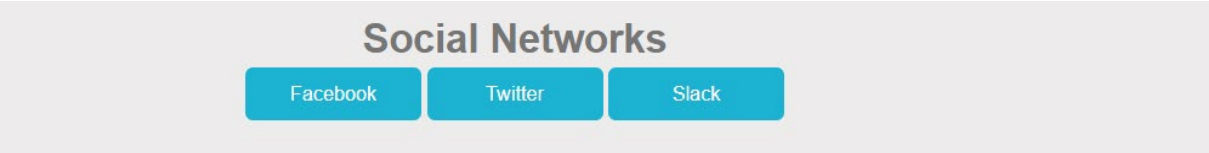
Rendu Challenge Cybersécurité

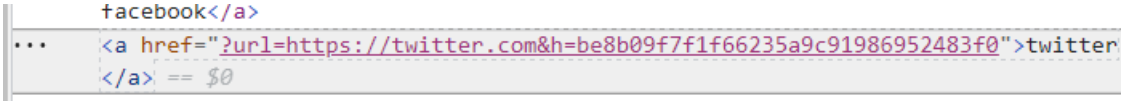
1. Web-Server: **HTTP - Open redirect.**

Ce Challenge consiste à trouver un moyen de redirection vers les pages souhaités (Facebook, Twitter, Slack).

Essayons de nous rediriger de manière basique vers la page twitter pour savoir si le lien href nous envoie directement vers la page souhaitée. Nous constatons que le lien fonctionne normalement.

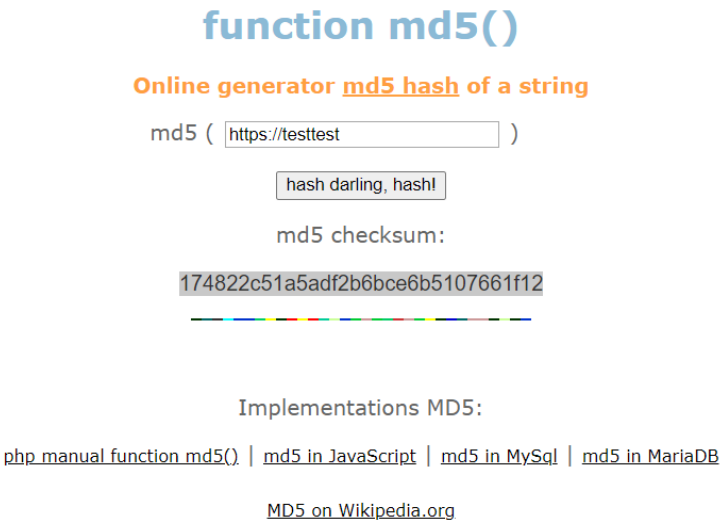


Copions le lien html de la page twitter pour l'utiliser rapidement dans la résolution du problème.



A l'aide du « reverse a MD5 hash » essayons de renverser la chaine **be8b09f7f1f66235a9c91986952483f0** et de trouver son inverse. Dans le lien, nous avons remplacé le mot twitter du lien par « **testtest** ».

Utilisons le https://testtest.com et à l'aide du générateur en ligne de MD5 essayons de générer la nouvelle chaine de mots

