LAUCKED

EXEMPLE PUBLIC

DIAGNOSTIC DE SURFACE FICTIF · 2026

Cartographie d'*exposition publique*

Exemple anonymisé d'un diagnostic Laucked sur un éditeur SaaS B2B fictif, **AcmeFictio SAS**. Lecture experte humaine, recommandation documentée GO ou NO-GO pour un pentest.

RÉFÉRENCE
LAUCK-DIAG-EXEMPLE-2026

CLIENT FICTIF
AcmeFictio SAS, éditeur SaaS B2B fictif

NIVEAU D'EXPOSITION
B, posture à surveiller

SIGNATAIRE
Rayan Dib, CTO Laucked

DATE D'ÉMISSION
Mai 2026

MÉTHODOLOGIE
Recon passif, OSINT, CT logs, OWASP WSTG

OBSERVATIONS
12 dont 4 à investiguer en pentest

CLASSIFICATION
Document public, exemple anonymisé

NIVEAU D'EXPOSITION OBSERVÉ

A **B** C D E F

12 observations, dont 4 à investiguer en pentest. Surface modérément exposée, posture cohérente avec un éditeur SaaS en croissance.

23	12	4	5	3
ACTIFS CARTOGRAPHIÉS	OBSERVATIONS	À INVESTIGUER PENTEST	À CORRIGER DIRECT	INFORMATIFS

Référence	LAUCK-DIAG-EXEMPLE-2026
Type	Exemple anonymisé, diagnostic de surface, livrable d'entrée de mission
Client fictif	AcmeFictio SAS, éditeur SaaS B2B de gestion documentaire pour PME et ETI françaises
Profil client fictif	~40 collaborateurs, ~200 tenants clients, CA fictif 4 M€, renouvellement assurance cyber en cours, démarche NIS2 sous-traitance
Périmètre observé	`acmefictio.example`, `app.acmefictio.example`, sous-domaines publics, API REST publique, espaces marketing
Période d'observation	Document d'exemple, dates non applicables
Date d'émission	Mai 2026
Version	1.0, version publique
Auteur (signature mission réelle)	Rayan Dib, CTO Laucked, OSCP / OSEP / OSWE
Classification	Document public, structure et observations 100 % fictives

Avertissement de portée

Ce document est un **exemple anonymisé fictif** publié par Laucked pour illustrer la structure d'un diagnostic de surface. **Aucune information n'est réelle**. Le client AcmeFictio SAS est fictif, les domaines utilisent le TLD `.example` réservé (RFC 2606), les URLs et identifiants sont fabriqués. La méthodologie, le ton et la profondeur reflètent en revanche ce que vous recevez après un vrai diagnostic Laucked.

Ce qu'un diagnostic vous permet

- Décider si un pentest est pertinent (ou pas), avec un avis tiers documenté.
- Cadrer le périmètre exact d'une future mission, fourchette budgétaire incluse.
- Donner à votre direction une photo de la surface publique réelle, lisible sans expert sécurité interne.
- Documenter une pièce d'entrée recevable face à un courtier d'assurance cyber ou un comité de souscription.

Sommaire

1. Synthèse exécutive

1.1 Verdict en une phrase

Surface publique d'AcmeFictio modérément exposée, avec quatre points de friction nets qui justifient un pentest cadré sur l'application principale et son API, pour un budget réaliste autour de 8 000 € HT.

1.2 Niveau d'exposition observé

Niveau B, exposition à surveiller. Posture cohérente avec un éditeur SaaS jeune, mais quatre zones structurantes restent à valider en boîte grise.

