Guide d’utilisation du site web Insp3ct

Insp3ct

Table des matières

1. Introduction : 2
2. Prérequis : 2
3. Accès au site : 2
4. Page d'accueil 3
5. Inscription : 5
6. Connexion : 7
7. Déconnexion 8
8. Utilisation des différents outils : 9
   - 8.1. Analyse réseau (Nmap) 9
   - 8.2. Fuzzing (Wfuzz) 10
   - 8.3. XSS (XSStrike) 10
   - 8.4. Injection SQL (SQLMap) 11
   - 8.5. Scan de vulnérabilités (Nikto) 12
9. Exemples des scans : 12
10. Exemple de rapport : 16

1. Introduction :

L'application web Insp3ct, est une plateforme dédiée à l'évaluation automatisée de la sécurité des sites web.

Elle a pour objectif de tester automatiquement les vulnérabilités de sécurité les plus courantes, telles que les attaques de type XSS, SQL injection, etc.

Une fois les tests effectués, un rapport détaillé est généré, résumant les vulnérabilités détectées, leur niveau de criticité, ainsi que des recommandations pour y remédier. Ce rapport constitue une aide précieuse pour renforcer la sécurité des applications web.

2. Prérequis :

Afin d'utiliser cette application web, il est nécessaire d'avoir l'autorisation du propriétaire du site dont vous voulez tester la sécurité.

Il est également nécessaire d'avoir un navigateur web à jour.

Il vous faudré créer un compte et être connecté à celui-ci.

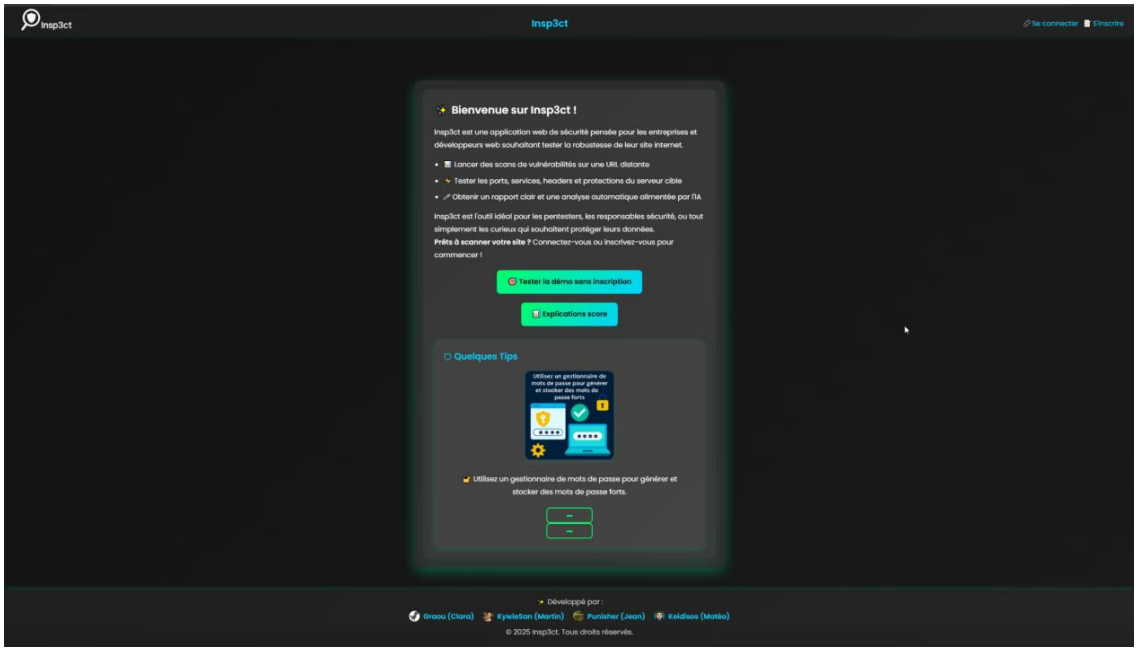
3. Accès au site :

L'accès au site web, se fait à l'aide de l'URL fourni lors de l'achat de la prestation.

Le site utilise une connexion sécurisée (HTTPS) afin de garantir la confidentialité des échanges. Une fois connecté vous arriverez sur la page d'accueil.

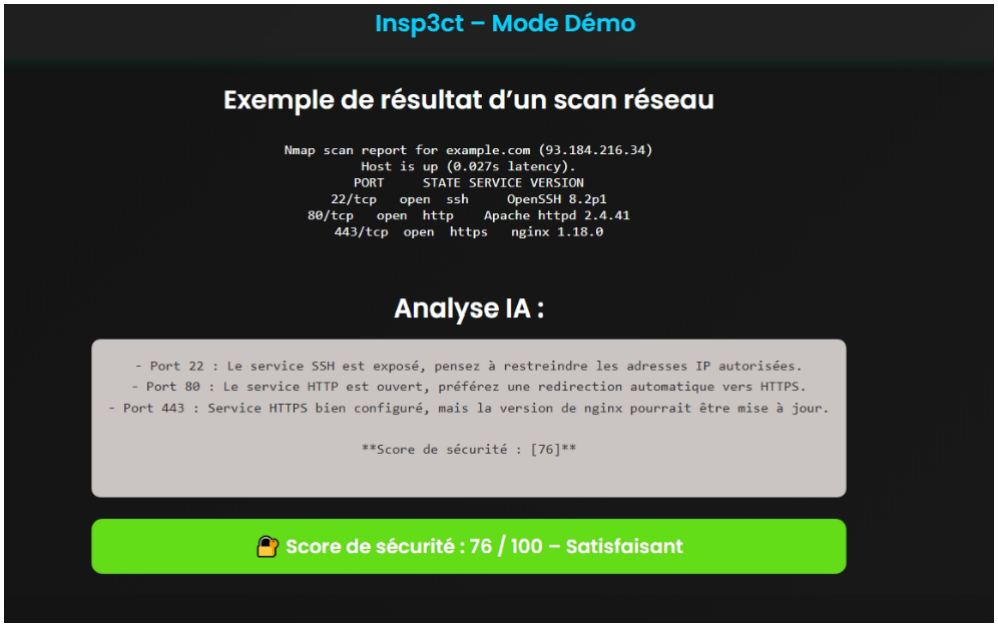
4. Page d’accueil

Une fois que vous vous êtes rendu sur la page d’accueil du site web Insp3ct, vous voyez ceci :

