COMPTE RENDU

WEB APP TESTING

Réalisé par :

- **OTHMANE TAYBI**

Encadré par :

- **M.Omor**

Web App Testing :

Le test Web, ou test de site Web, consiste à vérifier votre application Web ou votre site Web à la recherche de bogues potentiels avant sa mise en ligne et est accessible au grand public. Les tests Web vérifient la fonctionnalité, la convivialité, la sécurité, la compatibilité et les performances de l'application Web ou du site Web.

Au cours de cette étape, des questions telles que celle de la sécurité des applications Web, le fonctionnement du site, son accès aux utilisateurs handicapés ainsi qu'aux utilisateurs réguliers et sa capacité à gérer le trafic sont vérifiés.

Comment tester une application Web ?

Les types de test suivants peuvent être effectués en fonction de vos exigences de test Web.

Test de fonctionnalité d'un site Web :

- Testez tous les liens.
- Formulaires d'essai.
- Tester les cookies.
- Tester HTML et CSS.
- Tester le flux de travail de l'entreprise.

Tests d'utilisation :

- Testez la navigation sur le site.
- Testez le contenu.

Test d'interface :

- Application.
- Serveur Web.
- Serveur de base de données.

Test de base de données.

Test de compatibilité :

- Test de compatibilité du navigateur.

Test de performance.

Test de sécurité.

Test de foule.

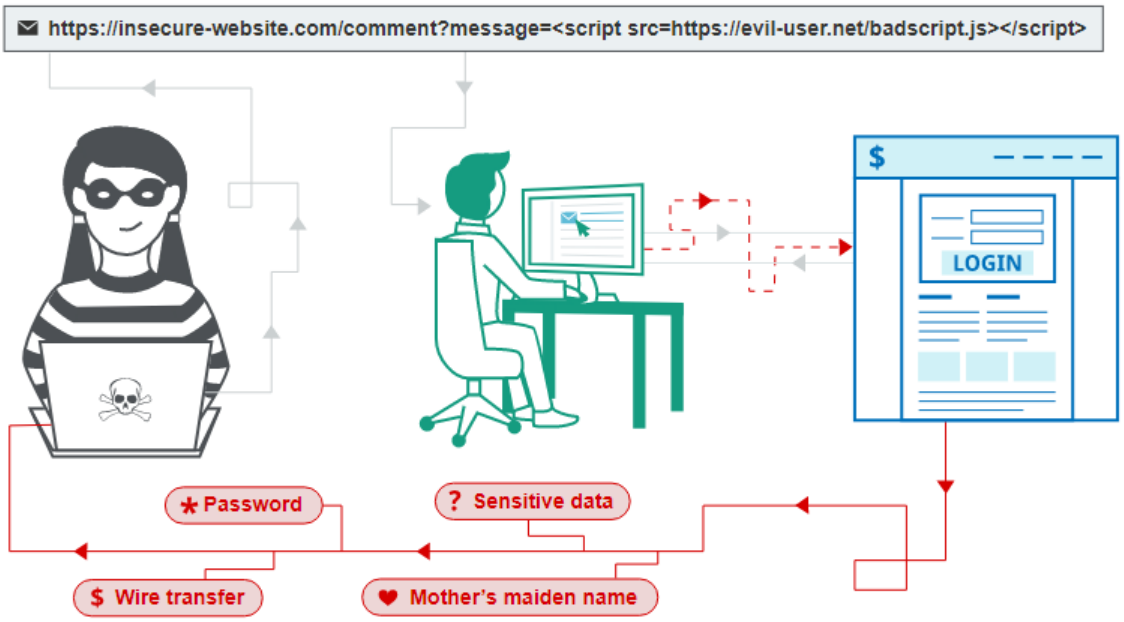
XSS

Qu'est-ce que XSS :

➢ XSS également connu sous le nom de (Cross-site Scripting) est une vulnérabilité de sécurité Web qui permet à un attaquant de compromettre les interactions des utilisateurs avec une application vulnérable. Cela permet à un attaquant de contourner la même politique d'origine, qui est conçue pour séparer différents sites Web les uns des autres. Les vulnérabilités de Cross-site Scripting permettent normalement à un attaquant de se faire passer pour un utilisateur victime, d'effectuer toutes les actions que l'utilisateur est capable d'effectuer et d'accéder à toutes les données de l'utilisateur. Si l'utilisateur victime dispose d'un accès privilégié au sein de l'application, l'attaquant peut être en mesure d'obtenir un contrôle total sur toutes les fonctionnalités et données de l'application.

Comment fonctionne XSS ?

Les scripts intersites fonctionnent en manipulant un site Web vulnérable afin qu'il renvoie du code JavaScript malveillant aux utilisateurs. Lorsque le code malveillant s'exécute dans le navigateur d'une victime, l'attaquant peut entièrement compromettre son interaction avec l'application.



