WRITE UP « LeBonNigglo »

CTF Inter IUT 2k18

ENSIBS CYBERDEFENSE

par @y0r3l

École d'ingénieurs
ensibs
Université Bretagne Sud

Date	Acteur	Mail de contact	Version
13/04/2018	@y0r3l	y0r3l@protonmail.com	1.0

INTRODUCTION

Ce challenge a été réalisé dans le cadre de la deuxième édition du CTF Inter IUT se tenant à l'ENSIBS de Vannes (Ecole Nationale Supérieur d'Ingénieurs de Bretagne Sud) le samedi 2 juin 2018.

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

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

Catégorie

OSINT (Open Source INTelligence)

Niveau de difficulté

Facile

Énonce

Le but de ce challenge est de récupérer le couple adresse mail et mot de passe d'un utilisateur de ce portail.

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

En effet, il devra tout d'abord analyser le site afin de trouver des informations pertinentes lui permettant d'obtenir des pistes pour ses futurs recherches.

Puis il devra trouver, sur des sites externes, l'adresse mail et le mot de passe du compte compromis 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. « Après vérification, tous les collaborateurs ont changé leur mot de passe. »
2. « monbocompte. »

Explication détaillée du challenge :

Tout d'abord, nous nous retrouvons face au portail web d'une entreprise nommée « LeBonNigglo ».

Ce site possède, à première vue, trois pages:

1. une page « Accueil » ;
2. une page « Se connecter » ; et
3. une page « Nos collaborateurs ».

La première page, « Accueil », contient trois news :

figure 1 – page « Accueil »

La première news sortie le 22 février 2018 nous informe que ce site est destiné aux différents collaborateurs de la société « LeBonNigglo ».

La seconde, sortie le 19 mars 2018, est une news concernant la sécurité des comptes utilisateurs du site. En effet, d'après cette dernière, l'ensemble de la base de données du site s'est retrouvé sur le deep web et certains comptes sont déjà référencés par des moteurs de recherche. De plus, afin de résoudre ce problème, il semblerait que des e-mails ait été envoyés aux collaborateurs afin que ces derniers changent leur mot de passe.

Enfin, la dernière news nous apprend que tous les mots de passe seront maintenant « hashés » et que seulement les « hashs » obtenus seront stockés dans la base de données.

La seconde page, « Se connecter », contient un formulaire. Ce dernier demande une adresse mail et un mot de passe afin de s'identifier sur le site.

Veuillez remplir tous les champs obligatoires (*) !

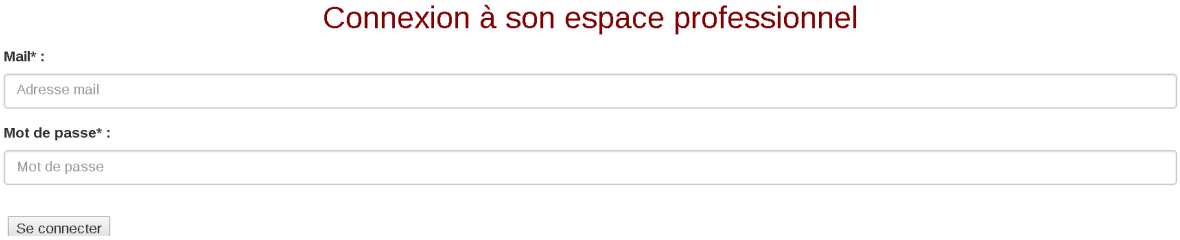

figure 2 – page « Se connecter »

La troisième, et dernière page, « Nos collaborateurs », contient une description de trois collaborateurs tout en incluant leur adresse mail professionnelle.

figure 3 – page « Nos collaborateurs »

Voici la liste des collaborateurs et leur adresse mail associée :

- David Zavatta – david.zatta@lebonnigglo.com
- Jason Reinhart – jason.reinhart@lebonnigglo.com
- Maria Reinhart – maria.reinhart@lebonnigglo.com

On peut donc en déduire que l'ensemble des adresses mails professionnelles des collaborateurs de l'entreprise « LeBonNigglo » est de la forme prénom.nom@lebonnigglo.com

Ainsi, au vu des news présentes sur la page d'accueil du site, les mots de passe associés à ces comptes se sont potentiellement retrouvés sur Internet.

