WRITE UP « DigiCarross » - Partie 1

NORZHCTF 2K19

ENSIBS CYBERDEFENSE

par @y0r3l

Date	Acteur	Mail de contact	Version
10/12/2018	@y0r3l	y0r3l@protonmail.com	1.0
07/08/2019	@y0r3l	y0r3l@protonmail.com	2.0

INTRODUCTION

Ce challenge a été réalisé dans le cadre du NORZHCTF se tenant à Lille le 22 janvier 2019. Ce dernier est un événement de type Capture The Flag (CTF) et est orgnaisé par les étudiants de la formation Cyberdéfense de L'ENSIBS (Ecole Nationale Supérieur d'Ingénieurs de Bretagne Sud).

C'est dans le but d'alimenter cet événement en épreuves que j'ai créé le challenge « DigiCarross ».

Ce challenge étant découpé en deux parties, ce document a pour but de vous présenter la démarche afin de résoudre la première étape du challenge.

Toute ressemblance avec des faits réels ne serait que pure et fortuite coïncidence.

Certaines ressources de ce challenge sont hébergées sur des plateformes tierces. La disponibilité dans le temps des données hébergées chez ces tiers n'est donc pas assurées. Ainsi, les informations présentes au sein de ce document peuvent s'avérées différentes de la réalité.

Catégorie

OSINT (Open Source INTelligence)

Niveau de difficulté

Facile

Énonce

Le but de ce challenge est de guider le challengeur dans l'identification de l'employé de DigiCarross susceptible d'être ciblée par de l'OSINT.

Le challengeur ne devra donc pas utiliser une vulnérabilité d'un langage de programmation pour résoudre ce challenge.

En effet, il devra tout d'abord analyser le site de l'entreprise, puis des ressources externes, afin d'identifier la cible.

Matériel nécessaire pour le résoudre

Accès à Internet
Compte LinkedIn

Matériel nécessaire pour le rejouer

Navigateur internet

Indices

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

1. « Des compétences classiques. »
2. « (47.645131 ;-2.7500159999999596) »
3. « Merci Vanessa pour ces explications. »

Explication détaillée du challenge :

Nous commençons ce challenge en analysant la page « Qui sommes-nous ? ». Cette dernière nous présente tout d'abord les activités de l'entreprise DigiCarross ainsi que l'ouverture d'un poste de chef de projet.

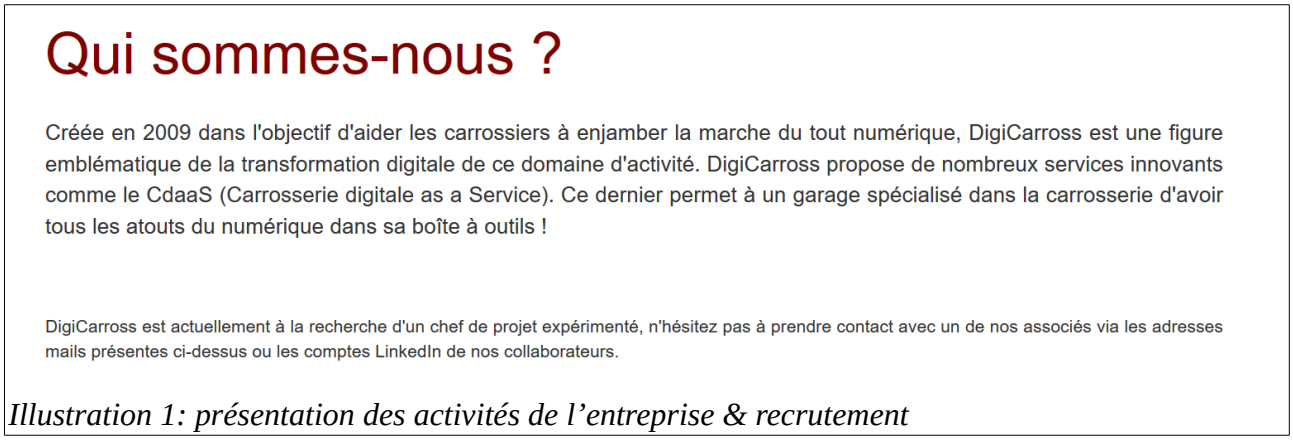

Illustration 1: présentation des activités de l'entreprise & recrutement

Puis nous retrouvons une présentation des employés de DigiCarross. A première vue, l'entreprise semble être composée de cinq personnes :

