



Votre nouvel **auditeur cyber**

L'audit offensif de votre surface externe, en continu.

 Compatible NIST 2 / ISO 27001

 Construit et hébergé à Paris

 Propulsé par Mistral AI

Flawfence chez nos **clients**

MSSP

Opérateur multcloud français

Transformation du SI de ses clients

Scans en marque blanche, en continu.

PREMIER SCAN

2 critiques

3 élevées

Exécution de code sur un WordPress (wp2shell)

↳ Environnement d'un client hébergé compromis

Identifiants de base de données exposés

↳ Données métier altérables

CLIENT FINAL

Courtier en protection sociale

Santé, prévoyance, retraite, épargne salariale

Périmètres externe et interne, services externalisés.

PREMIER SCAN

1 critique

2 élevées

Console d'administration sans authentification

↳ Prise de contrôle anonyme de l'application

XSS sur le portail assurés

↳ Vol silencieux des identifiants

Retour d'expérience : gestion de crise wp2shell

SURFACE EXPOSÉE

DÉCOUVERTE

41 sous-domaines exposés

Énumération passive, sans agent ni identifiant

IDENTIFICATION

Un WordPress non maintenu sur blog.client-heberge.fr

Empreinte des technologies et des versions

EXPLOITATION

Exécution de code à distance confirmée

CVE-2026-63030, exploitation rejouée

IMPACT

Accès en écriture à la base de données métier

wp-config.php lu, identifiants en clair

IMPACT MÉTIER

De la construction du PoC à l'alerte en quelques **heures**



Chronologie complète de wp2shell →

Un **instantané**, au prix d'une surveillance

3 mois

du cadrage à la restitution

20 k€

par audit

1 / an

onze mois sans visibilité

Ils exploitent plus **vite** que vous ne corrigez

31 %

des accès initiaux passent par une faille exploitée

Verizon DBIR 2026, plus de 22 000 brèches.
20 % un an plus tôt.

43 jours

pour corriger une faille activement exploitée

Verizon DBIR 2026, délai médian, catalogue KEV de la CISA. 32 jours un an plus tôt.

