

État de l'art

PER2024-050 - Flash audit automatisé pour la Cybersécurité Web : Conception d'un scanner de vulnérabilités proactif

Amandine Martin

Maxime BILLY

Evan TRANVOUEZ

Mohamed BOUCHENGUOUR

1. Introduction.....	3
2. Réglementation.....	4
2.1. Le RGPD : Règlement Général sur la Protection des Données.....	4
2.2. Directives NIS2 : sécurité des réseaux et des systèmes d'information.....	4
2.2.1. Entités Essentielles.....	4
2.2.2. Entités Importantes.....	5
2.3. Cyber Resilience Act : Résilience des produits numériques.....	5
2.4. Digital Operation Resilience Act (DORA) : Résilience Opérationnelle Numérique.....	5
2.5. Solutions d'accompagnement.....	6
2.6. Synthèse.....	6
3. Référentiels.....	7
3.1. OWASP TOP 10.....	7
3.2. CWE top 25.....	8
3.3. Bilan sur les vulnérabilités.....	11
4. Détection des vulnérabilités.....	12
4.1. Scanners de vulnérabilités commerciaux.....	12
4.2. Scanners de vulnérabilités gratuits et open source.....	14
4.3. Outils de vulnérabilités gratuits et open source.....	15
4.4. Synthèse comparative.....	18
5. La Cybersécurité pour tous.....	19
5.1. Analyse du modèle SEO.....	19
5.2. Notre proposition : Weakspotter.....	22
6. Conclusion de l'analyse de l'existant.....	23
Annexes.....	24
Annexes 1 : Lexique.....	24
Annexe 2 : Plan prévisionnel du rapport.....	26
Annexe 3: État d'avancement.....	26
Annexe 4 : Maquette.....	27
Annexe 5: diagramme.....	32
Annexe 6: Lien vers le projet.....	35
Bibliographie indicative.....	36

1.Introduction

La sécurité des applications web constitue aujourd'hui un enjeu stratégique majeur pour les entreprises, qu'elles soient de grande envergure ou de petite et moyenne taille ([TPE/PME](#)). Les menaces se diversifient et se multiplient, incluant les [fuites de données](#), les [rançongiciels](#), les [défacements](#), ainsi que le vol de propriétés intellectuelles. En 2022, selon l'[ANSSI](#), 40 % des attaques par [rançongiciel](#) traitées ou rapportées en France ciblaient des TPE et PME. De plus, en 2023, Cybermalveillance.gouv.fr note une hausse globale des recherches d'assistance pour des attaques informatiques liées à des actes malveillants en ligne (piratage de compte (+26 %), [hameçonnage](#) (+21 %), [rançongiciel](#) (+17 %), etc.).

Les [cyberattaques](#) entraînent des répercussions lourdes sur leur victime, notamment pour les TPE et PME, souvent moins protégées, car l'exploitation des [vulnérabilités](#) a un impact direct sur ces structures. En moyenne, selon [francenum.gouv.fr](#), une [cyberattaque](#) coûte 58 600 euros à une entreprise et entraîne une interruption du service informatique de 26 à 29 jours.

Des solutions existent déjà, mais celles-ci ne sont pas à la portée de ces entreprises. En effet, les solutions professionnelles de [test de pénétration](#) et de scan de vulnérabilités, bien que complètes et fiables, se révèlent généralement coûteuses, complexes à maîtriser et peu adaptées à un public non spécialiste. Les rendant donc non adaptées à ce public. De plus, des [outils gratuits](#) ou [open sources](#) existe également, pouvant être une solution peu coûteuse, mais celles-ci nécessitent fréquemment des compétences techniques avancées qui dépassent les capacités internes disponibles au sein des TPE/PME.

Par ailleurs, la législation européenne impose des exigences croissantes en cybersécurité, et ceci indépendamment de la taille des entreprises. Le RGPD (2018) exige des mesures de protection des données, tandis que la directive NIS2 (2022) élargit les obligations de cybersécurité à certaines PME et TPE opérant dans des secteurs critiques. Le Cyber Resilience Act et le Digital Operational Resilience Act obligent aussi des standards de sécurité sur les logiciels et infrastructures numériques. Face à ces obligations en matière de cybersécurité, les entreprises doivent adopter des solutions accessibles pour évaluer et corriger leurs vulnérabilités.

Ainsi, un écart significatif existe entre l'offre actuelle et les besoins réels des TPE et PME, lesquels souhaitent pouvoir effectuer un audit de sécurité à partir d'une simple URL, sans interventions techniques complexes et à un prix abordable.

Dans ce document, nous analyserons l'[IHM](#) des outils de SEO, qui ont réussi à rendre un outil d'analyse complexe et coûteux en quelque chose de simple d'utilisation et de compréhension.

Dans ce contexte, il est cohérent de proposer une solution qui offre simplicité et un prix abordable pour permettre un accès équitable aux entreprises de toute taille.

Ce document se concentre sur l'analyse des outils existants et l'étude préliminaire à la création de l'outil que nous avons surnommé "WeakSpotter". Nous explorerons l'évolution de la réglementation européenne, le panorama des [failles](#) de sécurité, les challenges posés par les outils existants et les adaptations nécessaires à la création de cette plateforme.

2. Réglementation

Les réglementations jouent un rôle clé pour protéger les systèmes et les données face aux cybermenaces croissantes. Ils obligent les entreprises à suivre des bonnes pratiques pour renforcer leur résilience et protéger les données personnelles.

Ces réglementations s'appliquent à toutes les entreprises, quelle que soit leur taille, et visent à garantir la protection des données, la sécurité des infrastructures numériques et la confiance entre les utilisateurs et les entreprises. Elles sont essentielles pour assurer la sécurité numérique et prévenir les cyberattaques.

2.1. Le RGPD : Règlement Général sur la Protection des Données

Le **RGPD** est entré en vigueur en mai 2018. Il impose des règles strictes pour la protection des données personnelles au sein de l'Union européenne. Ce règlement s'applique à toutes les entreprises traitant des données personnelles, quelle que soit sa taille.

Les entreprises doivent assurer la **confidentialité** et l'**intégrité** des données en mettant en place des mesures techniques et organisationnelles afin de prévenir tout accès ou traitement autorisé. En cas de violation de données, elles ont l'obligation de notifier les autorités dans un délai maximum de 72 h. Les organisations doivent également tenir un registre des traitements effectués et évaluer les risques qui y sont liés.

Le non-respect de ces obligations peut entraîner des sanctions financières sévères, pouvant atteindre **4 % du chiffre d'affaires** mondial annuel ou **20 millions d'euros**.

2.2. Directives NIS2 : sécurité des réseaux et des systèmes d'information

Adoptée en 2022, la directive **NIS2** (Network and Information Security) renforce le cadre établi par la directive NIS de 2016. Elle élève les exigences en matière de cybersécurité pour les secteurs critiques et **élargit son champ d'application** à un plus grand nombre d'entreprises, **y compris certaines TPE et PME**. Les entreprises concernées doivent identifier et gérer les risques liés à leurs réseaux et systèmes d'information en mettant en place des mesures techniques et organisationnelles appropriées.

La directive exige aussi la notification de tout incident majeur susceptible de compromettre la continuité des services ou la sécurité des données. Une notification initiale doit être transmise dans un délai de 24 heures, suivie d'un rapport détaillé sous 72 heures. Les dirigeants d'entreprise sont directement responsables de la conformité à ces obligations, ce qui inclut la formation en cybersécurité et la réalisation d'audits réguliers.

Les entités concernées par la directive sont classées en deux catégories : les **entités essentielles** et les **entités importantes**.

2.2.1. Entités Essentielles

Les entités essentielles regroupent les organisations publiques et privées opérant dans des secteurs critiques comme **l'énergie, les transports, la finance, la santé et l'approvisionnement en eau**.

Ces secteurs jouent un rôle clé dans le fonctionnement de la société et de l'économie, rendant impérative une protection renforcée contre les cybermenaces. En cas de non-conformité, ces entités risquent des sanctions pouvant atteindre **10 millions d'euros** ou **2 % de leur chiffre d'affaires** annuel global.

2.2.2. Entités Importantes

Les entités importantes, quant à elles, couvrent des secteurs tels que la **production alimentaire**, les **services numériques**, les **fournisseurs de services postaux**, ou encore la **gestion des déchets**. Bien que ces secteurs soient considérés comme moins critiques que ceux des entités essentielles, leur bon fonctionnement reste vital pour la société. Les sanctions en cas de non-respect des obligations sont également significatives, atteignant jusqu'à **7 millions d'euros** ou **1,4 % du chiffre d'affaires** annuel général.

2.3. Cyber Resilience Act : Résilience des produits numériques

Proposé par la Commission européenne en 2022, le **Cyber Resilience Act** (CRA) établit des normes de cybersécurité obligatoires pour tous les **produits numériques commercialisés** dans l'UE, qu'il s'agisse de logiciels, d'applications ou d'équipements connectés.

Les fabricants doivent garantir la sécurité de leurs produits dès la conception, ce qui inclut l'intégration de mesures préventives contre les vulnérabilités. Ils sont aussi tenus de fournir des mises à jour régulières pour corriger les failles identifiées après la mise sur le marché. Une documentation claire sur les risques et les mesures prises pour les atténuer doit être mise à disposition des utilisateurs.

Les exigences du CRA s'appliquent à toutes les entreprises, y compris les TPE et PME, qui doivent s'assurer de la conformité de leurs produits pour éviter des sanctions financières ou le retrait de leur offre du marché européen. En cas de non-respect, une amende pouvant atteindre **15 millions d'euros** ou **2,5 % du chiffre d'affaires annuel mondial**, en fonction de l'infraction. Les entreprises ne respectant pas les normes de sécurité ou omettant de signaler les incidents dans les délais risquent également des sanctions supplémentaires.

2.4. Digital Operation Resilience Act (DORA) : Résilience Opérationnelle Numérique

Adopté en 2022, le Digital Operational Resilience Act (DORA) renforce la résilience numérique des entreprises opérant dans le secteur financier. Ce règlement impose des normes strictes en matière de gestion des risques technologiques, en exigeant l'identification des vulnérabilités liées aux technologies de l'information et de la communication (TIC).

Les entreprises doivent effectuer des tests réguliers de leurs systèmes pour évaluer leur robustesse face aux cybermenaces et gérer de manière proactive les risques associés à leurs fournisseurs de services numériques. De plus, les incidents significatifs doivent être signalés aux

autorités compétentes dans des délais précis, ce qui renforce la transparence et la réactivité des entreprises en cas de cyberattaques.

Le non-respect des obligations prévues par le DORA peut entraîner des sanctions financières importantes pouvant aller jusqu'à 1 % du chiffre d'affaires journalier global pour chaque jour non respecté. Cela souligne l'importance pour les acteurs financiers, y compris leurs prestataires, de se conformer à ces exigences.

2.5. Solutions d'accompagnement

En complément des cadres réglementaires européens, de nombreux États membres de l'UE ont mis en place des **initiatives nationales** pour renforcer la cybersécurité des entreprises, en particulier des TPE et PME.