INDICATEUR	VALEUR
Actifs publics cartographiés	23
Sous-domaines actifs	11
Services exposés (HTTP, HTTPS, autres)	9
Observations remontées	12
Dont à investiguer en pentest	4
Dont à corriger sans pentest	5
Dont informatifs	3
Durée du diagnostic (recon passif)	6 heures cumulées

1.3 Message dirigeant

L'application principale `app.acmefictio.example` est correctement servie derrière un reverse proxy Cloudflare avec une chaîne TLS propre. Deux sous-domaines de préproduction (`staging`, `qa`) sont accessibles depuis Internet sans restriction d'IP visible, l'un d'eux héberge la même base applicative que la production avec, vraisemblablement, des données de test réalistes. L'API REST `/api/v1` répond aux requêtes non authentifiées sur deux endpoints qui retournent des métadonnées de structure (versions, schéma OpenAPI public). Le portail partenaire `partners.acmefictio.example` expose un formulaire de récupération de mot de passe qui révèle l'existence ou l'absence d'un email donné, ce qui facilite l'énumération.

Aucun de ces points n'est une vulnérabilité au sens strict. Ce sont des **zones grises** que seul un pentest peut convertir en réponse claire : est-ce exploitable, dans quelles conditions, avec quel impact métier. Le reste de la surface, marketing, blog, statique, ne justifie pas d'investissement complémentaire en sécurité.

1.4 Priorités proposées

PRIORITÉ	ACTION	EFFORT ESTIMÉ
P1	Restreindre l'accès aux sous-domaines `staging` et `qa` par IP, Basic Auth ou bastion	0,5 j-h
P1	Lancer un pentest boîte grise sur `app.acmefictio.example` + API `/api/v1`	mission 5 à 7 j-h
P2	Standardiser les réponses du flux de reset password (réponse uniforme)	1 j-h
P2	Désactiver l'exposition publique du schéma OpenAPI complet	0,5 j-h
P3	Mettre à jour la chaîne TLS sur `legacy.acmefictio.example` (cert expiré)	0,5 j-h

2. Pourquoi ce diagnostic, quel contexte business

AcmeFictio SAS commercialise une plateforme de gestion documentaire (contrats, factures, annexes RH) pour environ 200 tenants clients. Plusieurs clients exigent désormais une **preuve de pentest indépendant** dans leurs questionnaires sécurité fournisseur, notamment depuis l'entrée en vigueur de NIS2 pour les sous-traitants critiques. En parallèle, le courtier d'assurance cyber annonce une majoration de prime de 18 % au prochain renouvellement, sauf production d'un rapport de pentest récent réalisé par un tiers qualifié.

Le diagnostic répond à une question simple : **avant d'investir dans un pentest complet, quelle est la photographie de ce qui est exposé aujourd'hui ?** L'objectif n'est pas d'exploiter, c'est de cadrer. Un pentest mal périmètré coûte cher pour ce qu'il rapporte. Un pentest bien périmètré rapporte beaucoup pour un coût raisonnable.

ENJEU	RÉPONSE APPORTÉE PAR LE DIAGNOSTIC
Renouvellement assurance cyber	Justifier la prochaine étape (pentest cadré) avec un livrable horodaté signé d'un tiers.
Questionnaires clients NIS2	Documenter la démarche d'audit régulier, traçable, pas de réponse vague.
Pression budgétaire interne	Éviter un pentest mal calibré, valider la valeur ajoutée attendue avant signature.
Doute sur l'exposition réelle	Cartographier la surface, identifier les sous-domaines orphelins, services oubliés.

3. Méthodologie, ce que veut dire « passif »

3.1 Principes

Un diagnostic de surface est **strictement passif**. Aucune requête n'est envoyée vers l'infrastructure du client en dehors du trafic HTTP normal qu'un visiteur public produit naturellement (chargement de page, lecture du sitemap, accès aux fichiers publics référencés). Aucun scan de vulnérabilité, aucun bruteforce, aucune intrusion, aucune tentative d'authentification.

Le diagnostic exploite uniquement ce qui est **déjà public** :

1. Données DNS publiques et historisées (passive DNS).
2. Registres de certificats publics (CT logs).
3. Réponses HTTP des serveurs interrogés depuis un navigateur classique.
4. Métadonnées exposées dans les robots.txt, sitemaps, fichiers `.well-known`.
5. Sources OSINT pour la qualification d'organisation (SIRET, dirigeants, pile technologique).