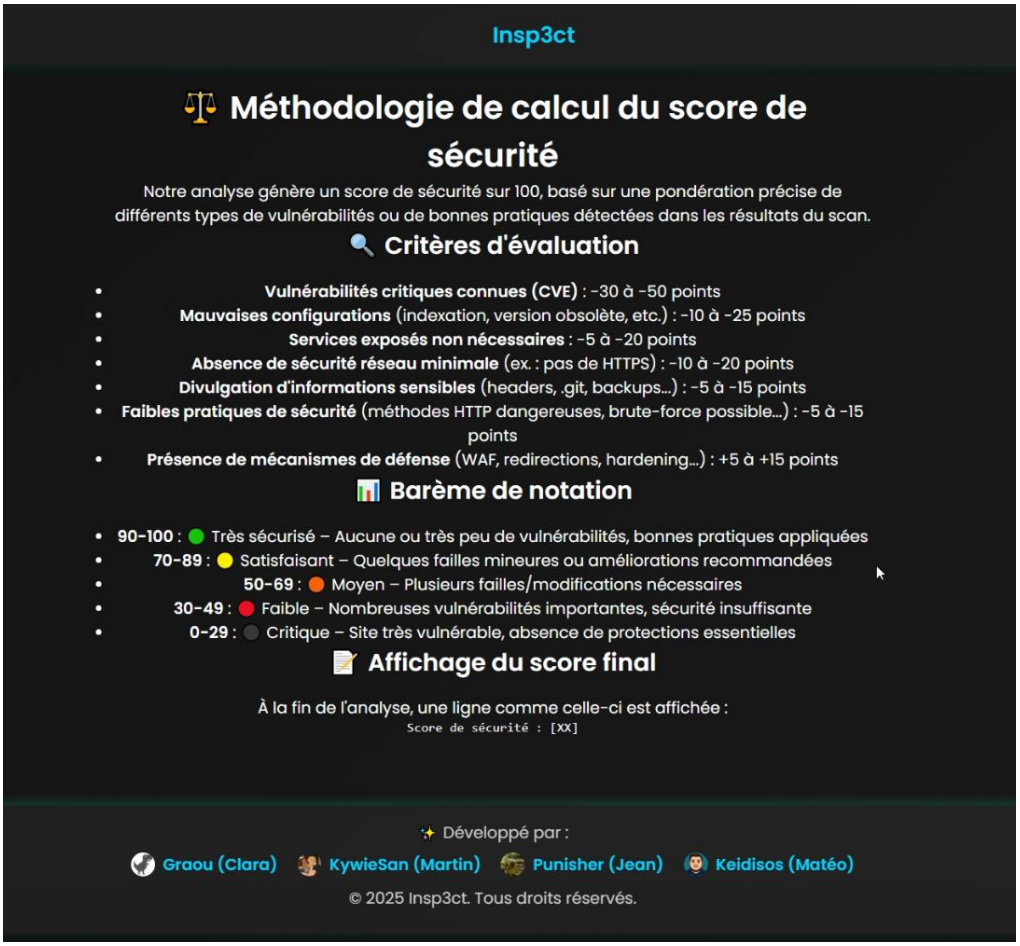


On peut observer, une brève présentation du site web, puis un lien vers un exemple de scan, ainsi qu’un autre vers une explication du score appliqué dans le rapport suite à un scan. Pour finir, vous trouverez un bandeau informatif déroulant faisant office de sensibilisation. Il permet d’afficher quelques bonnes pratiques de sécurité.

Exemple de scan :

