

CABINET DÉMO

Test applicatif web

Rapport d'audit de sécurité

PRÉPARÉ PAR	Cabinet Démo
DATE	06/08/2026
PÉRIMÈTRE	Application web exposée

Tableau de bord exécutif

9 VULNÉRABILITÉS	0 CRITIQUES	4 ÉLEVÉES
4 ACTIFS CONCERNÉS	7.5 CVSS MOYEN	1 À DISTANCE / SANS AUTHENTIFICATION

59

/100
SCORE DE RISQUE

Posture Globale

Le score est un indice d'exposition pondéré (0 = maîtrisée, 100 = critique) calculé à partir de la sévérité, du CVSS et de l'exploitabilité. Il ne mesure aucune conformité.

Répartition par Sévérité



Sévérité	Catégorie	Nombre
Élevée	Orange	4
Moyenne	Dark Blue	2
Faible	Light Grey	1
Info	Very Light Grey	2

Impact métier

Conséquences concrètes pour l'activité si les expositions majeures ne sont pas traitées.

F-001 Exposed .env file

Un attaquant peut récupérer des secrets applicatifs et accéder à des systèmes internes ou des bases de données, entraînant une compromission plus large de l'infrastructure.

NET-A-H1:443, NET-B-H1:443

F-002 Cross Site Scripting (Reflected)

Un attaquant peut exécuter du code JavaScript dans le navigateur des utilisateurs, permettant le vol de sessions ou la manipulation de l'interface applicative.

HOST-01:443

F-003 SQL Injection

Un attaquant peut lire, modifier ou supprimer des données de la base applicative, voire obtenir un accès plus large au système d'information.

HOST-01:443

Feuille de route de remédiation

Phase 1 IMMÉDIAT · 0-7 JOURS 3 FINDINGS

Contenir l'exécution de code à distance et les accès non authentifiés.

Responsable: Ingénierie sécurité · Charge: Faible

F-001, F-003, F-004

Phase 2 COURT TERME · 8-30 JOURS 3 FINDINGS

Corriger les services en sévérité élevée et supprimer les identifiants faibles.

Responsable: Ingénierie sécurité · Charge: Faible

F-002, F-005, F-006

Phase 3 MOYEN TERME · 31-90 JOURS 3 FINDINGS

Durcir la configuration, le TLS et la supervision ; retester le périmètre.

Responsable: Ingénierie sécurité · Charge: Faible
F-007, F-008, F-009

Contrôle du document

VERSION	1.0
DATE	06/08/2026
AUTEUR	Cabinet Démo
CLASSIFICATION	Confidentiel — diffusion restreinte
DIFFUSION	Client et cabinet émetteur ; ne pas rediffuser sans accord écrit.
CONTACT	Non renseigné

Synthèse exécutive

L'audit a porté sur l'exposition des applications et systèmes web du périmètre concerné. Plusieurs failles de sécurité de niveau élevé ont été identifiées, notamment liées à l'exposition de données sensibles et à des faiblesses dans le traitement des données par les applications. Ces failles pourraient permettre à un attaquant d'accéder à des informations confidentielles ou de perturber le fonctionnement des services. Des faiblesses de niveau moindre viennent renforcer ce constat en réduisant les protections de défense en profondeur. Il est recommandé de prioriser la correction des failles critiques avant toute autre action, et de statuer sur un plan de remédiation à court terme.

Risques majeurs

- Des données confidentielles (identifiants, informations clients ou internes) pourraient être exposées ou volées, avec un impact sur la réputation et la conformité.
- Des attaquants pourraient altérer ou détruire des données métier stockées dans les bases applicatives, affectant la continuité et la fiabilité des activités.
- Des utilisateurs finaux pourraient être ciblés via les applications compromises, entraînant une perte de confiance des clients et un risque juridique pour l'entreprise.

