



#TechforPeople

M2 EFREI Test d'Intrusion

TP 1 : Construction du laboratoire de travail et inscription sur le site HackTheBox

20 Octobre 2020

Table des matières

Objectif et attentes	3
Introduction	3
Construction du laboratoire	4
Installation de la machine virtuelle (Kali Linux)	4
Configuration de Burp Suite	4
Utilisation de Burp suite	8
Rejouer une requête	8
Comparer deux requêtes	8
Restreindre le scope	9
HackTheBox	10
Inscription	10
Fonctionnement	10
Challenge - Emdee five for life	11
Challenge - Illumination	12
Webographie	13

1 Objectif et attentes

1.1 Introduction

L'objectif principal du TP est la construction de votre laboratoire de travail. Grâce à la mise en place de cet environnement, vous aurez en votre possession l'ensemble des outils nécessaires pour effectuer les prochains TP.

Au sein de ce laboratoire, vous devez disposer d'une machine virtuelle avec la distribution Kali Linux. Grâce à l'utilisation de Kali Linux, vous aurez à votre disposition un portefeuille d'outils pré-installé.

L'ensemble des TPs sera réalisé sur la plateforme HackTheBox. HackTheBox est une plate-forme en ligne permettant de tester et de développer ses compétences en matière de tests d'intrusion et de cybersécurité. Elle contient plusieurs défis constamment mis à jour. Certains d'entre eux simulent des scénarios du monde réel et d'autres se tournent davantage vers un défi de type CTF.

Afin de s'inscrire à cette plateforme, vous devez relever un challenge. Vous aurez surement besoin de l'outil Burp Suite (**Version Community**) en tant que Proxy afin d'y arriver.

Burp Suite est une suite d'outils développée en Java par la société PortSwigger Ltd. Il existe trois versions de Burpsuite :

- **La version Community (Gratuite)**
- La version Professional (Payante)
- La version Enterprise (Payante)

2 Construction du laboratoire

2.1 Installation de la machine virtuelle (Kali Linux)

La première étape de ce TP consiste à installer la machine virtuelle “Kali Linux”.

Pour cela, merci de suivre les étapes ci-dessous :

1. Téléchargez la dernière version sur le site officiel
 - a. <https://www.kali.org/downloads/>
2. Créez une machine virtuelle sur votre hyperviseur de type 2
3. Installez la distribution
 - a. <https://www.kali-linux.fr/installation/installer-kali-linux-en-francais>

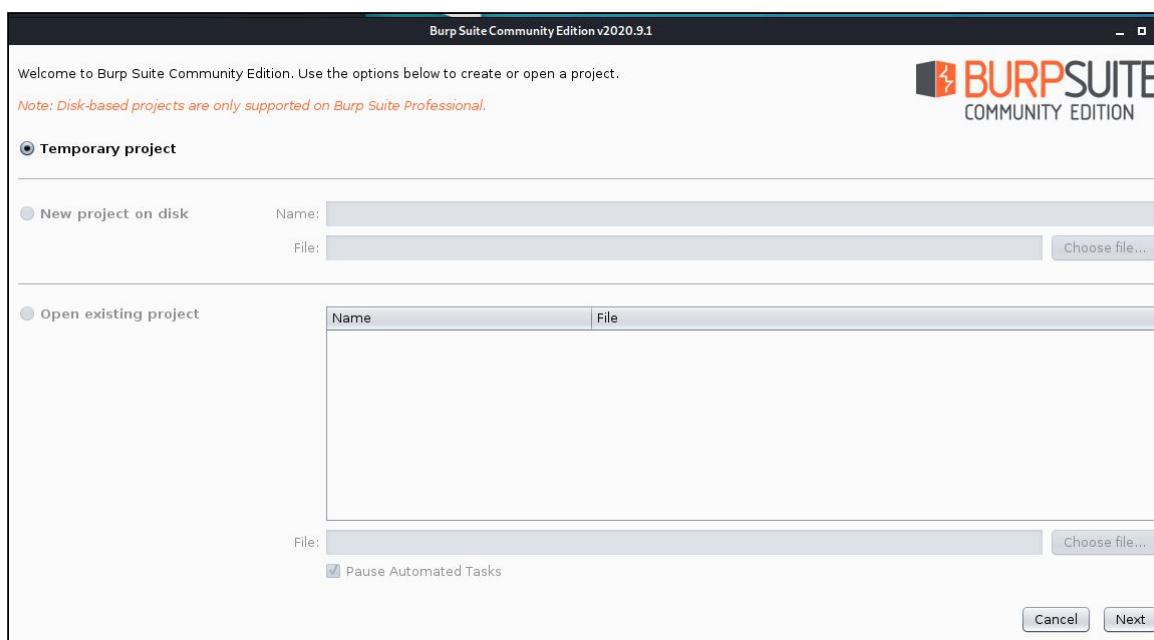
[TIPS]

