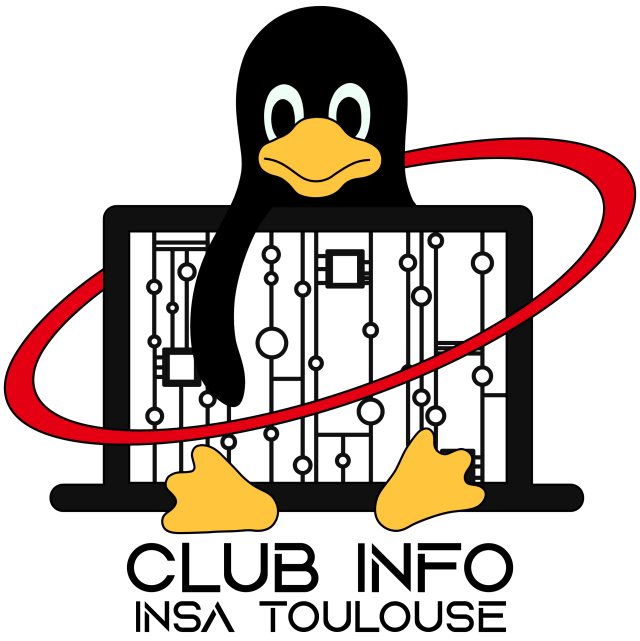
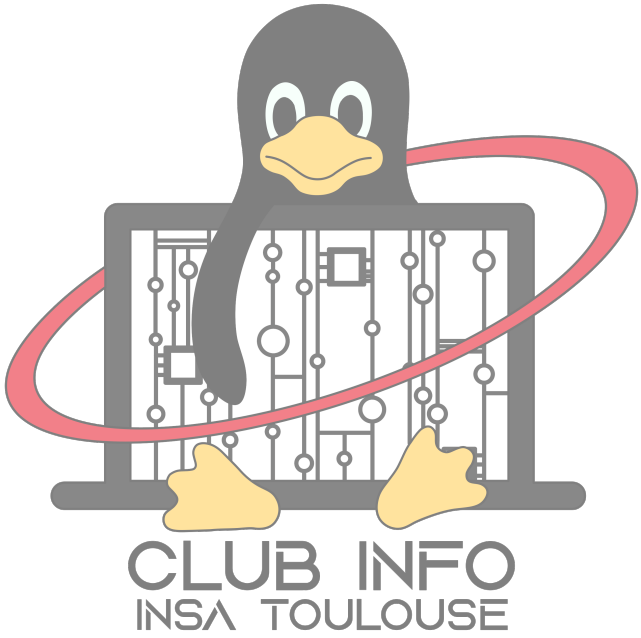
# Parcours de formation hacking : fiche outils web 1 : le navigateur

Daresse(Thomas Hernandez)

2024-2025



## Table des matières



# 1 Prérequis

Cette formation est accessible à tout débutant. Évidemment, des connaissances préalables en informatique et l'habitude d'utiliser des sites webs dans la vie de tous les jours seront des atouts utiles pour être confortable tout au long de cette formation. Si des bases n'ont pas été couvertes ou si des concepts vous semblent flous n'hésitez pas à demander à votre responsable formation hacking pour plus d'explications. (NB. N'hésitez pas à sauter certaines partis si vous pensez déjà maitriser le concept en question et à y revenir si vous en ressentez le besoin.)

Prérequis :

— Savoir se rendre sur un site web.
— Savoir ce que sont un fichier et un dossier.
— Pour certains exercices pratiques l'utilisation d'un "proxy" sera necessaire, l'installation de BURP est donc conseillée mais non nécessaire pour ce module.