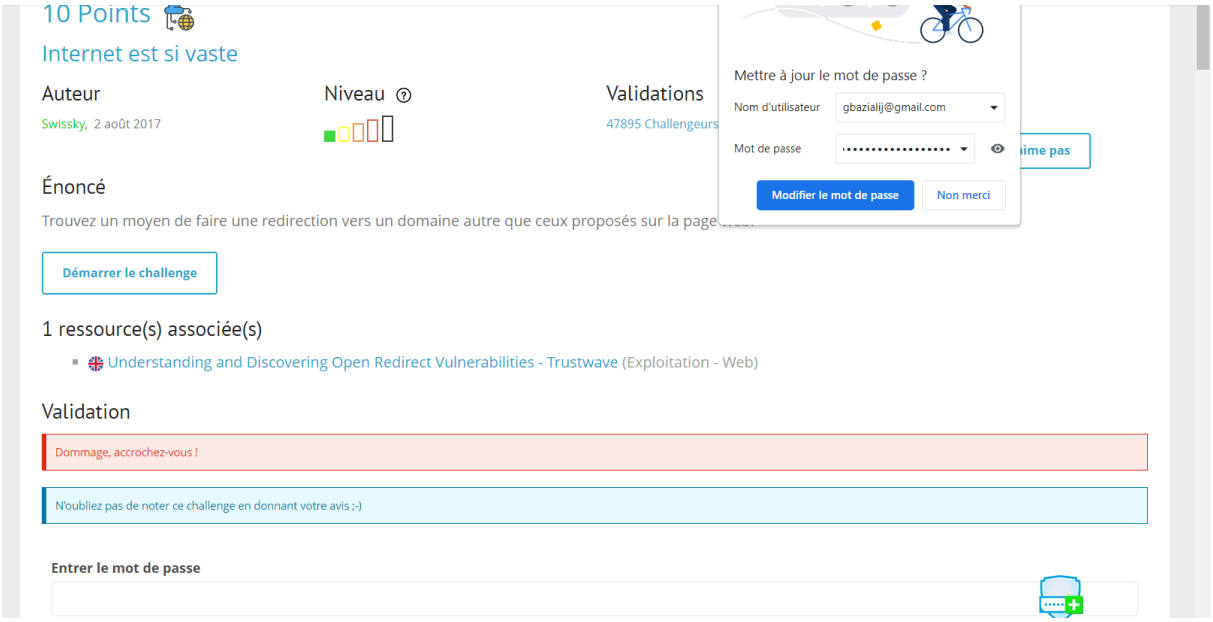


Nous avons maintenant le nouvel string « **174822c51a5adf2b6bce6b5107661f12** » nous allons le placer dans le lien pour obtenir un nouveau lien de redirection.

Utilisons le nouveau lien obtenu à l'aide des reverses effectués avec MD5 hash.

twitter.

Probablement nous serons rediriger vers une page qui va nous afficher le code pour la validation du challenge.



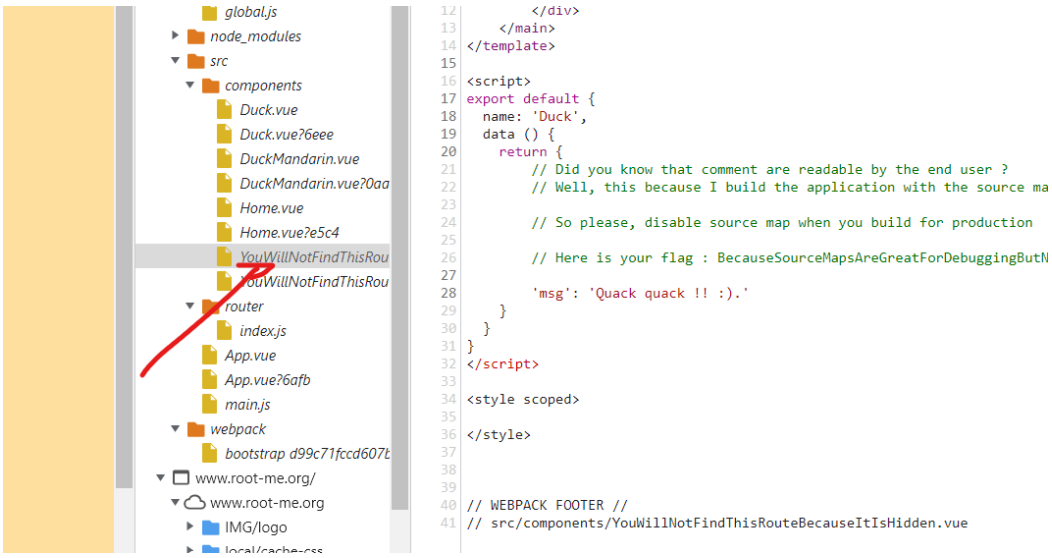
2. Web-Client : **JavaScritp WebPack**.

Ce Challenge consiste à trouver le mot de passe pour le compte utilisateur. Tout d'abord nous commençons par inspecter le code de la page en question.

