

Guide d'utilisation du site web 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 faudra créer un compte et être connecté à celui-ci.

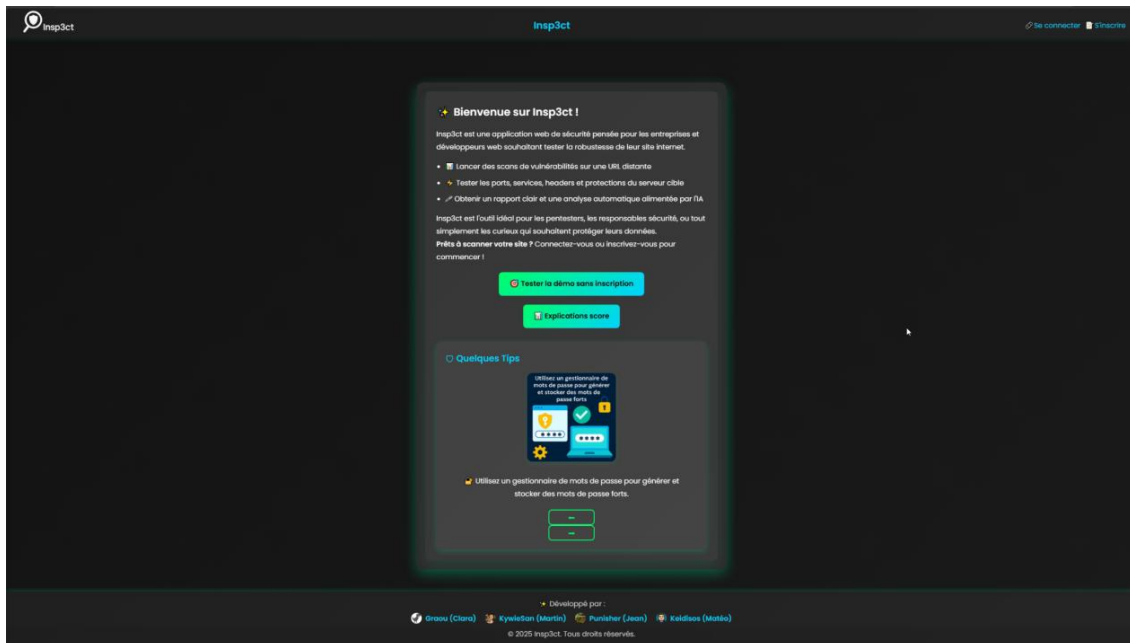
3. Accès au site :

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.

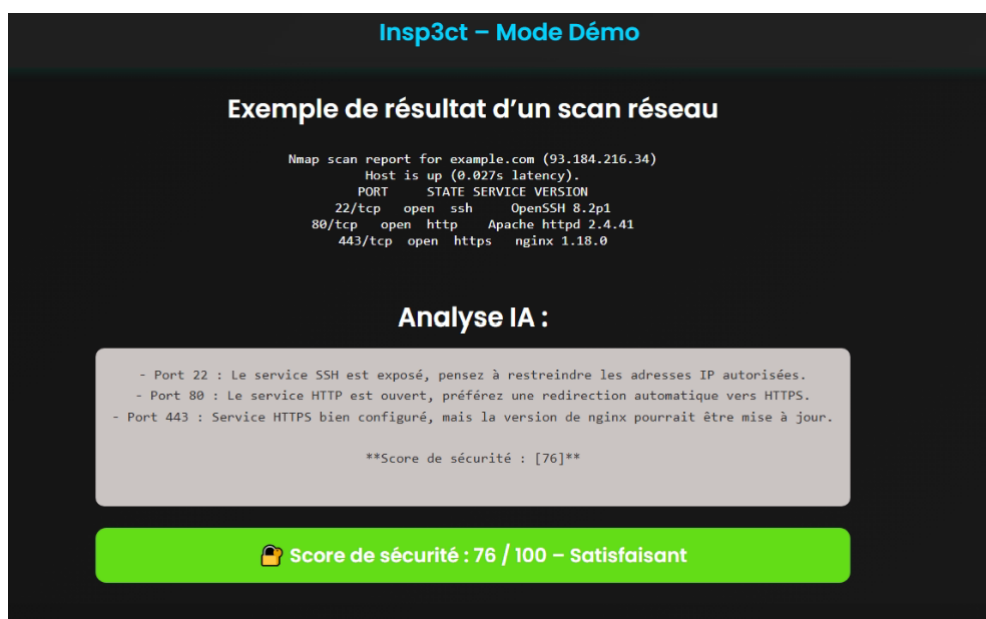
4. Page d'accueil

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 :




Explication des scores :









 **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
- **Divulgaration 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]