# 2 Lexique

— le navigateur : Une application qui permet d'accéder à internet et de lire des pages web. (exemples : Brave, Chrome, Edge, Opéra, firefox) ( /!\à ne pas confondre avec le moteur de recherche)
— le moteur de recherche : Programme utilisé généralement par le navigateur pour parcourir le Web à la recherche de la ressource souhaitée. (exemples : Google, yahoo, duckduckgo, Ecosia ).
— le web ou world wide web(WWW) : Ensemble des ressources auquels vous pouvez accéder via un navigateur (exemples : serveurs, fichiers, page web )
— Internet : Infrastructure mondiale consistant en une interconnexion de réseau, permettant à votre ordinateur, seulement connecté à votre box de communiquer avec un serveurs se trouvant à l'autre bout du monde.
— requête http (ou requête web) : message envoyé via internet, le plus souvent par un navigateur à un serveur, afin d'intéragir avec une ressource web.
— URL : (Uniform Ressource Locator) une adresse web qui permet d'accéder à une ressource spécifique sur Internet, comme une page web, une image, un fichier, etc.
— code source : Ensemble de fichier contenant du code écrit en HTML, CSS et JavaScript. Le code source est la partie que votre navigateur reçoit pour pouvoir afficher votre page web.
— cookie : petit fichier déposée par un site web dans votre navigateur et qu'il récupèrera lorsque vous reviendrez. (ex : les cookies d'authentification vous permettent de ne pas avoir à vous reconnecter à chaque fois que vous retournez sur votre réseau social favoris)
— HTML : (HyperText Markup Language) Langage de balisage utilisé pour structurer le contenu d'une page web, comme les textes, les images, les liens, et les listes.
— CSS : (Cascading Style Sheets) Langage de style utilisé pour décrire l'apparence et la mise en forme d'une page web, tels que les couleurs, les polices, les marges, et les dispositions.
— JavaScript : Langage de programmation utilisé pour ajouter de l'interactivité et des fonctionnalités dynamiques aux pages web, comme les animations, les formulaires interactifs, et les mises à jour de contenu en temps réel.

# 3 Internet et le web :

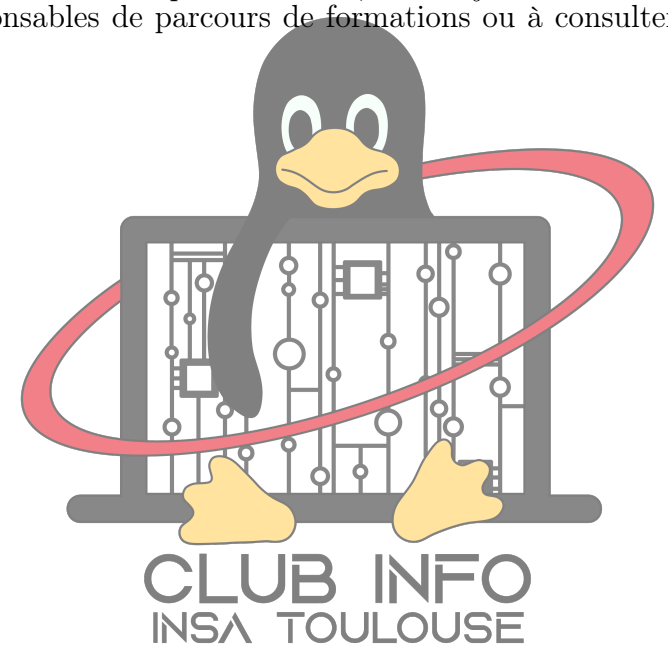
## 3.1 définitions :

**Internet :** Infrastructure mondiale consistant en une interconnexion de réseau, permettant à votre ordinateur, seulement connecté à votre box de communiquer avec un serveurs se trouvant à l'autre bout du monde. (date de création : début des années 1960)

FIGURE 1 – Diagramme d'une connexion internet

Afin de "cartographier" internet chaque réseau possède une addresse ip *ex :* 10.10.2.15, chaque nombre pouvant aller de 0 à 255. Celle-ci permettant d'identifier chaque machine sur les réseaux et chaque réseau sur internet.

Ces adresses ip sont connus par les routeurs et enregistrés dans des tables de routage ce qui leur permet de communiquer entre-eux, si ce sujet vous intéresse n'hésitez pas à contacter vos responsables de parcours de formations ou à consulter les ressources en annexe.



# 4 La Page Web :

On se rend tous sur plein de sites webs tous les jours, mais que se passe t-il au moment où nous cliquons sur un résultat fourni par notre moteur de recherche et affiché dans notre navigateur.