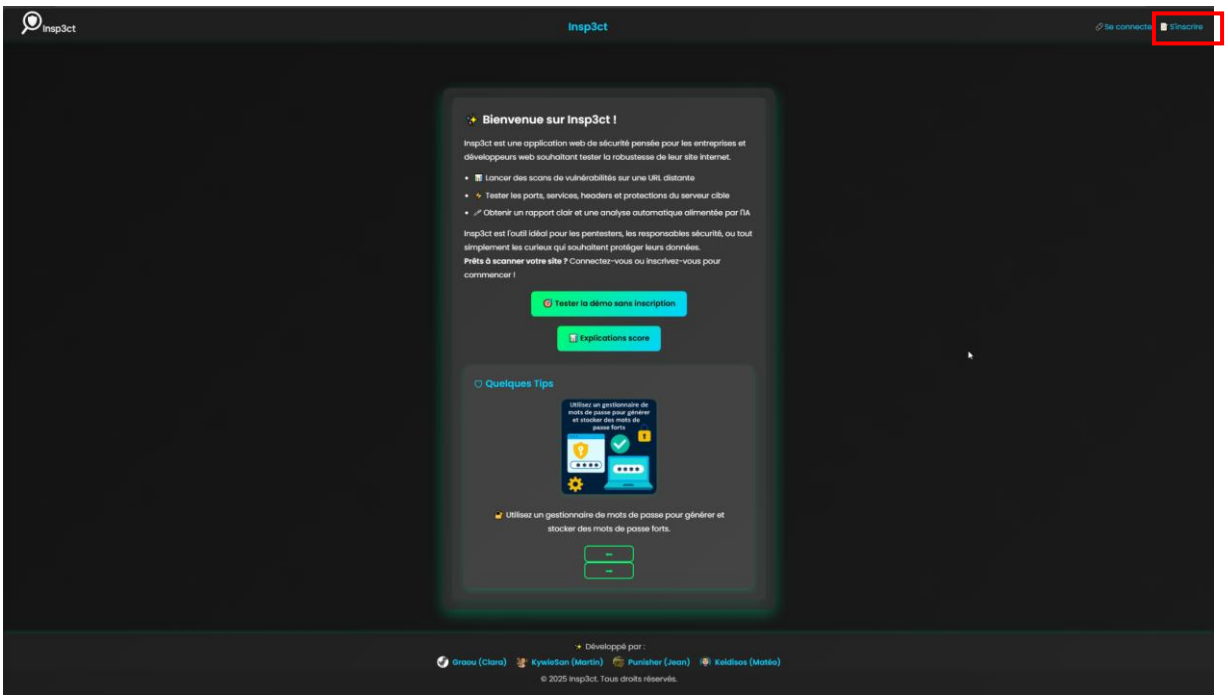


Explication des scores :

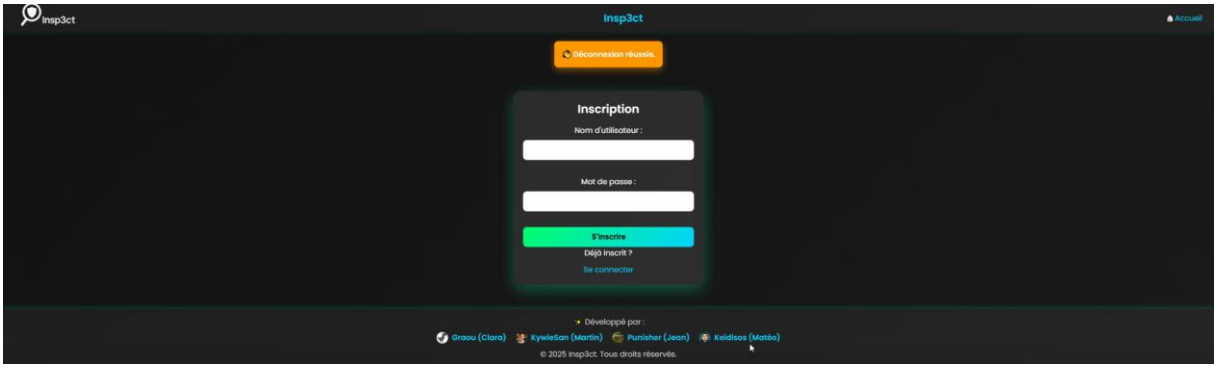


5. Inscription :

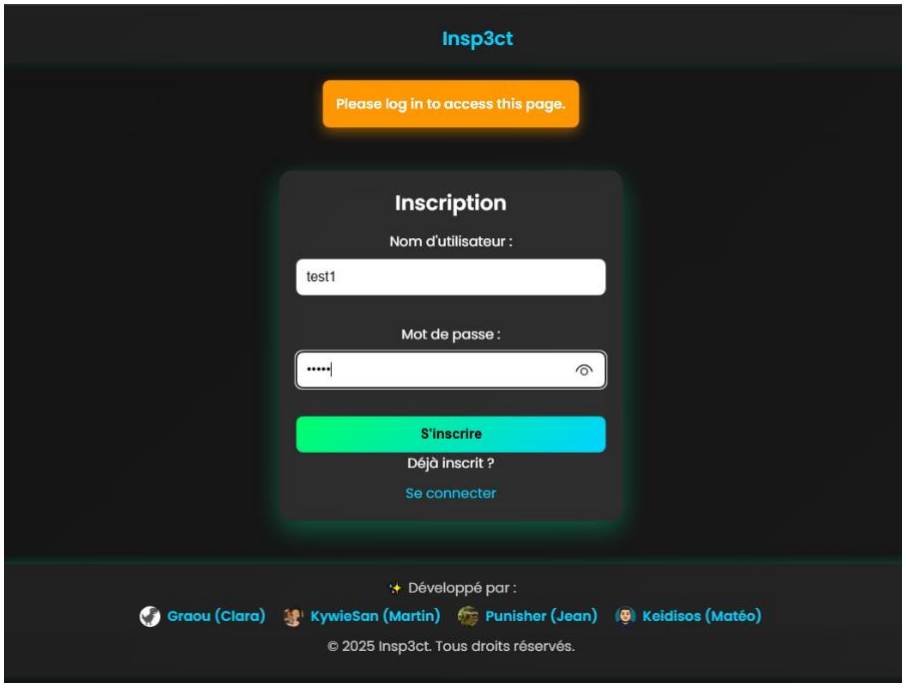
Afin de vous créer un compte, il est nécessaire de cliquer sur « s'inscrire » en haut à droite de votre écran :



Vous allez donc arriver sur la page d'inscription :



Vous choisirez un identifiant et un mot de passe, puis cliquerez sur « s'inscrire » :