Lançons tout d'abord un recherche Google pour le champs « @lebonnigglo.com » :

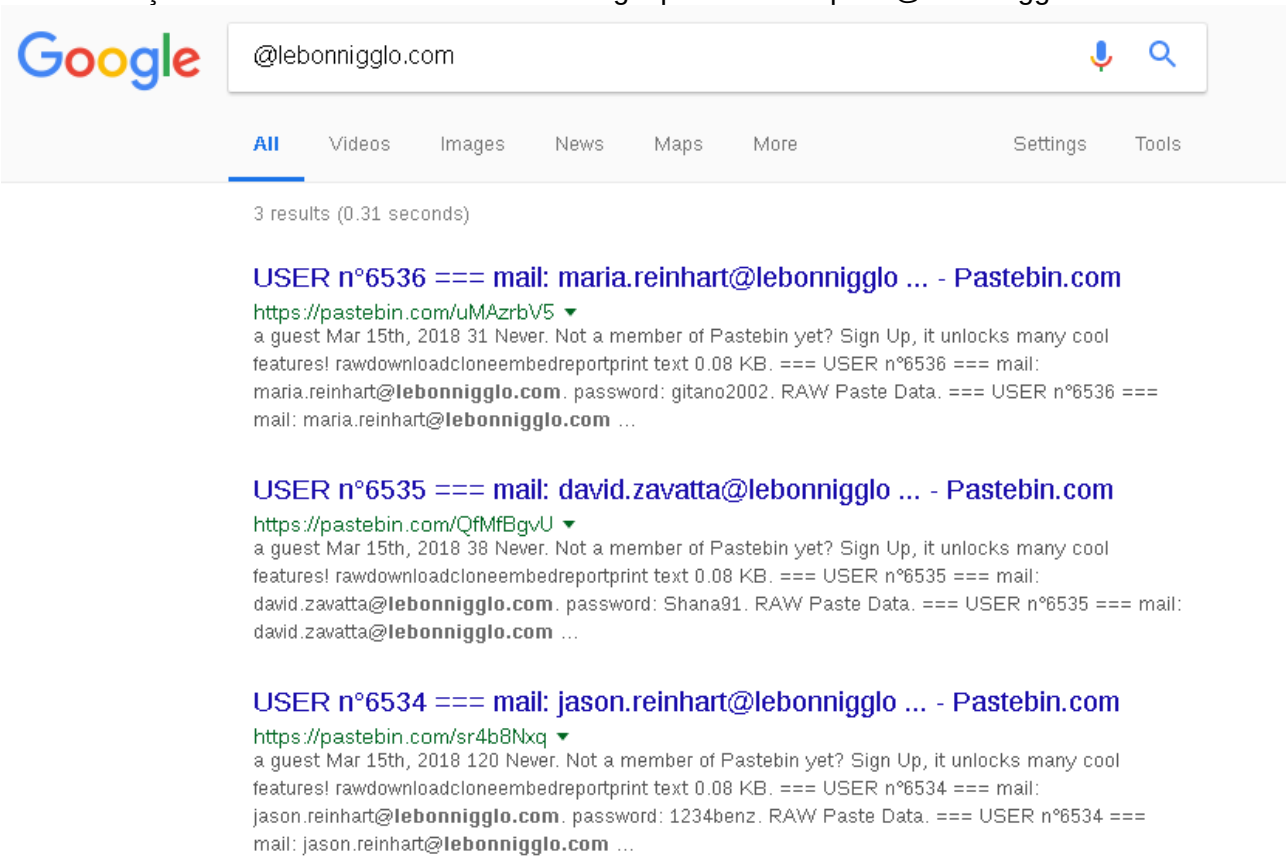

figure 4 – recherche Google sur le champs « @lebonnigglo.com »

La recherche retourne trois résultats, tous provenant du site « pastebin.com ». Ce site permet de mettre à disposition du texte facilement et rapidement : une fois le texte à partager renseigné sur le site, ce dernier va générer une url via laquelle d'autres internautes pourront accéder au texte.

Chacun des résultats semblent correspondre à un collaborateur.