Cette posture présente deux avantages. D'une part, elle est **légalement neutre** : pas besoin d'autorisation préalable. D'autre part, elle reflète exactement la **vue d'un attaquant externe sans accès** qui prépare une cible. C'est la seule lecture pertinente avant un pentest.

3.2 Outils utilisés

Toutes les recherches sont logguées et traçables. Les sources utilisées pour ce diagnostic sont les suivantes :

CATÉGORIE	SOURCES
Passive DNS	bases DNS historiques (CT logs, RDAP, archives)
Énumération sous-domaines	CT logs, sitemap, robots.txt, listing public OSINT
Certificats	Certificate Transparency, validation chaîne via OpenSSL côté Laucked
Headers HTTP	requêtes navigateur standard, inspection des réponses
Stack technique	`Wappalyzer`-like passif, en-têtes `Server`, `X-Powered-By`, JS fingerprint
OSINT entreprise	INSEE / Pappers / LinkedIn public
Compromission historique	bases publiques de fuites indexées (sans extraction de mots de passe)

3.3 Ce qu'un diagnostic ne fait pas

Quatre limites importantes à garder en tête. Le diagnostic ne valide pas l'absence de vulnérabilité (un endpoint testé en GET peut être vulnérable en POST avec un payload qu'on ne tente jamais). Il ne couvre pas les **APIs authentifiées** (vu qu'on ne s'authentifie pas). Il ne joue pas de **scénario métier** (parcours utilisateur, escalade, latéralité). Il ne produit pas de **score CVSS** par finding, parce qu'il n'y a pas

d'exploitation. Si l'un de ces objectifs est attendu, c'est un pentest qu'il faut commander, pas un diagnostic.

4. Périmètre observé et exclusions

4.1 Actifs observés

TYPE	ÉLÉMENT	STATUT
Domaine racine	`acmefictio.example`	Actif, redirection HTTPS vers www
Application principale	`app.acmefictio.example`	Actif, derrière Cloudflare
Préproduction	`staging.acmefictio.example`	Actif, exposé Internet
Préproduction	`qa.acmefictio.example`	Actif, exposé Internet
API	`api.acmefictio.example/v1`	Actif, schéma OpenAPI partiellement public
Portail partenaire	`partners.acmefictio.example`	Actif, formulaire de connexion
Marketing	`www.acmefictio.example`	Actif, site vitrine
Blog	`blog.acmefictio.example`	Actif, WordPress hébergé
Documentation	`docs.acmefictio.example`	Actif, Docusaurus
Status page	`status.acmefictio.example`	Actif, Statuspage tiers
Ancien service	`legacy.acmefictio.example`	Actif, certificat expiré