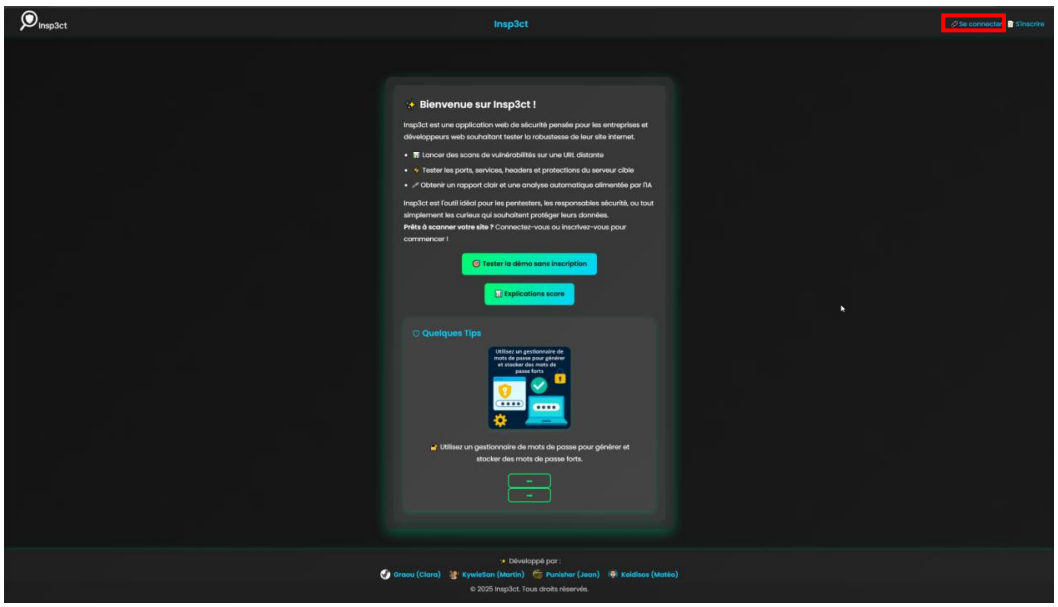


Si aucun message d'erreur indiquant que ce nom d'utilisateur existe déjà ne s'affiche, alors votre compte aura été créé.

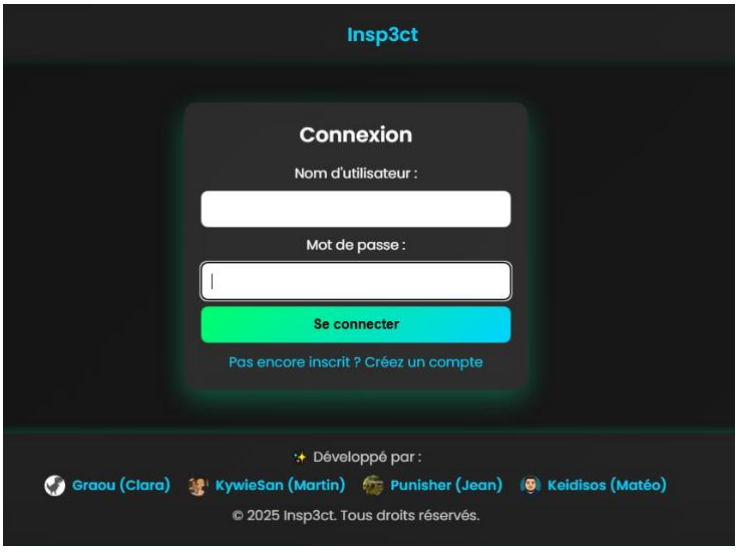
6. Connexion :

Une fois que votre compte est créé vous pouvez vous connecter à tout moment pour lancer vos scans.

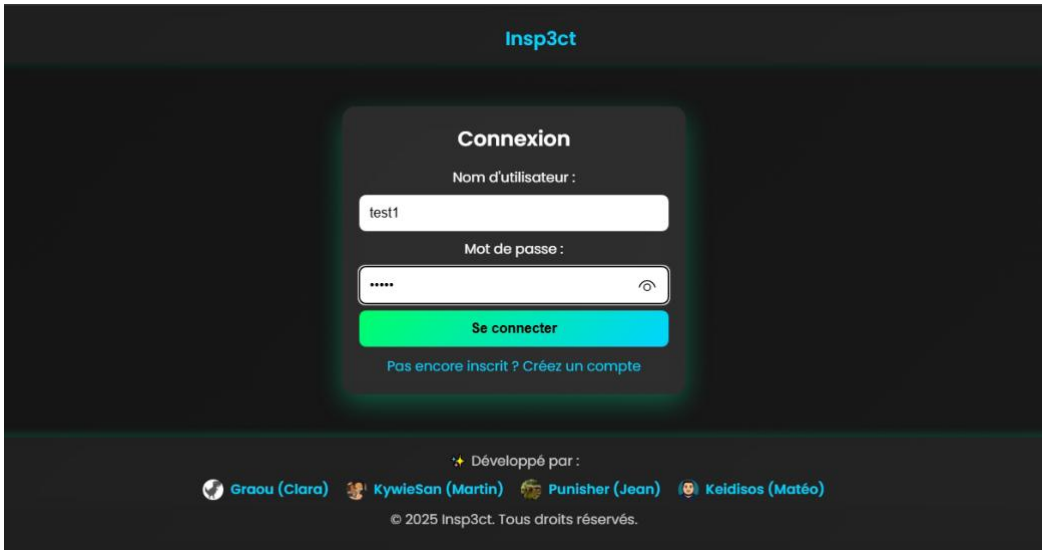
Pour faire, vous allez cliquer sur « se connecter » en haut à droite de votre écran :



Une fois que vous avez cliqué dessus, vous allez arriver sur la plage de connexion suivante :