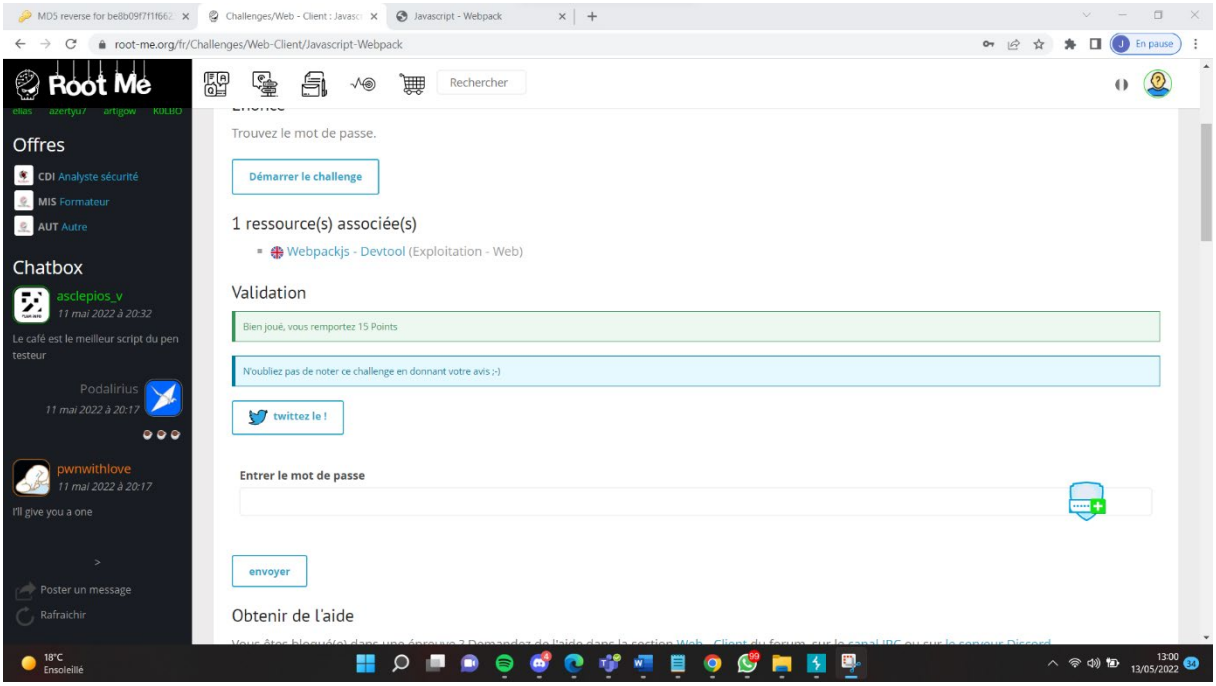
Pour une meilleure inspection, il faut vérifier chaque redirection du text/javascript pour avoir une idée sur son contenu.

Analysons chaque dossier contenu dans la page affichée.

Pour se rendre dans chaque dossier. Dans le dossier src cherchons les composants React Js. Parmi les composants il y a un dossier renommé ci-dessous.



Dans ce fichier React il est écrit en commentaire « He is a flag » c'est que le mot de passe pour la validation de cette page est : **BecauseSourceMapsAreGreatForDebuggingButNotForProduction.**



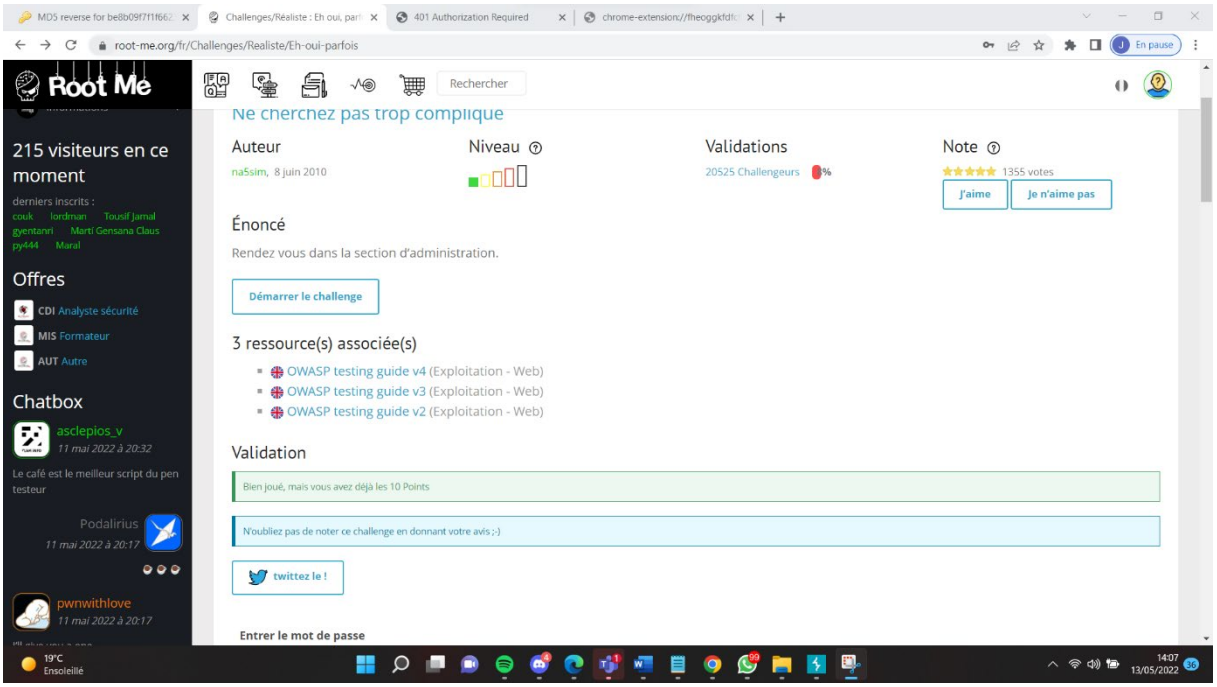
3. Réaliste : **Eh oui, parfois.**

Ce challenge consiste à aller dans la section administration.

Commençons par inspecter la page en question en analysant son code source.