Si votre clavier est en anglais lors du démarrage de la machine virtuelle, vous pouvez effectuer la commande “setxkbmap fr” dans un terminal

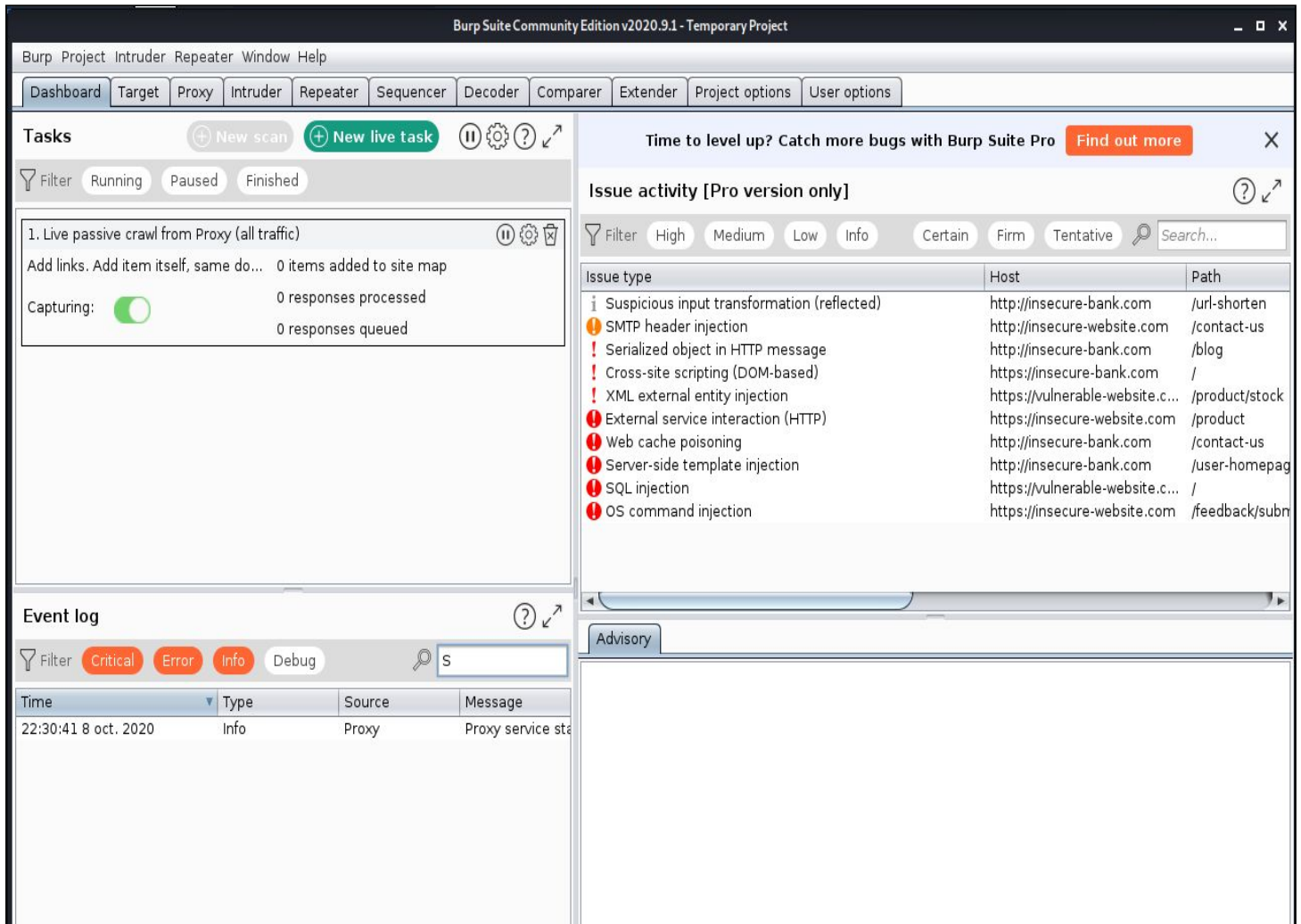
2.2 Configuration de Burp Suite

La première étape consiste à lancer Burp suite à l'aide de la commande “Burpsuite” dans un terminal.