Ces initiatives incluent des subventions pour l'acquisition de solutions de cybersécurité, des campagnes de sensibilisation et des guides de bonnes pratiques adaptés aux spécificités locales. Certains pays offrent également des outils d'évaluation gratuits ou des audits simplifiés pour aider les entreprises à identifier leurs faiblesses et à se conformer aux réglementations européennes.

En ce qui concerne la **France**, celle-ci a mis en place un programme d'appui et de conseil qui permet le diagnostic, la mise en œuvre d'un plan et d'achat de solutions.

Cyber PME est une action conjointe entre la **Direction générale des Entreprises** (DGE) et **Bpifrance**. Ainsi, pour la somme de 8 800 € (subventionné à 50 %), cet outil permet d'identifier et de prioriser les actions de sécurisation.

Ces mesures visent à pallier les difficultés financières et techniques des petites structures, en leur offrant un soutien concret pour améliorer leur résilience face aux cybermenaces.

2.6. Synthèse


Toutes ces législations convergent sur une conclusion : il est **nécessaire d'investir** dans la cybersécurité en France et plus généralement en Europe. Dans le cas où celle-ci serait ignorée, les entreprises s'exposent à de **lourdes peines** et à des **coûts d'interruption de services** qui représentent un coût bien plus élevé qu'une mise en conformité.


3. Référentiels


La sécurité des applications web repose sur la protection de trois piliers fondamentaux : la confidentialité, l'intégrité et la disponibilité (CIA). Ce principe vise à garantir que les données sensibles ne soient accessibles qu'aux personnes autorisées (confidentialité), que les informations et les systèmes soient protégés contre toute modification non autorisée (intégrité), et que les services soient disponibles pour les utilisateurs sans interruption (disponibilité).

Pour mieux comprendre ces risques, nous nous sommes appuyés sur des référentiels reconnus, tels que OWASP et CWE, qui recensent et classifient les vulnérabilités.

De plus, nous avons mis en place une légende afin de voir quel pilier est corrompu et pour faciliter la compréhension des risques encourue.

 **Intégrité Corrompue:** une fois l'intégrité corrompue, les données et le système ne peuvent plus être considérés comme fiables.

 **Confidentialité Corrompue:** une fois la confidentialité corrompue, les données et le système sont accessibles par des personnes qui ne sont pas censé y avoir accès.

 **Disponibilité Corrompue:** une fois la disponibilité corrompue, les données et le système n'est plus accessible.

3.1. OWASP TOP 10

Le référentiel OWASP (Open Web Application Security Project) constitue une référence internationale incontournable. Son classement "Top 10" recense les failles de sécurité les plus critiques dans les applications web (OWASP, 2021).

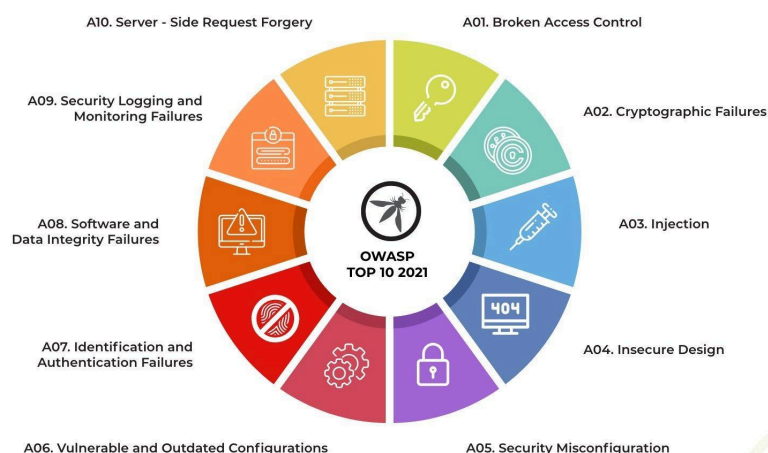














Figure 1 - OWASP top 10 - 2021

Parmi ces vulnérabilités, on retrouve notamment :

- **Contrôle d'accès rompu [A01]**   : C'est quand un système ne protège pas correctement l'accès aux données ou aux fonctions. Cela peut porter atteinte à l'intégrité des données mais aussi à leur confidentialité.
- **Injectons [A03]** ([SQL](#), [XSS](#), etc.)    : C'est quand un attaquant insère du code ou des commandes malveillantes dans une application via des failles de sécurité. Cela permet de manipuler des bases de données (suppression, modification ou ajout de données) ou d'exécuter du code malveillant dans les navigateurs (XSS).
- **Mauvaise configuration de sécurité [A05]**    : Cela arrive quand un système ou une application n'est pas bien protégé, par exemple avec des mots de passe par défaut, des permissions trop larges, ou des sécurités désactivées.
- **Composants vulnérables ou obsolètes [A06]**    : Les composants vulnérables ou obsolètes sont des logiciels ou matériels qui ne sont plus à jour et qui contiennent des failles de sécurité bien connues. Ces composants peuvent inclure des systèmes d'exploitation, des bibliothèques de code, des applications ou des dispositifs matériels. Si un attaquant exploite cette vulnérabilité, il peut tirer parti de failles de sécurité qui ont déjà été identifiées, ce qui facilite l'intrusion dans le système. Cela peut entraîner le vol ou la fuite de données sensibles, compromettant ainsi la confidentialité des informations. De plus, l'attaquant pourrait propager des attaques à d'autres systèmes connectés ou provoquer une interruption des services, rendant le système instable ou inutilisable.
- **Défaillances d'identification et d'authentification [A07]**  : elles se produisent lorsque les mécanismes qui vérifient l'identité des utilisateurs ne fonctionnent pas correctement. Cela peut permettre à des utilisateurs non autorisés d'accéder à des systèmes ou des données sensibles. Ces défaillances peuvent être le résultat de mots de passe faible, d'une absence de validation de l'identité ou de processus de connexion mal sécurisés.

3.2. CWE top 25

Un autre référentiel est le Common Weakness Enumeration (CWE) Top 25. Il s'agit d'un référentiel qui recense les 25 failles de sécurité critique dans les logiciels. Ce classement est basé sur la prévalence et la gravité des vulnérabilités, il aide les développeurs et les professionnels de la sécurité à se concentrer sur les problèmes de sécurité les plus fréquents.









2024 CWE Top 25



















Rank	ID	Name	Score	CVEs in KEV	Rank Change vs. 2023
1	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	56.92	3	+1
2	CWE-787	Out-of-bounds Write	45.20	18	-1
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	35.88	4	0
4	CWE-352	Cross-Site Request Forgery (CSRF)	19.57	0	+5
5	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12.74	4	+3
6	CWE-125	Out-of-bounds Read	11.42	3	+1
7	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11.30	5	-2
8	CWE-416	Use After Free	10.19	5	-4
9	CWE-862	Missing Authorization	10.11	0	+2
10	CWE-434	Unrestricted Upload of File with Dangerous Type	10.03	0	0
11	CWE-94	Improper Control of Generation of Code ('Code Injection')	7.13	7	+12
12	CWE-20	Improper Input Validation	6.78	1	-6
13	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	6.74	4	+3
14	CWE-287	Improper Authentication	5.94	4	-1
15	CWE-269	Improper Privilege Management	5.22	0	+7
16	CWE-502	Deserialization of Untrusted Data	5.07	5	-1
17	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	5.07	0	+13
18	CWE-863	Incorrect Authorization	4.05	2	+6
19	CWE-918	Server-Side Request Forgery (SSRF)	4.05	2	0
20	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	3.69	2	-3
21	CWE-476	NULL Pointer Dereference	3.58	0	-9
22	CWE-798	Use of Hard-coded Credentials	3.46	2	-4
23	CWE-190	Integer Overflow or Wraparound	3.37	3	-9
24	CWE-400	Uncontrolled Resource Consumption	3.23	0	+13
25	CWE-306	Missing Authentication for Critical Function	2.73	5	-5

Figure 2 - CWE top 25

Parmi ces vulnérabilités, on retrouve notamment :

- **Injection de commandes OS (CWE-78) [7]**    : Un attaquant peut envoyer des commandes malveillantes à un système. Ceci lui permettrait de prendre le contrôle du serveur, d'effacer ou de modifier des fichiers, d'installer des logiciels malveillants ou d'accéder à d'autres systèmes du réseau. Cela compromettrait la sécurité du système, entraînant des pertes de données et un accès non autorisé à des informations sensibles.
- **Injection SQL (CWE-89) [3]**    : Technique où des requêtes malveillantes sont envoyées à une base de données, exploitant des failles de sécurité. Ces requêtes sont ensuite exécutées par la base de données, ce qui peut permettre à l'attaquant d'accéder, de modifier ou de supprimer des données sans autorisation.
- **CSRF (Cross-Site Request Forgery) (CWE-352) [4]**   : Attaque où un utilisateur est trompé pour effectuer des actions non autorisées sur un site web où il est déjà connecté. Cela peut inclure des actions telles que changer de paramètre, effectuer des transactions, ou publier du contenu, tout cela sans que l'utilisateur s'en aperçoive.

- **Traversée de Répertoire (CWE-22) [5]**   : Faille où un attaquant peut accéder à des fichiers ou des répertoires au-delà de leurs restrictions prévues. Cela est souvent possible en manipulant les chemins de fichier dans les entrées utilisateur, comme en utilisant des séquences de caractère spécieux pour monter et descendre dans les répertoires (par exemple ../).
- **Lecture en dehors des limites (CWE-125) [6]**  : Faille où un programme lit des données en dehors des limites d'un tampon de mémoire, ce qui peut entraîner des comportements imprévus, et que des fuites d'information sensibles surviennent.
- **Utilisation après libération (CWE-416) [8]**   : Faille où un programme continue d'utiliser une mémoire qui a été libérée, ce qui peut entraîner des comportements imprévus, comme le plantage du programme ou des failles de sécurité exploitées par des attaquants.
- **Absence d'autorisation (CWE-862) [9]**   : Faille où un utilisateur non autorisé peut accéder à des ressources ou des fonctions pour lesquelles il n'a pas les permissions appropriées. Cela peut résulter de failles dans les mécanismes de contrôle d'accès ou de configuration incorrect, permettant ainsi à des individus non autorisés de consulter, modifier ou supprimer des données sensibles.
- **Téléchargement non restreint de fichiers dangereux (CWE-434) [10]**    : Faille où un attaquant peut télécharger des fichiers dangereux sur un serveur, exploitant des failles de sécurité. Cela peut permettre à des attaquants d'introduire des fichiers malveillants qui pourraient exécuter du code dangereux ou compromettre la sécurité du système.
- **Injection de Code (CWE-94) [11]**    : Technique où un attaquant introduit du code malveillant dans une application, en exploitant des failles de sécurité. Cela se produit souvent lorsqu'une application ne valide pas correctement les entrées utilisateur.
- **Validation d'entrée incorrecte (CWE-20) [12]**    : Faille où les entrées utilisateur ne sont pas correctement validées, permettant ainsi des attaques par injection de données malveillantes qui peuvent exploiter des failles de sécurité, comme des injections SQL, des scripts malveillants, ou d'autres attaques.

3.3. Bilan sur les vulnérabilités

On peut alors identifier des catégories de vulnérabilité critiques.