- Eugène Lacrymo, fondateur et certainement directeur de l'entreprise ;

Eugène Lacrymo

Eugène est le créateur de l'entreprise "DigiCarross".
Carrossier de formation, Eugène a décidé de se tourner vers l'Informatique au début du 21ème siècle.
Ne pouvons se détacher de son premier métier, Eugène créa DigiCarross dans le but de fournir aux carrossiers des solutions informatiques fiables et pertinentes.

✉ e.lacrymo@digicarross.fr

Illustration 2: présentation Eugène Lacrymo

- Samantha Damien, responsable en ressources humaines ;

Samantha Damien

Samantha est la responsable en ressources humaines de la société. Elle sera la première à vous contacter si vous souhaitez nous rejoindre !

✉ s.damien@digicarross.fr

Illustration 3: présentation Samantha Damien

- Bob Lefebvre, secrétaire de l'organisation ;

Bob Lefebvre

Bob est le secrétaire de la société DigiCarross. Il est le point de contacts à privilégier pour vos différentes requêtes. Bob gère le standard téléphonique de l'entreprise, vous arriverez donc facilement à le joindre.
Il sera vous accompagner au mieux dans votre expérience digitale !

✉ b.lefebvre@digicarross.fr

Illustration 4: présentation Bob Lefebvre

- Patrick Dubois, expert « DevOps » ; et

Patrick Dubois

Fan de l'Open Source, Patrick est l'expert DevOps de DigiCarross. En effet, une digitalisation pertinente nécessite un accompagnement spécialisé. Ainsi, Patrcik accompagne le client tout au long de la réalisation et développera quasiment en temps réel les nouvelles attentes du client.
Patrick dispose également de compétences en intelligence artificielle, pour les carrossiers désirant la pointe de la technologie !

✉ p.dubois@digicarross.fr

Illustration 5: présentation Patrick Dubois

- Vanessa Lambert, Développeuse.

Vanessa Lambert

Dévelopeuse pour DigiCarross depuis plus de cinq années, Vanessa sait comprendre les besoins de nos clients si particuliers.
Via sa gestion de projet Agile, Vanessa vous accompagnera tout au long du projet afin de concrétiser vos ambitions d'un garage totalement digitale.

✉ v.lambert@digicarross.fr

Illustration 6: présentation Vanessa Lambert

Le début de la page semble nous donner un élément essentiel : l'entreprise cherche un nouveau chef de projet. DigiCarross incite les intéressés à contacter un de leurs employés par mail ou par le biais de LinkedIn. Nous en déduisons donc que l'entreprise et ses employés sont présents sur le réseau professionnel le plus utilisé au monde.

Une simple recherche « DigiCarross » sur LinkedIn nous renvoie quatre résultats :