Vous devrez obtenir la fenêtre ci-dessous :



Cliquez sur « Next » puis sur « Start Burp ». Vous atterrirez sur la page principale de Burp:



Issue activity [Pro version only]

Issue type	Host	Path
Suspicious input transformation (reflected)	http://insecure-bank.com	/url-shorten
SMTP header injection	http://insecure-website.com	/contact-us
Serialized object in HTTP message	http://insecure-bank.com	/blog
Cross-site scripting (DOM-based)	https://insecure-bank.com	/
XML external entity injection	https://vulnerable-website.c...	/product/stock
External service interaction (HTTP)	https://insecure-website.com	/product
Web cache poisoning	http://insecure-bank.com	/contact-us
Server-side template injection	http://insecure-bank.com	/user-homepag
SQL injection	https://vulnerable-website.c...	/
OS command injection	https://insecure-website.com	/feedback/subn

Event log

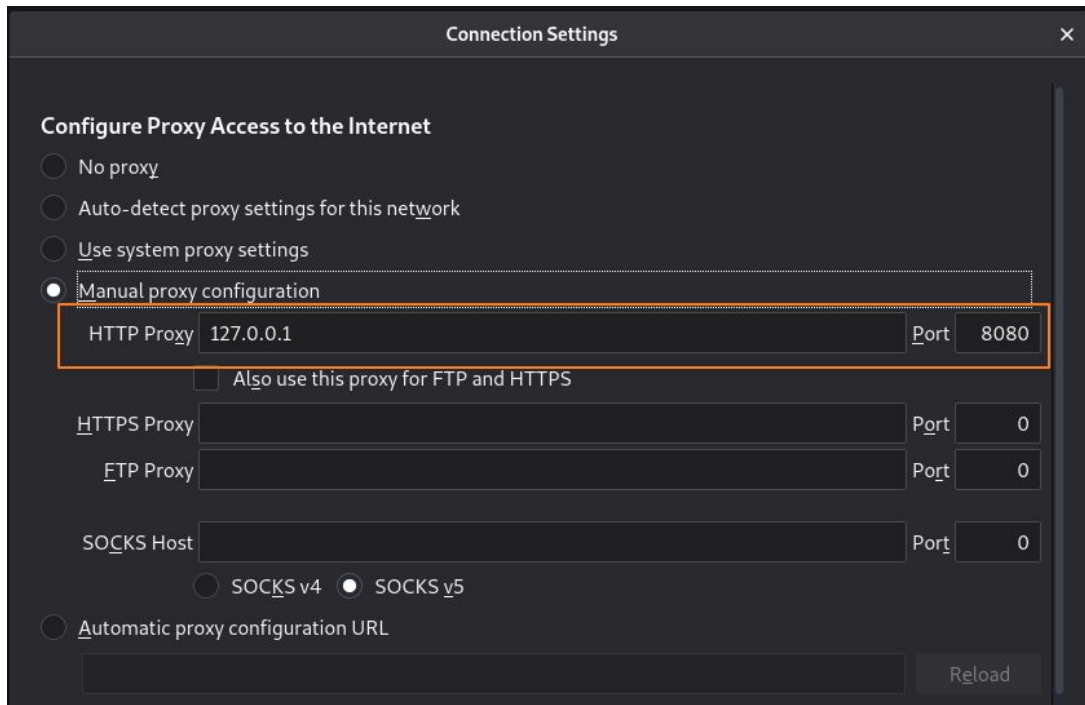
Time	Type	Source	Message
22:30:41 8 oct. 2020	Info	Proxy	Proxy service sta

Sur la barre du dessus, vous avez les différents outils disponibles. Au cours de ce TP nous verrons comment rejouer une requête et comparer deux requêtes.

Cependant, il faut commencer par configurer le proxy. C'est l'outil le plus utilisé de la suite et pour cause, il permet d'intercepter toutes les requêtes envoyées depuis le navigateur, de les modifier/rejouer/interrompre et de réceptionner la réponse du serveur.

Pour cela il va falloir configurer le navigateur pour qu'il envoie toutes les requêtes au Burp Proxy. Vous trouverez les étapes à effectuer sur la page suivante.