Lorsque vous effectuez ce clic, votre navigateur envoie une requête au serveur qui héberge le site voulu. (NB. Pour en savoir plus sur cette étape, approfondissez les concepts d'address IP et de DNS. Ces concepts sont des concepts de réseaux que nous survolerons plus tard.) Le serveur qui reçoit cette requête répondra alors avec un fichier : le code source de la page web désirée.

Afin de localiser la ressource précise souhaitée le naviagateur utilise un URL (Uniform Ressource Locator)

**Structure :** Protocole ://NomDeDomaine.ExtensionDeNomDeDomaine/Dossier/.../Dossier/Fichier

**Exemple :** https ://fr.wikipedia.org/wiki/World_Wide_Web

Ce fichier est ensuite interprété par votre navigateur pour donner la page que vous avez demandé. Nous pouvons accéder à ce fichier grâce au raccourcis Ctrl+u. Ce fichier contient du code écrit en HTML(structure le site), CSS(rend le site joli) et JavaScript(permet de rendre les pages webs interactives).

**Exemples :** HTML :

- cette balise représente un paragraphe
- <a href="https ://destination-du-lien.fr">texte du lien</a>
- <img src="lien-ou-chemin-de-fichier-vers-limage-a-afficher">
  à noter que, pour cette dernière balise, lorsqu'interprété par votre navigateur celui-ci enverra une requête GET (destinée à obtenir une ressource) vers l'url contenu dans le paramètre src afin d'obtenir l'image, cette information pourra être très importante plus tard.

CSS : (le css sert quasi exclusivement à l'aspect esthétique du site et nous intéresse donc peu)

JS : Le JavaScript en revanche permet d'intéragir avec le navigateur et d'executer des instructions ( ouvrir une nouvelle page, rediriger l'utilisateur, intéragir avec les cookies etc...)

- location="http ://destination.com" permet de rediriger l'utilisateur vers un autre site
- console.log(Document.cookie) permet d'afficher les cookies de l'utilisateur dans la console

Si vous ne comprenez pas tout à ce dernier langage ne vous inquiétez pas nous l'approfondirons dans des cas pratiques.

# 5 les fonctionnalités importantes du navigateur :

Dans cette section nous verrons tout ce qu'il est possible de faire avec un navigateur et que l'utilisateur classique n'utilise pas. Tous les exemples présentés ici seront réalisé avec firefox, les autres navigateur sont capable des mêmes choses avec des interfaces différentes, libre à vous d'utiliser celui qui vous convient le mieux. Nous avons déjà vu le raccourcis Ctrl+u pour afficher le code source mais ce n'est pas la seule manière d'intéragir avec le code source d'une page web. En effet, souvent on préferera utiliser le raccourcis Ctrl+shift+i (shift = maj) afin d'ouvrir l'inspecteur.

FIGURE 2 – Inspecteur du navigateur

1. Ce bouton permet de selectionner l'élément souhaité directement sur la page web et d'accéder au code source correspondant.
2. Le code source affiché.
3. La console qui permet d'avoir possiblement des messages d'erreurs ou d'executer du JS (JavaScript)
4. Menu vous permettant d'accéder à vos cookies.
5. Debugger : vous permet d'accéder aux scripts JS et de gérer leur execution

## 5.1 Exercices :

Afin de pratiquer un peu rendez vous sur le site `https://www.root-me.org/` puis dans la section challenge, web client et explorez à l'aide de ce que vous venez d'apprendre.

- Web CLIENT : HTML - boutons désactivés
- Web CLIENT : Javascript - Authentification
- Web CLIENT : Javascript - Source
- Web CLIENT : Javascript - Authentification 2
- Web CLIENT : Javascript - Obfuscation 1 (NB. Pour celui-ci n'hésitez pas à utiliser le siteweb CyberChef et à vous renseigner sur la cryptographie. ça tombe bien, il existe un parcours de formation du club info sur ce sujet.)

# 6 Annexes :

## 6.1 ressources supplémentaires :

— `https://www.ionos.fr/digitalguide/serveur/know-how/quest-ce-quune-adresse-ip/`les adresses ip
— `https://www.cloudflare.com/fr-fr/learning/network-layer/what-is-routing` le routage
— `https://www.w3schools.com/html/default.asp` pour apprendre le HTML.