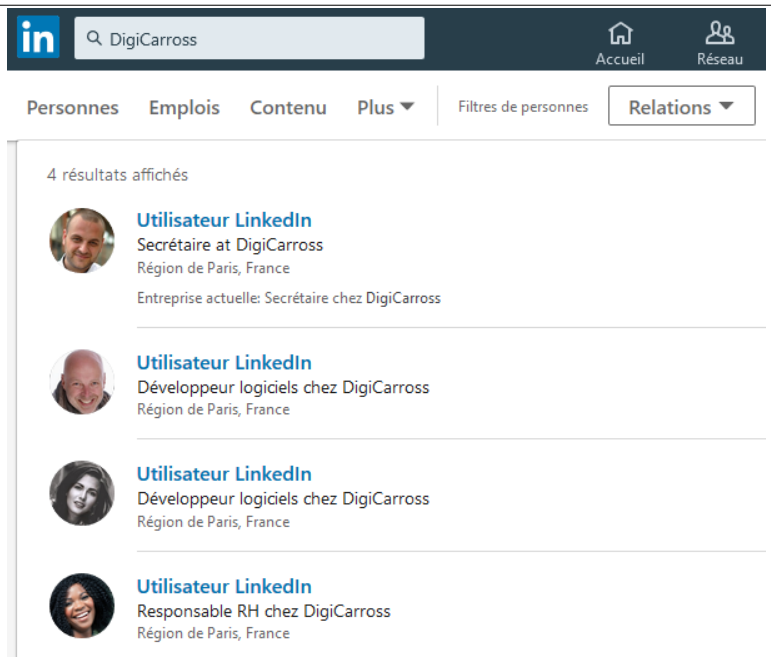

Illustration 7: recherche LinkedIn "DigiCarross"

Au vu des photos des profils LinkedIn présents dans le résultat de la recherche tous les employés de DigiCarross disposent d'un compte LinkedIn, excepté Eugène Lacrymo.

Cependant, nous ne pouvons pas accéder à ces profils à travers la simple recherche « DigiCarross ». Il faudra donc veiller à rechercher les différents employés via des requêtes plus précises : <Prénom>+<Nom>+ « DigiCarross » (ex : Samantha Damien DigiCarross).

Illustration 8: recherche LinkedIn "Samantha Damien DigiCarross"

Les profils des quatre employés de DigiCarross sont remplis et similaires. En effet, chacun explique sa formation et ses missions au sein de son entreprise actuelle.