Les types d'attaques XSS

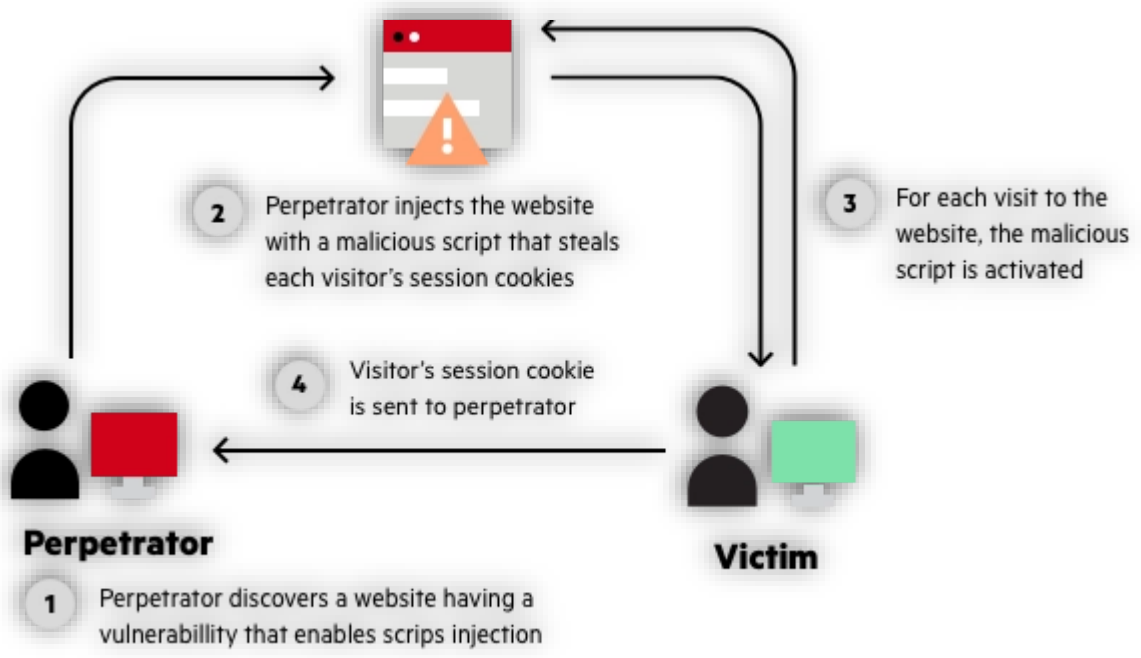
Il existe trois principaux types d'attaques XSS. Ceux-ci sont :

- Reflected XSS.
- Stored XSS.
- DOM-based XSS.

Reflected XSS :

Où le script malveillant provient de la requête HTTP actuelle.

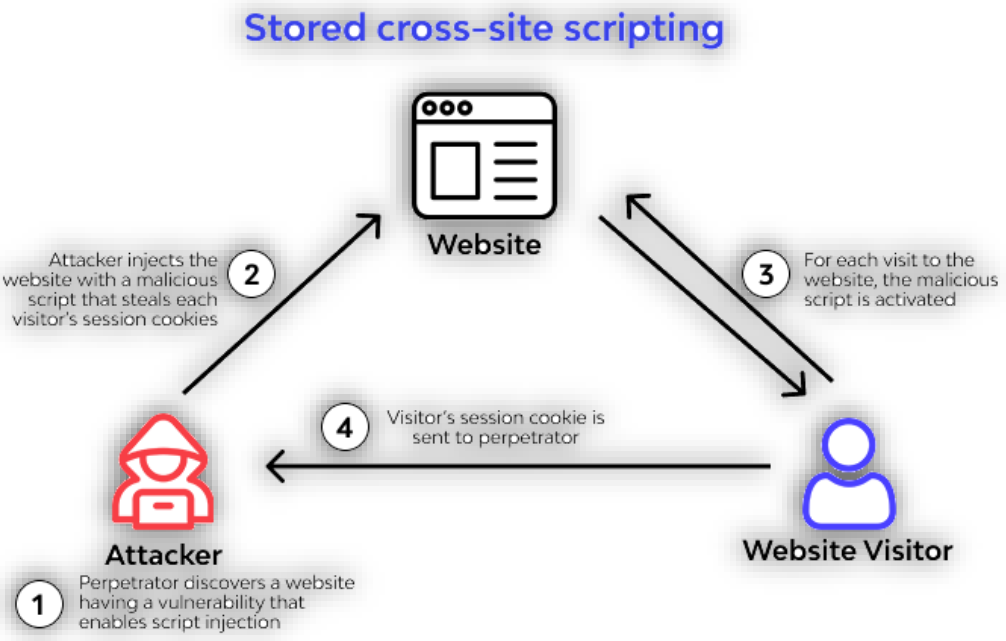
Exemple :



Stored XSS :

Où le script malveillant provient de la base de données du site Web.

