SecuriGeek

CABINET D'EXPERTISE CYBER

Rapport de Test d'Intrusion Application Web

Exemple SAS — extranet.exemple-sas.fr — Septembre 2026

Référence : SG-2026-EX-001 · Test en boîte grise · 10 jours

DOCUMENT EXEMPLE — DONNÉES ENTIÈREMENT FICTIVES

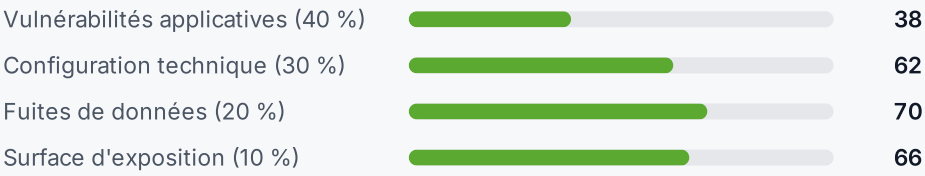
Résumé Exécutif

Vue d'ensemble de la posture de sécurité de l'application, destinée aux décideurs.

Ce rapport présente les résultats du test d'intrusion réalisé sur l'application web **extranet.exemple-sas.fr**. Nos équipes ont identifié **6 vulnérabilités**, dont **1 critique** et **2 élevées**, ainsi que **2 identifiants compromis** dans des fuites publiques. Une vulnérabilité critique permet d'accéder à la base de données clients : elle doit être corrigée en priorité absolue.

54
/ 100

Risque élevé



Score global = moyenne pondérée des quatre composantes. Méthodologie détaillée en page 3.

Trois points d'attention immédiats

[VULN-001] Injection SQL sur la recherche clients

CRITIQUE CVSS 9.1 Correction sous 48 h

Un attaquant peut lire l'intégralité de la base de données — y compris les données personnelles de vos clients — sans aucun identifiant.

[VULN-003] Authentification sans double facteur (MFA)

ÉLEVÉE CVSS 7.8 Correction sous 1 semaine

Un mot de passe volé suffit pour se connecter. Deux identifiants de collaborateurs circulent déjà dans des fuites publiques.

[VULN-002] Code malveillant injectable dans les commentaires (XSS)

ÉLEVÉE CVSS 7.4 Correction sous 1 semaine

Un commentaire piégé peut voler la session de chaque utilisateur qui le consulte, y compris celle d'un administrateur.

Méthodologie

Comment le test a été mené : périmètre, méthode et limites.

Le test d'intrusion a été réalisé par nos équipes selon le référentiel **OWASP Top 10 (2021)** et la méthodologie **PTES**, avec l'autorisation écrite d'Exemple SAS. L'approche en « boîte grise » combine des tests automatisés et une exploitation manuelle par un auditeur, à partir d'un compte utilisateur standard fourni par le client.

Périmètre du test.
Application : extranet.exemple-sas.fr (front-end + API REST)
Période : du 7 au 18 septembre 2026 — environnement de production, hors horaires de pointe
Comptes fournis : 1 utilisateur standard, 1 administrateur restreint

10
Jours de test (reconnaissance, exploitation, validation)

120+
Scénarios d'attaque éprouvés manuellement

100 %
Des failles confirmées par une preuve d'exploitation

Couverture des tests

- **Injection et logique applicative** — SQL, XSS, falsification de requêtes, règles métier
- **Authentification et sessions** — robustesse des mots de passe, MFA, jetons, déconnexion
- **Contrôles d'accès** — cloisonnement entre utilisateurs et entre rôles (BOLA/IDOR)
- **Configuration** — en-têtes de sécurité, versions des composants, fichiers exposés
- **Exposition externe** — sous-domaines, fuites d'identifiants dans des sources publiques

Limites du test

Ce test porte uniquement sur l'application web et son API, dans le périmètre convenu. L'infrastructure d'hébergement interne, les applications mobiles et les tests d'hameçonnage sur les collaborateurs ne sont pas couverts par ce rapport. Aucune donnée réelle n'a été extraite ni modifiée : les preuves d'exploitation ont été réalisées sur des jeux de données de démonstration.

Le saviez-vous ? Un test d'intrusion reproduit le raisonnement d'un attaquant réel, mais dans un cadre contractuel et maîtrisé. L'objectif n'est pas de « casser » l'application, mais de mesurer précisément ce qu'un attaquant pourrait faire — et de le corriger avant lui.

Vulnérabilités Identifiées

Six vulnérabilités confirmées, classées par niveau de gravité (CVSS 3.1).

1	2	2	1
Critique — action sous 48 h	Élevées — action sous 1 semaine	Moyennes — action sous 30 jours	Faible — action sous 90 jours

[VULN-001] Injection SQL sur la page de recherche clients

CRITIQUE CVSS 9.1 CWE-89 OWASP A03:2021 — Injection

En langage simple. Le champ de recherche transmet la saisie de l'utilisateur directement à la base de données, sans filtrage. Un attaquant peut y glisser une « consigne cachée » et obtenir des informations que l'application ne devrait jamais afficher — comme un client qui, au guichet d'une banque, ajouterait une note à sa demande pour se faire remettre tous les dossiers.

Impact métier. Lecture complète de la base : fiches clients, historiques de commandes, identifiants de connexion. Risque RGPD majeur (notification CNIL sous 72 h en cas d'exploitation réelle).

