

# **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 (XSSStrike)	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 faudra créer un compte et être connecté à celui-ci.

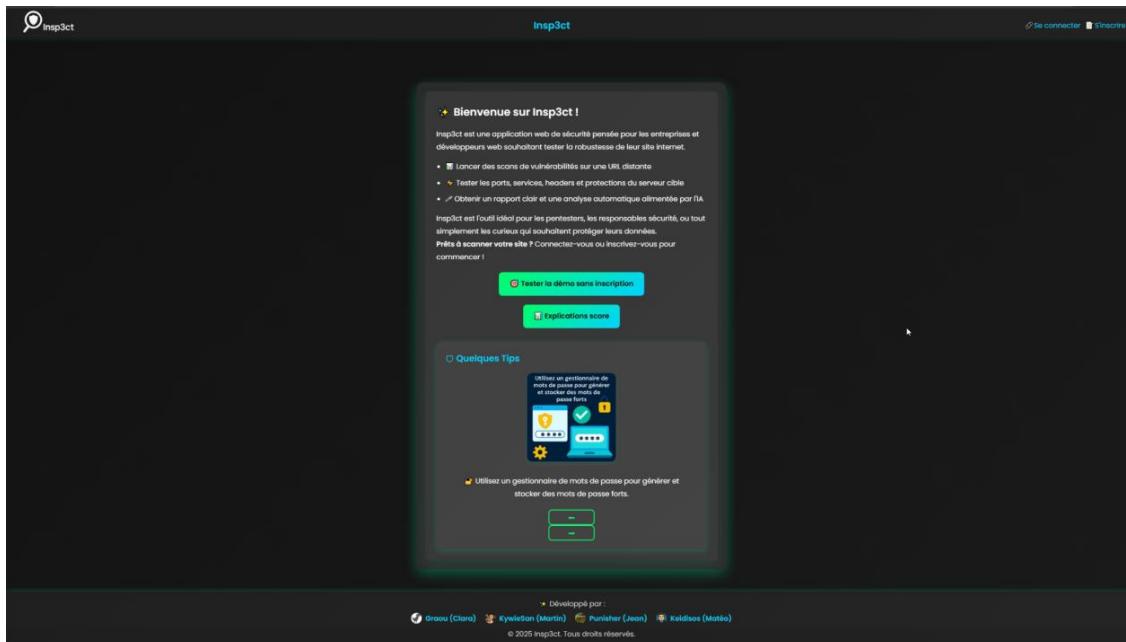
## 3. Accès au site :

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.

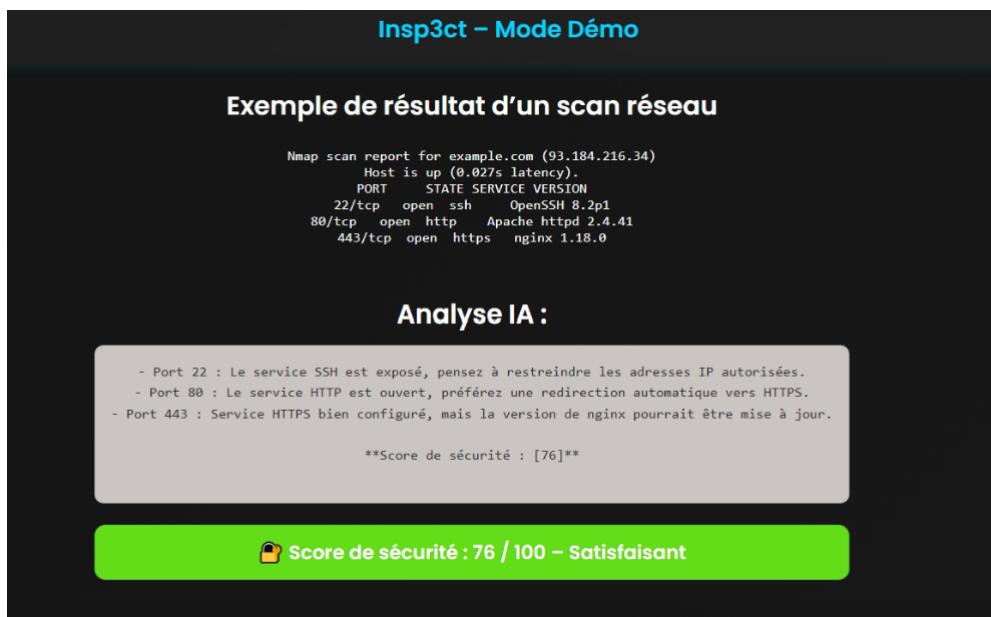
## 4. Page d'accueil

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 :



The screenshot shows the "Insp3ct – Mode Démo" interface. It starts with a title "Exemple de résultat d'un scan réseau" and displays an Nmap scan report for example.com:

```
Nmap scan report for example.com (93.184.216.34)
Host is up (0.027s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh        OpenSSH 8.2p1
80/tcp    open  http       Apache httpd 2.4.41
443/tcp   open  https     nginx 1.18.0
```

Below the report is an "Analyse IA :" section containing a list of findings:

- Port 22 : Le service SSH est exposé, pensez à restreindre les adresses IP autorisées.
- Port 80 : Le service HTTP est ouvert, préférez une redirection automatique vers HTTPS.
- Port 443 : Service HTTPS bien configuré, mais la version de nginx pourrait être mise à jour.