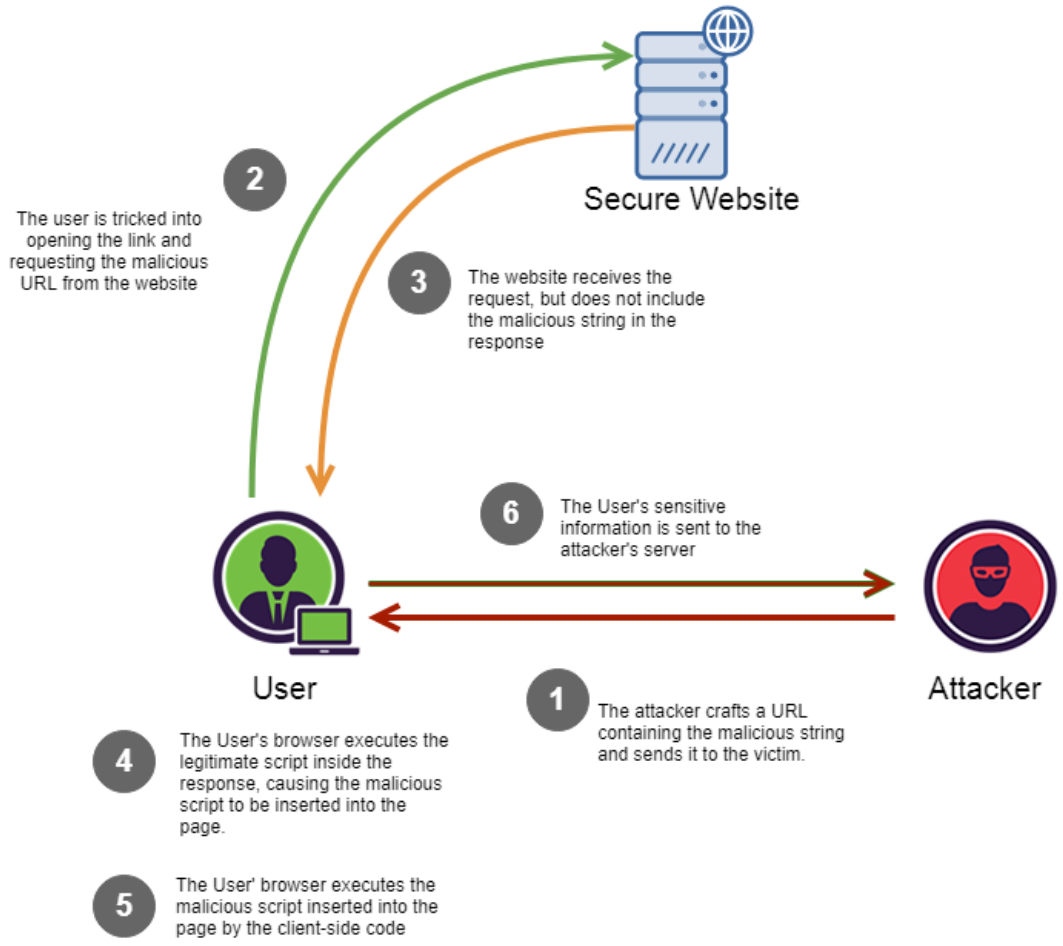
Exemple :



DOM-based XSS :

Où la vulnérabilité existe dans le code côté client plutôt que dans le code côté serveur.

Exemple :