Répartition par sévérité

SÉVÉRITÉ	#	%	
CRITIQUE	0	0%	
ÉLEVÉE	4	44%	
MOYENNE	2	22%	
FAIBLE	1	11%	
INFO	2	22%	

Périmètre et méthodologie

Dans le périmètre

Application web exposée

4 host(s)

NET-A-H1, NET-B-H1, HOST-01, NET-B-H2

Hors périmètre

Tout actif non présent dans les exports fournis. Aucune exploitation active, aucun test d'ingénierie sociale, aucun test de déni de service.

Fichiers analysés

FICHIER	OUTIL DÉTECTÉ	ÉTAT
zap-sample.json	ZAP	Analysé
zap-sample.xml	ZAP	Analysé
burp-sample.xml	BURP	Analysé
nuclei-sample.jsonl	NUCLEI	Analysé

Méthodologie et limites

Les données proviennent d'exports de scanners automatisés (Nmap, Nessus, Trivy, Nuclei, Burp Suite, OWASP ZAP). Les findings sont corrélés et dédoublés entre outils, scorés à partir du CVSS et rattachés aux contrôles techniques pertinents.

Aucun enrichissement externe n'a pu être appliqué (CISA KEV et EPSS indisponibles) : la notation repose uniquement sur le CVSS et les sévérités rapportées par les outils.

Ce rapport est établi à partir de scans automatisés et ne constitue pas un test d'intrusion complet.

This report is based on automated scans and does not constitute a full penetration test.

Méthode de notation et de priorisation

Échelle de sévérité

SÉVÉRITÉ	CVSS
CRITIQUE / CRITICAL	9.0 - 10.0
ÉLEVÉE / HIGH	7.0 - 8.9
MOYENNE / MEDIUM	4.0 - 6.9
FAIBLE / LOW	0.1 - 3.9
INFO	0.0

Ajustements appliqués

Deux ajustements peuvent relever la sévérité d'un niveau, plafonnés à CRITIQUE. Chaque ajustement appliqué est indiqué sur la fiche du finding concerné :

- +1 niveau — exposition publique constatée (port ouvert sur une adresse routable).
- +1 niveau — exploitation connue (présence au catalogue CISA KEV, ou exploit signalé par l'outil de scan).

Aucun pourcentage de conformité n'est calculé. Les contrôles cités sont des éléments de preuve, la décision de conformité appartient à l'auditeur.

Signification des priorités

PRIORITÉ	
1	À traiter immédiatement / Immediate
2	À planifier dans le cycle courant / Planned
3	À suivre / Monitor

Synthèse des findings

RÉF	INTITULÉ	SÉVÉRITÉ	CVSS	PRIORITÉ	STATUT
F-001	Exposed .env file	ÉLEVÉE	7.5	1	Ouvert
F-002	Cross Site Scripting (Reflected)	ÉLEVÉE		2	Ouvert
F-003	SQL Injection	ÉLEVÉE		1	Ouvert
F-004	SQL injection	ÉLEVÉE		1	Ouvert
F-005	Content Security Policy (CSP) Header Not Set	MOYENNE		2	Ouvert
F-006	Weak TLS cipher	MOYENNE		2	Ouvert
F-007	Nginx detected	INFO		3	Ouvert
F-008	Timestamp Disclosure	INFO		3	Ouvert
F-009	Observations de sévérité faible — configuration	FAIBLE		3	Ouvert

Findings — détail

Extrait : 3 findings sur 9 sont détaillés ci-dessous. Les 6 findings restants, leurs preuves et leur plan de remédiation figurent dans le rapport complet.

F-001 Exposed .env file

ÉLEVÉE CVSS 7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N CWE-200 Sources: NUCLEI

Sévérité high : score CVSS de 7.5.

Détail CVSS — Vecteur d'attaque: Réseau · Complexité: Faible · Privilèges requis: Aucun · Interaction utilisateur: Aucune · Portée: Inchangée · Confidentialité: Élevé · Intégrité: Aucun · Disponibilité: Aucun

ACTIFS CONCERNÉS

NET-A-H1:443, NET-B-H1:443

Un fichier .env a été trouvé exposé publiquement sur deux actifs. Ce type de fichier contient habituellement des identifiants, clés d'API ou paramètres de connexion à des bases de données. Le scan nuclei a confirmé son accessibilité directe via HTTPS.