A note at the bottom of this section says "Score de sécurité : [76]".

At the bottom of the page is a large green button with the text "Score de sécurité : 76 / 100 – Satisfaisant".

## Explication des scores :

Insp3ct

### Méthodologie de calcul du score de sécurité

Notre analyse génère un score de sécurité sur 100, basé sur une pondération précise de différents types de vulnérabilités ou de bonnes pratiques détectées dans les résultats du scan.

#### Critères d'évaluation

- **Vulnérabilités critiques connues (CVE)** : -30 à -50 points
- **Mauvaises configurations** (indexation, version obsolète, etc.) : -10 à -25 points
- **Services exposés non nécessaires** : -5 à -20 points
- **Absence de sécurité réseau minimale** (ex : pas de HTTPS) : -10 à -20 points
- **Divulgation d'informations sensibles** (headers, .git, backups...) : -5 à -15 points
- **Faibles pratiques de sécurité** (méthodes HTTP dangereuses, brute-force possible...) : -5 à -15 points
- **Présence de mécanismes de défense** (WAF, redirections, hardening...) : +5 à +15 points

#### Barème de notation

- **90-100** : ● Très sécurisé – Aucune ou très peu de vulnérabilités, bonnes pratiques appliquées
- **70-89** : ● Satisfaisant – Quelques failles mineures ou améliorations recommandées
- **50-69** : ● Moyen – Plusieurs failles/modifications nécessaires
- **30-49** : ● Faible – Nombreuses vulnérabilités importantes, sécurité insuffisante
- **0-29** : ● Critique – Site très vulnérable, absence de protections essentielles

#### Affichage du score final

À la fin de l'analyse, une ligne comme celle-ci est affichée :

Score de sécurité : [XX]

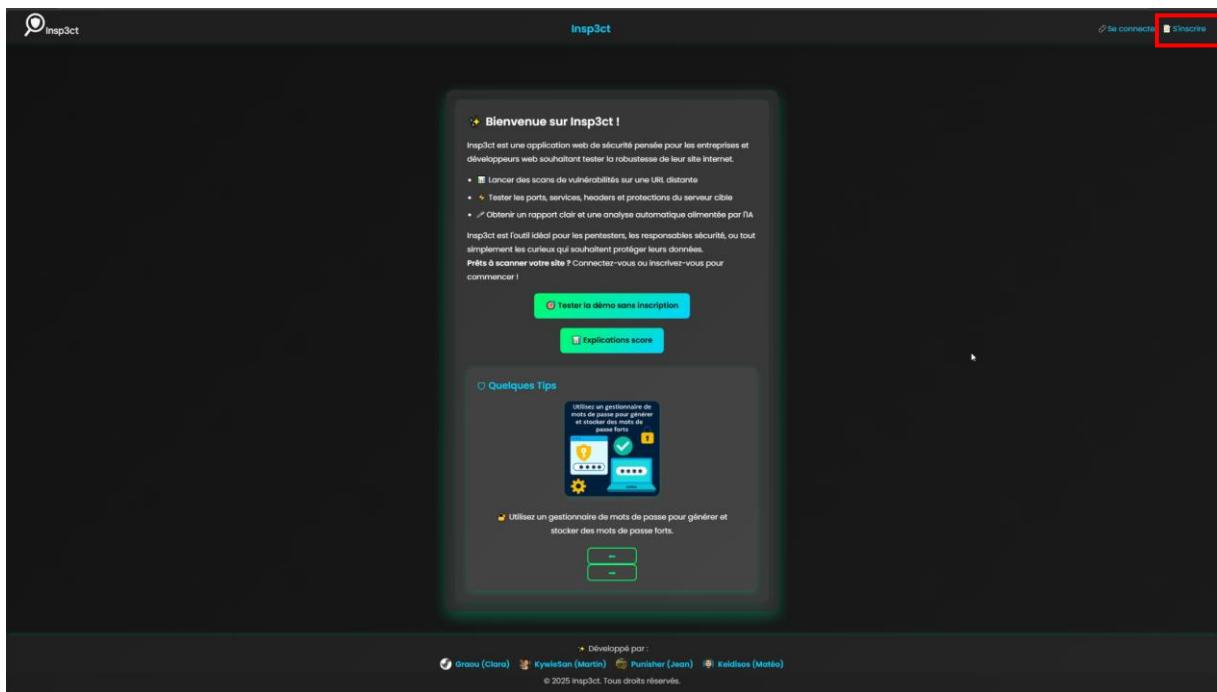
\*: Développé par :