En cliquant sur un des liens pastebin, nous obtenons quelque chose ressemblant à un utilisateur de la base de données du site « LeBonNigglo » :

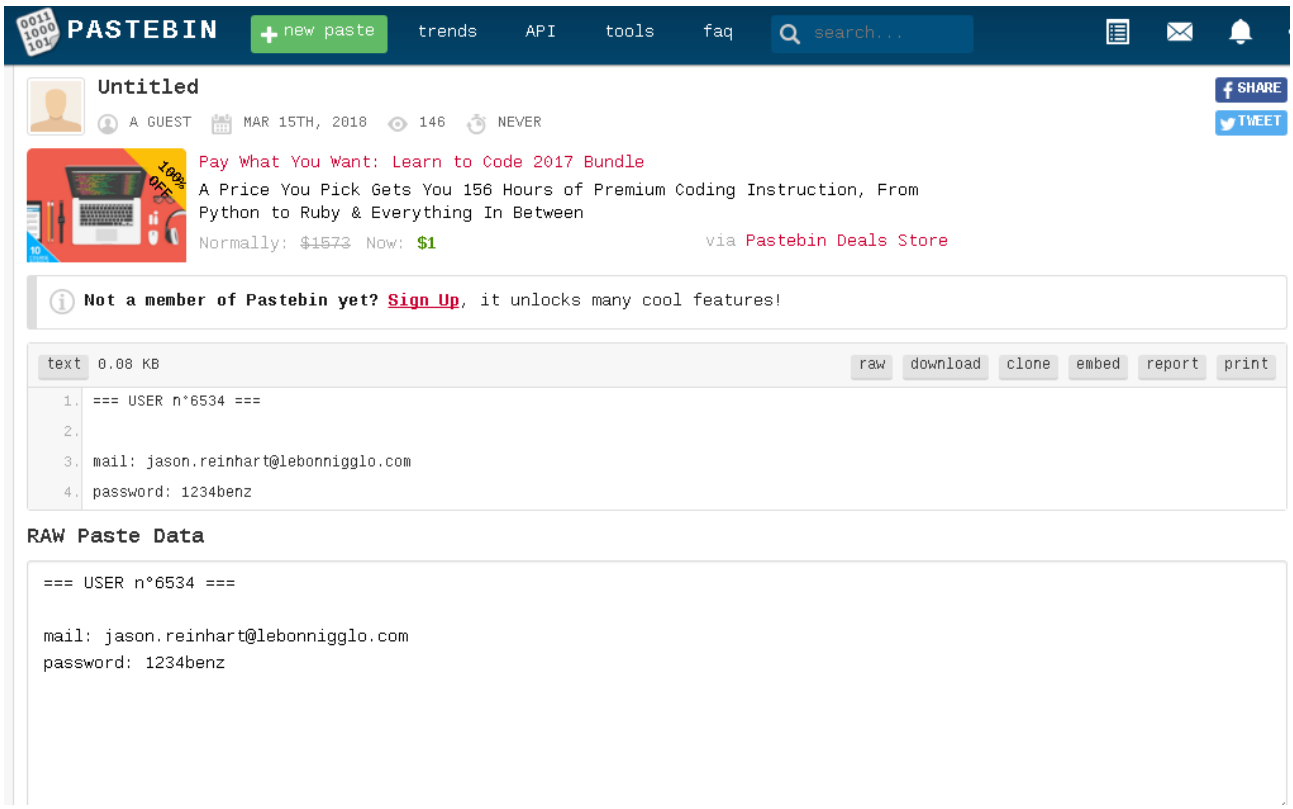

figure 5 – pastebin dont le mail est « jason.reinhart@lebonnigglo.com »

Chacun des trois pastebin trouvés par Google sont de cette forme : une adresse mail et un mot de passe.

Il est alors intéressant d'essayer de se connecter sur le portail professionnel de l'entreprise « LeBonNigglo » via les trois comptes utilisateurs disponibles sur pastebin.

Cependant, aucun des couples adresse mail/mot de passe ne fonctionnent :