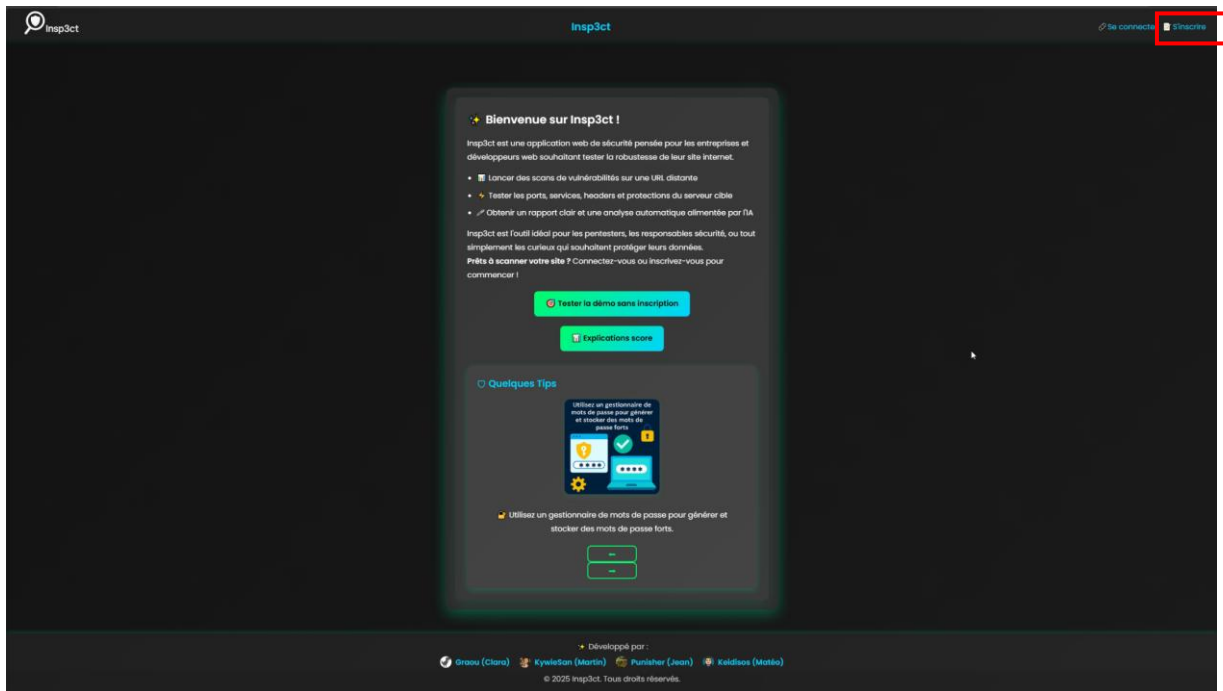
✦ Développé par :

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

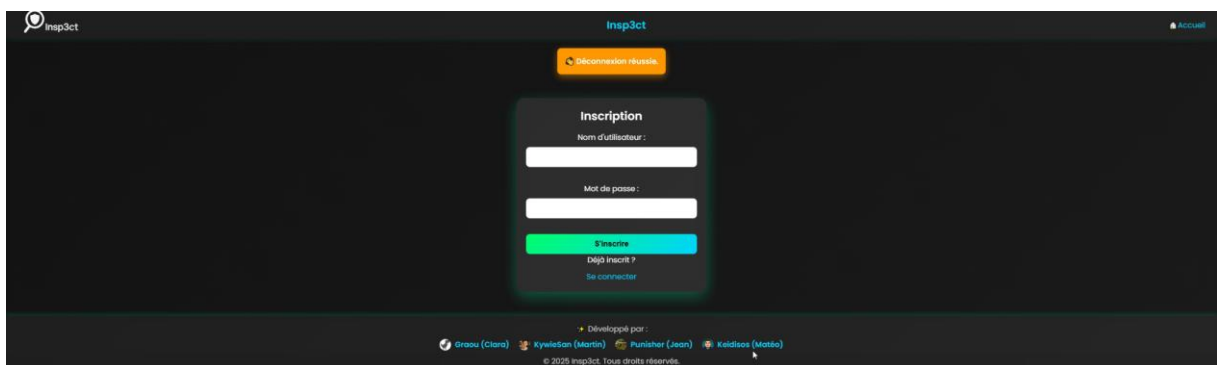
© 2025 Insp3ct. Tous droits réservés.