 **Graou (Clara)**  **KywieSan (Martin)**  **Punisher (Jean)**  **Keidisos (Matéo)**

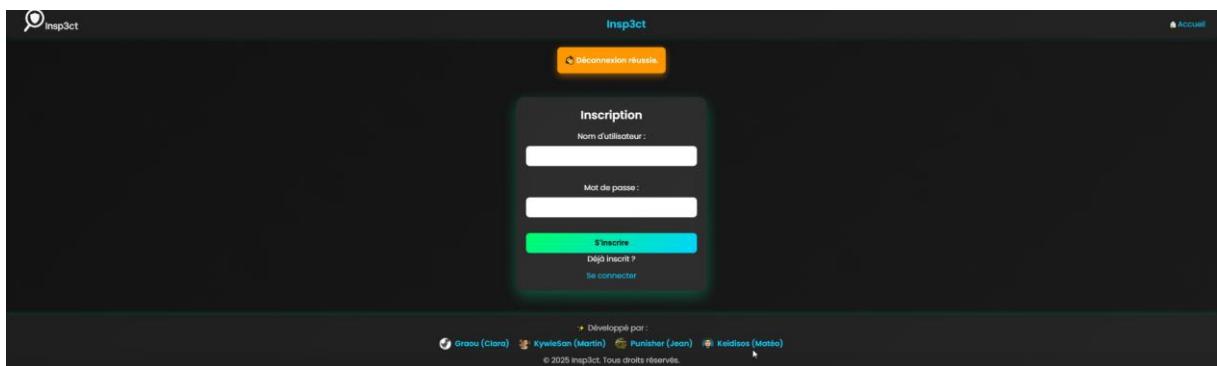
© 2025 Insp3ct. Tous droits réservés.

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

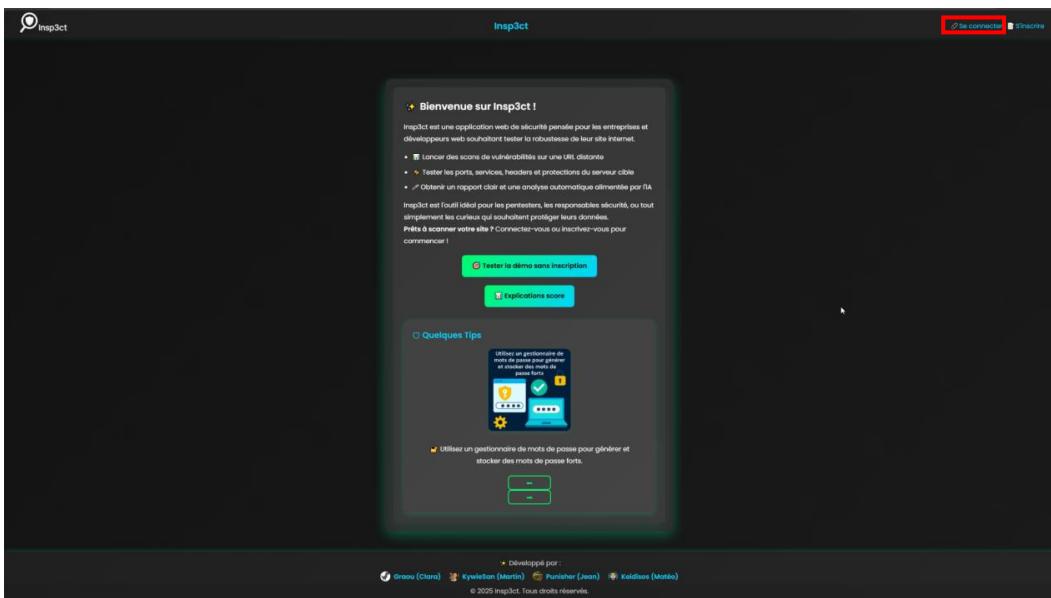
A screenshot of the Insp3ct registration page. The page has a dark background with a central light gray rectangular form. At the top of the form, it says "Inscription". Below that, there is a label "Nom d'utilisateur:" followed by an input field containing "test1". Underneath, there is a label "Mot de passe:" followed by an input field containing ".....". To the right of the password field is a small eye icon for password visibility. Below the input fields is a green button labeled "S'inscrire". Underneath the button, there are two links: "Déjà inscrit ?" and "Se connecter". At the bottom of the page, there is a footer section with the text "Développé par:" followed by four developer profiles: "Graou (Clara)", "KywieSan (Martin)", "Punisher (Jean)", and "Keidisos (Matéo)". Below these profiles, it says "© 2025 Insp3ct. Tous droits réservés.".