Ensuite dans l'url de la page, nous avons écrit le mot « admin ».

A l'aide de Burp Suite Community nous allons compiler le code HTML en suivant les requêtes dans le terminal. En suivant l'évolution du réseau sur le proxy nous voyons comment les informations se modifient sur la page. Et Quand le http est OK le code s'affiche de la sorte : **0010110111101001.**



4. Réseau : **TELNET – authentification**

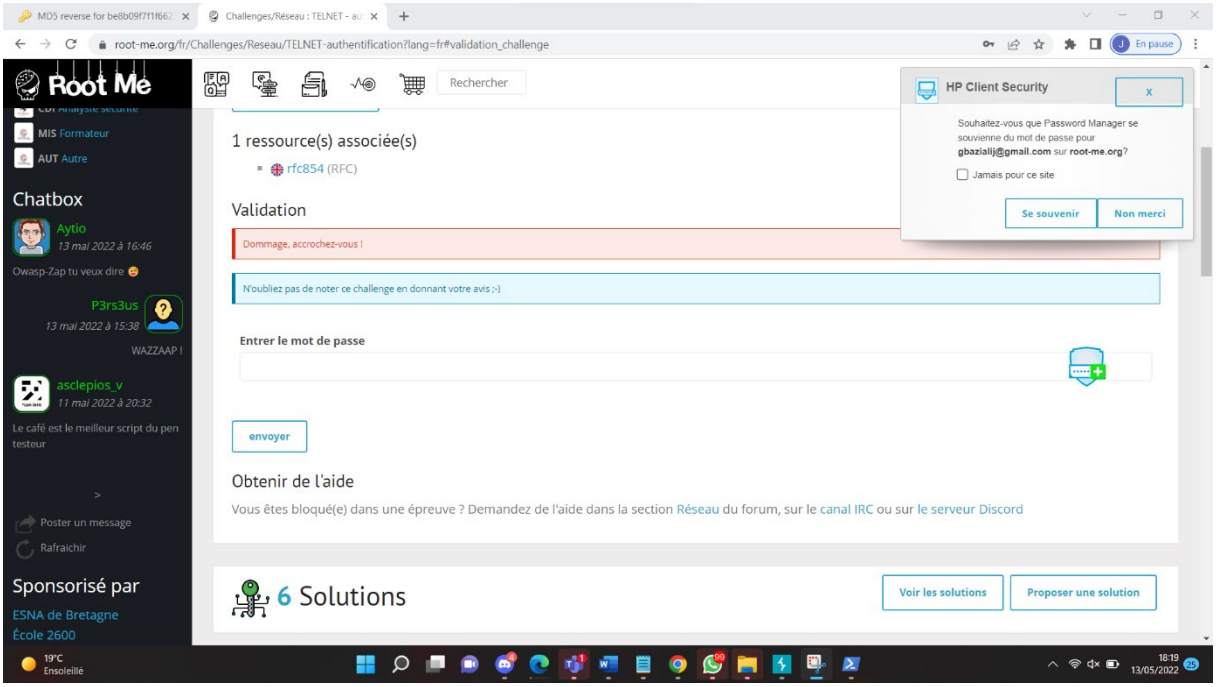
Ce challenge consiste à retrouver le mot de passe de l'utilisateur.

Tout d'abord commençons par démarrer le challenge. Le fichier téléchargé sera lu dans le centre de réseau de notre pc. Une fois que le rooter se met en marche nous allons essayer de décrypter le message envoyé par le réseau à notre server.

Dans l'url de notre réseau nous avons mis le mot TELNET à la place pour voir le résultat escompté.

D'où le code de ce challenge est : **cdts3500**

S


Root Me
Rechercher
MIS Formateur
AUT Autre
Chatbox
Aytio
13 mai 2022 à 16:46
Owasp-Zap tu veux dire
P3rs3us
13 mai 2022 à 15:38
WAZZAAP !
asclepios_v
11 mai 2022 à 20:32
Le café est le meilleur script du pen testeur
Poster un message
Rafraichir
Sponsorisé par
ESNA de Bretagne
École 2600
1 ressource(s) associée(s)
rfc854 (RFC)
Validation
Dommage, accrochez-vous !
N'oubliez pas de noter ce challenge en donnant votre avis ;-)
Entrer le mot de passe
envoyer
Obtenir de l'aide
Vous êtes bloqué(e) dans une épreuve ? Demandez de l'aide dans la section Réseau du forum, sur le canal IRC ou sur le serveur Discord
6 Solutions
Voir les solutions
Proposer une solution
HP Client Security
Souhaitez-vous que Password Manager se souvienne du mot de passe pour gbazialij@gmail.com sur root-me.org?
Jamais pour ce site
Se souvenir
Non merci
19°C
Ensoleillé
18:19
13/05/2022