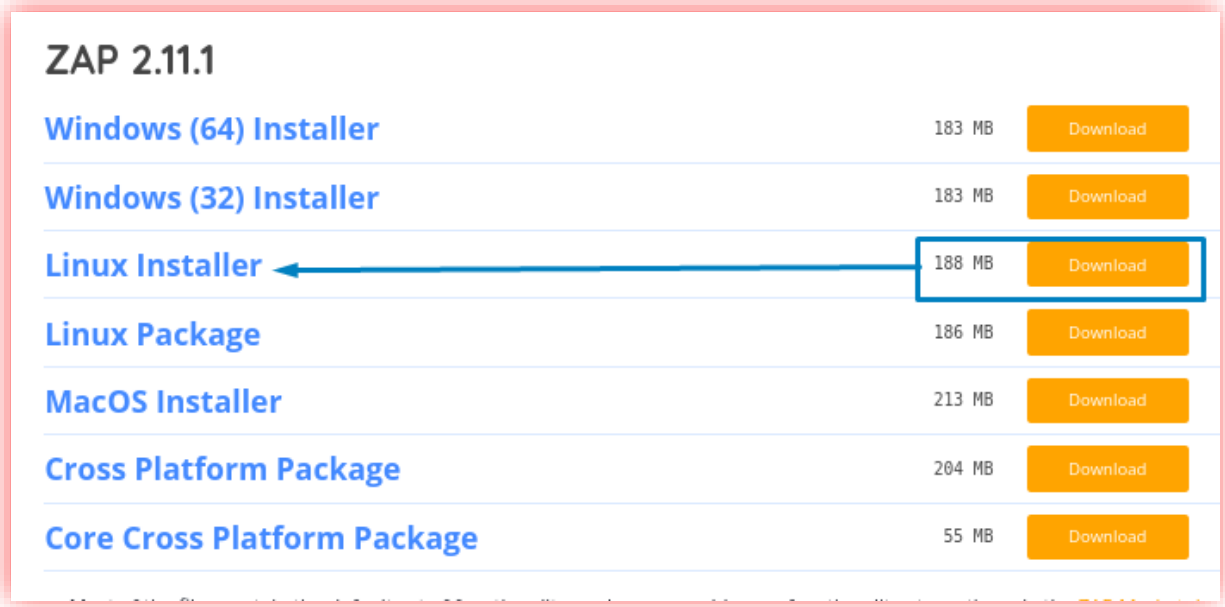
OWASP ZAP

OWASP ZAP :

OWASP (Open Source Web Application Security Project) est une communauté en ligne qui produit et partage des publications, des méthodologies, des documents, des outils et des technologies gratuits dans le domaine de la sécurité des applications. ZAP (Zed Attack Proxy) est l'un des outils les plus importants développés par cette communauté. L'objectif principal de cet outil est d'effectuer une analyse de sécurité pour les applications Web.

Installation :

On télécharger le fichier sous linux.