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

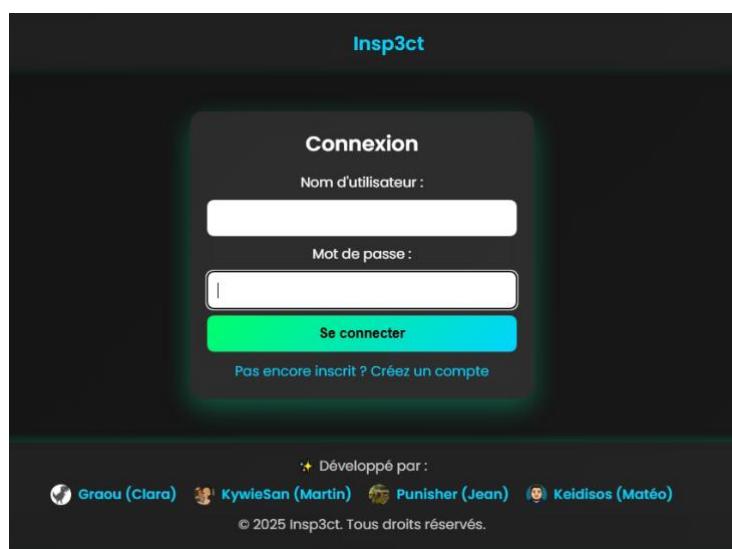
## 6. Connexion :

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 :

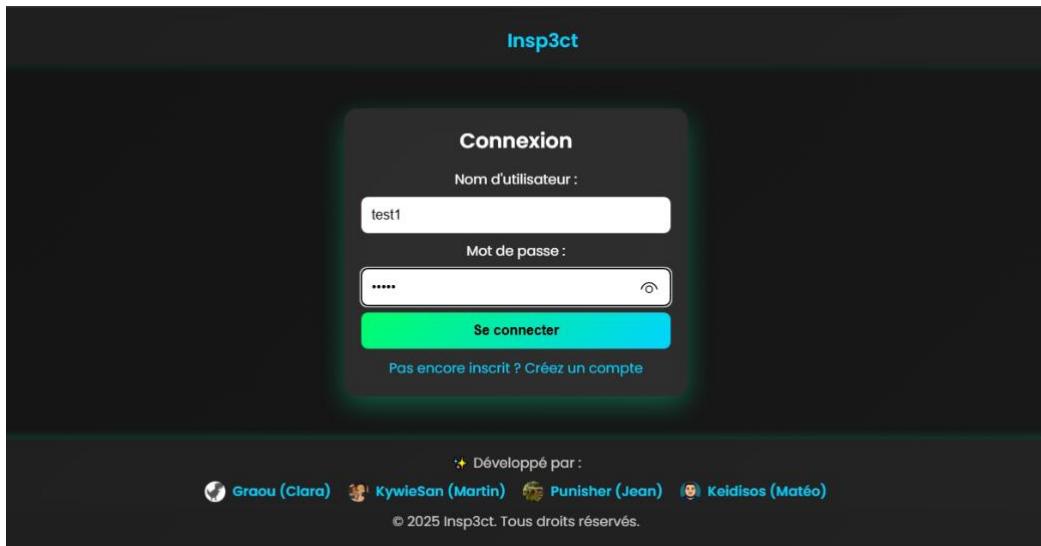


Une fois que vous avez cliqué dessus, vous allez arriver sur la plage de connexion suivante :





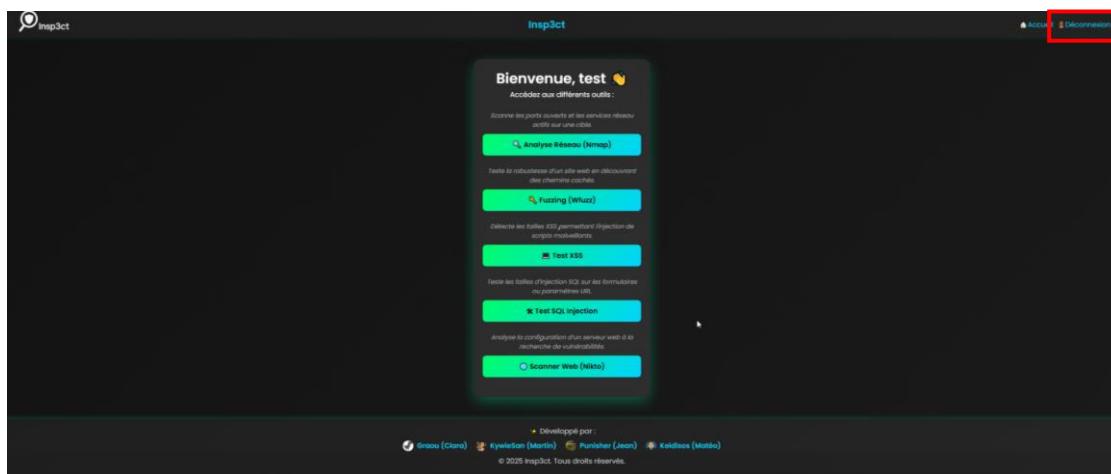
Il vous suffit de renseigner votre identifiant et votre mot de passe et de cliquer sur se connecter :



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 :