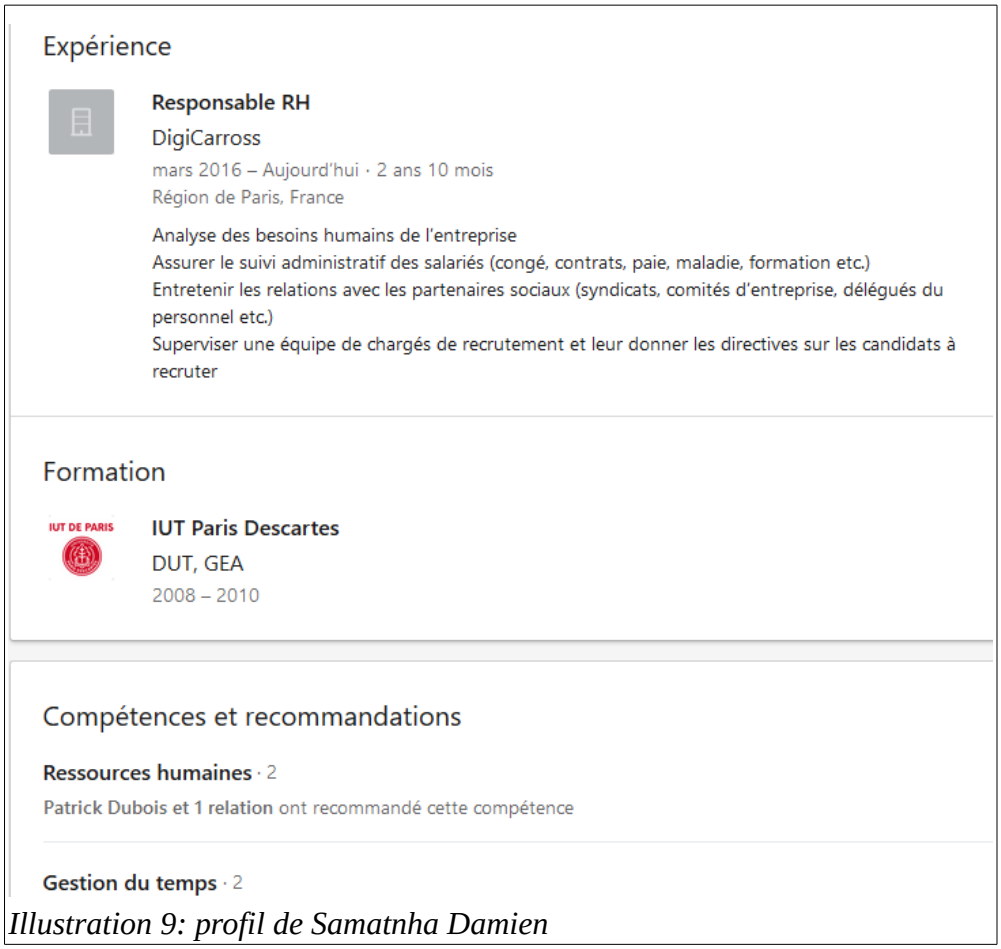

Illustration 9: profil de Samatnha Damien

Ces profils plutôt banals ne semblent pas disposer d'informations pouvant identifier une cible potentielle d'OSINT.

Cependant, les deux développeurs de la société (Patick Dubois et Vanessa Lambert) ont mentionné une compétence intéressante : « GitHub ».

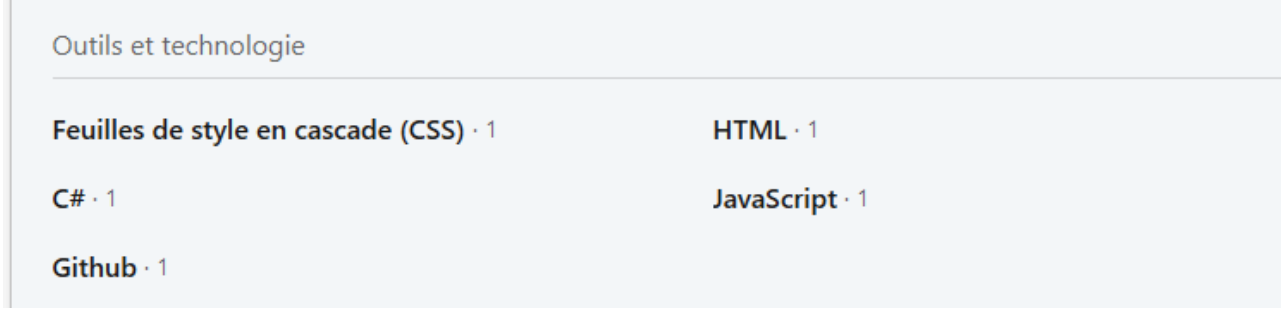

Illustration 10: compétence "GitHub" sur le profil de Vanessa Lambert

Ces deux personnes disposent donc certainement d'un compte sur la célèbre plateforme d'hébergement et de gestions de développement. Dorénavant, l'objectif est d'accéder à ces comptes.

LinkedIn propose à ses utilisateurs de rajouter des sites externes au sein des profils. Pour accéder au(x) site(s) externe(s) qu'un utilisateur a renseigné, il faut se rendre tout en haut du profil et cliquer sur « Voir les coordonnées » :