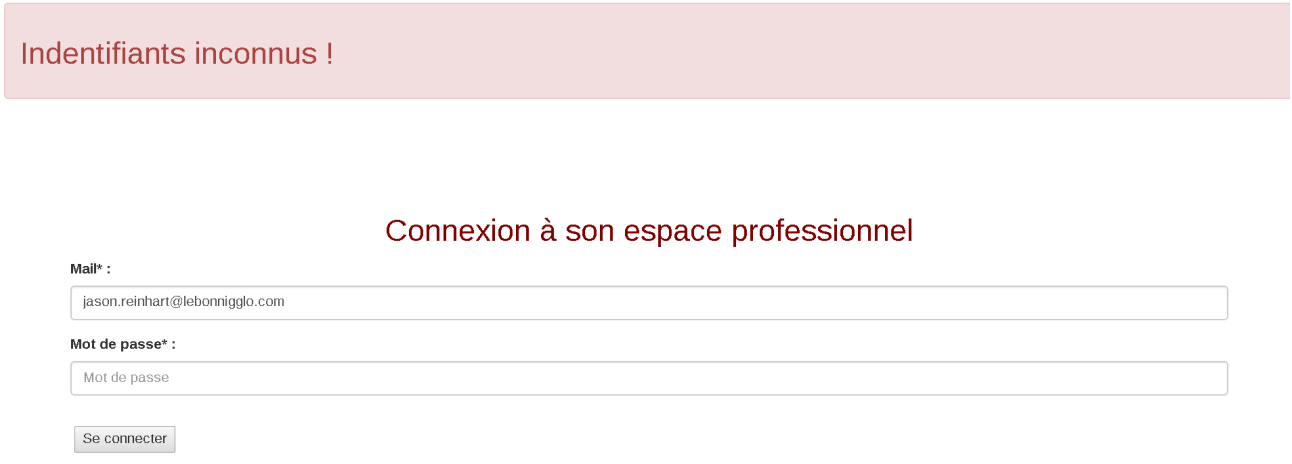

figure 6 – tentative de connexion avec le couple « jason.reinhart@lebonnigglo.com/1234benz »

On peut alors en déduire que les collaborateurs ont respecté les consignes et ont donc changé leur mot de passe sur ce portail.

Il est donc temps d'analyser de nouveau le site web afin de trouver un élément qui nous aurait échappé. Si on regarde bien le footer du portail professionnel, on y découvre que l'entreprise « LeBonNigglo » a fait appel à un prestataire extérieur afin de réaliser son site web :

figure 7– footer du site

La société ayant développée le portail se nomme « monbositeweb ». Il peut être alors intéressant d'effectuer une recherche Google sur le champs « @monbositeweb.com » en espérant que cette entreprise dispose d'un compte pour se connecter sur le site :

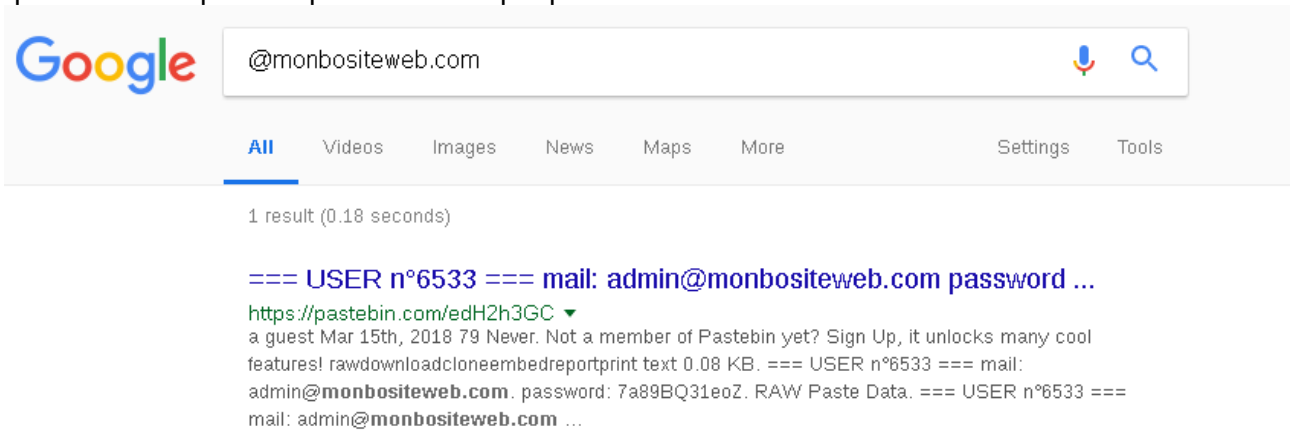

figure 8 – recherche Google sur le champs « @monbositeweb.com »

La recherche renvoie un résultat qui est encore une fois un pastebin :