IMPACT

Un attaquant peut récupérer des secrets applicatifs et accéder à des systèmes internes ou des bases de données, entraînant une compromission plus large de l'infrastructure.

PREUVE

```
Template: exposed-env-file
Matched at: https://NET-A-H1/.env

Template: exposed-env-file
Matched at: https://NET-B-H1/.env
Extracted: DB_PASSWORD=redacted
```

VÉRIFICATION

Pour vérifier, exécuter la commande : nuclei -id exposed-env-file -u https://NET-A-H1

REMÉDIATION — PRIORITÉ 1 (IMMÉDIAT)

Retirer immédiatement le fichier .env de l'arborescence accessible publiquement. Régénérer tous les secrets et identifiants qu'il contenait. Configurer le serveur web pour bloquer l'accès aux fichiers de configuration sensibles. Vérifier l'absence d'autres fichiers de configuration exposés.

RÉFÉRENCES

<https://cwe.mitre.org/data/definitions/200.html>

<https://github.com/projectdiscovery/nuclei-templates/search?q=exposed-env-file>

Contrôles rattachés: A.8.12, A.8.3, 21.2.i, 21.2.e · Statut: Ouvert

F-002 Cross Site Scripting (Reflected)

ÉLEVÉE CWE-79 Sources: ZAP

Sévérité high : sévérité rapportée par l'outil (high).

ACTIFS CONCERNÉS

HOST-01:443

Une vulnérabilité de type Cross Site Scripting réfléchi a été identifiée sur le paramètre q du point d'accès /search. Le scanner ZAP a démontré l'injection d'un script exécutable via ce paramètre.

IMPACT

Un attaquant peut exécuter du code JavaScript dans le navigateur des utilisateurs, permettant le vol de sessions ou la manipulation de l'interface applicative.

PREUVE

```
URI: https://HOST-01/search
Method: GET
Parameter: q
Evidence: <script>alert(1)</script>
```

REMÉDIATION — PRIORITÉ 2 (À PLANIFIER)

Appliquer un encodage systématique des sorties HTML pour les données utilisateur. Mettre en place une politique de validation stricte des entrées côté serveur. Déployer une politique CSP restrictive pour limiter l'exécution de scripts non autorisés.

RÉFÉRENCES

<https://cwe.mitre.org/data/definitions/79.html>

Contrôles rattachés: A.8.26, A.8.28, 21.2.e · Statut: Ouvert

F-003 SQL Injection

ÉLEVÉE CWE-89 Sources: ZAP

Sévérité high : sévérité rapportée par l'outil (high).

ACTIFS CONCERNÉS

HOST-01:443

Une vulnérabilité d'injection SQL a été détectée sur le paramètre q du point d'accès /search. Le scanner ZAP a obtenu une erreur de syntaxe SQL en soumettant une charge utile d'injection classique.

IMPACT

Un attaquant peut lire, modifier ou supprimer des données de la base applicative, voire obtenir un accès plus large au système d'information.

PREUVE

```
URI: https://HOST-01/search
Method: GET
Parameter: q
Attack: ' OR '1'='1
Evidence: SQL syntax error
```

REMÉDIATION — PRIORITÉ 1 (IMMÉDIAT)

Utiliser des requêtes paramétrées ou des procédures préparées pour tous les accès à la base de données. Valider et filtrer les entrées utilisateur côté serveur. Auditer le code applicatif pour identifier d'autres points d'injection potentiels.

RÉFÉRENCES

<https://cwe.mitre.org/data/definitions/89.html>

Contrôles rattachés: A.8.26, A.8.28, 21.2.e · Statut: Ouvert

Plan de remédiation

Immédiat (priorité 1)

Ce plan de remédiation présente les actions par ordre de priorité, sans échéance chiffrée imposée. Trois findings de sévérité élevée requièrent un traitement sans attendre : l'exposition du fichier .env (F-001) ainsi que deux injections SQL (F-003, F-004). Ces failles permettent potentiellement un accès direct à des données sensibles ou à la base applicative. Aucune de ces vulnérabilités n'est référencée comme exploitée activement (KEV), mais leur sévérité justifie une correction prioritaire.