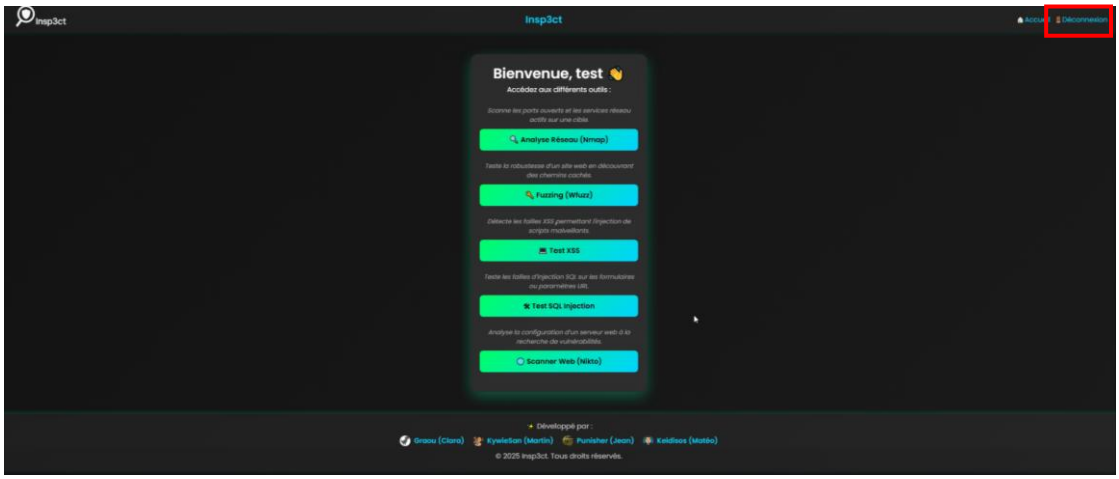
Il vous suffit de renseigner votre identifiant et votre mot de passe et de cliquer sur se connecter :



Une fois connecté, vous serez redirigé automatiquement sur la page Dashboard.

7. Déconnexion

Une fois connecté et vos scans réalisés, vous pouvez vous déconnecter en cliquant sur « Déconnexion » en haut à droite de votre écran :

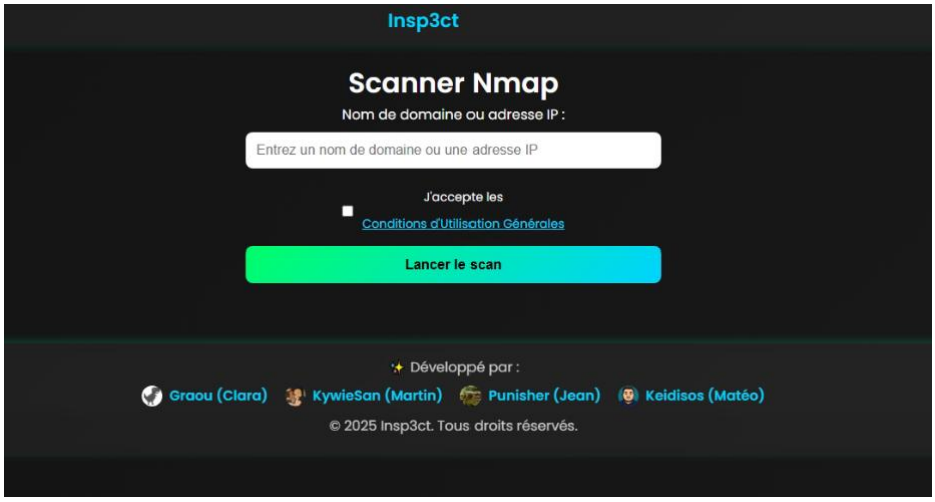


8. Utilisation des différents outils :

Une fois connecté sur votre session, vous avez accès à tous les outils proposés par Insp3ct.

8.1. Analyse réseau (Nmap)

Lorsque vous choisissez d'utiliser l'outil Nmap, afin de scanner les ports ouverts et les services réseaux actifs sur votre cible, vous arrivez sur la page suivante :



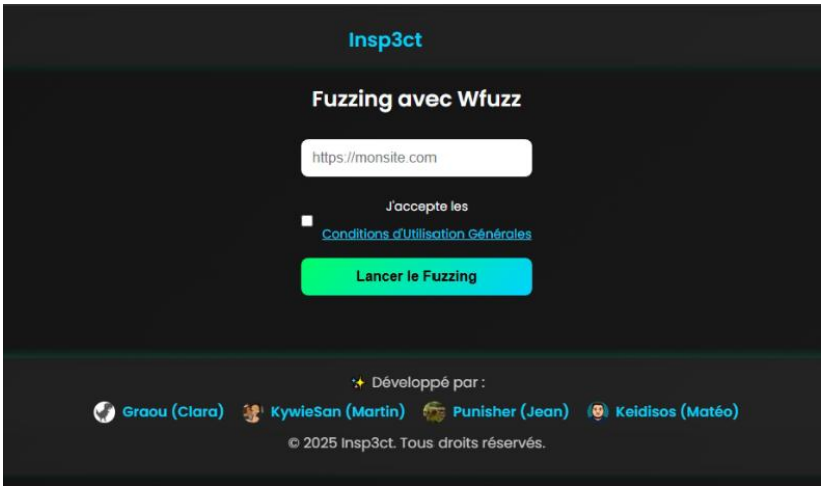
Afin de lancer un scan Nmap, il vous sera nécessaire d'indiquer le nom de domaine ou l'adresse IP de votre site web. Exemple : monsite.fr ou X.X.X.X.

> N'oubliez pas de lire et d'accepter (si vous êtes d'accord) les Conditions Générales d'Utilisation.

Une fois le scan terminé, vous pouvez télécharger votre rapport en PDF.