Catégorie	Impact principal
Problèmes liés aux Injections	Compromets l'intégrité des données et permet des actions non autorisées
Contrôle d'accès défaillant	Accès à des ressources sensibles sans autorisation
Mauvaise configuration de sécurité	Introduction de vulnérabilité exploitable par des erreurs de configuration
Défaillance d'authentification	Usurpation d'identité et compromission des comptes
Validation insuffisante des entrées	Exploitation via des données malveillantes
Vulnérabilité liée à la mémoire	Plantages ou exploitation des erreurs de programmation
Attaques spécifiques aux sessions	Actions non autorisées effectuées à l'insu des utilisateurs

Tableau 1- tableau récapitulatif des catégories des vulnérabilités les plus communes

Il existe aujourd'hui de nombreux types de vulnérabilités dans les applications web. Sans connaissances préalables ni outils de détection adaptés, il est difficile de les repérer efficacement. Pour les identifier toutes, il est essentiel de maîtriser un large éventail de domaines. Cependant, dans les TPE et PME, le dirigeant, souvent responsable de la gestion informatique, manque souvent de temps et des compétences nécessaires pour accomplir cette tâche. Cela est particulièrement crucial pour ces petites structures, car elles sont fréquemment les plus exposées aux cybermenaces en raison de leurs ressources limitées. D'où l'importance de proposer des outils adaptés, faciles à comprendre et à utiliser par leurs dirigeants.

Il est donc essentiel de pouvoir identifier et corriger ces vulnérabilités dès qu'elles se manifestent, et ce, dans toutes les applications web, quelle que soit la taille de l'entreprise. Toute entreprise doit se conformer aux exigences et réglementations européennes, indépendamment de ses ressources ou de sa taille.

4. Détection des vulnérabilités

Aujourd'hui, il existe plusieurs solutions pour détecter les vulnérabilités, mais celles-ci présentent certaines limites pour les dirigeants de TPE et PME. En effet, cette détection peut être classée en trois grandes catégories : les scanners de vulnérabilités commerciaux, les scanners open source et les outils open-source. Nous allons examiner leurs avantages et leurs inconvénients, en tenant compte des contraintes spécifiques des TPE et PME pour leur mise en application.

4.1. Scanners de vulnérabilités commerciaux

Des solutions, souvent proposées sous forme de services, sont conçues pour offrir une expérience clé en main, combinant efficacité, support technique et mises à jour régulières.

Cependant, leur adoption peut représenter un défi pour les TPE et PME. En raison de budgets généralement limités, ces entreprises peuvent rencontrer des difficultés à justifier l'investissement nécessaire pour ces outils payants. Selon un sondage réalisé par l'usine digital pendant l'été 2024, les TPE et PME ont un budget moyen de 2000 €. Et dans 80 % des entreprises de ce type, il s'agit du chef d'entreprise qui s'occupe de gérer l'informatique.

Il est essentiel de comprendre les avantages et les limites des scanners de vulnérabilités commerciales afin d'évaluer leur pertinence pour les petites structures. Cette section explore ces aspects pour mieux appréhender leur application dans un contexte de contraintes financières et opérationnelles.

OUTIL	PRIX	SIMPLICITÉ D'UTILISATION	COUVERTURE	SUPPORT
Acunetix (Invicti)	★★★★☆ 4 495 \$/an	★★★★★ Interface intuitive, rapports clairs, mais demande quelques bases en sécurité	★★★★★ Excellente couverture des vulnérabilités complexes, y compris applications dynamiques	★★★★★ Support client réactif et bien documenté
Burp Suite Pro (PortSwigger)	★★★★★ 449 \$/an	★★★★☆ Moins intuitif, courbe d'apprentissage pour non-experts	★★★★★ Couverture très détaillée pour des tests approfondis	★★★★★ Support et communauté très présents
Nessus (Tenable)	★★★★☆ 2 990 \$/an	★★★★☆ Interface accessible, mais exige des compétences techniques	★★★★★ Très bon pour les réseaux, configurations système, moins pour le web	★★★★★ Support fiable et réactif
VRx (Vicarius)	★★★☆☆ 10 000 \$/an	★★★★☆ Accessible avec des outils avancés, mais nécessite une équipe IT	★★★★★ Focus exceptionnel sur la correction proactive	★★★★★ Support haut de gamme
Qualys TruRisk	★★★★★ Version gratuite ou 199 \$/mois	★★★★☆ Interface technique, nécessite un peu d'adaptation	★★★★★ Bonne couverture des vulnérabilités générales	★★★★★ Support disponible, bonnes ressources
Intruder (Intruder System)	★★★★★ ~145 €/mois	★★★★★ Extrêmement simple d'utilisation	★★★★☆ Couverture correcte, mais limitée sur des failles complexes	★★★★★ Support réactif, notifications automatiques utiles

Tableau 2 -tableau récapitulatif des scanners commerciaux

Nous avons réalisé un panorama des plus grosses solutions de cybersécurité proposées. Nous avons retenu six entreprises. (cf. Tableau 2).

Parmi les **avantages et inconvénients** qu'une solution propriétaire apporte à une alternative open source, nous avons les points suivants :

- **Support Client**

Une solution payante offre généralement un **support plus complet** qu'une solution Open Source. Certaines entreprises comme Acunetix et PortSwigger (Burp Suite) proposent également des **formations** pour enseigner les bonnes pratiques de cybersécurité aux professionnels. Un plus non négligeable pour une TPE/PME voulant se mettre à niveau dans ce domaine.

- **Simplicité d'utilisation**

Toutes ces plateformes ont pour but de simplifier la prise en main et l'utilisation de leur outil et, avec l'aide de professionnels, ils réussissent à **supprimer une grande partie de la complexité** de la mise en place initiale. Malgré tout, ce sont des outils professionnels, adressés à un personnel qualifié. C'est ce même personnel qui manque cruellement aux TPE/PME. Selon une étude réalisée en 2024 pour [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr), **72 % des TPE et PME** ne disposent pas de personnel qualifié dans ce domaine, montrant l'importance du support client. De plus, **56 %** des entreprises interrogées disent qu'elles ont un manque de connaissance et d'expertise

- **Couverture [CVE](#)**

Les outils payants ont généralement de plus grandes ressources leur permettant d'avoir une **plus grande couverture de vulnérabilités plus rapidement**. Malgré tout, en prenant l'exemple de Nessus et OpenVAS (une alternative open source à Nessus), selon intruder.io¹, Nessus couvrirait 41,8 % des vulnérabilités connues contre 37,4 % pour OpenVAS. Même si cela représente une différence notable, c'est une différence qui va plutôt intéresser les professionnels et non les petites entreprises en recherche d'une sécurité informatique basique.

- **Des coûts élevés**

Les licences des scanners commerciaux représentent une barrière financière importante. Elles varient traditionnellement entre **500 et 10 000 euros par an**, ce coût est souvent une barrière dans l'obtention et de leur mise en place. Alors que selon l'étude réalisée pour [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr), **68 %** des entreprises interrogées ont un budget alloué de moins de **2 000 euros par an**.

Bien que ces services offrent de nombreux avantages, tels que leur **simplicité d'utilisation** et une **couverture importante** des vulnérabilités, leur **coût élevé** les rend généralement inaccessibles pour les PME et TPE dans le cadre de leurs campagnes de sécurité.

¹ Intruder est un concurrent à Nessus, cette étude est donc à prendre avec du recul.

4.2. Scanners de vulnérabilités gratuits et open source

Face aux coûts élevés des solutions commerciales, de nombreuses alternatives gratuites et open source sont disponibles. Ces solutions sont entièrement gratuites et libres d'utilisation, mais généralement moins complètes que leurs homologues commerciaux.

De plus, ils sont aussi souvent plus difficiles d'utilisation, ou dans **72 % des TPE et PME**, aucun personnel n'est qualifié dans le domaine de la cybersécurité, selon l'étude faite pour Cybermalveillance.gouv.fr.

OUTIL	SIMPLICITÉ D'UTILISATION	COUVERTURE	SUPPORT
OWASP ZAP	★★★★☆ Courbe d'apprentissage avec doc technique	★★★★★ Excellente couverture des vulnérabilités complexes, y compris applications dynamiques	★★★★☆ Support communautaire actif, mais pas de premium
Nikto	★★★☆☆ Moins intuitif, courbe d'apprentissage pour non-experts	★★★★☆ Couverture très détaillée pour des tests approfondis	★★★★☆ Support limité à la communauté (non-officiel)
WPScan	★★★★★ Très simple si l'entreprise utilise WordPress	★★★★☆ Limité aux vulnérabilités WordPress (43,3 % de tous les sites web)	★★★★☆ Support communautaire ou premium limité
OpenVAS	★★★☆☆ Complexité élevée, demande une infrastructure dédiée (Fort malus pour l'interface graphique)	★★★★★ Large couverture des vulnérabilités réseau et web	★★★★☆ Support communautaire actif mais sans garantie

Tableau 3 -tableau récapitulatif des scanners

Pour notre analyse comparative, nous avons retenu quatre scanners (cf. Tableau 3) dont deux spécialisés dans le scan web.

Ces scanners/plateformes ont tous un point commun, ils publient leur code source et sont **libres de droits**. Créés par la communauté, ces outils sont mis à disposition gratuitement, **sans discriminer** le client mais aussi **sans garantie d'aucune sorte**.

Après analyse, voici les **avantages et inconvénients** que nous avons trouvés pour ces plateformes :

- **Complexité**

Là où les outils propriétaires étaient complexes seulement dans leur interprétation, les outils open source nécessitent aussi une **installation et configuration complexe** avant de pouvoir être utilisés. En effet, un travail préalable concernant l'installation de paquets spécifiques à chaque outil est nécessaire. Cela représente une barrière conséquente, nécessite l'intervention d'un personnel formé et d'une compréhension des besoins au préalable de la configuration. De plus, lors de l'utilisation de certains scanners comme nikto, tout se fait par ligne de commande, nécessitant une connaissance sur l'utilisation d'un terminal. La connaissance des commandes de l'outil et l'interprétation des résultats sont également nécessaires, car ces résultats sont souvent présentés dans un format non traditionnel.

- **Support**

Malgré cette complexité plus importante, le support lui aussi est souvent manquant. L'absence d'une structure de soutien formelle, combinée à une participation limitée de la communauté, et exacerbée par un manque de financement, peut rendre difficile pour les projets open-source de fournir un soutien adéquat à leurs utilisateurs. Les entreprises n'ont pour autre choix que de consulter la **documentation** écrite par la communauté, qui peut être **complexe** et/ou **lacunaire**. C'est une des raisons principales qui expliquent que les TPE/PME n'utilisent pas ce genre d'outils.

- **Couverture [CVE](#)**

Pour les mêmes raisons que le support vient à manquer, les scanners open source ont généralement un peu de **retard** sur les outils propriétaires en ce qui concerne la quantité de vulnérabilités prise en charge. Encore une fois, c'est un point plus susceptible de préoccuper les spécialistes que les petites entreprises qui recherchent uniquement une sécurité informatique de base.

4.3. Outils de vulnérabilités gratuits et open source

En plus des scanners de vulnérabilité, des outils pour pouvoir détecter des vulnérabilités existent. Ceux-ci sont spécifiques à une fonctionnalité ou un domaine très restreint.