PREUVE D'EXPLOITATION (EXTRAIT ANONYMISÉ)

```
GET /api/clients?search=%27%20UNION%20SELECT%20email,password%20FROM%20users-- HTTP/1.1
HTTP/1.1 200 OK — 1 247 enregistrements retournés (jeu de démonstration)
```

Correction recommandée. Utiliser des requêtes paramétrées (l'application ne doit jamais construire ses requêtes en assemblant du texte) et valider la saisie côté serveur. Effort estimé : 2 à 4 jours de développement.

[VULN-002] XSS stocké dans l'espace commentaires

ÉLEVÉE CVSS 7.4 CWE-79 OWASP A03:2021 — Injection

En langage simple. Les commentaires publiés par les utilisateurs ne sont pas nettoyés : un attaquant peut y déposer un message piégé qui s'exécute automatiquement dans le navigateur de chaque visiteur — comme un courrier piégé qui s'ouvrirait tout seul chez chaque destinataire.

Impact métier. Vol de sessions utilisateurs (y compris administrateur), usurpation d'identité, diffusion de faux contenus au nom de l'entreprise.

Correction recommandée. Encoder systématiquement les contenus affichés et déployer une politique de sécurité de contenu (CSP). Effort estimé : 2 jours.

Vulnérabilités — Suite

Authentification, vulnérabilités moyennes et faibles, fuites d'identifiants.

[VULN-003] Authentification sans double facteur et politique de mots de passe insuffisante

ÉLEVÉE CVSS 7.8 CWE-308 OWASP A07:2021 — Authentification

En langage simple. La connexion repose sur un seul mot de passe, sans vérification supplémentaire (code envoyé sur téléphone, par exemple). La politique accepte encore des mots de passe de 6 caractères. Si un mot de passe fuite — et deux ont déjà fuité, voir ci-dessous — un attaquant entre comme dans un moulin.

Correction recommandée. Activer l'authentification multi-facteur (MFA) pour tous les comptes, exiger 12 caractères minimum et bloquer les mots de passe connus comme compromis. Effort estimé : 1 jour (fonction native de la plupart des frameworks).

Vulnérabilités moyennes et faibles

Réf.	Description	Sévérité	CVSS	Délai
VULN-004	En-têtes de sécurité HTTP manquants (CSP, HSTS, X-Frame-Options)	MOYENNE	5.3	30 j
VULN-005	Bibliothèque JavaScript obsolète exposant une faille connue (CVE-2024-XXXXX)	MOYENNE	5.4	30 j
VULN-006	Cookies de session sans attributs complets (Secure, SameSite)	FAIBLE	3.7	90 j

Identifiants compromis dans des fuites publiques

Notre surveillance des sources publiques a identifié **2 identifiants professionnels** associés au domaine exemple-sas.fr dans des fuites de données connues. S'ils sont réutilisés sur l'extranet, ils offrent un accès immédiat à un attaquant.

Identifiant (anonymisé)	Donnée exposée	Source	Année	Risque
j.d***@exemple-sas.fr	Mot de passe	Fuite publique « Collection #1 »	2025	ÉLEVÉ
m.l***@exemple-sas.fr	Mot de passe	Fuite site e-commerce	2024	ÉLEVÉ

Action immédiate : forcer la réinitialisation de ces deux mots de passe et vérifier qu'ils ne sont réutilisés sur aucun autre service professionnel.

Plan de Remédiation

Actions priorisées par impact sur le risque et effort de mise en œuvre.

Priorité	Réf.	Action	Effort	Gain de score	Échéance
P1	VULN-001	Corriger l'injection SQL (requêtes paramétrées)	Moyen	+14 pts	48 h
P1	LEAK-001	Réinitialiser les 2 identifiants compromis	Faible	+6 pts	24 h
P1	VULN-003	Activer le MFA pour tous les comptes	Faible	+8 pts	1 sem.
P2	VULN-002	Encoder les commentaires + déployer une CSP	Moyen	+6 pts	2 sem.
P2	VULN-004	Ajouter les en-têtes de sécurité HTTP	Faible	+3 pts	30 j
P3	VULN-005/006	Mettre à jour la bibliothèque JS et les cookies	Faible	+3 pts	90 j

Trajectoire de score. La mise en œuvre des priorités P1 seules ferait passer le score global de **54/100 à environ 82/100** (risque faible). Un contre-audit de validation, réalisé 4 à 6 semaines après correction, confirme l'efficacité des mesures et met à jour le score officiel.

Glossaire

Injection SQL
Technique qui détourne une saisie utilisateur pour faire exécuter à la base de données des commandes non prévues.

XSS (Cross-Site Scripting)
Injection de code malveillant dans une page web, exécuté dans le navigateur des visiteurs.

MFA
Authentification multi-facteur : vérification d'identité en deux étapes (mot de passe + code temporaire).

CVSS
Échelle internationale de gravité d'une vulnérabilité, de 0.0 (nulle) à 10.0 (maximale).

CSP
Politique de sécurité de contenu : règle qui limite ce qu'une page web est autorisée à exécuter.

Contre-audit
Second test réalisé après correction, pour vérifier que chaque faille est bien colmatée.

SecuriGeek

CABINET D'EXPERTISE CYBERSÉCURITÉ

Sécurisez votre périmètre. Mesurez votre risque.

246	125	18
Audits réalisés	Entreprises protégées	Secteurs d'activité

Audit gratuit — places limitées

contact@securigeek.com · 01 87 07 94 86 · securigeek.com

Securigeek SASU — 14 Av. de l'Europe, 77144 Montévrain