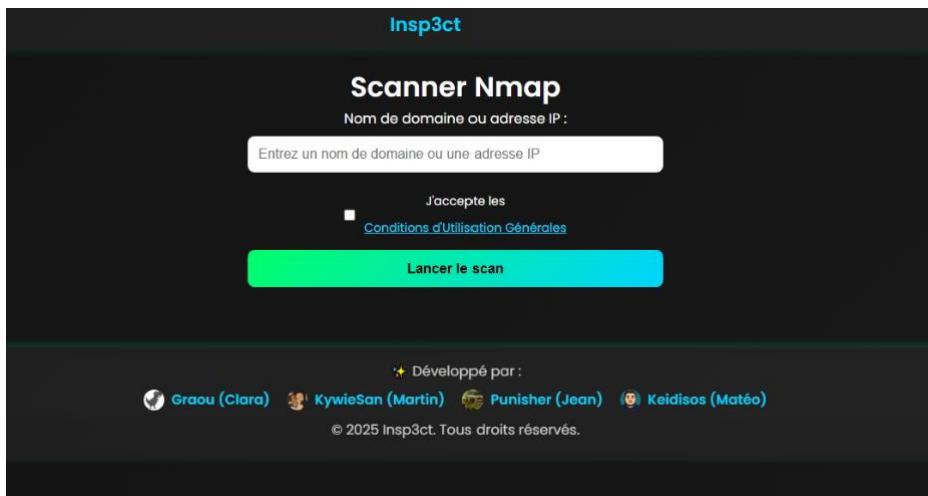


## 8. Utilisation des différents outils :

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 (XSSStrike)

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



Afin de lancer un XSSStrike, 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 :



The screenshot shows a dark-themed web application window titled "Injection SQL avec SQLMap". At the top, there is a text input field containing the URL "https://monsite.com/login.php". Below the URL is a checkbox labeled "J'accepte les Conditions d'Utilisation Générales". A large green button at the bottom is labeled "Lancer le scan SQL". At the bottom of the window, it says "Développé par:" followed by four developer profiles: "Graou (Clara)", "KywieSan (Martin)", "Punisher (Jean)", and "Keidisos (Matéo)". It also includes the copyright notice "© 2025 Insp3ct. Tous droits réservés."

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 XSSStrike, afin de détecter d'éventuelles vulnérabilités dans la configuration du serveur, vous arrivez sur la page suivante :



The screenshot shows a dark-themed web interface for the 'Scan de vulnérabilités avec Nikto' tool. At the top, it says 'Scan de vulnérabilités avec Nikto'. Below that is a text input field containing 'monsite.com'. Underneath the input field is a checkbox labeled 'J'accepte les Conditions d'Utilisation Générales' with a link to the 'Conditions d'Utilisation Générales'. A large green button at the bottom right says 'Lancer le scan Nikto'. At the bottom of the page, it says 'Développé par:' followed by four developer profiles: Graou (Clara), KywieSan (Martin), Punisher (Jean), and Keidosos (Matéo). It also includes a copyright notice: '© 2025 Insp3ct. Tous droits réservés.'

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

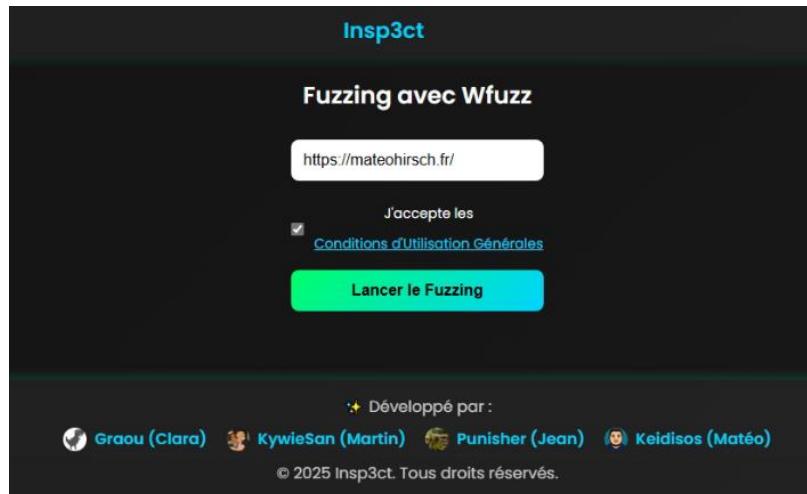
Exemple : monsite.fr.



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/>.