Exemple pour Firefox : Allez dans les “préférences” puis dans les “paramètres réseau” afin de renseigner la configuration du proxy avec l'adresse de loopback et le port 8080



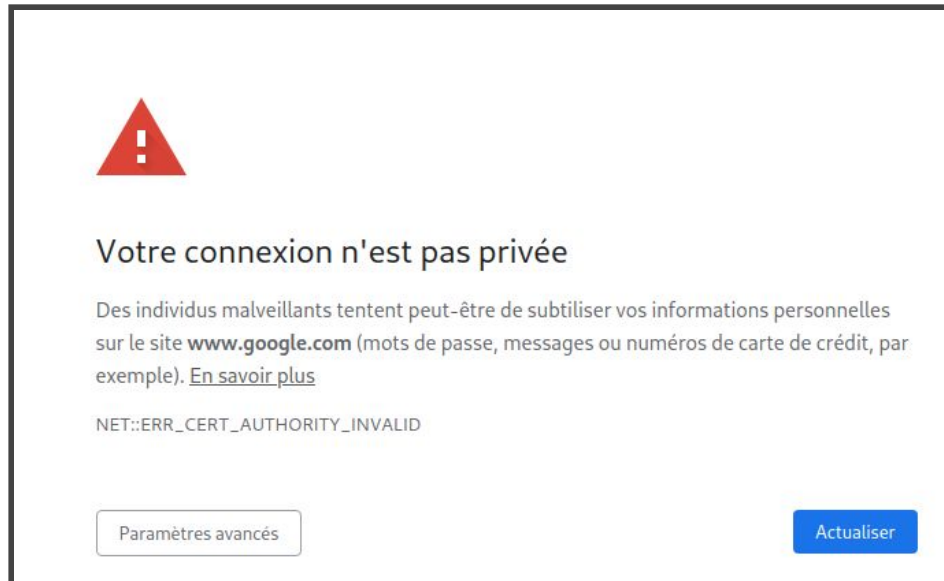
Grâce à cette configuration, toutes les requêtes sont envoyées au proxy Burp.

[TIPS]

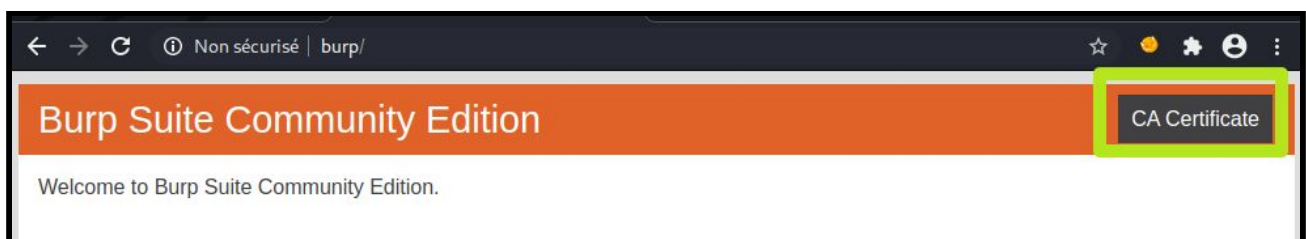
Il existe plusieurs plugins pour Firefox et Chrome qui permettent de basculer entre plusieurs configuration proxy comme Foxy Proxy, Proxy SwitchyOmega.

Penser à bien cocher la case “Also use this proxy for FTP and HTTPS” pour intercepter aussi le trafic en HTTPS.

Maintenant que toutes les requêtes sont envoyées au proxy Burp, si vous essayez d'effectuer une requête vous allez obtenir le message suivant :



Pour régler ce problème, il faut télécharger le certificat d'autorité de Burp et l'installer dans votre navigateur. Pour cela, accédez à l'url "<http://Burp/>" en ayant le proxy activé. Puis cliquez sur CA Certificate et téléchargez le certificat.



Comme vous vous en doutez, après avoir exporter le certificat d'autorité il faut l'importer. Vous pouvez suivre les étapes ci-dessous :

Pour Firefox :

<https://portswigger.net/Burp/documentation/desktop/getting-started/proxy-setup/certificate/firefox>

Pour Chrome :

<https://portswigger.net/Burp/documentation/desktop/getting-started/proxy-setup/certificate/chrome>

2.3 Utilisation de Burp suite

2.3.1 Rejouer une requête

Pour rejouer une requête à l'aide de Burp, il y a la fonctionnalité "Burp Repeater". Burp Repeater est un outil simple permettant de manipuler et de réémettre manuellement des messages HTTP et WebSocket individuels, et d'analyser les réponses de l'application.