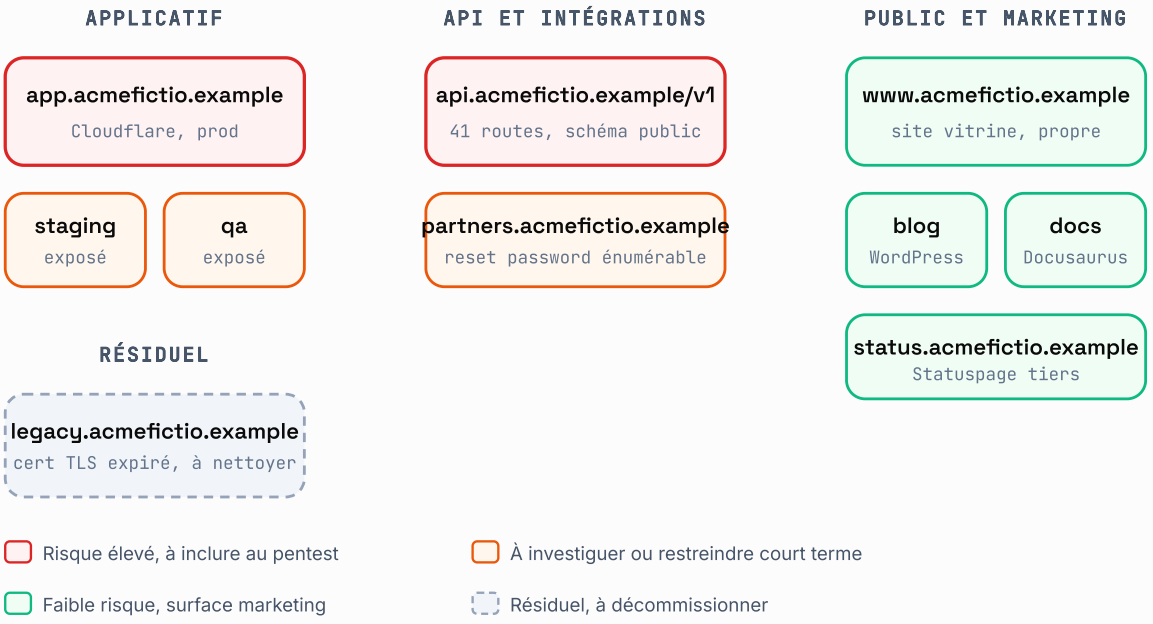
4.2 Exclusions

Les éléments suivants n'ont pas été pris en compte dans la cartographie ou l'analyse :

1. Adresses IP non publiques (réseau interne, VPN, bureaux).
2. Comptes ou interfaces administratives accessibles uniquement après authentification.
3. Outils SaaS tiers (CRM, ERP, comptabilité) référencés par AcmeFictio.
4. Applications mobiles iOS et Android (non périmètrées ici, peuvent faire l'objet d'un diagnostic dédié).
5. Communications internes (mail, messagerie, signature de domaine SPF / DKIM / DMARC). À traiter dans un volet séparé si pertinent.

5. Cartographie des actifs publics

FIGURE 1, CARTOGRAPHIE DE LA SURFACE PUBLIQUE OBSERVÉE



Cartographie des 11 sous-domaines publics actifs au moment de l'observation.
Quatre familles distinguées par fonction métier. Les cadres rouges (app, api) regroupent la valeur cible. Les cadres orange (staging, qa, partners) signalent une exposition non maîtrisée à clarifier. La famille verte regroupe les actifs publics à faible risque. Le bloc en pointillé identifie un résiduel à nettoyer (certificat TLS expiré sur legacy).

L'écosystème public se structure autour de quatre familles : applicatif (app, staging, qa), API et intégrations (api, partners), public et marketing (www, blog, docs, status), résiduel (legacy). La séparation entre familles est correcte au niveau DNS, mais la **chaîne TLS et la politique de cache** diffèrent selon les sous-domaines, ce qui suggère une absence de pipeline centralisé pour la gestion des certificats et des en-têtes de sécurité.

FAMILLE	ACTIFS	RISQUE RELATIF	INCLURE AU PENTEST
Applicatif	app, staging, qa	Élevé	Oui (app + accès staging)
API et intégrations	api, partners	Élevé	Oui (api complète, partners selon scope)
Public et marketing	www, blog, docs, status	Faible	Non
Résiduel	legacy	Faible (mais à nettoyer)	Non, décommissionner

6. Observations détaillées

Douze observations remontent du diagnostic. Elles sont **classées par niveau d'attention**, pas par CVSS (le diagnostic n'exploite rien). Quatre d'entre elles justifient un pentest pour trancher leur exploitabilité réelle.

O-01, staging et qa accessibles sans restriction visible

Niveau d'attention : Élevé, à investiguer en pentest.