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

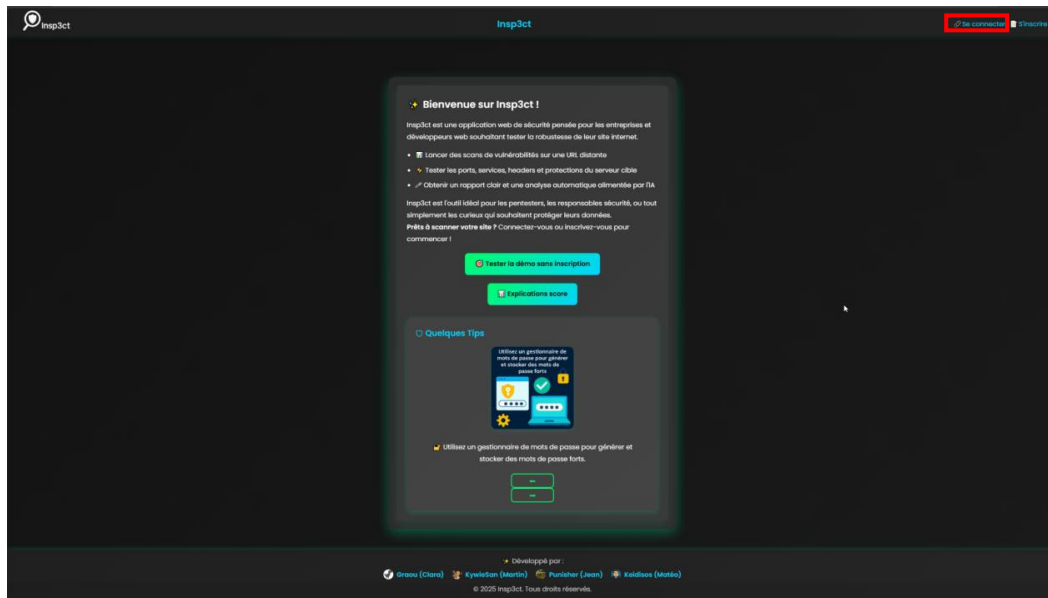
A screenshot of the Insp3ct registration page. The page has a dark background. At the top, the "Insp3ct" logo is in blue. Below it, an orange button says "Please log in to access this page.". In the center, a dark gray box contains the "Inscription" form. The form has two input fields: "Nom d'utilisateur :" with the text "test1" and "Mot de passe :" with masked characters "****". Below the fields is a large blue "S'inscrire" button. Underneath the button are two links: "Déjà inscrit ?" and "Se connecter". At the bottom of the page, it says "Développé par :" followed by four names with profile icons: "Graou (Clara)", "KywieSan (Martin)", "Punisher (Jean)", and "Keidisos (Matéo)". The footer text is "© 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.

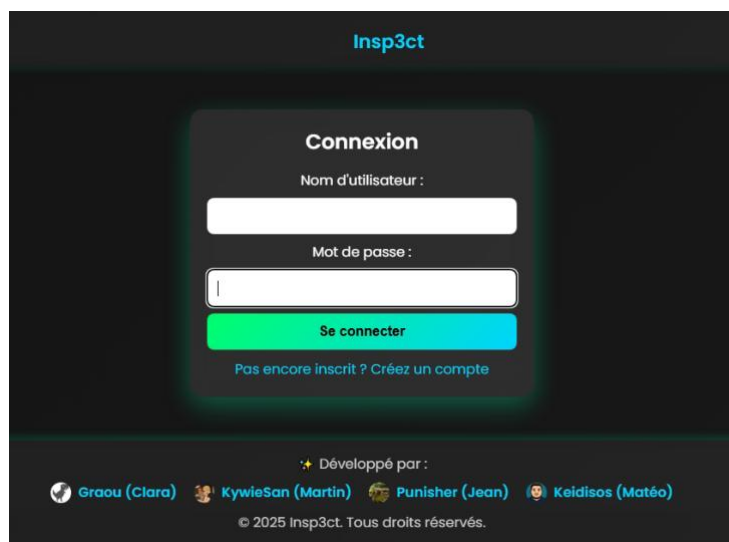
6. Connexion :

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

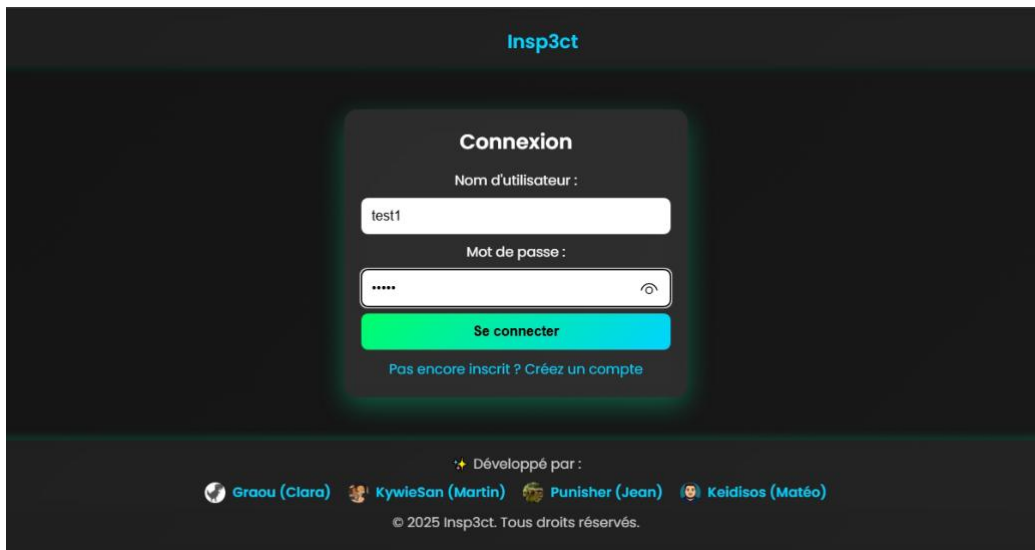
Pour faire, vous allez cliquer sur « se connecter » en haut à droite de votre écran :