Vous pouvez utiliser Repeater à toutes sortes de fins, telles que la modification des valeurs de paramètres pour tester les vulnérabilités basées sur les entrées, l'émission de requêtes dans un ordre spécifique pour tester les failles de logique, et la réémission de requêtes à partir de problèmes du Burp Scanner pour vérifier manuellement les problèmes signalés.

L'interface principale du répéteur vous permet de travailler simultanément sur plusieurs messages différents, chacun dans son propre onglet. Lorsque vous envoyez des messages à Repeater, chacun d'entre eux s'ouvre dans son propre onglet numéroté. Vous pouvez renommer les onglets en double-cliquant sur l'en-tête de l'onglet.

Afin de mieux comprendre le fonctionnement, vous pouvez visionner la vidéo suivante :

<https://portswigger.net/Burp/documentation/desktop/tools/repeater/using>

[TIPS]

Pour envoyer une requête dans le Repeater, vous pouvez utiliser le raccourci clavier "CTRL+R"

2.3.2 Comparer deux requêtes

L'outil comparer est utile lorsque vous voulez voir comment les différentes valeurs des paramètres et des en-têtes permettent des changements subtils dans les réponses que vous recevez. Par exemple, il est utile de voir comment l'application réagit à un utilisateur valide, à une combinaison de mots de passe invalide par rapport à un utilisateur invalide et à une combinaison de mots de passe invalide. Cela peut aider à énumérer les noms d'utilisateurs.

Plus d'information disponible sur le lien suivant :

<https://portswigger.net/Burp/documentation/desktop/tools/comparer>

2.3.3 Restreindre le scope

Grâce à la configuration proxy, toutes les requêtes sont capturées par Burp sans aucun filtre. Cependant, il existe un outil nommé Target qui permet de filtrer la ou les cibles.

Pour plus d'information sur l'utilisation de l'outil, vous pouvez visionnez la vidéo suivante :

<https://portswigger.net/Burp/documentation/desktop/tools/target/using>

2.3.4 Les autres fonctionnalités

Si vous souhaitez obtenir plus d'information quant au fonctionnement des autres outils disponible dans la suite Burp , vous pouvez consulter le lien suivant <https://portswigger.net/Burp/documentation/desktop/tools>

3 HackTheBox

3.1 Inscription

Après avoir configuré votre machine virtuelle ainsi que Burp, il est temps de vous inscrire sur la plateforme HackTheBox.

HackTheBox est une plateforme en ligne permettant de tester et de développer ses compétences en matière de tests d'intrusion et de cybersécurité. Elle contient plusieurs défis constamment mis à jour. Certains d'entre eux simulent des scénarios du monde réel et d'autres se tournent davantage vers un défi de type CTF.

Afin de s'inscrire à cette plateforme, vous devez relever un challenge. Après avoir réussi ce défi, vous recevrez un code d'invitation.

Le lien du challenge est : <https://www.hackthebox.eu/invite>

Vous aurez surement besoin de l'outil Burp...

3.2 Fonctionnement

Après avoir réussi à vous inscrire, il faut que vous vous connectiez au réseau de machine à auditer via VPN.

Pour cela, vous pouvez suivre les instructions disponibles sur le site de HackTheBox : <https://help.hackthebox.eu/getting-started/v2-introduction-to-vpn-access>

[RAPPEL]

