profile picture is a close-up of a Shetland Sheepdog. The name 'Gisèle Lovier-Malcuit' is displayed prominently. Below the profile picture is a small image of white roses. The page features a navigation bar with links to 'Journal', 'À propos', 'Amis', 'Photos', and 'Plus'. The 'Photos' section is expanded, showing a grid of images including a snowy landscape, a building, and a fire. The 'Photos' section also includes a link to 'Intro' and location information ('Habite à Lille', 'De Lille'). A status update from Gisèle reads 'Attention le froid est de retour...couvrez vous bien....' (Attention the cold is back...dress well....) with a photo of a frozen landscape.

figue 14 – Profil de «Gisèle Lovier-Malcuit » sur Facebook

A la différence du profil de son fils, Mme Lovier-Malcuit possède un profil Facebook remplit avec une multitude de photos. Ces dernières ont pour thème le climat ou les animaux et sont toujours accompagnées d'un petit mot sympathique.

Mais parmi tous ces clichés, une photo nous intéresse tout particulièrement. Cette dernière représente un enfant accompagné d'un petit chien et semble avoir été prise il y a un certain temps :



figue 15 – Une photo de «Gisèle Lovier-Malcuit» sur Facebook

En outre, la photo est accompagnée du texte suivant : « Mon fils et notre petit chien Petitpapanoel... que de souvenirs.... ». On en déduit donc que Petitpapanoel est le nom du chien sur cette photo.

A moins que ce soit l'enfant qui se prénomme comme ça et que le fils de Gisèle Lovier-Malcuit soit un chien. Très peu probable.

Allons tout de suite tester nos deux éléments que nous avons trouvé qui semble correspondre à l'indice donné par l'adresse « harold.malcuit@gmail.com ».

Rendons-nous sur la page « Se connecter », renseignons « harold.malcuit@gmail.com » comme adresse mail et « Petitpapanoel59 » comme mot de passe.

Bingo ! En cliquant sur « Se connecter » avec les identifiants précédents, le site nous affiche la page suivante :

Connexion réussie en tant qu'administrateur!

Flag : ENSIBS{[A REMPLIR]le mot de passe de l'administrateur que vous venez de trouver}

figue 16 – Page administrateur

La supposition comme quoi il existait une page dédiée aux administrateurs était bonne. Nous pouvons ainsi construire le flag avec le mot de passe de Harold Malcuit :

ENSIBS{Petitpapanoel59}

Conclusion

Tout cela aurait pu être facilement évité si seulement Harold avait respecté quelques préconisations bien connues. En effet, la lecture de deux notes techniques de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) aurait permis à Harold d'améliorer aisément le niveau de sécurité de son compte d'administration :

- Note technique - Recommandations de sécurité relatives aux mots de passe (https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf)
- Note technique - Recommandations relatives à l'administration sécurisée des systèmes d'information(https://www.ssi.gouv.fr/uploads/2015/02/NP_SDE_DAT_NT_Archi_Admin.pdf)

Ainsi, Harold Malcuit aurait dû implémenter une politique de mot de passe efficace. De plus, il aurait dû utiliser un compte différent pour l'administration fonctionnelle dont le login n'est pas une adresse mail qu'il utilise au quotidien.

Pour conclure, notre molubdotémophile aurait dû également surveiller l'activité de ses proches sur les réseaux sociaux et les informer des dangers auxquels ces derniers s'exposent en affichant le quotidien de leur vie privée.