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



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

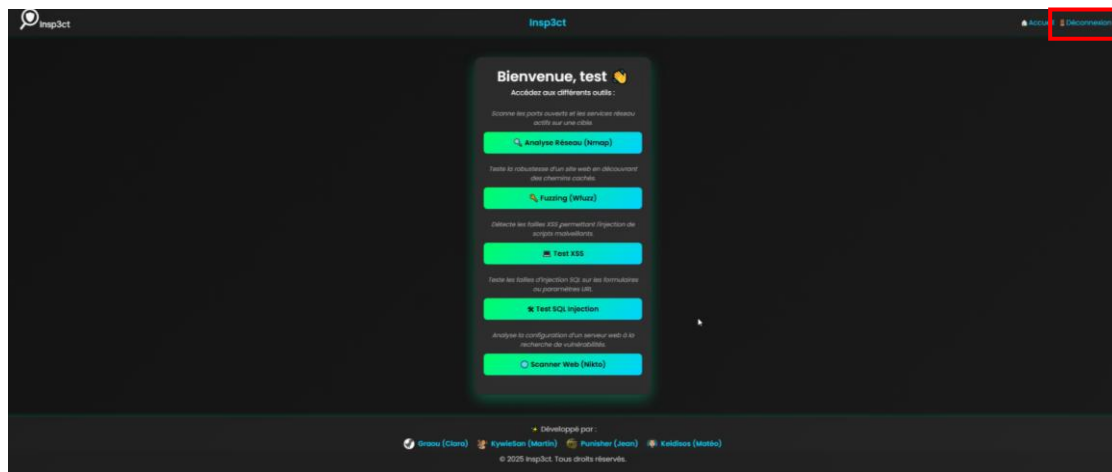


The image shows the login page of the Insp3ct application. At the top, the 'Insp3ct' logo is displayed in blue. Below it, a dark grey box contains the login form. The form has a title 'Connexion' in white. It includes a 'Nom d'utilisateur :' field with the text 'test1' and a 'Mot de passe :' field with masked characters '*****' and an eye icon to toggle visibility. A red 'Se connecter' button is positioned below the password field. Underneath the button is a link 'Pas encore inscrit ? Créez un compte'. At the bottom of the page, a footer section lists the developers: 'Développé par : Graou (Clara), KywieSan (Martin), Punisher (Jean), Keidisos (Matéo)' with their respective GitHub icons, followed by the copyright notice '© 2025 Insp3ct. Tous droits réservés.'

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 :

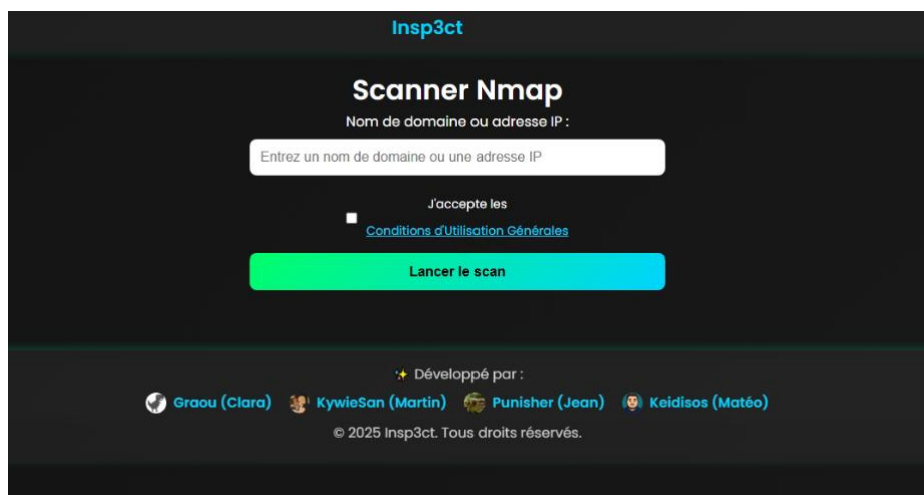


8. Utilisation des différents outils :

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 :



The screenshot shows the 'Scanner Nmap' interface within the Insp3ct application. At the top, the 'Insp3ct' logo is visible. Below it, the title 'Scanner Nmap' is displayed. A label 'Nom de domaine ou adresse IP :' is followed by a text input field containing the placeholder 'Entrez un nom de domaine ou une adresse IP'. Below the input field, there is a checkbox labeled 'J'accepte les' followed by a link 'Conditions d'Utilisation Générales'. A large blue button labeled 'Lancer le scan' is positioned below the checkbox. At the bottom of the interface, it says 'Développé par :' followed by four developer names with their avatars: 'Graou (Clara)', 'KywieSan (Martin)', 'Punisher (Jean)', and 'Keidisos (Matéo)'. The footer text reads '© 2025 Insp3ct. Tous droits réservés.'