8.2. Fuzzing (Wfuzz)

Lorsque vous choisissez d'utiliser l'outil Wfuzz, afin de chercher les chemins cachés de votre site web, vous arrivez sur la page suivante :

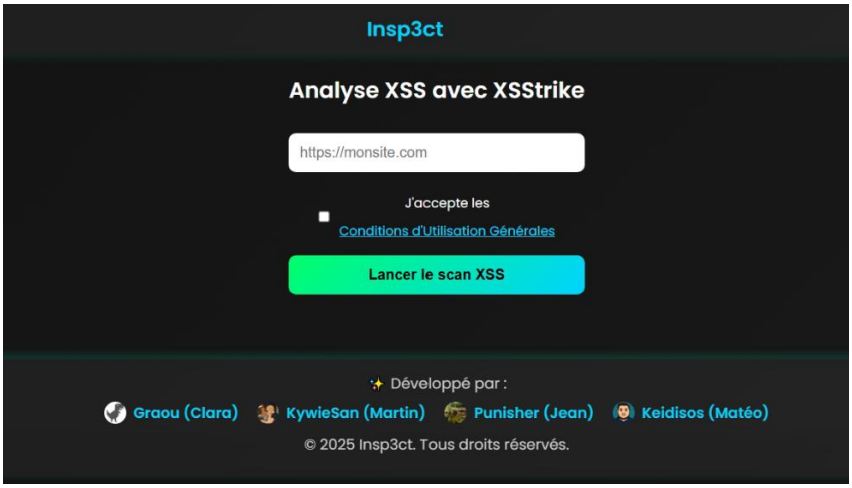


Afin de lancer un scan Wfuzz, il vous sera nécessaire d'indiquer l'URL de votre site web. Exemple : https://monsite.com.

> N'oubliez pas de lire et d'accepter (si vous êtes d'accord) les Conditions Générales d'Utilisation.

8.3. XSS (XSStrike)

Lorsque vous choisissez d'utiliser l'outil XSStrike, afin de détecter les failles XSS qui pourraient permettre d'injecter des scriptes malveillants, vous arrivez sur la page suivante :



Afin de lancer un XSStrike, il vous sera nécessaire d'indiquer l'URL de votre site web.
Exemple : https://monsite.fr.

> N'oubliez pas de lire et d'accepter (si vous êtes d'accord) les Conditions Générales d'Utilisation.

8.4. Injection SQL (SQLMap)

Lorsque vous choisissez d'utiliser l'outil SQLMap, afin de détecter les failles SQL sur vos formulaires ou les paramètres de votre URL, vous arrivez sur la page suivante :

Afin de lancer un scan SQLMap, il vous sera nécessaire d'indiquer l'URL de votre site web avec le chemin vers votre page de connexion.

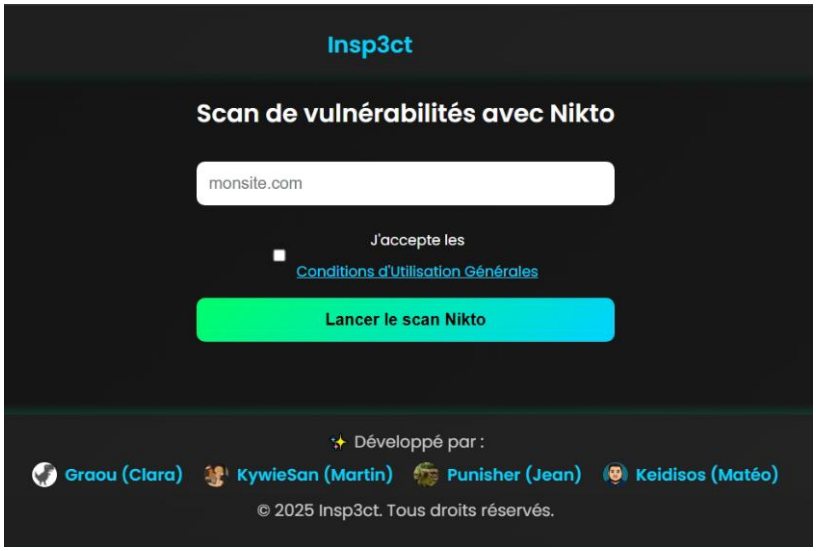
Exemple : https://monsite.fr/login.php.

> N'oubliez pas de lire et d'accepter (si vous êtes d'accord) les Conditions Générales d'Utilisation.

Une fois le scan terminé, vous pouvez télécharger le rapport en PDF.

8.5. Scan de vulnérabilités (Nikto)

Lorsque vous choisissez d'utiliser l'outil XSStrike, afin de détecter d'éventuelles vulnérabilités dans la configuration du serveur, vous arrivez sur la page suivante :

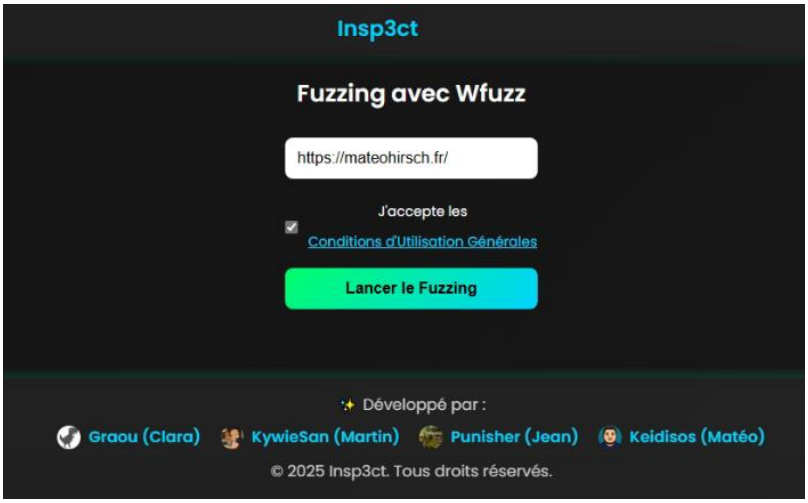


Afin de lancer un scan Nikto, il vous sera nécessaire d'indiquer le nom de domaine.
Exemple : monsite.fr.