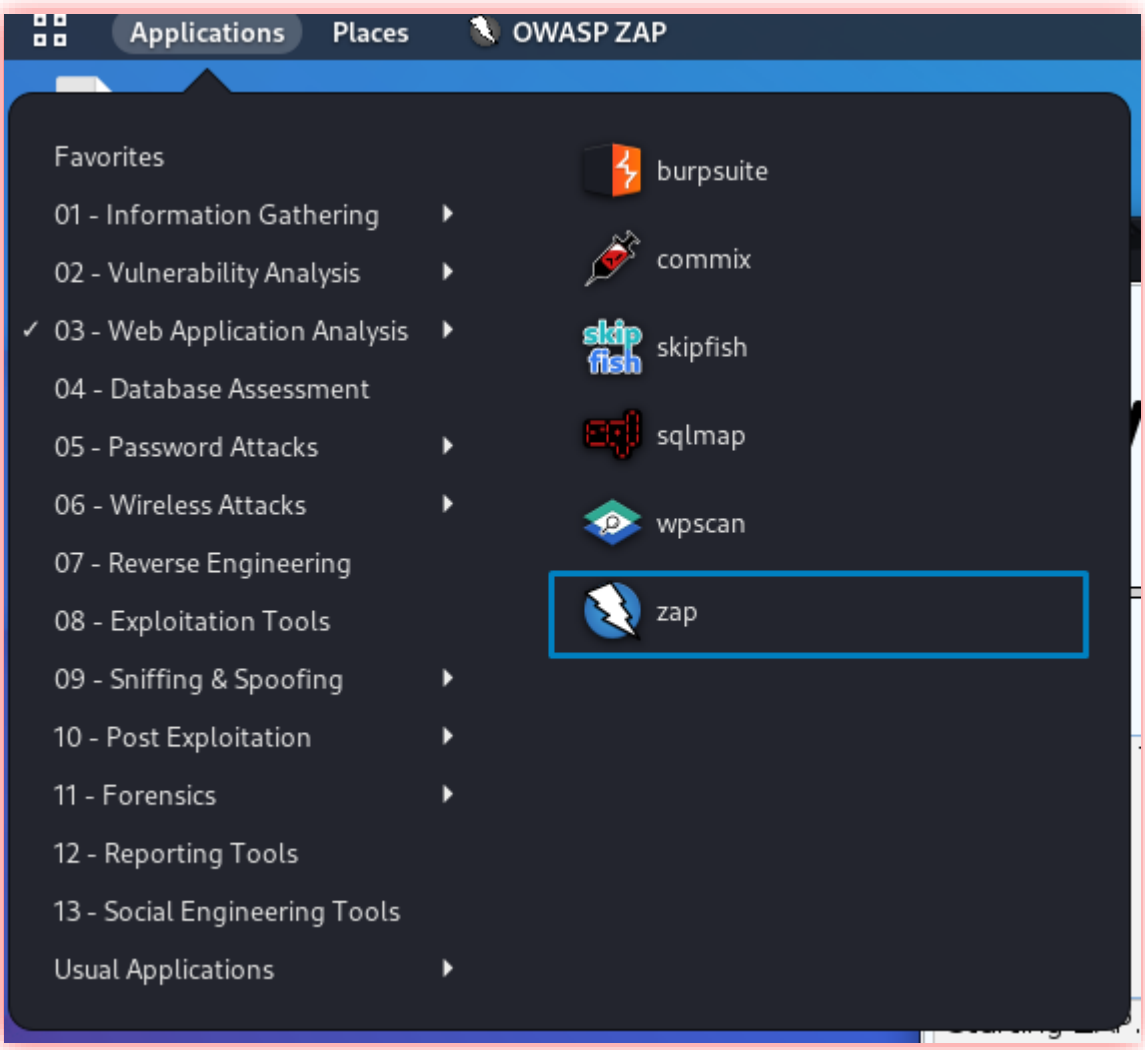


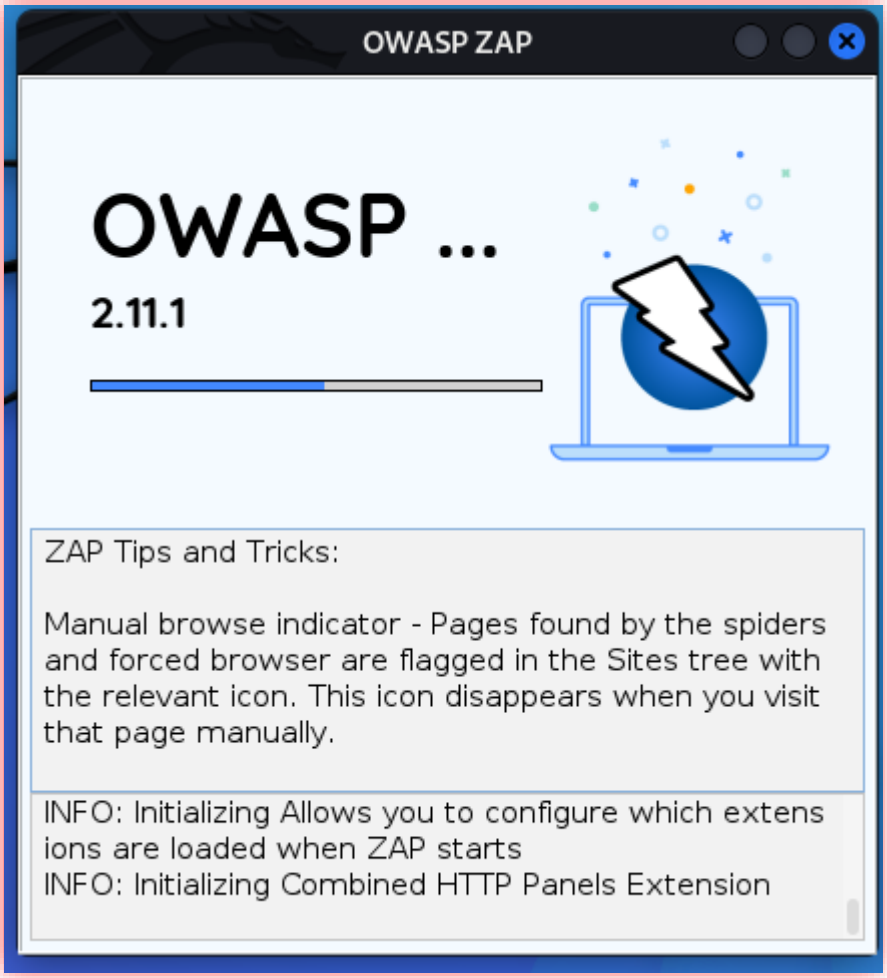
On exécuter le fichier qui on a télécharger :

```
┌──(taybiothmane㉿serverDNS)-[~/Downloads]
└─$ sudo ./ZAP_2_11_1_unix.sh                                    126 ×
[sudo] password for taybiothmane:
Starting Installer ...
```