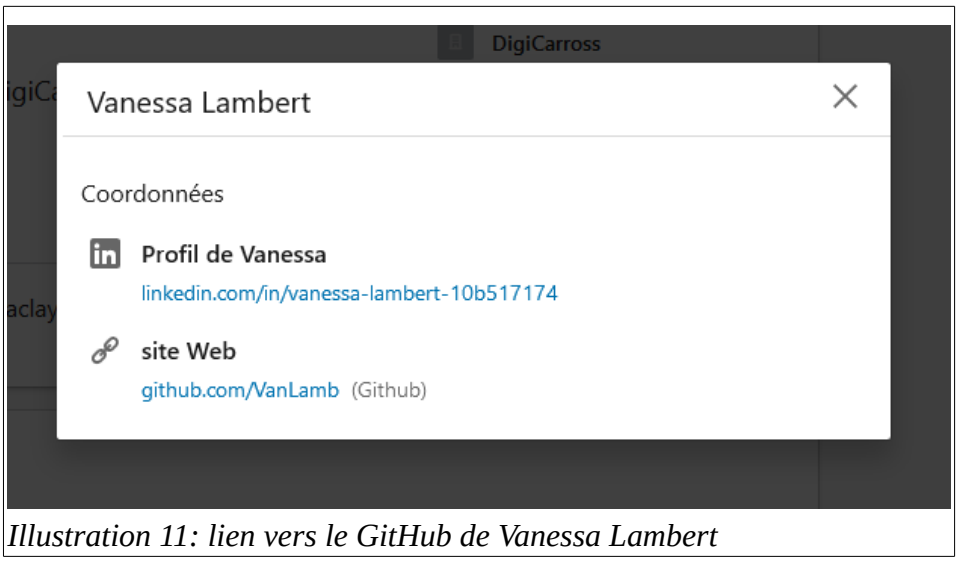

Illustration 11: lien vers le GitHub de Vanessa Lambert

Patick Dubois et Vanessa Lambert ont tous deux renseigné leur profil GitHub sur LinkedIn.

Illustration 12: lien vers le GitHub de Patrick Dubois

Le profil GitHub de Vanessa Lambert est rempli de petits projets :

- « SqueletteHtml » ;
- « ExempleVarBash » ;
- « JavaScriptObfuscation » ; et
- « SalutJS ».