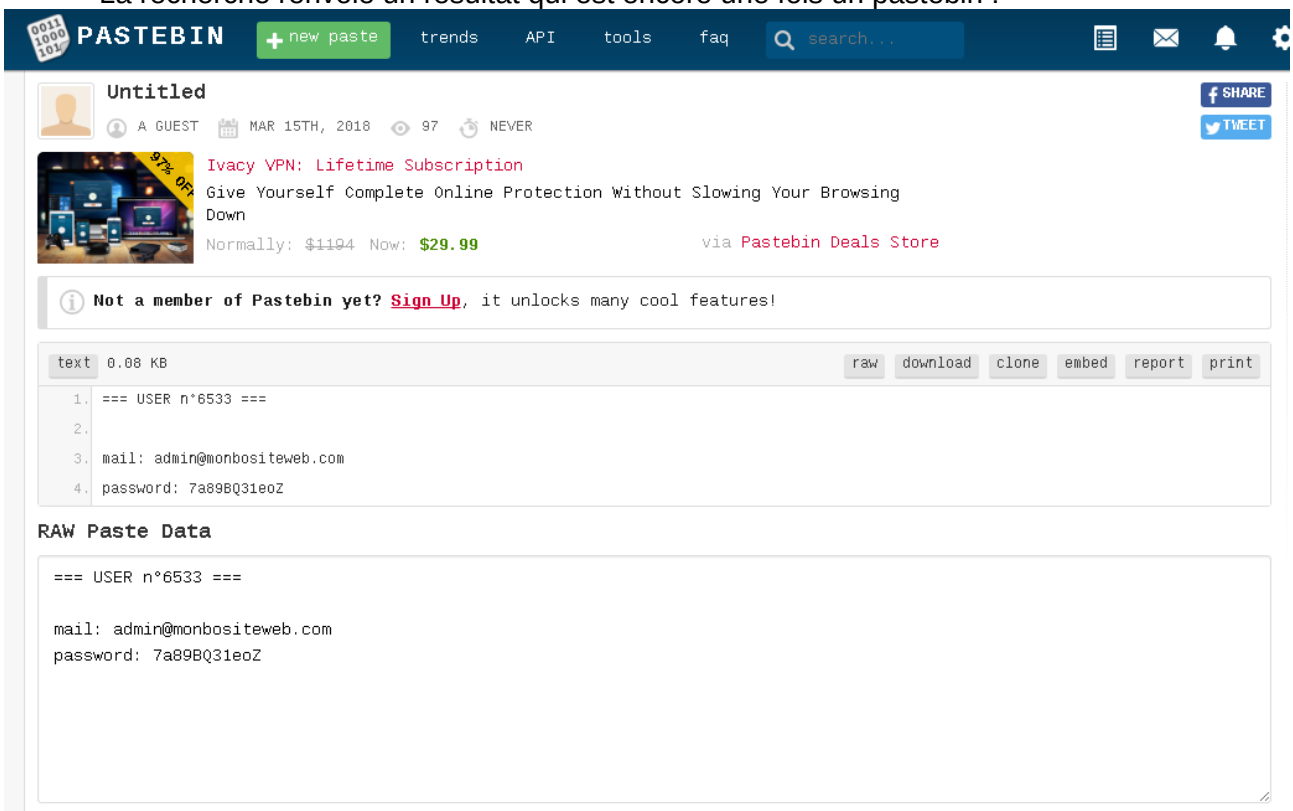

figure 9 – pastebin concernant la société « monbositeweb »

Ce dernier comprend également un couple adresse mail/mot de passe et est du même format que les pastebins trouvés auparavant. On peut donc en déduire que le couple d'identifiants est disponible sur Internet suite à la divulgation de la base de données du portail professionnel de l'entreprise « LeBonNigglo ».

Étant donné que ce compte n'est pas lié à un collaborateur, nous pouvons espérer que le mot de passe soit resté inchangé.

Essayons de nous connecter sur le portail web avec comme adresse mail « admin@monbositeweb.com » et comme mot de passe « 7a89BQ31eoZ ».

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

figure 10 – connexion réussie

Nous pouvons ainsi construire le flag avec le mot de passe du compte « admin@monbositeweb.com » :

ENSIBS{7a89BQ31eoZ}

Conclusion

Tout cela aurait pu être facilement évité si seulement l'entreprise « LeBonNigglo » avait tout d'abord vérifié quelle niveau de sécurité avait été mis en place sur leur base de données par le prestataire (monbositeweb.com).

En effet, ce dernier aurait dû seulement stocker le « hash » des mots de passe et non les mots de passe en clairs dans la base de données.

En outre, l'entreprise « LeBonNigglo » aurait dû également vérifier les comptes dormants et oubliés dans leur base de données. Que ce soit dans sites webs ou des services d'annuaires (comme l'Active Directory), les comptes dormants sont facilement compromis car ces derniers possèdent généralement des droits trop élevés, et des mots de passe ne respectant pas la politique de mots de passe de l'entreprise.

Cependant, dans le cas de TPE ou de PME, les compétences en informatique sont souvent limitées et peu de personnes sont vigilantes par rapport à ce genre de détails, pensant généralement qu'un contrat avec un prestataire leur assure un niveau de sécurité maximum.