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 :



The screenshot shows the 'Fuzzing avec Wfuzz' interface. At the top, the 'Insp3ct' logo is visible. Below it, the title 'Fuzzing avec Wfuzz' is centered. A text input field contains the URL 'https://monsite.com'. Below the input field, there is a checkbox labeled 'J'accepte les' followed by a link to 'Conditions d'Utilisation Générales'. A large green button labeled 'Lancer le Fuzzing' is positioned below the checkbox. At the bottom of the interface, it says 'Développé par :' followed by four user avatars and names: 'Graou (Clara)', 'KywieSan (Martin)', 'Punisher (Jean)', and 'Keidisos (Matéo)'. The footer text reads '© 2025 Insp3ct. Tous droits réservés.'

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 scripts malveillants, vous arrivez sur la page suivante :



The screenshot shows the 'Analyse XSS avec XSStrike' interface. At the top, the 'Insp3ct' logo is visible. Below it, the title 'Analyse XSS avec XSStrike' is centered. A text input field contains the URL 'https://monsite.com'. Below the input field, there is a checkbox labeled 'J'accepte les' followed by a link to 'Conditions d'Utilisation Générales'. A large green button labeled 'Lancer le scan XSS' is positioned below the checkbox. At the bottom of the interface, it says 'Développé par :' followed by four user avatars and names: 'Graou (Clara)', 'KywieSan (Martin)', 'Punisher (Jean)', and 'Keidisos (Matéo)'. The footer text reads '© 2025 Insp3ct. Tous droits réservés.'

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 :



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>.

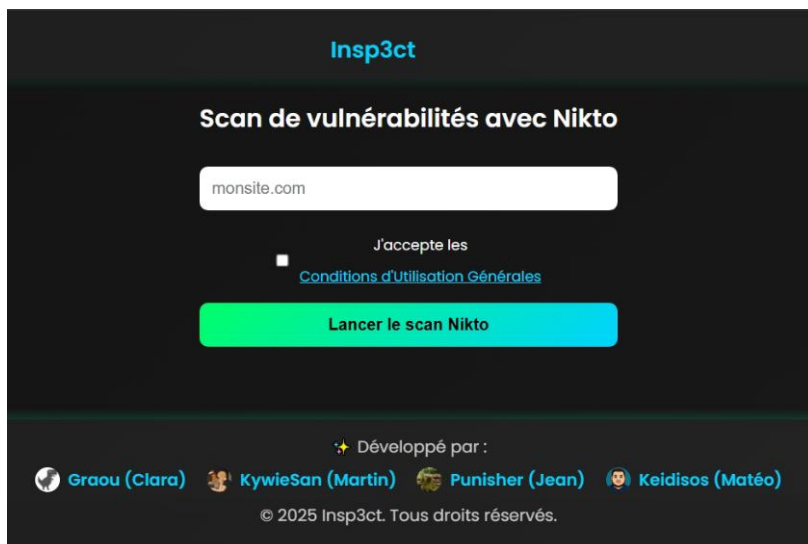


N'oubliez pas de lire et d'accepter (si vous êtes d'accord) les Conditions Générales d'Utilisation.

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 web interface for 'Insp3ct' with the title 'Scan de vulnérabilités avec Nikto'. It features a text input field containing 'monsite.com'. Below the input is a checkbox labeled 'J'accepte les' followed by a link 'Conditions d'Utilisation Générales'. A large orange button labeled 'Lancer le scan Nikto' is positioned below the checkbox. At the bottom, it lists developers: 'Développé par : Graou (Clara), KywieSan (Martin), Punisher (Jean), Keidisos (Matéo)' and a copyright notice '© 2025 Insp3ct. Tous droits réservés.'

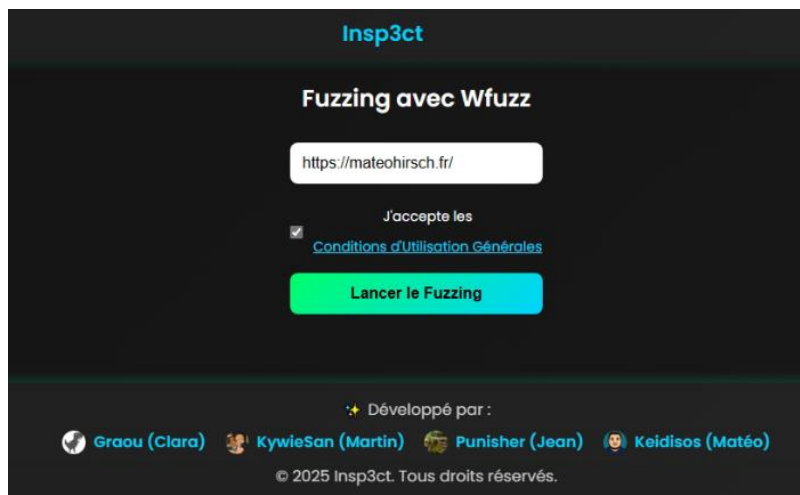
Afin de lancer un scan Nikto, il vous sera nécessaire d'indiquer le nom de domaine.
Exemple : monsite.fr.