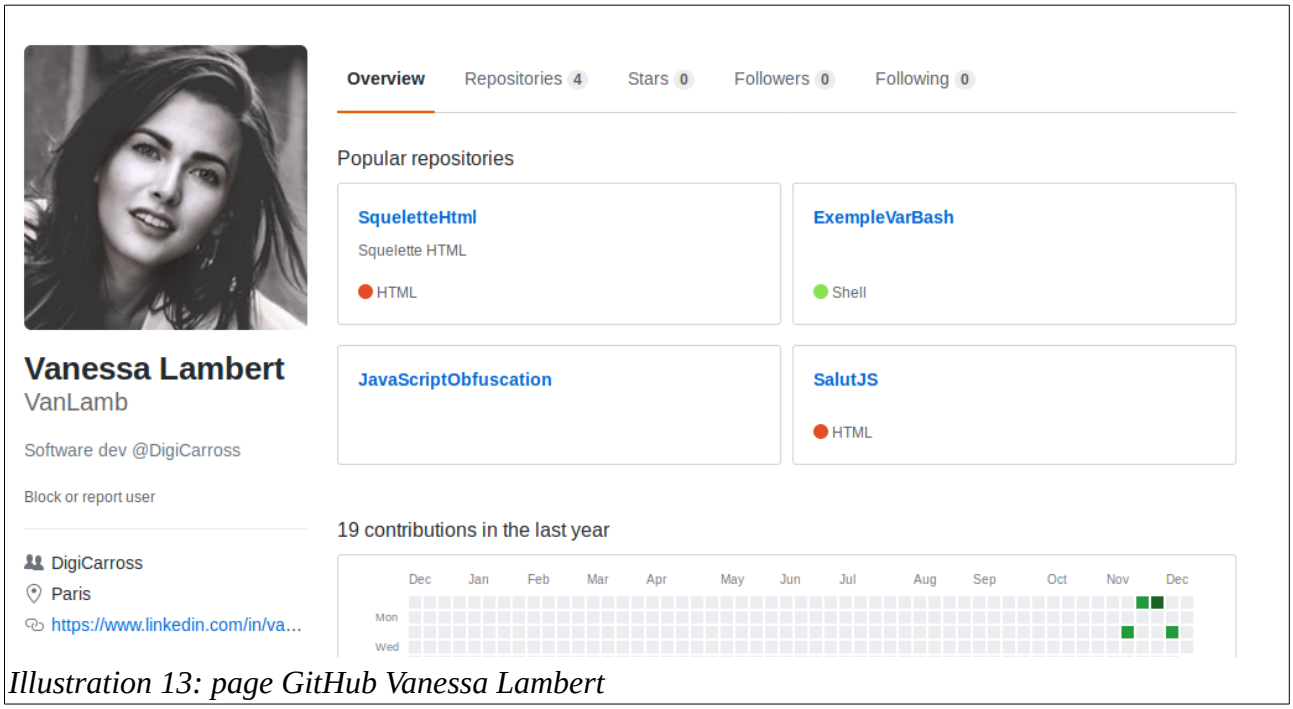

Illustration 13: page GitHub Vanessa Lambert

Ces derniers semblent non pertinents excepté le projet « JavaScriptObfuscation ».Ce projet est une impasse car le message obfusqué est simplement « JS obfusqué ».

Nous nous penchons donc maintenant sur la page GitHub de Patrick Dubois. Ce dernier a également déposé sur cette plateforme de nombreux projets :

- « Stars » ;
- « TriBulles » ;
- « MonBlog » ;
- « TriParInsertion » ; et
- « hashMDP ».

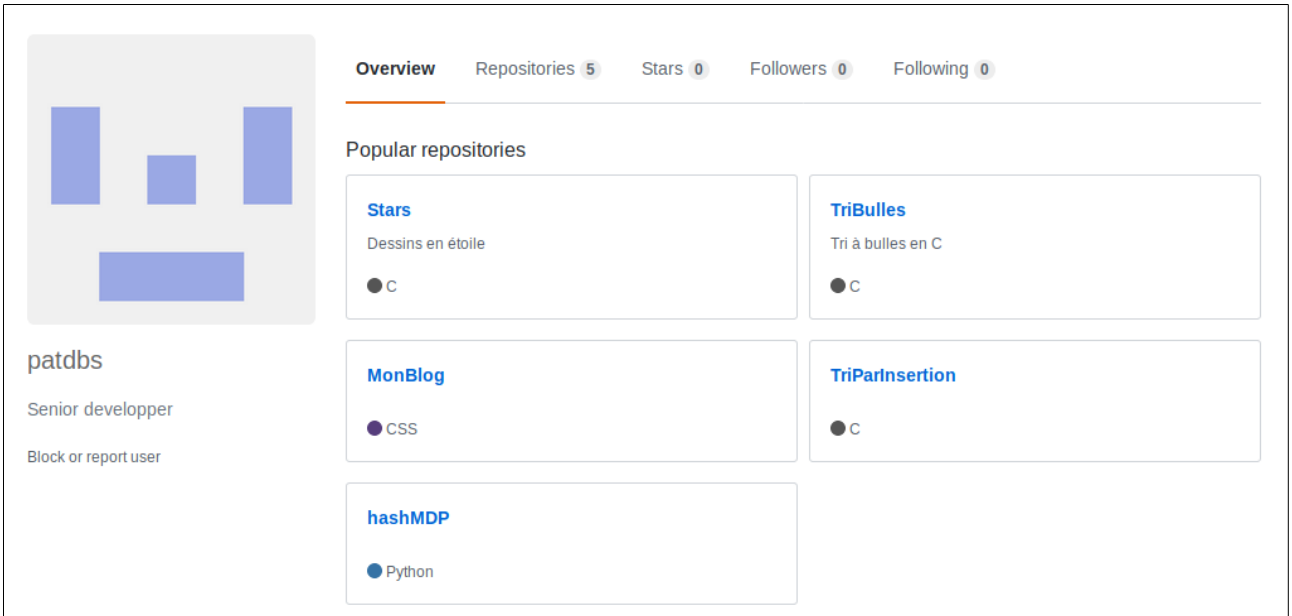

Illustration 14: page GitHub Patrick Dubois

Le projet le plus intéressant semble être « MonBlog ». La lecture du « README.md » confirme notre idée :

Illustration 15: README.md du projet "MonBlog"

Conformément à la présentation du personnel de DigiCarross, Patrick Dubois est une personne favorisant le partage et l'Open Source. C'est dans ce principe qu'il a ajouté les sources de son blog personnel au sein de son GitHub.