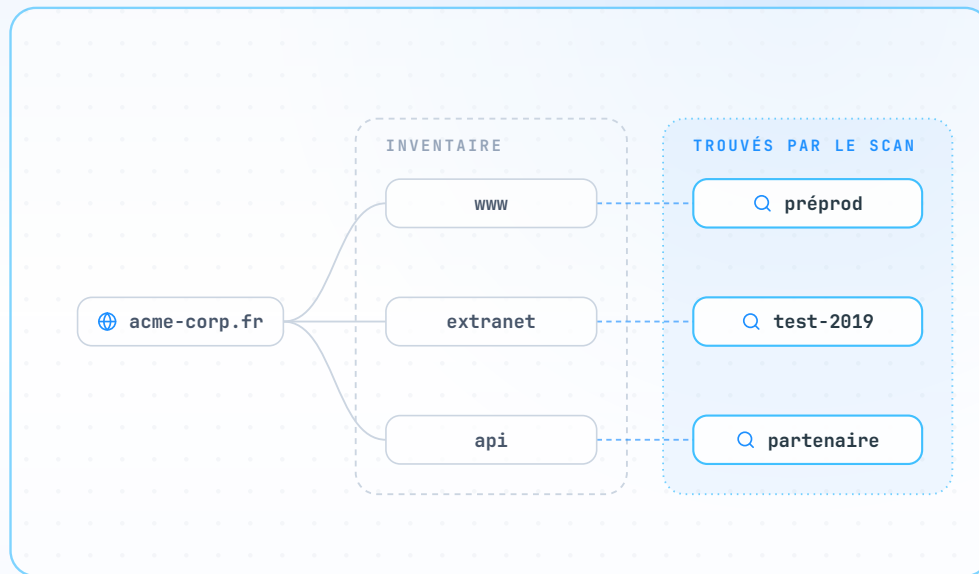
4,99 M\$

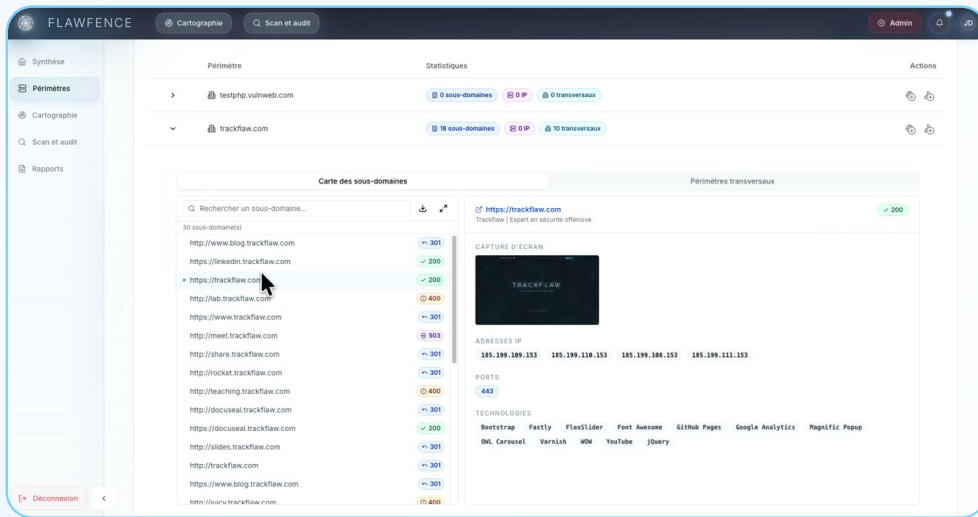
coût moyen d'une violation de données

IBM Cost of a Data Breach 2026, 602 organisations. En hausse de 12 % sur un an.

Votre inventaire n'est pas votre **périmètre**

- ✓ Une préproduction ouverte pour une démo
- ✓ Un sous-domaine de test jamais éteint
- ✓ Un partenaire qui pointe encore chez vous





Un auditeur qui ne **dort** pas

Un email professionnel, rien à installer.

- ✓ Le périmètre se reconstitue seul
- ✓ Premier rapport en moins de 24 h
- ✓ Le scan ne s'arrête plus

Quatre maillons, rejoués en boucle

01



Cartographier

Un sous-domaine de préproduction absent de l'inventaire.

DNS

OSINT

WHOIS

02



Identifier

Un Swagger public qui décrit l'API interne.

Banner grabbing

Nuclei

Httpx

03



Exploiter

Une injection SQL confirmée par la donnée renvoyée.

Fuzzing

Agentique

Dast

04



Alerter

Une alerte critique dans Slack, la nuit même.

CVSS v4

NIST 2

SIEM

Le détail technique de chaque maillon →



Une **preuve** d'exploitation par vulnérabilité

- ✓ Rien de remonté sans exploitation confirmée
- ✓ Le test se rejoue avant d'ouvrir un ticket

The screenshot shows the FLAWFENCE interface with a sidebar on the left containing 'ADMINISTRATION', 'Utilisateurs', 'Périphères (admin)', 'Vulnérabilités', 'Scans programmés', and 'Déconnexion'. The main area displays a table of vulnerabilities for the target 'trackflaw.com'.

Vulnérabilités	Sevérité	Statut	Date
Injection de commande - Fonctionnalité de documents de compte https://hackazon.trackflaw.com:443/account/documents	Critique 4/4	Découverte	06 août 2026
Connexion SSH par défaut - Port 15345 31.220.95.27:15345	Critique 4/4	Découverte	06 août 2026
Injection SQL - Fonctionnalité de vue de catégorie https://hackazon.trackflaw.com/category/view?id=...	Critique 4/4	Découverte	06 août 2026
Mot de passe faible - Service FTP https://31.220.95.27:21314	Critique 4/4	Découverte	06 août 2026
Téléchargement de fichier non restreint - Page de profil utilisateur https://hackazon.trackflaw.com:443/account/profile	Critique 4/4	Découverte	06 août 2026
Injection SQL - Fonctionnalité de visualisation de produits https://hackazon.trackflaw.com:443/product/view?id=...	Critique 4/4	Découverte	06 août 2026
Faiblesse d'authentification FTP - Service FTP 31.220.95.27:21314	Haute 3/4	Découverte	06 août 2026
XSS stocké - Page de foire aux questions	Moyenne 2/4	Reconnue	06 août 2026

The screenshot shows the detail page for the vulnerability 'Injection de commande - Fonctionnalité de documents de compte'. It includes a description, a proof of exploit (POC), and a verification command.