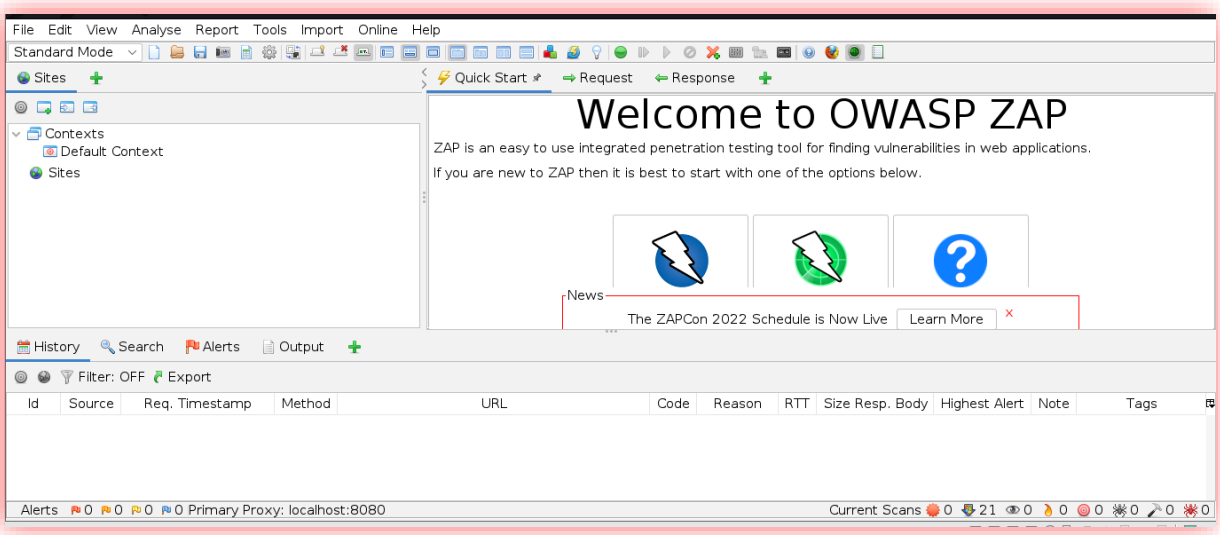
On terminer l'installation :

Voilà l'app :


Applications
Places
OWASP ZAP
Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
Usual Applications
burpsuite
commix
skipfish
sqlmap
wpscan
zap