F-001 — Exposed .env file

F-003 — SQL Injection

F-004 — SQL injection

À planifier (priorité 2)

Trois findings de sévérité moyenne à élevée doivent être intégrés au cycle de correction courant. Le XSS réfléchi (F-002) et l'absence d'en-tête CSP (F-005) concernent la sécurisation du rendu côté client. La faiblesse identifiée sur les suites de chiffrement TLS (F-006) doit également être corrigée. Ces éléments ne présentent pas de risque immédiat critique mais réduisent la surface d'exposition globale s'ils sont traités rapidement.

F-002 — Cross Site Scripting (Reflected)

F-005 — Content Security Policy (CSP) Header Not Set

F-006 — Weak TLS cipher

À surveiller (priorité 3)

Trois observations de faible sévérité ou informatives sont à surveiller sans action immédiate. La détection du serveur Nginx (F-007) et la divulgation d'horodatage (F-008) relèvent de la fuite d'informations techniques. Une observation de configuration de sévérité faible (F-009) complète ce volet. Ces points peuvent être réévalués lors d'un prochain cycle d'audit.

F-007 — Nginx detected

F-008 — Timestamp Disclosure

F-009 — Observations de sévérité faible — configuration

Annexe — Rattachement aux contrôles

Ces éléments constituent des preuves techniques rattachées aux contrôles ci-dessous. Ils ne constituent pas une évaluation de conformité : aucun pourcentage n'est calculé, la décision de conformité appartient à l'auditeur.

CONTRÔLE	INTITULÉ	FINDINGS
A.8.12	Data leakage prevention	F-001, F-008
A.8.24	Use of cryptography	F-006
A.8.26	Application security requirements	F-002, F-003, F-004, F-007
A.8.28	Secure coding	F-002, F-003, F-004, F-007
A.8.3	Information access restriction	F-001, F-008
A.8.9	Configuration management	F-005, F-009

NIS2

MESURE	INTITULÉ	FINDINGS
21.2.e	Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	F-001, F-002, F-003, F-004, F-007, F-008
21.2.f	Policies to assess the effectiveness of cybersecurity risk-management measures	F-005, F-009
21.2.g	Basic cyber hygiene practices and cybersecurity training	F-005, F-009
21.2.h	Policies on the use of cryptography and, where appropriate, encryption	F-006
21.2.i	Human resources security, access control policies and asset management	F-001, F-008
21.2.j	Use of multi-factor authentication, secured communications and secured emergency communication systems	F-006

Annexe technique

RÉF	INTITULÉ	SÉVÉRITÉ	CVSS	ACTIFS
F-001	Exposed .env file	ÉLEVÉE	7.5	2
F-002	Cross Site Scripting (Reflected)	ÉLEVÉE		1
F-003	SQL Injection	ÉLEVÉE		1
F-004	SQL injection	ÉLEVÉE		1
F-005	Content Security Policy (CSP) Header Not Set	MOYENNE		1
F-006	Weak TLS cipher	MOYENNE		1
F-007	Nginx detected	INFO		1
F-008	Timestamp Disclosure	INFO		1
F-009	Observations de sévérité faible — configuration	FAIBLE		1

Annexe — Re-test

À compléter lors du contrôle de remédiation.

RÉF	INTITULÉ	STATUT	DATE	VÉRIFICATION
F-001	Exposed .env file	Ouvert		
F-002	Cross Site Scripting (Reflected)	Ouvert		
F-003	SQL Injection	Ouvert		
F-004	SQL injection	Ouvert		
F-005	Content Security Policy (CSP) Header Not Set	Ouvert		
F-006	Weak TLS cipher	Ouvert		
F-007	Nginx detected	Ouvert		
F-008	Timestamp Disclosure	Ouvert		
F-009	Observations de sévérité faible — configuration	Ouvert		