Les sous-domaines `staging.acmefictio.example` et `qa.acmefictio.example` répondent en HTTP 200 sans page d'authentification visible côté Internet. La page d'accueil est identique en structure à la production. Les robots.txt n'interdisent rien d'exotique. Aucun en-tête de réponse n'indique une protection IP ou un proxy bastion.

Conséquence possible : un attaquant non authentifié peut explorer une version potentiellement moins durcie de l'application, contenant les mêmes endpoints, peut-être avec des comptes de test connus ou des feature flags expérimentaux activés. Les données réelles sont en principe absentes, mais ce n'est pas vérifiable depuis l'extérieur.

Recommandation court terme : restreindre par IP (whitelist VPN équipe), Basic Auth, ou bastion d'accès, avant tout pentest pour éviter qu'un autre acteur ne « grille » la surface.

Recommandation pentest : inclure `staging` au périmètre boîte grise, à des fins de validation que les fonctionnalités sensibles n'y sont pas accessibles avec moins de contrôle qu'en production.

O-02, API `/api/v1` expose un schéma OpenAPI partiellement public

Niveau d'attention : Élevé, à investiguer en pentest.

L'endpoint `GET /api/v1/openapi.json` renvoie une description partielle de l'API, listant 41 routes et leurs paramètres attendus. Plusieurs routes sont des candidats classiques pour des défauts d'autorisation (BOLA, énumération d'identifiants numériques), notamment `/api/v1/documents/{id}`, `/api/v1/invoices/{id}`, `/api/v1/tenants/{id}/users`.

Le schéma rend publique la connaissance de la structure interne sans qu'aucune authentification ne soit requise. Côté défense, il accélère un attaquant en lui évitant la phase de cartographie endpoint. Côté business, c'est aussi un signal de maturité (l'API est documentée), donc ce n'est pas un drapeau rouge en soi.

Recommandation court terme : vérifier que le schéma public est intentionnel. Si oui, lister explicitement les routes documentées comme telles (pas d'oubli). Si non, restreindre à un usage authentifié uniquement.

Recommandation pentest : tester chaque route listée pour les classes d'autorisation (OWASP API Top 10 #1 BOLA, #3 BOPLA, #5 BFLA).

O-03, portail partenaire, formulaire de reset password révèle l'existence d'un compte

Niveau d'attention : Élevé, à investiguer en pentest.

Sur `partners.acmefictio.example/auth/reset`, le formulaire répond avec un message différencié selon que l'email saisi correspond à un compte existant ou pas. La réponse en JSON contient un champ

`account_exists: true | false`. Cette différence permet d'**énumérer** la base d'emails partenaires en envoyant une liste OSINT (LinkedIn, sites d'entreprise) jusqu'à isoler les comptes valides.

Recommandation court terme : unifier la réponse côté API et côté UI. Même message, même délai de réponse, même statut HTTP, indépendamment de l'existence du compte.

Recommandation pentest : vérifier l'absence de bypass, d'observation par timing, et la robustesse du rate limiting sur ce flux.

0-04, deux serveurs exposent des en-têtes révélateurs de version

Niveau d'attention : Moyen, à corriger sans pentest.

Les en-têtes `Server: nginx/1.20.1` et `X-Powered-By: PHP/7.4.33` sont retournés sur `legacy.acmefictio.example` et `blog.acmefictio.example`. PHP 7.4 est en fin de support depuis novembre 2022, nginx 1.20.1 est ancien. Ces en-têtes facilitent le ciblage d'attaques connues (CVE publiques) et donnent une indication de gestion du parc.

Recommandation : désactiver `server_tokens` côté nginx, retirer la directive `expose_php` côté WordPress, planifier la mise à niveau du parc PHP.

0-05, en-tête CSP absent ou très permissif sur 3 sous-domaines

Niveau d'attention : Moyen, à corriger sans pentest.