Ces **outils** comblent les lacunes des scanners en ciblant des aspects précis, comme les ports ouverts, la configuration des serveurs ou les vulnérabilités propres à certains logiciels, permettant ainsi une analyse plus approfondie.

Parmi les outils existants, une partie sert à la détection de CMS. En effet, un **système de gestion de contenu (CMS)** est une plateforme logicielle permettant de créer, gérer et publier un site web sans nécessiter de compétences en programmation. Grâce à une interface intuitive, les utilisateurs peuvent ajouter du contenu, personnaliser l'apparence et intégrer des fonctionnalités via des extensions ou des modules.

Ces solutions sont particulièrement adoptées par les **TPE et PME**, qui ne disposent souvent ni des compétences techniques ni des moyens financiers pour développer un site sur mesure. Elles offrent une alternative accessible aux développements nécessitant des ressources spécialisées. Selon **l'AFNIC**, **83 %** des TPE/PME et **63 %** des microentreprises disposent d'un site web. ([AFNIC](#)), cela illustre l'importance pour ces entreprises d'avoir une présence en ligne, et le rôle essentiel des CMS pour y parvenir sans nécessiter de ressources techniques ou financières importantes.

En 2024, parmi l'ensemble des sites web, environ **68,7 % utilisent un CMS** ([WPADE](#)). WordPress domine largement avec **62,7 % de part de marché**, suivi par Shopify (6,4 %), Wix (3,9 %) et Squarespace (3 %). ([Bloggerspassion](#))

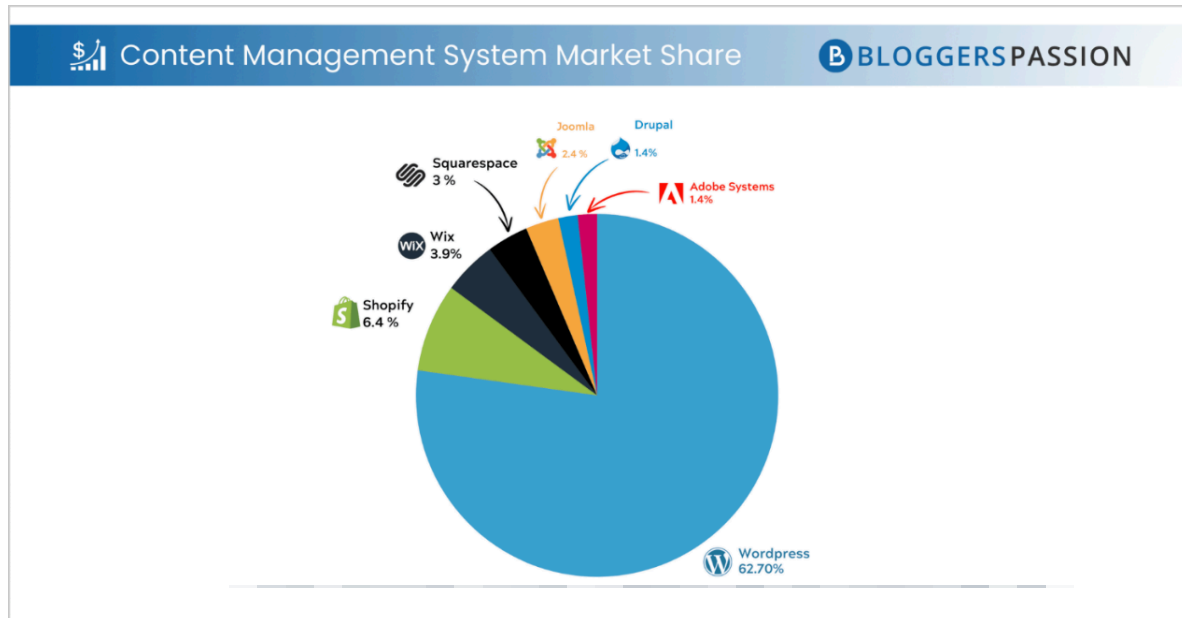


Figure 3 - part de marché des CMS

Cependant, cette popularité fait aussi des CMS une cible privilégiée des cyberattaques. Selon une étude menée par Sucuri en 2019 ([Sucuri](#)), **94 % des sites piratés utilisaient WordPress**, suivi par Joomla (2,5 %) et Drupal (1,2 %). Ces chiffres s'expliquent notamment par le fait que de nombreux sites WordPress sont créés et administrés par des personnes n'ayant pas nécessairement de connaissances en cybersécurité. Cela augmente ainsi le risque d'erreurs de configuration et d'utilisation de plugins vulnérables. Ce manque de sécurisation attire donc particulièrement les [cybercriminels](#), qui y voient une opportunité d'exploitation facile.

Étant donné leur large adoption et leur **forte exposition aux cyberattaques**, les CMS nécessitent une attention particulière en matière de sécurité. Pour mieux identifier les vulnérabilités spécifiques à ces plateformes, nous utiliserons des outils spécialisés qui viendront compléter les scanners précédents en ciblant des éléments propres à chaque système :

- **WPScan** : Analyse des sites WordPress pour identifier les vulnérabilités des extensions, des thèmes et des paramètres de configuration. Il aide également à repérer les versions obsolètes et les pratiques à risque.
- **Joomscan** : Conçu pour Joomla, il détecte les failles dans les composants du site, y compris les extensions vulnérables et les erreurs de configuration pouvant être exploitées.
- **Droopescan** : Spécialisé dans l'évaluation des sites Drupal, il permet d'identifier les modules obsolètes, les thèmes vulnérables et d'autres éléments pouvant compromettre la sécurité du site.

En revanche, des outils similaires n'existent pas pour des CMS comme Shopify, Wix ou Squarespace, ce qui limite les possibilités d'analyse spécifique. Dans ces cas, seuls les scanners généralistes seront utilisés, offrant un niveau de détection plus limité que pour les CMS bénéficiant d'outils spécialisés.

En plus de ces scanners, d'autres outils que les scanners de CMS existent

Catégorie	Outil	Description
Cartographie et découverte d'infrastructures	SUBLIST3R, CSmap, Whois, Dig, Oralyzer	Énumération des sous-domaines, identification des technologies, récupération des informations administratives (Whois), interrogation DNS et analyse des fichiers robots.txt.
Analyse de la configuration et des services	Nmap (NSE), SSH Audit, Wapiti	Détection des services actifs, audit de la sécurité SSH, analyse des configurations et des protections web (CSP, HSTS...).
Exploration et tests d'accès	GoBuster, FUZZ, Cloudflare Detect	Recherche de répertoires cachés, tests d'injection et d'accès, identification des protections Cloudflare.
Recherche de vulnérabilités et d'exploits	Searchsploit, Metasploit	Recherche d'exploits dans des bases de données publiques et exploitation automatisée des vulnérabilités.
Collecte d'informations (OSINT)	Email Harvester	Extraction automatique d'adresses email depuis des sources publiques.

Tableau 4 - tableau des outils par intermédiaire

Aucune automatisation n'existe pour l'utilisation de ces outils. À chaque fois qu'on souhaite en utiliser un, on doit alors exécuter une ligne de commande détaillée, et ce, pour chaque outil. De plus, ils ont tous des configurations spécifiques, ce qui est impossible pour un dirigeant de TPE et PME à suivre et à mettre en place. De plus, une fois chaque outil utilisé, ils ont chacun une façon différente de présenter les résultats, et de façon plus ou moins compréhensible. Il faut donc être aussi capable d'interpréter les résultats.

4.4. Synthèse comparative

Le tableau ci-dessous synthétise les caractéristiques des différentes catégories d'outils existants :

Catégorie	Coût approximatif (licence)	Complexité	prise en main	Adapté PME
Scanners commerciaux	de ~500 €/an à ~6000 \$/an	Moyenne	Interface professionnelle, configuration complexe	Faible (coût trop élevé)
Scanneurs gratuits/open source	0 €	Moyenne	configurations	Moyenne (compréhensibilité trop compliqué)
Outils	0 €	Élevée	ligne de commande et configuration technique	faible (mise en place des outils compliquée)

Tableau 5 - tableau récapitulatif des trois catégorie

Ce tableau met en évidence le fossé existant entre les solutions commerciales, complètes, mais coûteuses et complexes, et les outils gratuits ou open sources, abordables, mais nécessitant des compétences techniques et des intégrations manuelles. Les PME, en quête d'une approche simplifiée (champ URL, un clic, rapport clair), ne trouvent pas de solution adéquate dans l'offre actuelle du marché.

5. La Cybersécurité pour tous

5.1. Analyse du modèle SEO

Les outils d'analyse SEO, bien que centrés sur l'optimisation des moteurs de recherche, partagent des points communs avec les scanners de vulnérabilités en termes de fonctionnement et d'expérience utilisateur.

Une analyse SEO est traditionnellement **une analyse complète et complexe** à interpréter nécessitant l'intervention de personnel qualifié. Malgré cela, des outils ont été mis à disposition du public, gratuitement ou non, permettant la vulgarisation de ce sujet et l'analyse simplifiée d'un site web.

Dans cette partie, nous analyserons l'interface de **PageSpeed Insights** (Google Light house), un outil proposé gratuitement par Google à l'interface simple.



Figure 4 - Page d'accueil de PageSpeed Insights

Lors de la navigation vers le site de la plateforme, nous sommes accueillis par un simple champ de texte annoté de "Saisir l'URL d'une page Web" (cf. Figure 7). C'est un **design simple** qui attire l'attention via un **call to action** incitant à lancer l'analyse.

On remarque qu'il n'y a **pas d'étape d'installation** du logiciel et **pas d'étape de configuration**. C'est un grand avantage pour permettre l'accessibilité à tous. Quel que soit le budget, peu importe les compétences techniques, il est simple de créer une analyse.