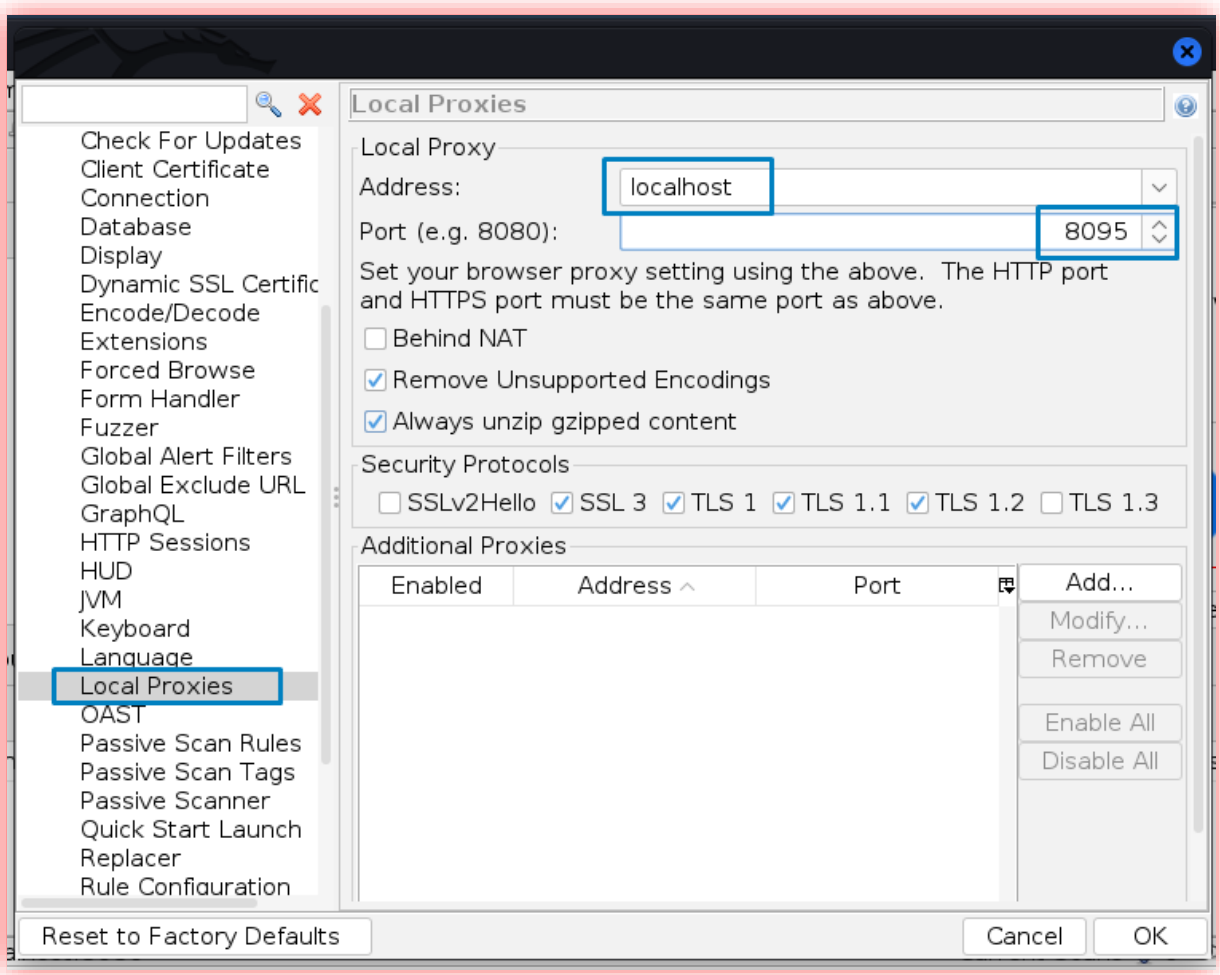


Voilà l'interfaces :

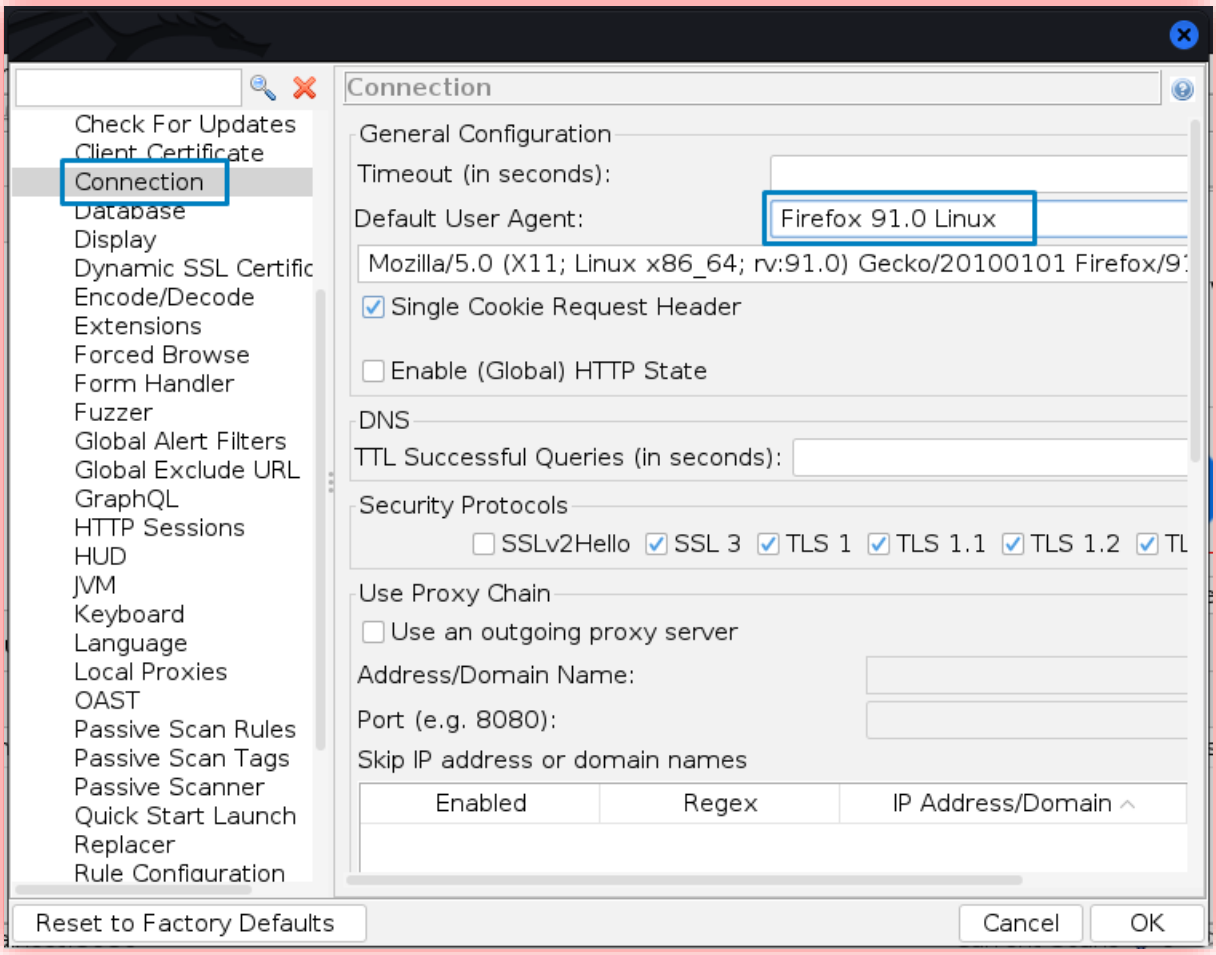


Configuration :