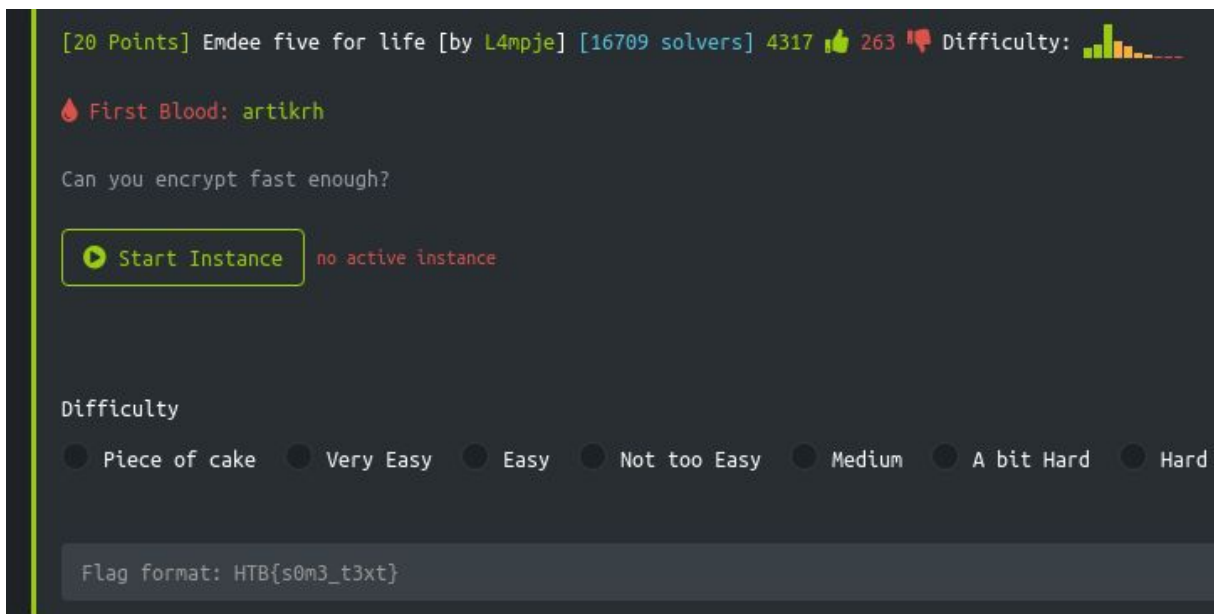
Afin de lancer une connexion VPN, vous pouvez utiliser la commande `sudo openvpn --config /path`

```
0:34:23 lx6xc@CryptoJoker ~ sudo openvpn --config ~/.htb.ovpn 1 ↵
Fri Oct 9 00:34:53 2020 OpenVPN 2.4.9 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [
EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 2 2020
Fri Oct 9 00:34:53 2020 library versions: OpenSSL 1.1.1g 21 Apr 2020, LZO 2.10
Fri Oct 9 00:34:53 2020 Outgoing Control Channel Authentication: Using 256 bit message
hash 'SHA256' for HMAC authentication
Fri Oct 9 00:34:53 2020 Incoming Control Channel Authentication: Using 256 bit message
hash 'SHA256' for HMAC authentication
```

3.3 Challenge - Emdee five for life

Votre première mission sur HackTheBox est de résoudre le challenge “Emdee five for life” (catégorie web).

Pouvez-vous chiffrer assez rapidement ?



Quelques indices :

- Afficher le code source
- Automatiser le process

3.4 Challenge - Illumination


Vous êtes mandatés par une entreprise suite à un changement de plateforme. En effet, un développeur junior vient de passer à une nouvelle plateforme de contrôle des sources.

Pouvez-vous trouver le jeton secret ?

Merci de réaliser le challenge Illumination dans la catégorie Forensics.



The screenshot shows the challenge details for 'Illumination' on the Devoteam platform. At the top, it displays a trophy icon, '[20 Points]', the challenge name 'Illumination', the author '[by SherlockSec]', '[7131 solvers]', '1730' likes, '38' dislikes, and a difficulty bar. Below this, it shows 'First Blood: jkr'. The challenge description reads: 'A Junior Developer just switched to a new source control platform. Can you find the secret token?'. At the bottom, there is a 'Download' button and the zip password: 'hackthebox', followed by the sha256 hash: 'cbd6cd9a9379d0f4193f35c09fa60c0753c0d31cb2848ed5d575ba99062a1331'.

[20 Points] Illumination [by SherlockSec] [7131 solvers] 1730 38 Difficulty: 

First Blood: jkr

A Junior Developer just switched to a new source control platform. Can you find the secret token?

[Download](#) Zip Password: hackthebox sha256: cbd6cd9a9379d0f4193f35c09fa60c0753c0d31cb2848ed5d575ba99062a1331

4 Webographie

- Présentation des différents outils Burp
 - <https://portswigger.net/burp/documentation/desktop/tools>
- HackTheBox
 - <https://www.hackthebox.eu/>
- Kali
 - <https://www.kali.org/>
- FoxyProxy
 - <https://chrome.google.com/webstore/detail/foxyproxy-standard/gcknhkkoolaabfmInjonogaafnjlfnp?hl=en>