Rapport du 26 janv. 2025, 14:52:12

<https://ozeliurs.com/>

Analyser

Mobile

Bureau

Découvrez l'expérience de vos utilisateurs

Aucune donnée

Analysez les problèmes de performances

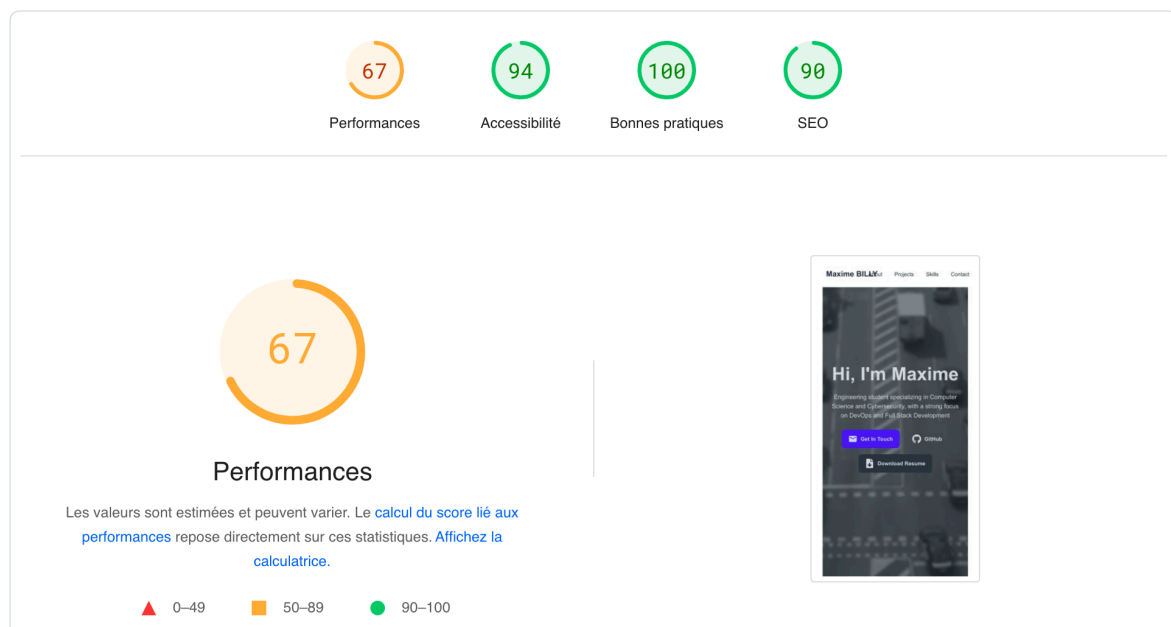


Figure 5 - Résultats d'une analyse

Après qu'une analyse soit terminée, une interface simple nous est présentée. Celle-ci comporte, à gauche, un simple **score global** accompagné d'un **code couleur tricolore**. À droite, un aperçu du site web scanné. Et au-dessus, quatre scores détaillant le résultat par catégorie.

Nous retiendrons que l'interface **ne surcharge pas l'utilisateur**, il lui présente le strict nécessaire quitte à manquer de détails.

DIAGNOSTIC		
▲	Élément identifié comme "Largest Contentful Paint" — 6 200 ms	▼
▲	Diffusez des images aux formats nouvelle génération — Économies potentielles de 323 Kio	▼
▲	Précharger l'image Largest Contentful Paint — Économies potentielles de 930 ms	▼
■	Diffusez des éléments statiques grâce à des règles de cache efficaces — 2 ressources trouvées	▼
■	Réduisez les ressources JavaScript inutilisées — Économies potentielles de 21 Kio	▼
○	Le temps de réponse initial du serveur était court — Le document racine a pris 50 ms	▼
○	Éviter d'énormes charges utiles de réseau — La taille totale était de 705 Kio	▼
○	Éviter une taille excessive de DOM — 946 éléments	▼

Figure 6 - Suite des résultats d'une analyse

Plus bas sur la page, la suite de l'analyse devient **plus technique** mais se concentre sur les éléments d'amélioration. Cette partie **garde le code tricolore** et **priorise le diagnostic**.

▲	Diffusez des images aux formats nouvelle génération — Économies potentielles de 323 Kio	^
<p>Les formats d'image comme WebP et AVIF proposent souvent une meilleure compression que PNG et JPEG. Par conséquent, les téléchargements sont plus rapides et la consommation de données est réduite. En savoir plus sur les formats d'image récents LCP FCP</p>		
URL	Taille de la ressource	Économies potentielles
credly.com	472,2 KiB	280,8 KiB
...20082fc1-94af-4773-9df0-28856b566748/image.png (images.credly.com)	195,1 KiB	128,2 KiB
...22a0ece5-f05-4594-8320-25e55e9ae203/image.png (images.credly.com)	200,6 KiB	125,0 KiB
...70d71df5-.../CCNAITN__1_.png (images.credly.com)	37,4 KiB	14,0 KiB
...f4ccdba9-.../CCNASRWE__1_.png (images.credly.com)	39,2 KiB	13,6 KiB
picsum.photos	88,9 KiB	41,9 KiB
...1920/1080.jpg?blur=5&hmac=EcEtUQvcZ...	88,9 KiB	41,9 KiB

Figure 7 - Détail d'un élément de l'analyse

Finalement, l'utilisateur peut cliquer sur un élément de l'analyse pour en voir les détails et **consulter les liens** vers divers guides et **ressources en relation avec le problème**.

L'expérience utilisateur de PageSpeed Insights représente une source d'inspiration en termes de vulgarisation. En effet, cette simplicité de lecture et de compréhension nous semble être un élément primordial pour que le domaine de la cybersécurité soit accessible à tous. Notre cible utilisateur est peu qualifiée, comme peut l'être le personnel d'une TPE et PME.

5.2. Notre proposition : Weakspotter

Nous proposons une solution, Weakspotter, qui a pour but d'être facilement compréhensible, quel que soit le public et utilisable peu importe les compétences informatiques.

	Coût	Installation	Complexité	Utilisation Automatique
scanner commerciaux	entre 500 et 10 000 € euros par ans	Simple	à comprendre les rapports	Oui
scanner open-source	0 €	Complexe	à comprendre les rapports	Oui
outils open-source	0 €	Complexe	à comprendre les sorties	Non
Weakspotter	0 €	Simple	simple	Oui

Tableau 6 - Tableau récapitulatif des solutions envisageables pour une TPE et/ou PME

Notre solution **Weakspotter** répondra donc parfaitement au besoin des TPE et PME. Un service gratuit, composé de scanners et outils open-source, qui propose un scan complet et intuitif de n'importe quelle plateforme web.

Notre interface est fortement inspirée de sites d'analyse de SEO, avec le principal input de l'URL pour effectuer le scan, puis une vue d'ensemble du site et des améliorations, avec possibilité d'aller plus en détails et de consulter les ressources externes.

Nous découpons chaque analyse en quatre catégories, la sécurité du **backend** web, la sécurité du **frontend** web, la sécurité du **serveur web sous-jacent** et finalement la sécurité du **DNS**. Ces catégories sont encore sujettes à changer au fil de nos recherches.

Pour rendre les analyses abordables par les chefs d'entreprise, nous comptons utiliser l'**IA** intelligemment pour **rédigier des descriptions des CVE** abordables par les non-initiés. Nous explorons également la possibilité de faire un résumé global IA.

Nous avons finalement réalisé un travail de **documentation** détaillé sur les méthodes de déploiement, dans le but d'assister les administrateurs système dans le déploiement de cet outil.

6. Conclusion de l'analyse de l'existant

L'analyse menée dans ce rapport met en évidence les défis majeurs rencontrés par les TPE et PME en matière de cybersécurité. Alors que les menaces numériques se multiplient et que les réglementations, telles que le **RGPD** ou la directive **NIS2**, imposent des exigences croissantes, ces petites structures peinent à trouver des solutions adaptées à leurs besoins et à leurs moyens.

L'offre existante présente des **incompatibilités** par rapport aux attentes et aux capacités des petites entreprises. Les solutions commerciales, bien que performantes, restent souvent inaccessibles en raison de leur **coût élevé** et de leur **complexité**. De l'autre côté, les outils open source, bien qu'abordables, exigent des **compétences techniques** que ces structures ne possèdent généralement pas.

C'est dans ce contexte que nous créons le projet WeakSpotter, une solution conçue pour **démocratiser la cybersécurité** auprès des TPE et PME. En s'inspirant des approches simplifiées des outils SEO, WeakSpotter offre une expérience intuitive, basée sur un simple champ URL, et génère un **audit clair et exploitable** sans nécessiter d'expertise technique. Cette solution se positionne comme un pont entre la complexité des outils actuels et les besoins réels des petites entreprises.

Annexes

Annexes 1 : Lexique

Cette section présente les termes techniques et spécifiques utilisés dans ce rapport, ainsi que leurs définitions pour faciliter la compréhension

- **TPE:** *Très Petite Entreprise, ce sont des entreprises de moins de 10 salariés et un chiffre d'affaire inférieur à 2 millions d'euros*
- **PME:** *Petit et Moyenne entreprise, ce sont des entreprises entre 10 et 250 salariés et un chiffre d'affaire inférieur à 50 millions d'euros*
- **Fuite de données :** *Une situation où des informations sensibles ou confidentielles (comme des données personnelles) sont accidentellement ou intentionnellement accessibles à des personnes non autorisées.*
- **Rançongiciels (Ransomware) :** *Un type de logiciel malveillant qui bloque l'accès aux fichiers ou systèmes d'une entreprise, en demandant une rançon pour les débloquer.*
- **Défacement :** *Une cyberattaque où un pirate modifie l'apparence d'un site web, souvent pour afficher un message ou un contenu non autorisé.*
- **ANSSI:** *Autorité française de cybersécurité qui protège les systèmes informatiques nationaux contre les cybermenaces. Elle conseille, prévient et régule la sécurité numérique des organisations publiques et privées en émettant des recommandations et en certifiant des produits de sécurité.*
- **Hameçonnage:** *L'hameçonnage est une technique de cyberattaque malveillante visant à tromper des individus pour voler des informations sensibles en se faisant passer pour une source légitime via des emails, messages ou sites web falsifiés.*
- **Cyberattaque :** *Une action malveillante visant à perturber, voler ou endommager un système informatique ou des données.*
- **Vulnérabilité :** *Une faiblesse dans un système, une application ou un réseau, que des pirates peuvent exploiter pour accéder ou nuire à des données ou des services.*
- **Test de pénétration (Pentest) :** *Une méthode pour évaluer la sécurité d'un système informatique en simulant des attaques pour identifier les failles.*

- **Outils Open-source:** logiciels dont le code source est librement accessible, modifiable et redistribuable par tous.
- **Outils Libre:** logiciel dont l'utilisation, la modification et la duplication en vue de sa diffusion est permise
- **IHM :** Interface Homme-Machine, domaine englobant l'UX (Expérience utilisateur) et UI (Interface utilisateur), améliorant le visuel et design d'une application.
- **Faille :** Une erreur ou une faiblesse dans un système informatique qui peut être exploitée par des pirates.
- **Cybercriminels :** Des individus ou groupes qui utilisent des technologies informatiques pour commettre des crimes, comme voler des données ou extorquer de l'argent.
- **Audit de sécurité :** Une analyse approfondie pour vérifier que les systèmes et données d'une entreprise sont bien protégés contre les menaces.
- **Flash audit :** Un audit rapide qui donne une vue d'ensemble de la sécurité d'une entreprise, pour identifier les points faibles en peu de temps.
- **SQL:** langage utilisé pour gérer les bases de données
- **XSS:** Vulnérabilité qui permet d'injecter du code malveillant dans les pages web
- **CVE:** système d'identification pour les vulnérabilités de sécurité connues.
- **Plugins :** Des extensions ou modules ajoutés à un logiciel (souvent un CMS) pour lui ajouter des fonctionnalités spécifiques, par exemple un formulaire de contact ou un outil de sécurité.