Les sous-domaines `app`, `partners` et `blog` ne servent pas d'en-tête `Content-Security-Policy` complet. Sur `app`, la CSP est définie mais avec `'unsafe-inline'` et `'unsafe-eval'` actifs. Sur `partners`, aucune CSP. Sur `blog`, CSP en mode `Report-Only` sans destination de report visible.

Cette configuration ne crée pas de faille en soi, mais elle **réduit la marge de manœuvre** en cas de XSS, et complique la conformité PCI-DSS et SOC2 si AcmeFictio vise ces certifications à terme.

Recommandation : définir une politique CSP de base avec `default-src 'self'`, `script-src` explicite, et l'élargir au cas par cas, avec un endpoint `report-uri` interne pour suivre les violations.

0-06, certificat TLS expiré depuis 47 jours sur `legacy.acmefictio.example`

Niveau d'attention : Moyen, à corriger sans pentest.

Le sous-domaine `legacy.acmefictio.example` répond toujours en HTTPS mais le certificat est expiré, sans renouvellement automatisé visible. Aucune redirection vers un service de remplacement.

Recommandation : soit décommissionner le sous-domaine (recommandé, si plus d'usage), soit basculer en certificat ACME automatisé (Let's Encrypt + script de renouvellement supervisé).

0-07, cookies sans `Secure` ni `SameSite` strict sur le portail partenaire

Niveau d'attention : Moyen, à corriger sans pentest.

Le cookie de session `partner_session` n'a pas l'attribut `Secure`, et son `SameSite` est positionné à `Lax`. Sur un portail B2B avec lien profond et tunnel d'authentification, `SameSite=Strict` et `Secure` devraient être les valeurs par défaut.

Recommandation : durcir la configuration du cookie au prochain déploiement. Pas de migration de données ni de retour utilisateur attendu.

0-08, en-tête `X-Frame-Options` manquant sur `app`

Niveau d'attention : Moyen, à corriger sans pentest.

L'application principale `app.acmefictio.example` n'expose pas `X-Frame-Options: DENY` ni la directive CSP `frame-ancestors 'none'`. Une partie des pages serait donc encadrable depuis une origine externe (risque de clickjacking dans des scénarios spécifiques d'attaque ciblée).

Recommandation : ajouter `frame-ancestors 'none'` à la CSP (ou `'self'` si l'application embarque des frames internes).

0-09, fuites historiques de credentials sur 6 emails publiquement listés

Niveau d'attention : Moyen, à corriger sans pentest.

Six emails issus du domaine `@acmefictio.example` apparaissent dans des bases publiques de fuites tierces (LinkedIn 2021, Dropbox 2012, services SaaS divers). Cinq des six concernent des comptes encore actifs dans l'organisation (visibles sur LinkedIn). Le risque dépend des pratiques de réutilisation de mot de passe par ces personnes et de la présence d'un MFA chez AcmeFictio.

Recommandation : lancer une vérification interne sur ces six comptes (rotation de mot de passe, audit des connexions récentes), et s'assurer que le MFA est actif sur tous les SaaS critiques utilisés.

0-10, infrastructure cloud, plusieurs noms d'instances divulgués

Niveau d'attention : Faible, informatif.

Les en-têtes de réponse de l'API laissent transparaître des identifiants d'instances cloud (forme `i-0abc1234`, ou références `eu-west-3a`). Ce n'est pas critique, mais c'est une donnée OSINT gratuite pour un attaquant qui prépare un scénario.

Recommandation : ne pas exposer ce type d'identifiant côté API publique. À traiter au niveau de la couche reverse proxy.

0-11, redirections trop laxistes sur `www`

Niveau d'attention : Faible, informatif.

Le sous-domaine `www.acmefictio.example` accepte des redirections paramétrées via `?returnTo=...`. Le filtrage n'est pas strict, ce qui pourrait servir de support à un phishing ciblé (`www.acmefictio.example/auth?returnTo=https://attacker.example`).

Recommandation : restreindre les valeurs de `returnTo` à une liste blanche, ou les ignorer si non préfixées par le domaine légitime.