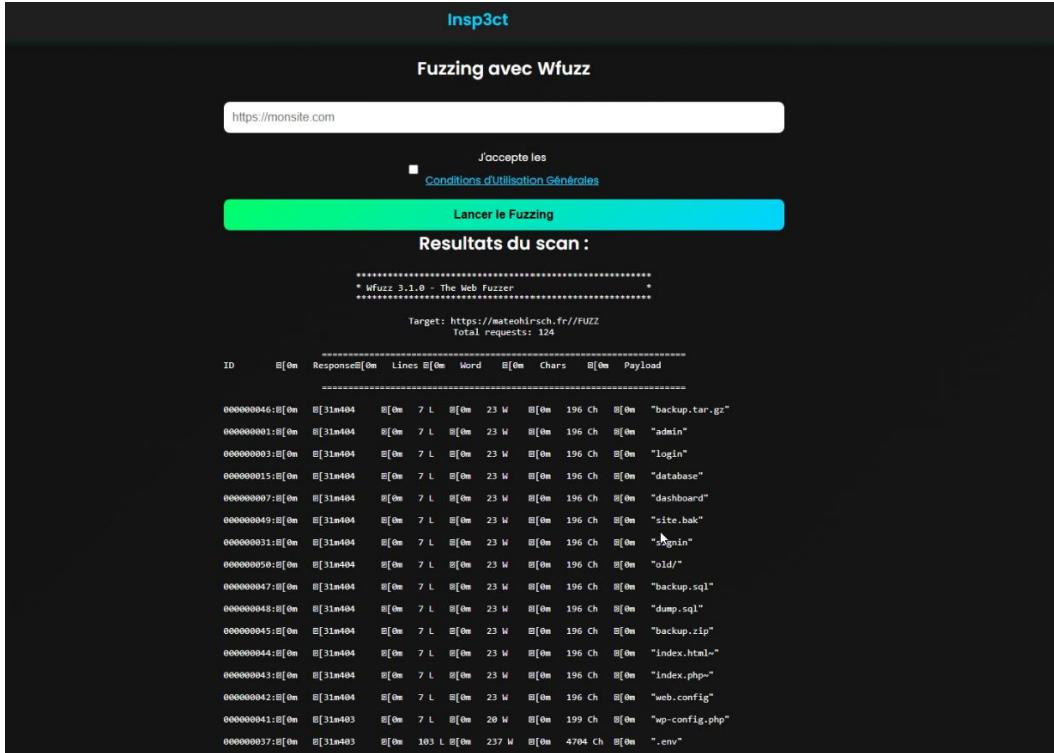


The screenshot shows a dark-themed web interface for the 'Fuzzing avec Wfuzz' tool. At the top, it says 'Fuzzing avec Wfuzz'. Below that is a text input field containing 'https://mateohirsch.fr/'. Underneath the input field is a checkbox labeled 'J'accepte les Conditions d'Utilisation Générales' with a link to the 'Conditions d'Utilisation Générales'. A large green button at the bottom right says 'Lancer le Fuzzing'. At the bottom of the page, it says 'Développé par:' followed by four developer profiles: Graou (Clara), KywieSan (Martin), Punisher (Jean), and Keidosos (Matéo). It also includes a copyright notice: '© 2025 Insp3ct. Tous droits réservés.'



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

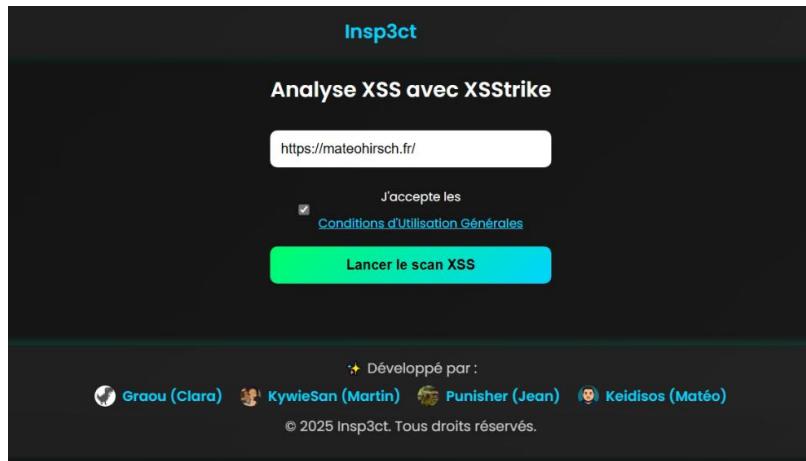
Une fois le scan fini, on peut voir des logs apparaître :



ID	Response	Lines	Word	Chars	Payload
000000045:	200	7 L	23 W	196 Ch	"backup.tar.gz"
000000001:	200	7 L	23 W	196 Ch	"admin"
000000002:	200	7 L	23 W	196 Ch	"login"
000000015:	200	7 L	23 W	196 Ch	"database"
000000007:	200	7 L	23 W	196 Ch	"dashboard"
000000049:	200	7 L	23 W	196 Ch	"site.bak"
000000031:	200	7 L	23 W	196 Ch	"admin"
000000050:	200	7 L	23 W	196 Ch	"old/"
000000047:	200	7 L	23 W	196 Ch	"backup.sql"
000000048:	200	7 L	23 W	196 Ch	"dump.sql"
000000045:	200	7 L	23 W	196 Ch	"backup.zip"
000000044:	200	7 L	23 W	196 Ch	"index.html~"
000000043:	200	7 L	23 W	196 Ch	"Index.php~"
000000042:	200	7 L	23 W	196 Ch	"web.config"
000000041:	200	7 L	20 W	199 Ch	"wp-config.php"
000000037:	200	103 L	237 W	4704 Ch	".env"