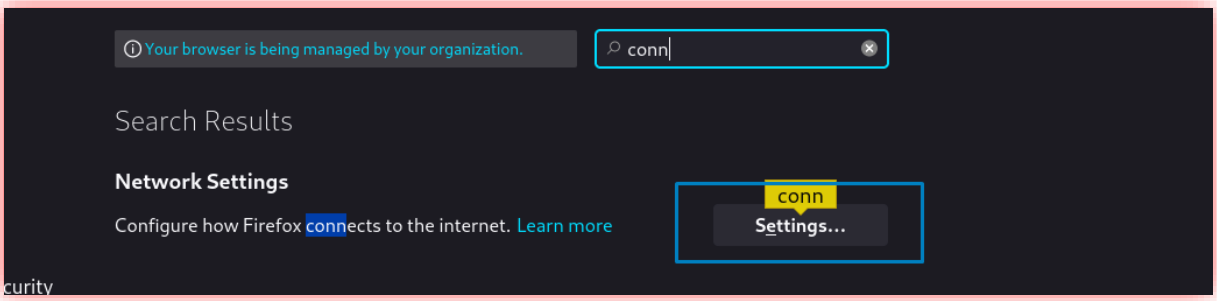
J'ai commencé à régler les paramètres, J'ai utilisé localhost :8095 J'ai défini ce paramètre sur Tools dans Options sur local Proxies.

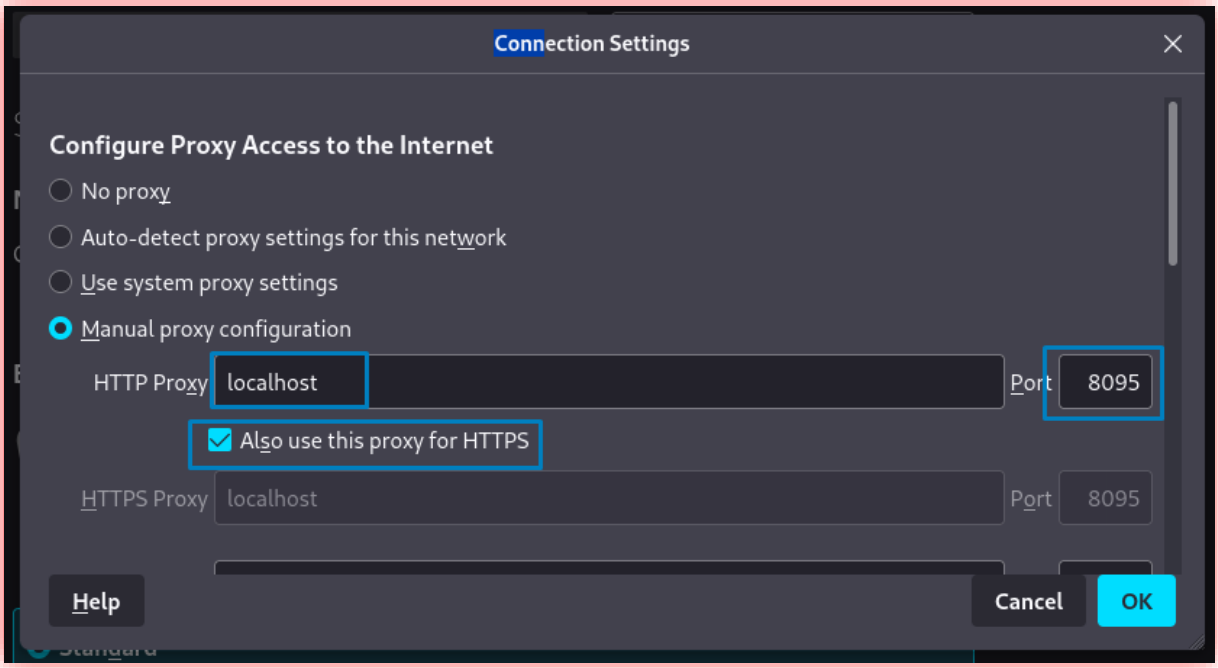


Après vous être connecté à Internet via un proxy, vous avez modifié les paramètres du proxy dans Outils sur Options a connection.



- Maintenant en configurer Firefox :
- J'ai modifié les paramètres de proxy de Firefox comme indiqué ci-dessous





Lorsque ces paramètres sont définis, nous redémarrons ZAP et Firefox, après quoi nous visitons n'importe quel site Web, voyons les lignes de requête HTTP et les alertes dans le panneau de la console ZAP, comme indiqué ci-dessous. Il s'agit de la manière manuelle d'effectuer des contrôles de sécurité.