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/>.

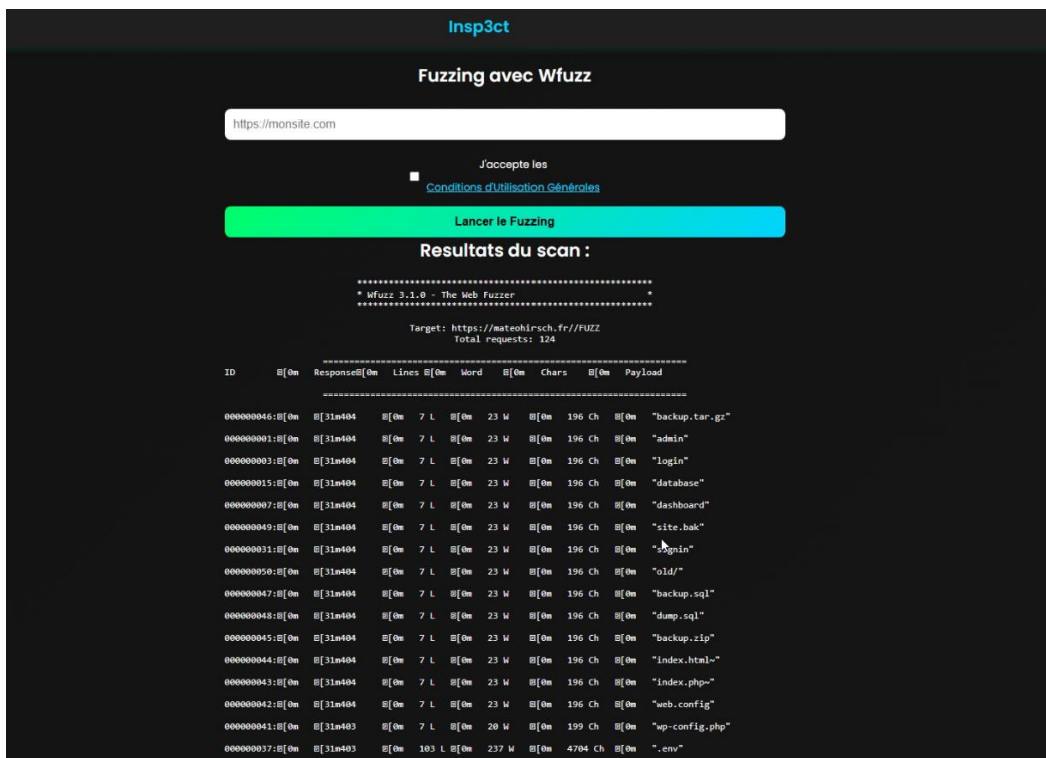


The screenshot shows a web interface for 'Insp3ct' with the title 'Fuzzing avec Wfuzz'. It features a text input field containing 'https://mateohirsch.fr/'. Below the input is a checked checkbox labeled 'J'accepte les' followed by a link 'Conditions d'Utilisation Générales'. A large orange button labeled 'Lancer le Fuzzing' is positioned below the checkbox. At the bottom, it lists developers: 'Développé par : Graou (Clara), KywieSan (Martin), Punisher (Jean), Keidisos (Matéo)' and 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 :



Fuzzing avec Wfuzz

https://monsite.com

☐ J'accepte les Conditions d'Utilisation Générales

Lancer le Fuzzing

Resultats du scan :

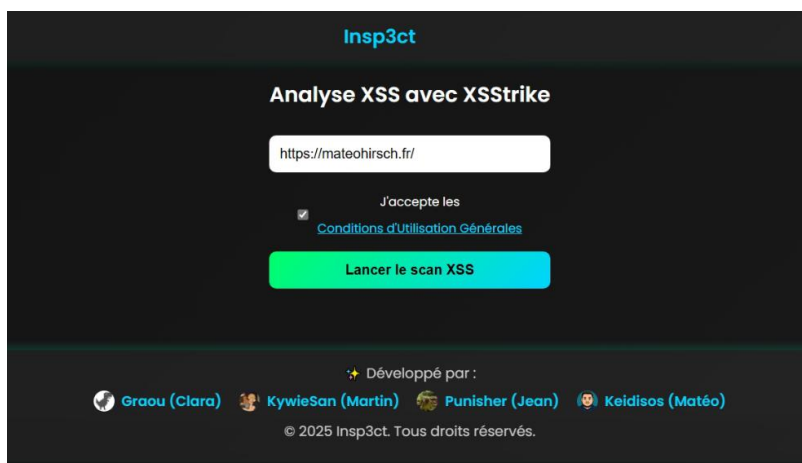
```
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: https://mateohirsch.fr//FUZZ
Total requests: 124
```