> N'oubliez pas de lire et d'accepter (si vous êtes d'accord) les Conditions Générales d'Utilisation.

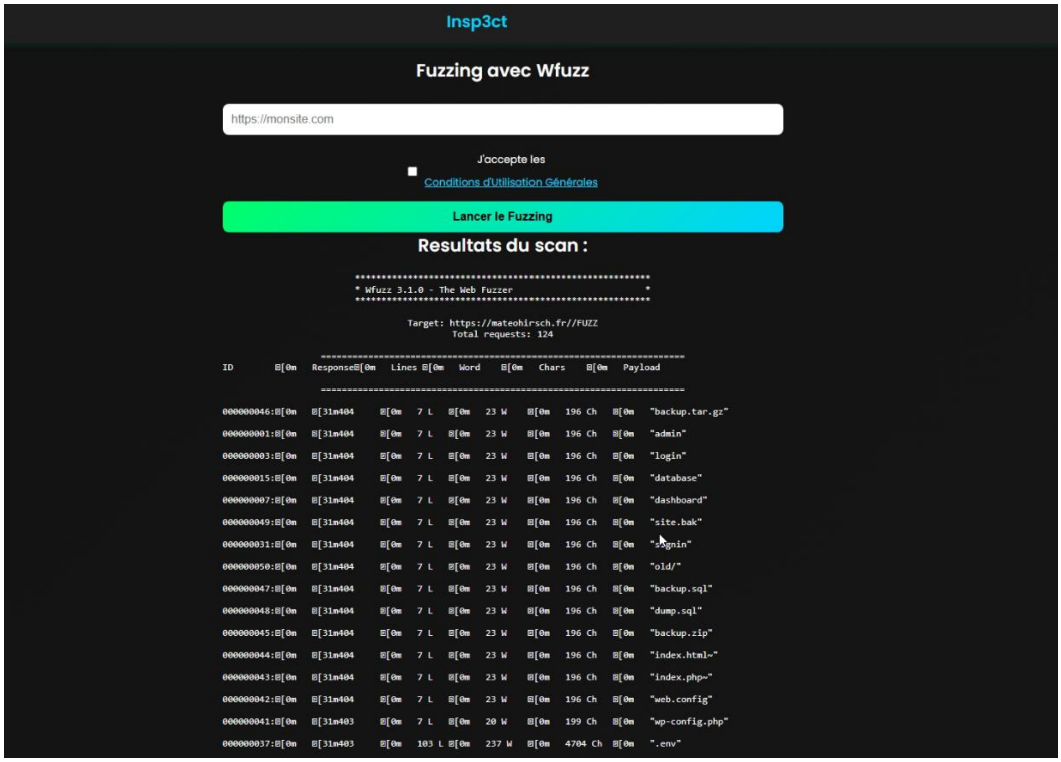
9. Exemples de scans :

Exemple Wfuzz : Je veux trouver les chemins cachés du site https://mateohirsch.fr/.



N’oubliez pas de lire et d’accepter (si vous êtes d’accord) les Conditions Générales d’Utilisation.

Une fois le scan fini, on peut voir des logs apparaitre :

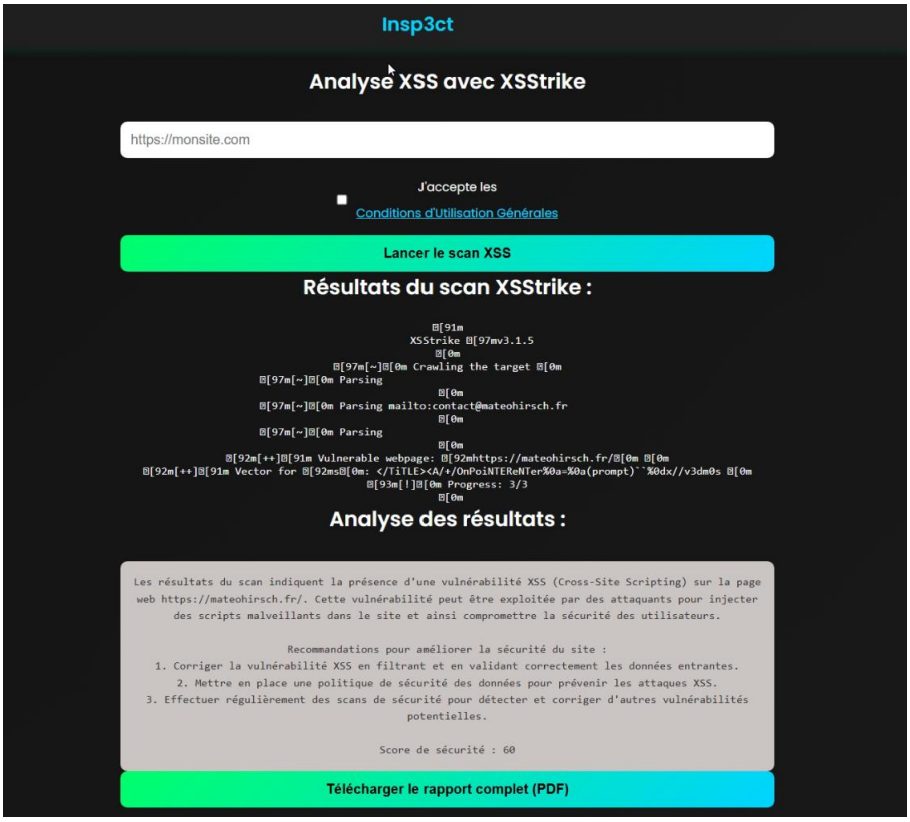


En bas de la page, vous trouverez l’option pour télécharger le rapport du scan en PDF.

<u>Exemple XSStrike :</u> Je veux trouver les failles XSS du site https://mateohirsch.fr/.