0-12, présence de fichiers `.well-known` non sécurisés

Niveau d'attention : Faible, informatif.

Le fichier `.well-known/security.txt` n'existe pas sur le domaine principal. Bonne pratique recommandée par l'ANSSI et le NIST pour permettre un canal de signalement de vulnérabilité par des chercheurs externes.

Recommandation : ajouter un `security.txt` (RFC 9116) sur `acmefictio.example/.well-known/security.txt`, avec un mail de contact dédié et un délai de réponse annoncé.

7. Lecture des risques métier

Les douze observations ne pèsent pas le même poids vis-à-vis du business d'AcmeFictio. La grille suivante remet les choses en perspective.

RISQUE MÉTIER	OBSERVATIONS CONTRIBUTRICES	PROBABILITÉ	IMPACT
Fuite de données inter-tenants	O-02 (API documentée), O-01 (préprod ouverte)	**Moyenne**	**Très élevé**
Compromission de compte partenaire	O-03 (énumération), O-07 (cookies), O-09 (fuites historiques)	**Moyenne**	**Élevé**
Atteinte à l'image (defacement, phishing)	O-04, O-05, O-08, O-11	Faible à moyenne	**Moyen**
Indisponibilité ciblée	aucune observation directe ici	**Faible**	**Moyen**
Difficulté lors d'un audit client	O-04 (composants obsolètes), O-06 (cert expiré), O-12 (security.txt absent)	**Élevée**	**Faible à moyen**

La probabilité reste **modérée** sur la plupart des scénarios. Aucune observation n'indique une compromission probable à court terme sans intervention attaquante motivée. En revanche, le poids combiné des observations O-01, O-02 et O-03 justifie de lever le doute par un pentest avant la prochaine échéance assurance.

8. Recommandation Laucked

8.1 GO pour un pentest cadré

Recommandation : oui, un pentest est pertinent dans les 60 jours. Le périmètre est mature, plusieurs zones grises remontent, et le contexte business (renouvellement assurance, demandes clients) crée une fenêtre logique.

Sans pentest, AcmeFictio garde quatre points d'interrogation non tranchés (O-01, O-02, O-03, et la cohérence d'autorisation côté API). Avec pentest, ces points basculent en findings exploitables ou en

zones validées. C'est exactement le rôle du pentest : trancher l'exploitabilité.

8.2 Périmètre proposé

PÉRIMÈTRE	DESCRIPTION	EFFORT
Web applicatif	`app.acmefictio.example`, parcours utilisateur multi-tenant, back-office admin	2,5 j-h
API	`api.acmefictio.example/v1`, 41 endpoints listés, focus BOLA / BOPLA / BFLA	2 j-h
Préproduction	`staging.acmefictio.example`, validation iso-prod ou divergence	0,5 j-h
Rédaction et retest	rapport, exec summary, plan de remédiation, retest 30 jours	1 j-h
Total mission		**5 à 7 j-h**

8.3 Fourchette budgétaire

Estimation : 7 500 à 9 500 € HT. Dans la grille publique Laucked, ce périmètre correspond au profil « Web + API multi-tenant, taille moyenne, complexité raisonnable ». Le devis exact sera émis après un cadrage de 30 minutes en visio, avec validation de l'authentification disponible (boîte grise multi-rôles).

8.4 Modalités

MODALITÉ	VALEUR
Type	Boîte grise (deux comptes test fournis, un tenant et un admin)
Méthodologie	OWASP WSTG, OWASP API Top 10 (2023), PTES, CVSS v3.1
Fenêtre	À convenir, 2 à 3 semaines calendaires
Livrable	Rapport complet exec + technique, plan de remédiation, retest inclus
Retest	1 j-h dans les 30 jours suivant la livraison des correctifs

8.5 Si NO-GO temporaire

Si le pentest ne peut pas être déclenché immédiatement (budget, planning, refonte applicative en cours), la posture acceptable consiste à traiter d'abord les quatre observations O-04, O-05, O-06, O-07, sans dépendance externe. Cela ne couvre pas les zones grises (O-01, O-02, O-03) mais réduit la surface d'erreur basse-friction.