Annexe 2 : Plan prévisionnel du rapport

1. **Introduction**
 - a. Contexte de la cybersécurité web
 - b. Problématique pour les PME
 - c. Objectifs et apports du projet
2. **État de l'art**
 - a. Introduction
 - b. Réglementation
 - c. Référentiels
 - d. Détection des vulnérabilité
 - e. la Cybersécurité pour tous
 - f. Conclusion de l'analyse de l'existant
3. **Phase de Conception**
 - a. Conception maquette du site
 - b. Architecture logicielle (intégration des briques open source)
 - c. Stratégie de détection, scoring, adaptation au type de site
 - d. Choix technologiques
4. **Implémentation**
 - a. Intégration des composants (ZAP, Nikto, Nmap, WPScan)
 - b. Interface utilisateur simplifiée (URL en entrée)
 - c. Automatisation des scans et génération du rapport
5. **Résultats et Évaluation**
 - a. Tests sur sites pilotes (vitrine, blog, e-commerce)
 - b. Comparaison avec outils existants
6. **Conclusion et Perspectives**
 - a. Bilan du projet
 - b. Améliorations futures (IA, ML, intégration CI/CD)

Annexe 3: État d'avancement

- Chapitres 1 & 2 (Introduction, État de l'art) : Version préliminaire.
- Chapitre 3 (Conception) : En cours, stratégie de scoring à définir.
- Chapitre 4 (Implémentation) : En cours, nécessite le choix définitif des briques.
- Chapitre 5 (Évaluation) : Non entamé, plans de test à définir.
- Chapitre 6 (Conclusion) : Non entamé.

Annexe 4 : Maquette



Figure 8 - maquette page d'authentification

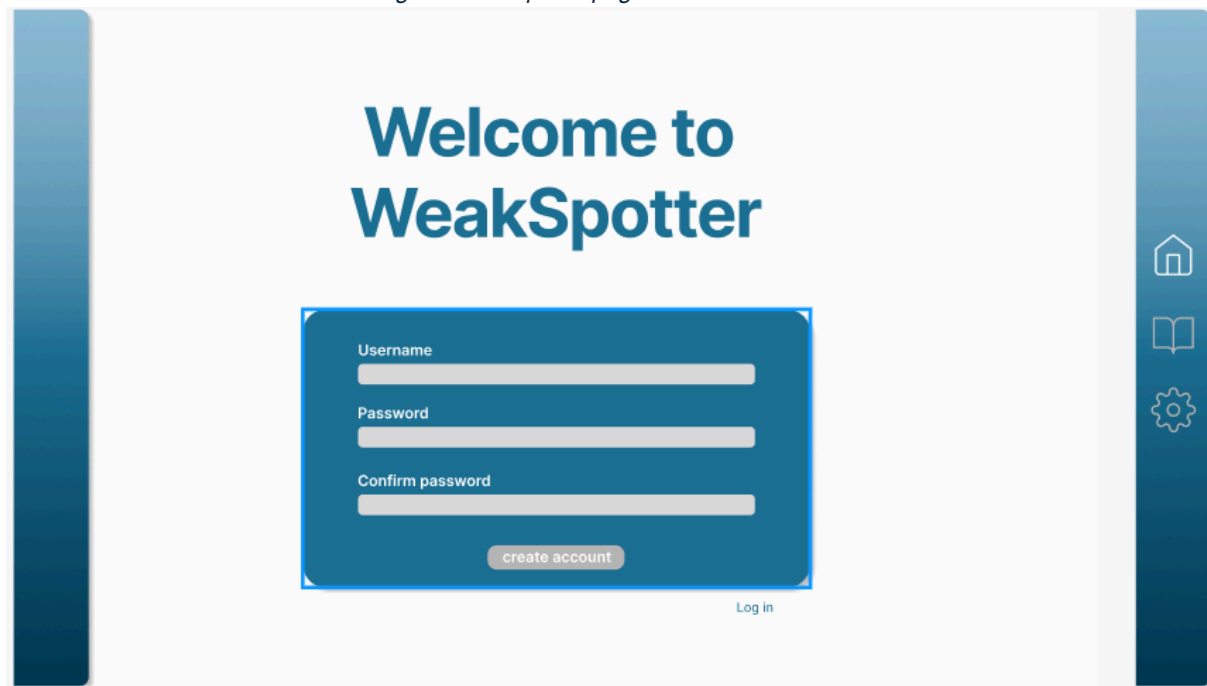

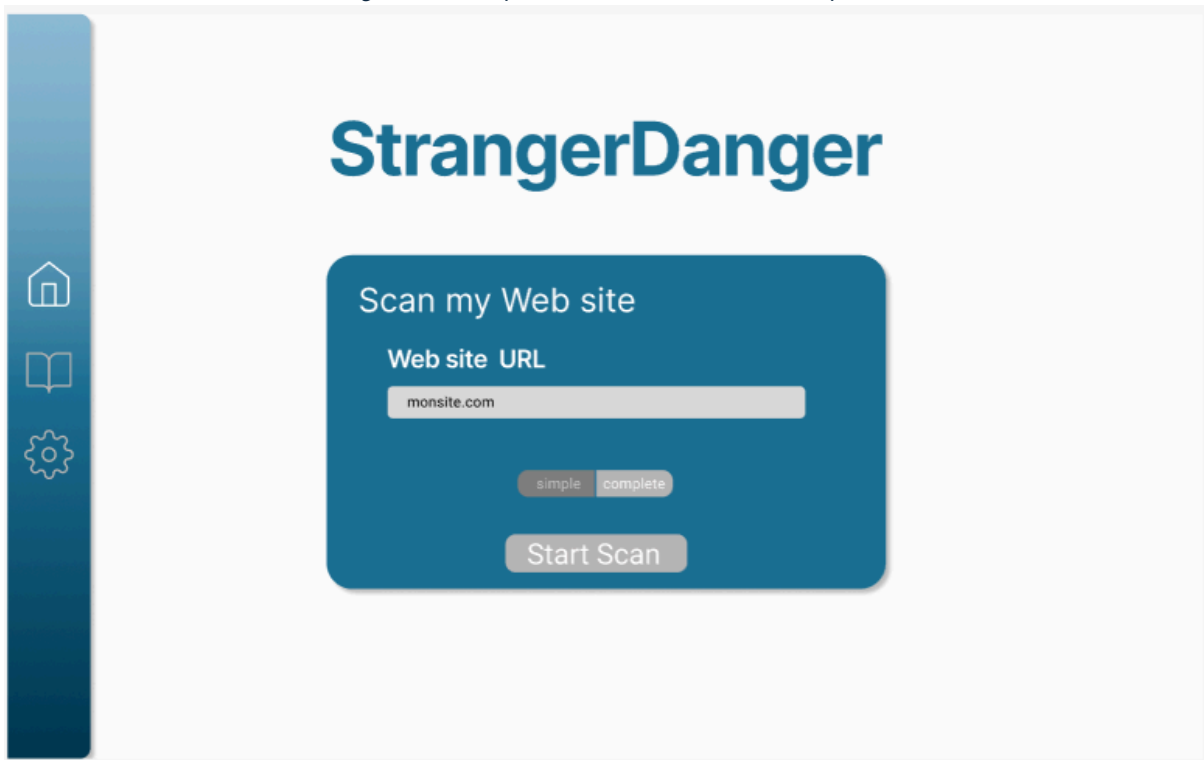


Figure 9 - maquette page de création de compte



The mockup shows a web interface for 'WeakSpotter'. On the left is a vertical sidebar with three icons: a house, an open book, and a gear. The main content area has a large heading 'WeakSpotter'. Below it is a dark blue rounded rectangle containing the text 'Scan my Web site'. Underneath is the label 'Web site URL' followed by a text input field containing 'monsite.com'. Below the input field are two radio buttons labeled 'simple' and 'complete', with 'simple' selected. At the bottom of the rectangle is a 'Start Scan' button.

Figure 10 - maquette commencer un scan simple



The mockup shows a web interface for 'StrangerDanger'. It has the same layout as Figure 9, with a sidebar on the left and a main content area. The heading is 'StrangerDanger'. The dark blue rounded rectangle contains the text 'Scan my Web site', followed by the label 'Web site URL' and a text input field containing 'monsite.com'. Below the input field are two radio buttons labeled 'simple' and 'complete', with 'simple' selected. At the bottom is a 'Start Scan' button.