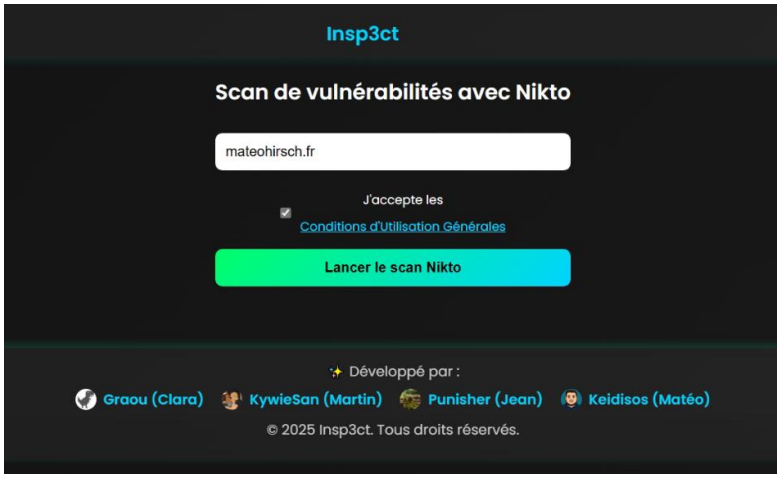
N’oubliez pas de lire et d’accepter (si vous êtes d’accord) les Conditions Générales d’Utilisation.

Une fois le scan fini, on peut voir des logs apparaître :



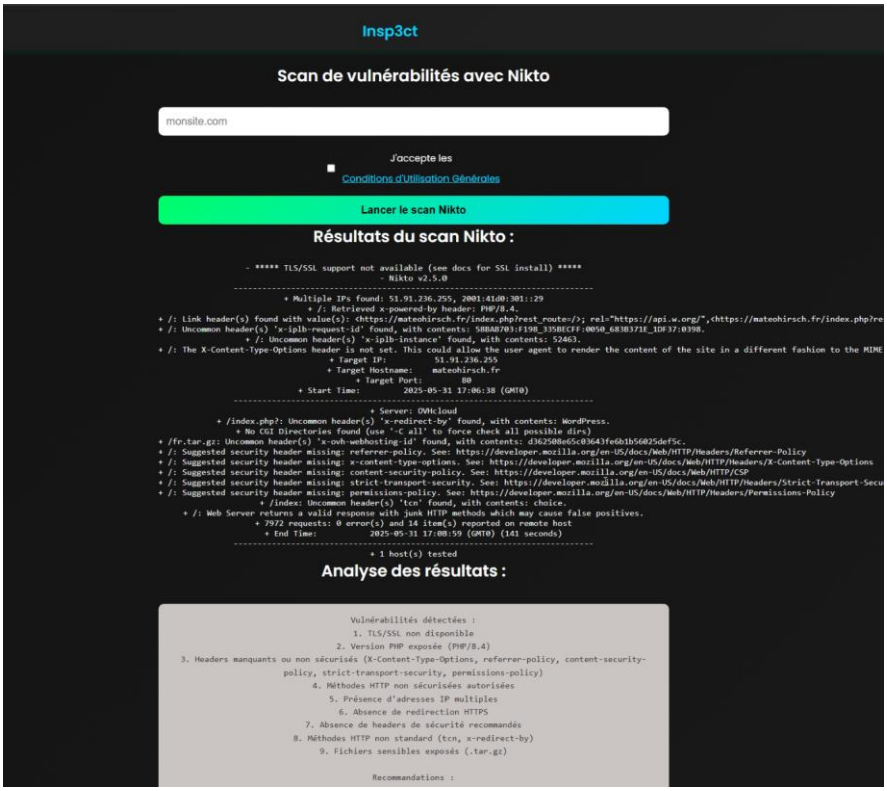
En bas de page, vous trouverez l’option pour télécharger le rapport du scan (cliquer sur « Télécharger le rapport complet (PDF) »).

<u>Exemple Nikto :</u> Je veux trouver les vulnérabilités du site https://mateohirsch.fr/.



> N’oubliez pas de lire et d’accepter (si vous êtes d’accord) les Conditions Générales d’Utilisation.

Une fois le scan fini, on peut voir des logs apparaitre :



En bas de page, vous trouverez l’option pour télécharger le rapport du scan (cliquer sur « Télécharger le rapport complet (PDF) »).

10. Exemple de rapport :

A la suite d'un de vos scans, vous pouvez visualiser le rapport sur votre écran mais également le télécharger en pdf. Voici un exemple de rapport téléchargeable en PDF :

Rapport d'analyse de sécurité

Analyse et recommendations :

Après analyse des résultats du scan de sécurité, voici les vulnérabilités détectées sur le site mateohirsch.fr :

1. Ports ou services exposés non nécessaires :
   - Le port 80 (HTTP) est ouvert mais renvoie une erreur 404 Not Found.
   - Le port 443 (HTTPS) est ouvert mais renvoie également une erreur 404 Not Found.

2. Absence de sécurité réseau minimale :
   - Le site ne semble pas utiliser de certificat SSL/TLS pour chiffrer les communications.

3. Informations sensibles divulguées :
   - Les headers renvoient des informations sur le serveur (OVHcloud) et des identifiants de webhosting.

Recommandations pour améliorer la sécurité du site mateohirsch.fr :

1. Configurer correctement les services web (HTTP et HTTPS) pour afficher une page d'accueil ou une erreur personnalisée au lieu de l'erreur 404.
2. Mettre en place un certificat SSL/TLS pour chiffrer les communications et garantir la confidentialité des données échangées.
3. Masquer les informations sensibles renvoyées par les headers du serveur pour limiter les risques d'attaques ciblées.

Score de sécurité : 60