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

[Exemple XSSStrike : Je veux trouver les failles XSS du site https://mateohirsch.fr/.](#)



★ Développé par:

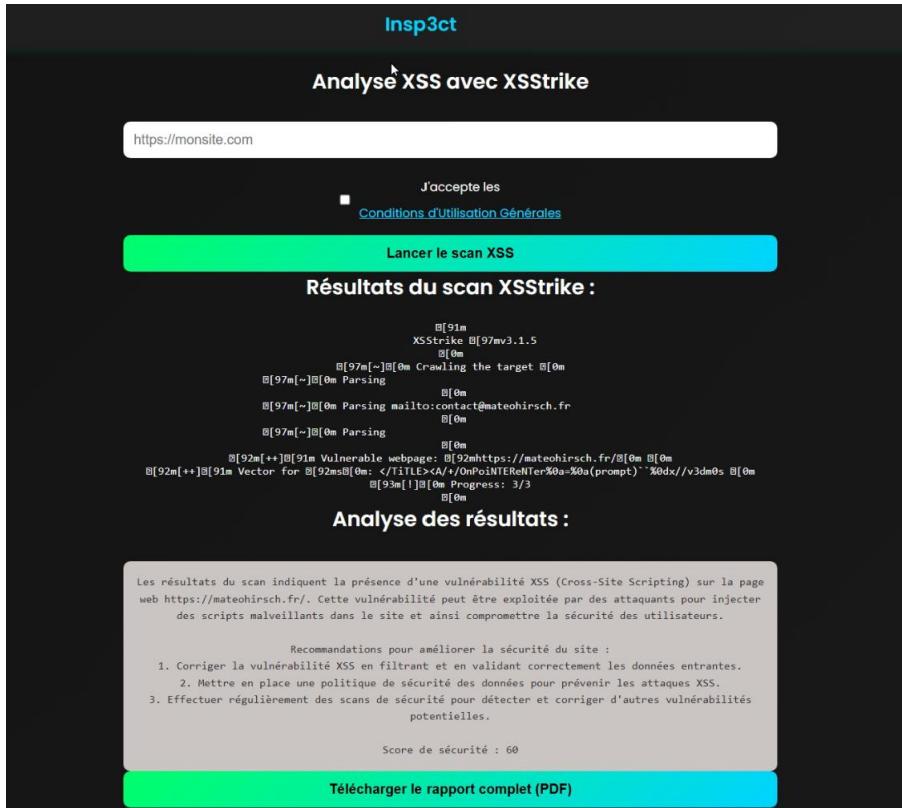
Graou (Clara) KywieSan (Martin) Punisher (Jean) Keidisos (Matéo)

© 2025 Insp3ct. Tous droits réservés.



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 :



The screenshot shows the Insp3ct interface for XSS analysis. At the top, it says "Analyse XSS avec XSStrike". Below that is a URL input field containing "https://monsite.com". A checkbox labeled "J'accepte les Conditions d'Utilisation Générales" is checked. A large green button at the bottom says "Lancer le scan XSS".

**Résultats du scan XSStrike :**

```
[91m
XSStrike [97mv3.1.5
[0m
[97m[-]@[0m Crawling the target @[0m
[97m[-]@[0m Parsing
[0m
[97m[-]@[0m Parsing mailto:contact@mateohirsch.fr
[0m
[97m[-]@[0m Parsing
[0m
[92m[+]@[91m Vulnerable webpage: [92mhttps://mateohirsch.fr/[0m [0m
[92m[+]@[91m Vector for [92ms@[0m: <TITLE>KA4/OnPointTERelTer%0a-%0a(prompt)%0dx//v3dm0s [0m
[93m[!]@[0m Progress: 3/3
[0m
```

**Analyse des résultats :**

Les résultats du scan indiquent la présence d'une vulnérabilité XSS (Cross-Site Scripting) sur la page web https://mateohirsch.fr/. Cette vulnérabilité peut être exploitée par des attaquants pour injecter des scripts malveillants dans le site et ainsi compromettre la sécurité des utilisateurs.

Recommandations pour améliorer la sécurité du site :

1. Corriger la vulnérabilité XSS en filtrant et en validant correctement les données entrantes.
2. Mettre en place une politique de sécurité des données pour prévenir les attaques XSS.
3. Effectuer régulièrement des scans de sécurité pour détecter et corriger d'autres vulnérabilités potentielles.

Score de sécurité : 60

[Télécharger le rapport complet \(PDF\)](#)

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

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



The screenshot shows the Insp3ct interface for Nikto scanning. At the top, it says "Scan de vulnérabilités avec Nikto". Below that is a URL input field containing "mateohirsch.fr". A checkbox labeled "J'accepte les Conditions d'Utilisation Générales" is checked. A large green button at the bottom says "Lancer le scan Nikto".