Figure 11 - maquette commencer scan complexe



Figure 12 - maquette écran de chargement

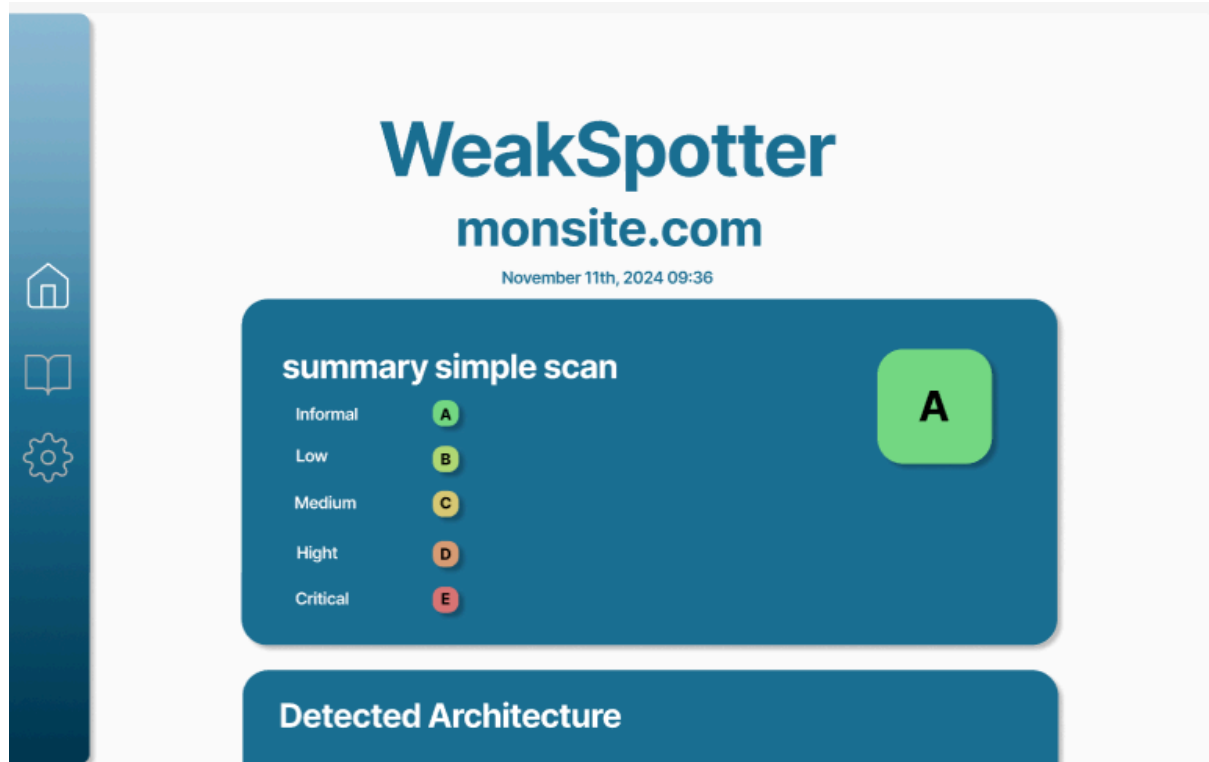


Figure 13 - maquette écran de résultats d'un scan

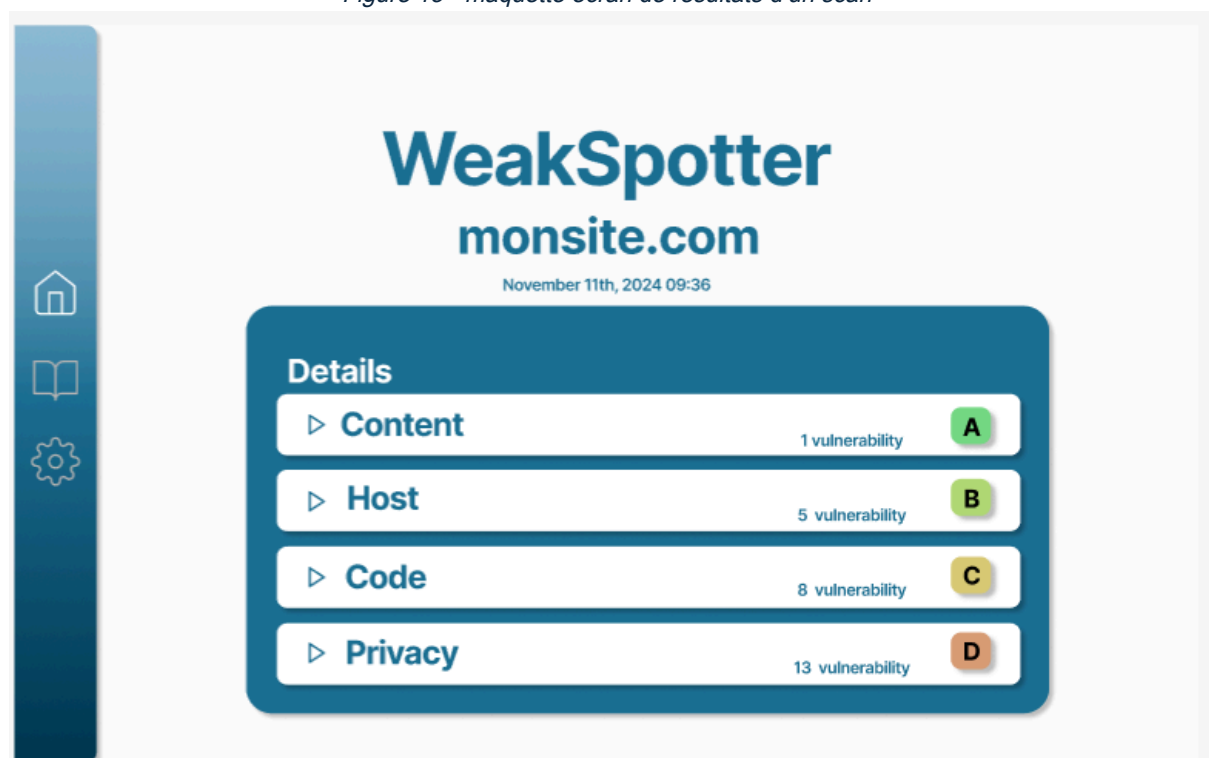


Figure 14 - maquette détails par catégorie

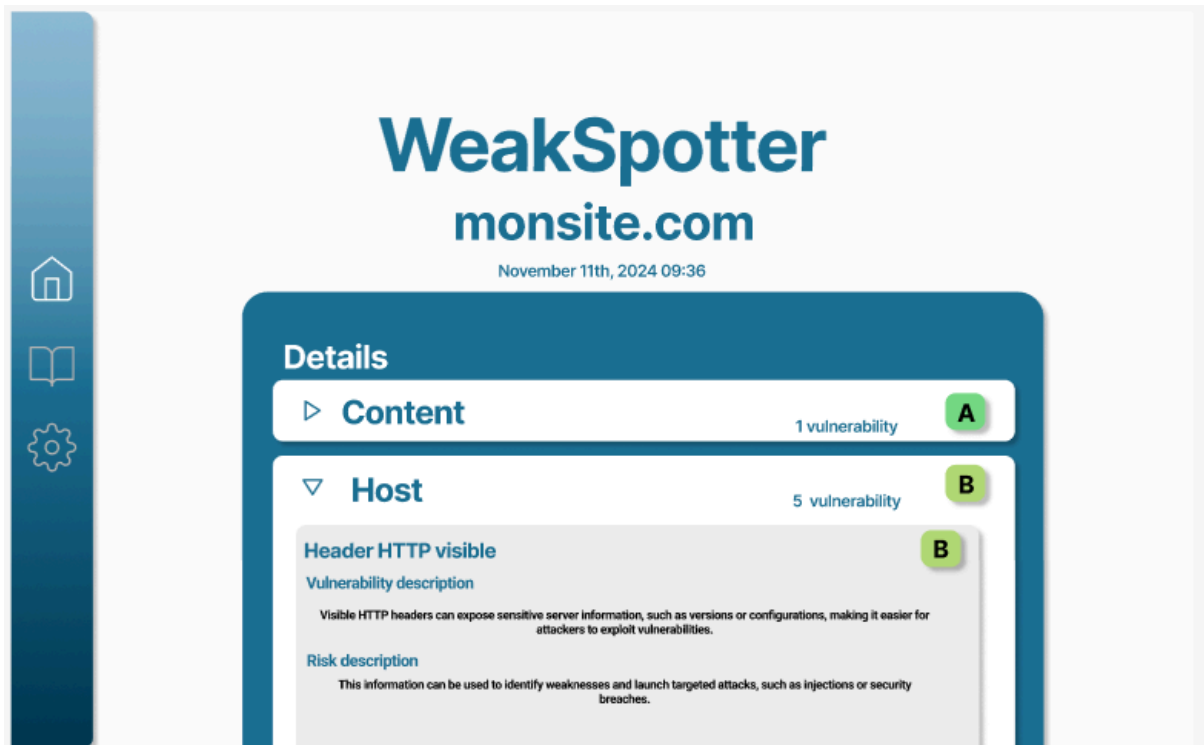


Figure 15 - maquette explication des détails

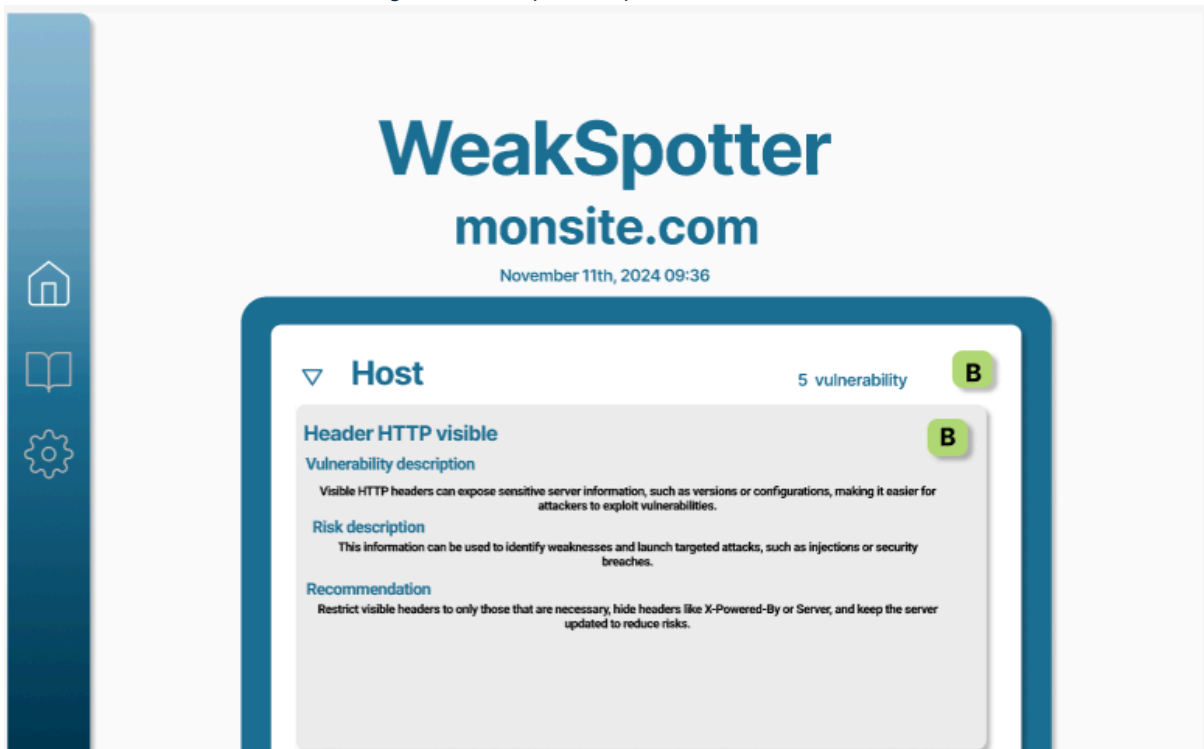


Figure 16 - maquette conseil pour remédier au vulnérabilité trouver



Figure 17 - maquette historique de scan

Annexe 5: diagramme

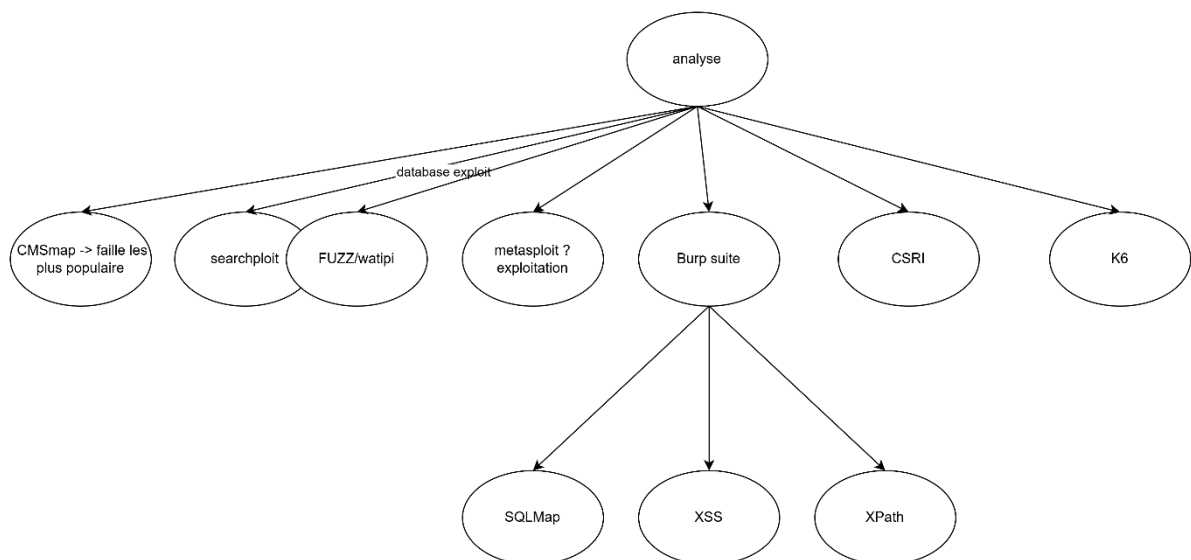


Figure 18 - diagramme Logique phase de reconnaissance

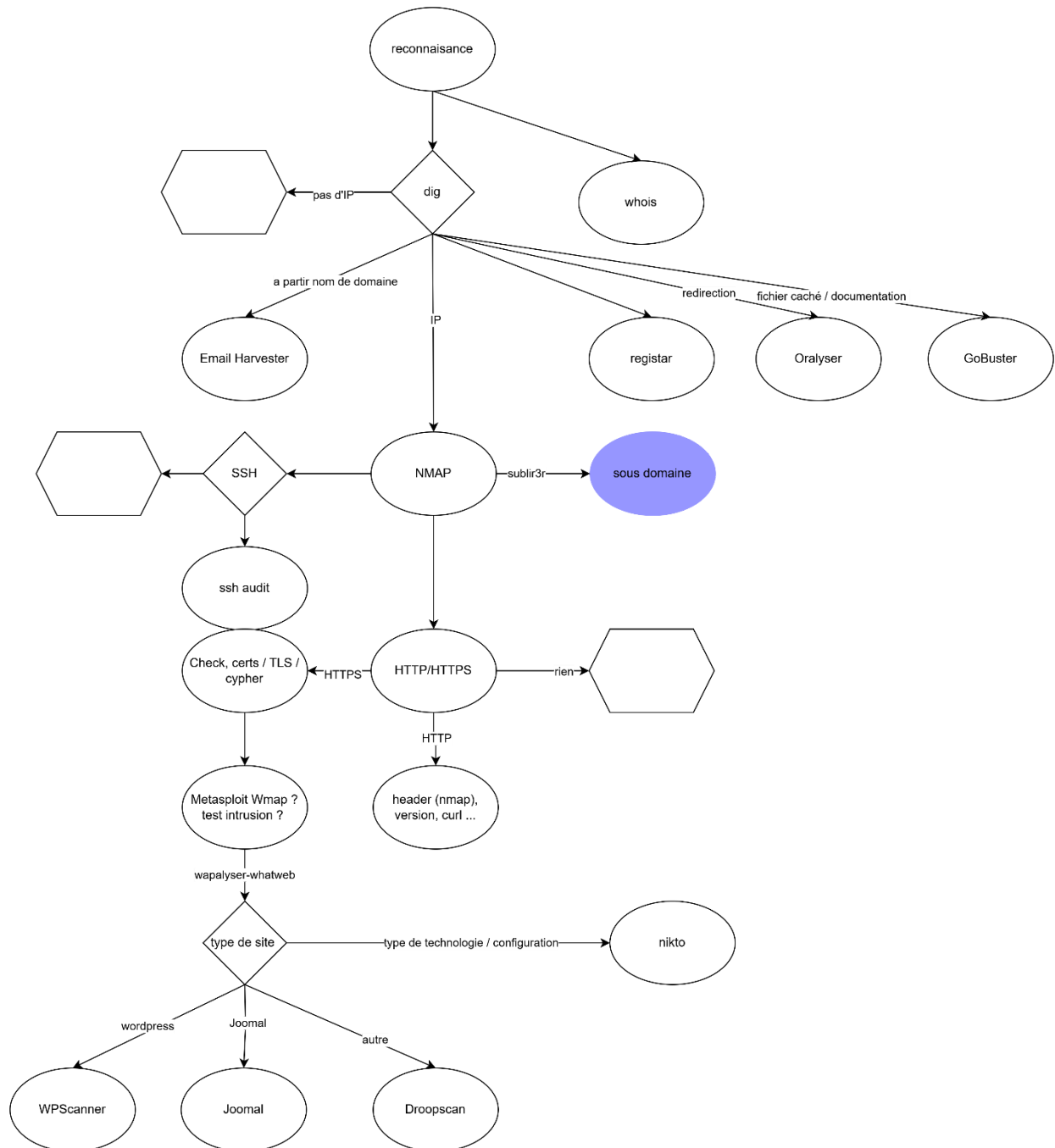


Figure 19- digramme Logique phase d'analyse

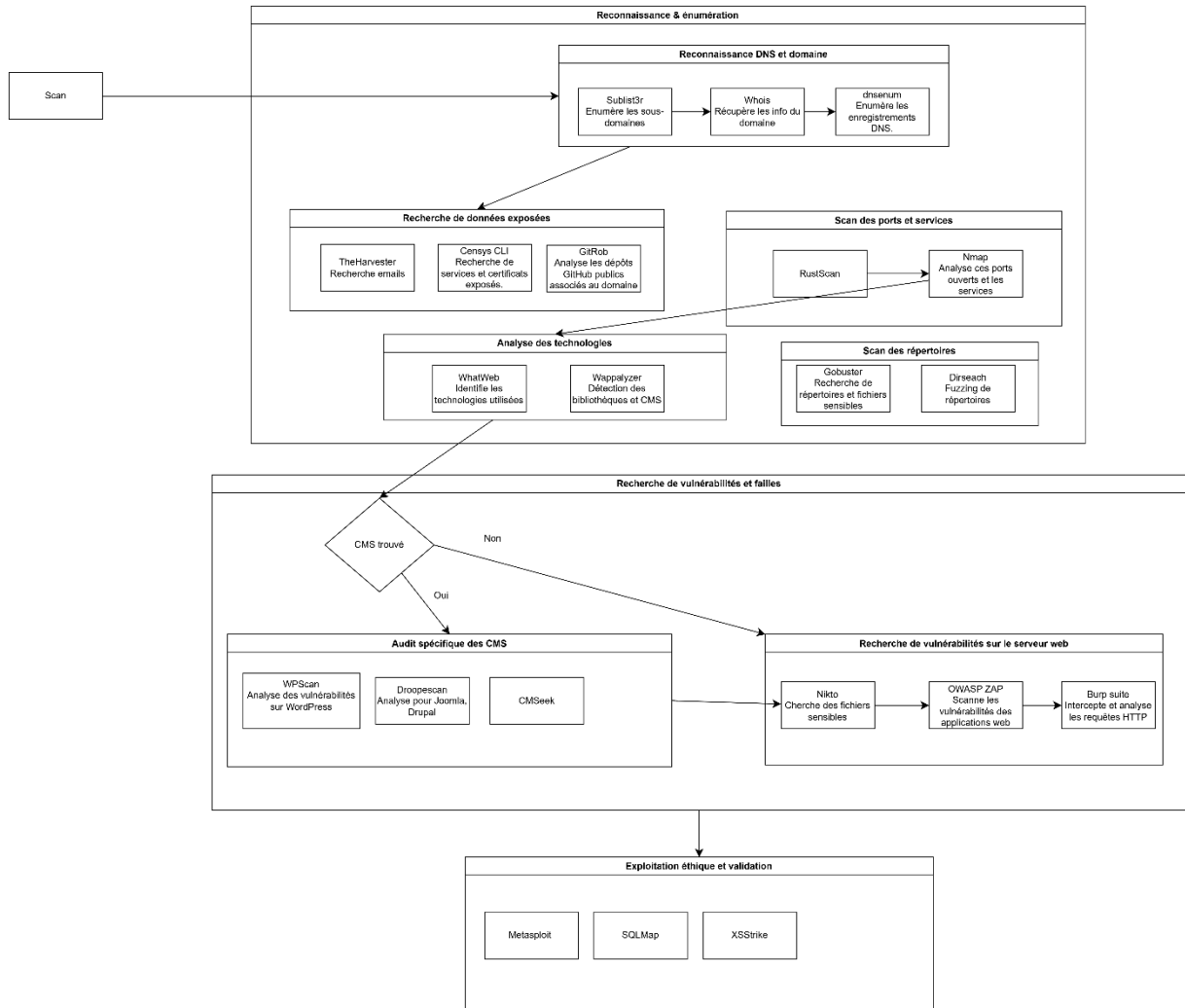


Figure 20 - diagramme logique avec container

Annexe 6: Lien vers le projet

Pour le moment, une implémentation a été commencée. Une première interface graphique a été réalisée et certains outils ont été intégrés. Une implémentation et une orchestration automatiques sont en cours, compte tenu de la complexité des exigences des outils.

WeakSpotter/WeakSpotter

Pour obtenir un retour sur les outils en cours d'intégration dans WeakSpotter, un tableau a été mis en place. Celui-ci permet de suivre les outils et leurs résultats.

Nom	key	required keys	Description	Tools Used	Retuns
Domain Extract	domain		Extract the domain of the url.	urllib.parse.urlparse	Structured Text
Whois	whois	domain	Retrieves the Whois info of the domain.	whois	Arbitrary Text
DNS Records	dns_records	domain	Gets A, AAAA, CNAME of the domain	dig	Structured Text
Cloudflare Detect	cloudflare	dns_records	Checks if a website is protected by cloudflare.	requests	Other
Nmap	nmap	domain	Scans the webserver of the website.	nmap	XML
HTTP Version	http_versions		Checks whet version of HTTP the website is running	curl	Other
Email Harvester	email_harvester	domain	Extract email from domain	theHarvester	JSON