ID	Response	Lines	Word	Chars	Payload
000000046	200	7	23	196	"backup.tar.gz"
000000047	200	7	23	196	"admin"
000000048	200	7	23	196	"login"
000000049	200	7	23	196	"database"
000000050	200	7	23	196	"dashboard"
000000051	200	7	23	196	"site.bak"
000000052	200	7	23	196	"login"
000000053	200	7	23	196	"old/"
000000054	200	7	23	196	"backup.sql"
000000055	200	7	23	196	"dump.sql"
000000056	200	7	23	196	"backup.zip"
000000057	200	7	23	196	"index.html"
000000058	200	7	23	196	"index.php"
000000059	200	7	23	196	"web.config"
000000060	200	7	20	199	"wp-config.php"
000000061	200	103	237	4704	".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/>.



Analyse XSS avec XSSStrike

https://mateohirsch.fr/

☒ J'accepte les Conditions d'Utilisation Générales

Lancer le scan XSS

🌟 Développé par :

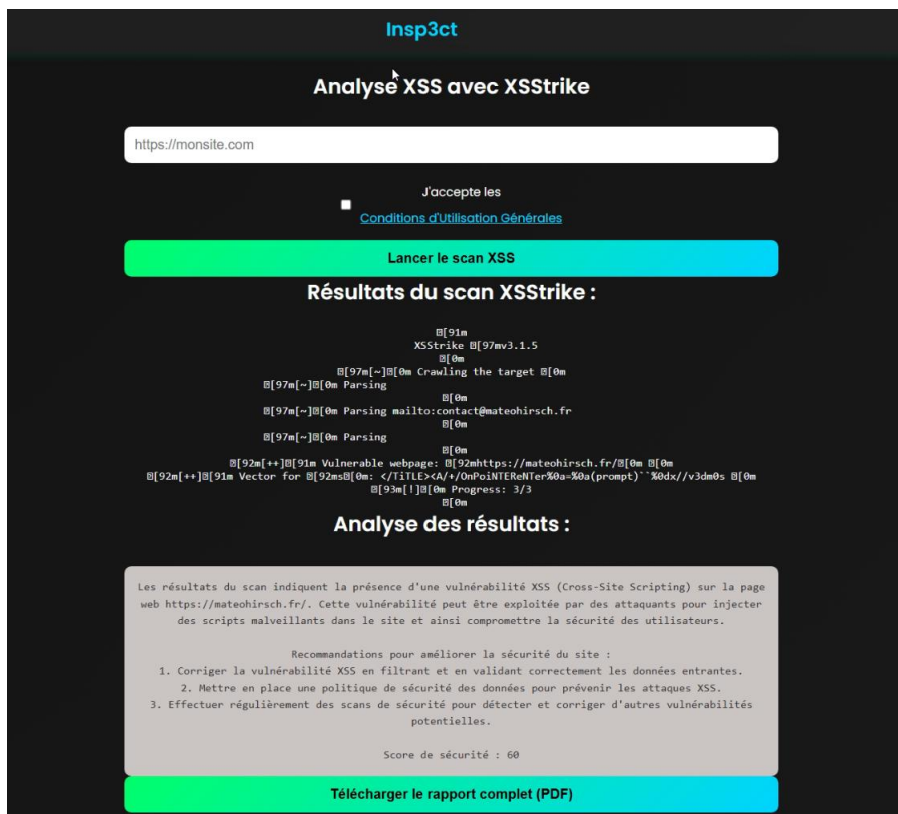
👤 Graou (Clara) 👤 KywieSan (Martin) 👤 Punisher (Jean) 👤 Keidisos (Matéo)

© 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

Analyse XSS avec XSSStrike

https://monsite.com

☐ J'accepte les [Conditions d'Utilisation Générales](#)