**Développé par :**

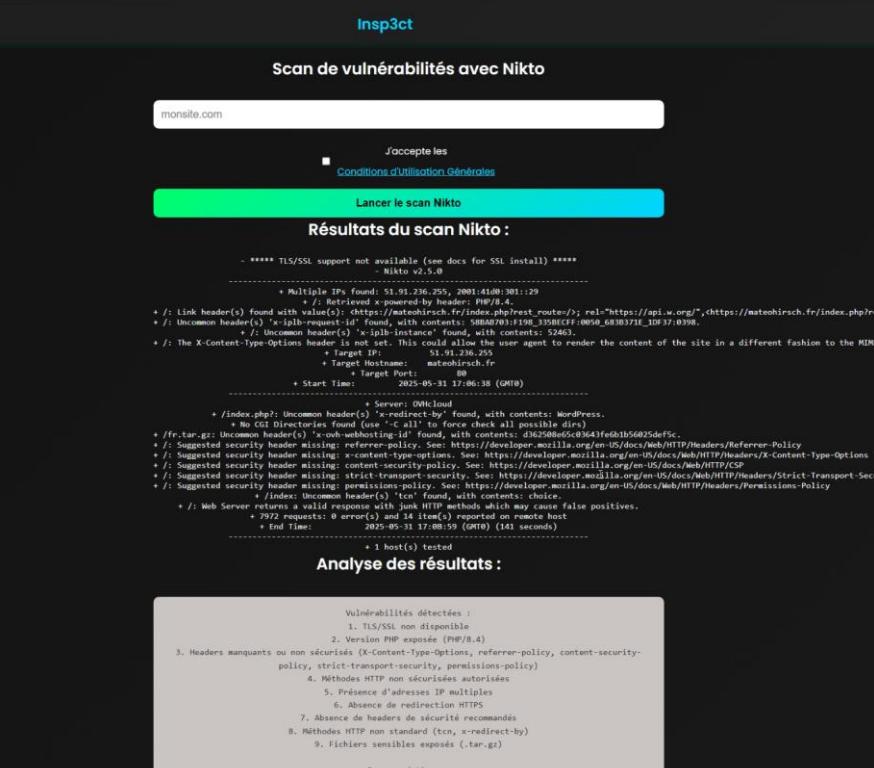
- Graou (Clara)
- KywieSan (Martin)
- Punisher (Jean)
- Keidisos (Matéo)

© 2025 Insp3ct. Tous droits réservés.



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 :



```

Insp3ct
Scan de vulnérabilités avec Nikto
monsite.com
J'accepte les
Conditions d'Utilisation Générales
Lancer le scan Nikto

Résultats du scan Nikto :

- ***** TLS/SSL support not available (see docs for SSL install) *****
  - Nikto v2.5.0

+ Multiple IPs found: 51.91.236.255, 2001:1d10:0:301:129
+ /: Retrieved x-powered-by header: PHP/8.4
+ /: Link header(s) found with valuel(s): <link href="/wp-content/themes/monsite/test-route/>; rel="https://api.w.org/", <https://mateohirsch.fr/index.php?re
+ /: Uncommon header(s) 'x-iph-instance-id' found, with contents: 50BABA701F1F98_339BECCF_0050_A80B372A_10F37:0398.
+ /: Uncommon header 'x-iph-instance' found, with contents: 52463.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME
  type. See https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options
+ /: Target Hostname: mateohirsch.fr
+ Target Port: 80
+ Start Time: 2025-05-31 17:06:38 (GMT)
+ Server: OWNLoud
+ /index.php: Uncommon header(s) 'x-redirect-by' found, with contents: Non-Poss.
+ /fr.tar.gz: Uncommon header(s) 'x-webhosting-id' found, with contents: d362588e5c03d43fedeb5d025def5c.
+ /: Suggested security header missing: referer-policy. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referer-Policy
+ /: Suggested security header missing: x-content-type-options. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options
+ /: Suggested security header missing: strict-transport-security. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: Suggested security header missing: permissions-policy. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Permissions-Policy
+ /: Web Server did respond with some HTTP methods which were false positives.
+ 2972 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time: 2025-05-31 17:08:19 (GMT) (141 seconds)

+ 1 host(s) tested

```

Vulnérabilités détectées :

1. TLS/SSL non disponible
2. Version PHP exposée (PHP/8.4)
3. Headers manquants ou non sécurisés (X-Content-Type-Options, referer-policy, content-security-policy, strict-transport-security, permissions-policy)
  - 4. Méthodes HTTP sécurité non recommandées
  - 5. Préférence d'adresse IP multiples
  - 6. Absence de redirection HTTPS
  - 7. Absence de headers de sécurité recommandés
  - 8. Méthodes HTTP non standard (tcn, x-redirect-by)
  - 9. Fichiers sensibles exposés (-tar.gz)

Recommandations :

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 recommandations :

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