DESCRIPTION

La page <https://hackazon.trackflaw.com:443/account/documents> est vulnérable à une attaque de type Command Injection dans le paramètre 'page'. Un attaquant peut injecter des commandes système arbitraires, ce qui peut conduire à une exécution de code distant (RCE) et potentiellement à un contrôle total du système. Cette vulnérabilité a été observée via une requête GET avec le paramètre 'page' modifié, ce qui a permis d'exécuter la commande 'id' et de récupérer des informations sur le système.

PREUVE D'EXPLOITATION

POC UTILISÉ

```
GET https://hackazon.trackflaw.com:443/account/documents?page=%3B%20id
Cookie: PHPSESSID=9263dd4ba0c8a388f2832235b4aeb2f8
```

DONNÉES DE PREUVE

PARAMÈTRE: page, query | ENDPOINT: /account/documents | PAYLOAD: id

Données extraites

```
uid=33{
```

Réponse complète

URL VULNÉRABLE

```
https://hackazon.trackflaw.com:443/account/documents?page=terms.html
```

COMMANDE DE VÉRIFICATION

```
curl -k 'https://hackazon.trackflaw.com:443/account/documents?page=%3B%20id' -H 'Cookie: PHPSESSID=9263dd4ba0c8a388f2832235b4aeb2f8'
```

Deux mesures, **méthode** comprise

+30 %

de sous-domaines découverts

tesla.com, sous-domaines avec un enregistrement DNS A actif.

+30 %

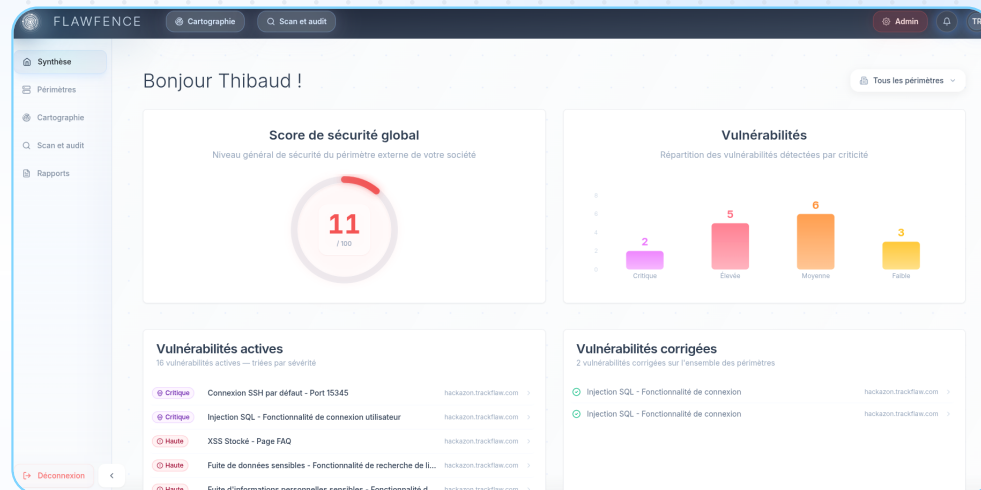
de vulnérabilités exploitables

Scan anonyme, configuration par défaut, plateforme hackazon.

Bug bounty sur YesWeHack · [Voir le compteur](#) →

Un rapport pour vos équipes, un autre pour votre **direction**

- ✓ Rapport PDF conforme NIST 2
- ✓ Alerte immédiate sur les critiques
- ✓ Remédiation priorisée par exploitabilité



Française, de l'équipe à l'hébergement



Hébergement à Paris, données en France



Modèles Mistral AI pour l'analyse



Exports conformes NIST 2 et ISO 27001

Un audit par an, ou toute l'**année**

L'audit ponctuel

20 k€ par audit

Le format habituel, refait chaque année.

- ✓ Cadrage, tests, restitution
- ✓ Un rapport daté du jour des tests

Flawfence

À partir de 5 000 € HT par an

Le périmètre se reconstitue seul, le scan tourne 24/7/365.

- ✓ Scan offensif continu
- ✓ Une preuve d'exploitation par vulnérabilité
- ✓ Alerte immédiate sur les critiques
- ✓ Rapports conformes NIST 2

Tarif selon la taille du périmètre.

Passons à votre **périmètre**

Une démonstration, sans engagement.

Demander une démonstration →

Lancer un aperçu gratuit

Aperçu passif, sans inscription.