Lancer le scan XSS

Résultats du scan XSSStrike :

```

[91m
XSSStrike [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><A+/>OnPoINTERnEr%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 :

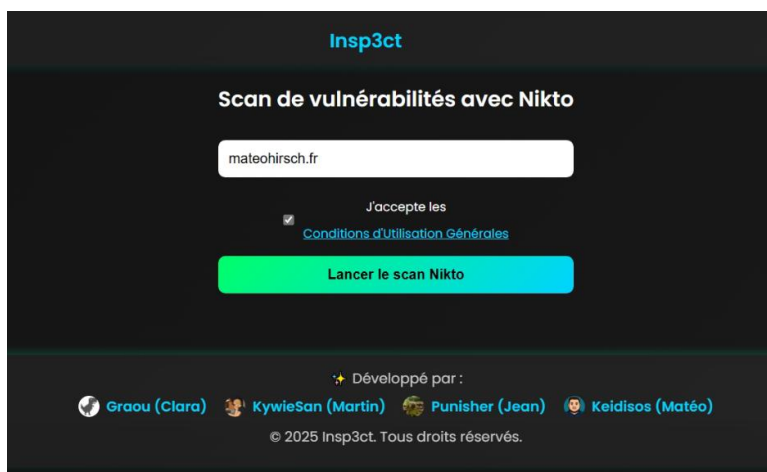
1. Corriger la vulnérabilité XSS en filtrant et en validant correctement les données entrantes.
2. Mettre en place une politique de sécurité des données pour prévenir les attaques XSS.
3. Effectuer régulièrement des scans de sécurité pour détecter et corriger d'autres vulnérabilités potentielles.

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/.



Insp3ct





Scan de vulnérabilités avec Nikto

mateohirsch.fr

☒ J'accepte les [Conditions d'Utilisation Générales](#)

Lancer le scan Nikto

✦ Développé par :

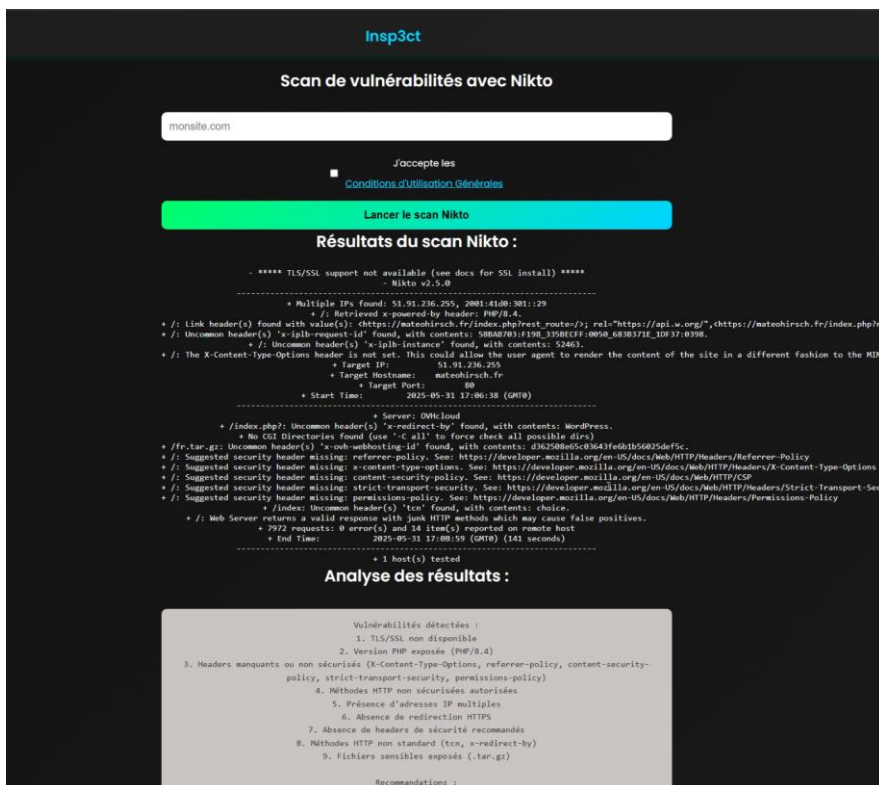
 Graou (Clara)  KywieSan (Martin)  Punisher (Jean)  Keidisos (Matéo)

© 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 :



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, 2001:41d0:301::29
+ /: Retrieved x-powered-by header: PHP/8.4.
+ /: Link header(s) found with value(s): <https://mateohirsch.fr/index.php?rest_route=/; rel="https://api.w.org"/>,https://mateohirsch.fr/index.php?rest_route=/; rel="https://api.w.org"/>,https://mateohirsch.fr/index.php?rest_route=/; rel="https://api.w.org"/>
+ /: Uncommon header(s) 'x-iplb-request-id' found, with contents: 58846783:1198_3358ECFF:0050_6030371E_ID37:0398.
+ /: Uncommon header(s) 'x-iplb-instance' found, with contents: 52462.
+ /: 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.
+ Target IP: 51.91.236.255
+ Target Hostname: mateohirsch.fr
+ Target Port: 80
+ Start Time: 2025-05-31 17:06:38 (GMT)
+ Server: OVHcloud
+ /index.php: Uncommon header(s) 'x-redirect-by' found, with contents: MueDPress.
+ No CGI Directories found (use '-c all' to force check all possible dirs)
+ /fr.tar.gz: Uncommon header(s) 'x-oh-uehosting-id' found, with contents: d362508e5c3643fedb156025def5c.
+ /: Suggested security header missing: referrer-policy. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-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: content-security-policy. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
+ /: 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
+ /index: Uncommon header(s) 'tcn' found, with contents: choice.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ 7972 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time: 2025-05-31 17:08:59 (GMT) (143 seconds)
+ 1 host(s) tested
  
```

Analyse des résultats :

Vulnérabilités détectées :

1. TLS/SSL non disponible
2. Version PHP exposée (PHP/8.4)
3. Headers manquants ou non sécurisés (X-Content-Type-Options, referrer-policy, content-security-policy, strict-transport-security, permissions-policy)
4. Méthodes HTTP non sécurisées autorisées
5. Présence d'adresses 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