En téléchargeant ces dernières sur notre ordinateur, nous pouvons visualiser le contenu de son site.

Illustration 16: un aperçu du blog personnel de Patrick Dubois

Son blog est composé de nombreux articles sur des sujets bien variés : le développement, les animaux et les grillages.

Un de ces articles évoque un sujet déjà évoqué par Vanessa Lambert : l'obfuscation de JavaScript. En effet, Patrick y consacre un article et propose un exemple. Nous pouvons espérer que son exemple d'obfuscation JavaScript nous donne cette fois ci une information profitable.

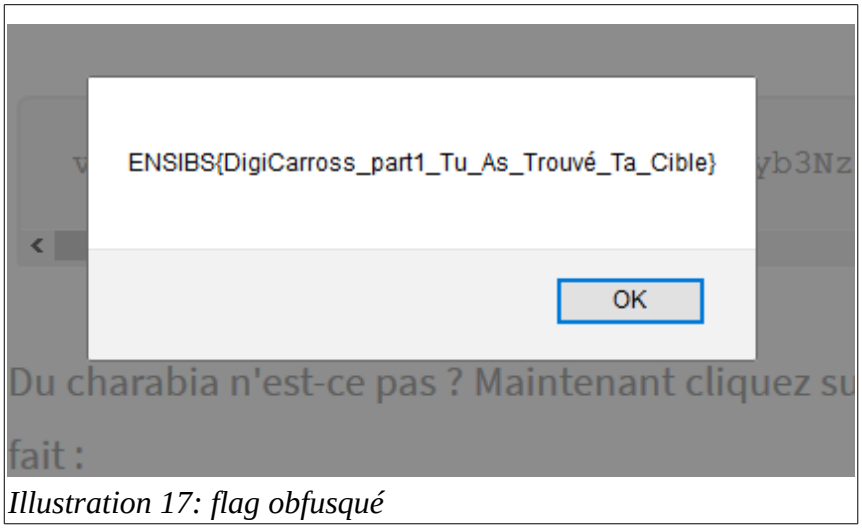

Illustration 17: flag obfusqué

Bingo ! En cliquant sur le bouton présent au sein de cet article, nous obtenons un flag qui nous confirme que nous nous intéressons bien à la bonne cible :

ENSIBS{DigiCarross_part1_Tu_As_Trouvé_Ta_Cible}

Patrick Dubois est donc une cible sur laquelle nous pouvons effectuer de l'OSINT. L'exploitation de cette cible correspond à la deuxième partie du challenge. Ainsi, la suite de ce challenge est expliquée dans le document « DigiCarross_WU_partie2.pdf ».

Conclusion

Comme de nombreuses personnes le savent, il est important de contrôler les différents éléments que nous mettons en ligne. Ceci vaut bien sûr pour les informations présentes au sein des projets GitHub. De nombreux systèmes et comptes en ligne sont compromis chaque jour à cause de dépôts de fichiers non contrôlés sur GitHub.

Pour information, GitHub propose un service payant (gratuit pour les étudiants) permettant de créer des projets GitHub privés et donc, normalement, seulement accessibles à des personnes autorisées.

Dans le cas de Patrick Dubois, les informations présentes au sein de son GitHub sont loin d'être critiques. D'autant plus que son blog a pour but final d'être mis en ligne et donc d'être accessible à tous.

Cependant, nous verrons dans la deuxième partie de ce challenge qu'il est également important de contrôler les informations contenues au sein d'un blog personnel.

Enfin, notre cible aurait dû créer un compte GitHub dédié à ses projets personnels. Ce compte GitHub n'aurait pas dû être mentionné dans son profil LinkedIn.