Nikto	nikto_scan	domain		Nikto	JSON

Tableau 7 - tableau des outils déjà incorporé dans le projet

Bibliographie indicative

- Présentation des travaux effectués par des groupes étudiant SAE41 : WebCheck, Audifity, SpiderScan et Arrow, *encadré par Christian DELETTRE*
- [OWASP Top Ten \(2021\)](#), OWASP
- [PageSpeed Insights](#), Google Developers
- [Hacked Websites Trend Report 2019](#), Sucuri
- [ANSSI](#), ANSSI
- [Attaques par rançongiciels, tous concernés](#), ANSSI
- [Assistance aux victimes de cybermalveillance](#), Cybermalveillance
- [Portail de la transformation numérique](#), FranceNum
- [RGPD](#), Ministère de l'économie
- [La directive NIS 2](#), ANSSI
- [Homepage](#), Cyber Resilience Act
- [Homepage](#), Digital Operational Resilience Act
- [Part de marché des CMS 2024 : tendances et statistiques d'utilisation](#), WPADE
- [WordPress Statistics In 2024](#), Bloggers Passion
- [Cyber PME](#), Bpifrance
- [Présentation de Lighthouse | Chrome for Developers](#), Google Developers
- [CWE - 2024 CWE Top 25 Most Dangerous Software Weaknesses](#), MITRE
- [Plateforme ouverte, évolutive, sécurisée et orientée utilisateur pour l'e-commerce](#), Christian DELETTRE

Scanners & Outils

- [Acunetix](#), Invicti
- [Burp Suite Pro](#), PortSwigger
- [Nessus](#), Tenable
- [Intruder](#), Intruder System
- [vRx](#), Vicarius
- [OWASP ZAP](#), OWASP
- [Nikto](#), CIRT
- [WPScan](#), WPScan
- [OpenVAS](#), Greenbone
- [TruRisk](#), Qualys
- [SUBLIST3R](#), Ahmed Aboul-Ela
- [Ssh Audit](#), Joe Testa
- [GoBuster](#), OJ Reeves
- [Nmap](#), Gordon Lyon (Fyodor)
- [Whois](#), rfc1036, Ken Harrenstien
- [Dig](#), tigeli
- [Email Harvester](#), Christian Martorella
- [Oralyser](#), laramies
- [Homepage](#), Metasploit

- [Joomla](#), *OWASP*
- [Droopscan](#), *SamJoan*
- [Searchsploit](#), *Exploit Database*
- [Watipi](#), *Wapiti-scanner*
- [Cloudflare detect](#), *christophetd*