9. Suite logique, prochaines étapes proposées

Trois chemins possibles, à choisir selon votre rythme.

1. **Cadrage pentest sous 7 jours.** Visio de 30 minutes pour valider le périmètre détaillé, les comptes test, la fenêtre de mission. Devis émis sous 48 h.
2. **Stabilisation de la surface d'abord.** Correction des observations P2 et P3 sur 4 semaines en interne. Reprise du dossier pentest à T+30 jours, avec un nouveau diagnostic rapide pour vérifier.
3. **Diagnostic complémentaire.** Si l'application mobile (iOS, Android) ou la couche email (SPF / DKIM / DMARC) sont en tension par ailleurs, un diagnostic dédié peut être lancé pour cadrer également ces périmètres avant pentest.

Le diagnostic de surface est **gratuit chez Laucked**. La prochaine étape engageante reste votre décision.

10. Annexes

10.1 Sources publiques utilisées

SOURCE	USAGE	VOLUME TRAITÉ
Passive DNS (CT logs publics)	Énumération sous-domaines	11 sous-domaines identifiés
Pages web publiques	Inspection HTTP, fingerprint stack	23 actifs observés
robots.txt, sitemap.xml	Détection contenus cachés	4 URLs supplémentaires détectées
Bases de fuites publiques	Vérification credentials historiques	6 entrées emails associées
INSEE, Pappers, LinkedIn public	Contexte organisationnel	1 organisation, ~40 personnes

10.2 Hypothèses retenues

Trois hypothèses ont guidé la lecture des observations. Premièrement, AcmeFictio est en croissance, ce qui explique des choix d'architecture pragmatiques (sous-domaines de préprod publics pour faciliter les démos commerciales) plutôt que des oublis. Deuxièmement, l'équipe technique compte une à deux personnes à plein temps sur l'infrastructure, ce qui limite la bande passante pour les durcissements de second ordre (en-têtes, CSP). Troisièmement, le contexte assurance impose une lecture orientée preuve plutôt que démonstration technique, ce qui oriente la recommandation vers un pentest plutôt qu'un audit interne.

10.3 Glossaire rapide

TERME	DÉFINITION COURTE
Diagnostic de surface	Cartographie passive de ce qui est exposé sur Internet pour une organisation donnée.
Pentest	Test d'intrusion actif, validation de l'exploitabilité réelle, avec rapport et plan de remédiation.
BOLA	Broken Object Level Authorization, défaut d'autorisation au niveau objet (OWASP API #1).
BOPLA	Broken Object Property Level Authorization, défaut au niveau attribut d'objet (OWASP API #3).
BFLA	Broken Function Level Authorization, défaut au niveau fonction (OWASP API #5).
OSINT	Open Source Intelligence, renseignement à partir de sources publiques.
Boîte grise	Pentest avec comptes utilisateurs fournis (sans accès code source ni admin infra).

10.4 Engagement Laucked

ENGAGEMENT	VALEUR
Délai diagnostic	48 à 72 h ouvrées après formulaire complété
Confidentialité	Aucune publication ni partage, données conservées 30 jours puis supprimées
Hébergement données	France, prestataire conforme RGPD
Refus possible	Si la surface est trop petite ou le pentest non pertinent, nous le disons
Auteur du livrable	Pentester senior signataire (OSCP / OSEP / OSWE)
Contact	sales@laucked.com, contact direct sous 24 h ouvrées

10.5 Mentions légales

Document fictif, classifié public, diffusé par Laucked SAS à des fins d'information commerciale. Aucune donnée réelle. Toute ressemblance avec une organisation existante est fortuite. Reproduction libre avec mention de la source.

Fin du document.