RAPPORT D'EXEMPLE · DONNÉES FICTIVES

beispiel-shop.example

Objet	Test de sécurité gratuit
Date	1er novembre 2026
Périmètre	21 requêtes, passif, sans connexion

ÉVALUATION GLOBALE

Insuffisant

Note F · 0 points sur 100

Action urgente : au moins un constat donne un accès direct à des informations internes.

1 Critique **0** Élevé **3** Moyen **4** Faible

ÉVALUATION PAR DOMAINE

Chiffrement (TLS)

Actions requises

Chiffrement obsolète accepté (TLS 1.0, TLS 1.1)

En-têtes de sécurité

Actions requises

Content-Security-Policy absente; HSTS absent +1 autres

Cookies

Bon

Cookie « shop_session » sans SameSite

Fichiers exposés

Insuffisant

Répertoire Git accessible publiquement; Pas de contact sécurité (security.txt)

Versions visibles

Bon

Version logicielle visible (nginx/1.18.0)

Expéditeur e-mail (DNS)

Bon

Pas d'enregistrement DMARC pour beispiel-shop.example

Ce que la note ne couvre pas

Il s'agit du test de base : 21 requêtes depuis l'extérieur, sans connexion. Les catégories de vulnérabilités les plus fréquentes de l'OWASP Top 10 – le contrôle d'accès au 1er rang, l'injection au 3e – ainsi que les secrets et les dépendances dans le code ne sont pas visibles de l'extérieur. Ce test ne peut ni confirmer ni exclure que votre application soit concernée.

NON VÉRIFIÉ
Connexion et sessions
Réinitialisation du mot de passe, durée de session, limites de débit
→ Inclus dans l'audit d'application

NON VÉRIFIÉ
Droits d'accès
L'utilisateur A voit-il les données de B ?
→ Inclus dans l'audit d'application

NON VÉRIFIÉ
Saisies et API
Injection, XSS, API non protégées
→ Inclus dans l'audit d'application

NON VÉRIFIÉ
Code source et dépendances
Secrets dans le code, bibliothèques avec CVE connues
→ Inclus dans l'audit de code

NOTRE RECOMMANDATION POUR BEISPIEL-SHOP.EXAMPLE

Audit de code

Un fichier au contenu vraisemblablement confidentiel est accessible depuis l'extérieur. L'audit de code détermine quels identifiants sont concernés et à quels autres endroits du code ils figurent – en 24 heures avec l'option Express.

890 € HT · rapport en 5 jours ouvrés

Réserver l'audit de code →

Ce que couvre l'audit de code

Constats en détail

Répertoire Git accessible publiquement

CRITIQUE

Le répertoire de gestion de versions de l'application est servi sous /.git/HEAD. On peut en général en télécharger tout le code source et son historique, souvent avec mots de passe et clés.

CORRECTIF Bloquer immédiatement l'accès à `/.git` sur le serveur web, puis vérifier quels identifiants figurent dans le dépôt et les remplacer.

PREUVE `/.git/HEAD`

CORRECTIF RAPIDE **Mesure immédiate : bloquer le fichier, remplacer les identifiants qu'il contient**

Chiffrement obsolète accepté (TLS 1.0, TLS 1.1)

MOYEN

Le serveur accepte des versions de protocole officiellement dépréciées depuis 2021 (RFC 8996). Elles autorisent des algorithmes plus faibles et échouent aux contrôles de type PCI DSS ou ANSSI.

CORRECTIF N'autoriser que TLS 1.2 et TLS 1.3 sur le serveur web ou le répartiteur de charge.

PREUVE `TLS 1.0, TLS 1.1`

CORRECTIF RAPIDE **Inclus dans le correctif rapide**

Content-Security-Policy absente

MOYEN

Sans CSP, le navigateur exécute tout script injecté. Une seule faille XSS suffit alors à détourner des sessions ou à lire les saisies.

CORRECTIF Mettre en place une Content-Security-Policy, d'abord en `Content-Security-Policy-Report-Only`, puis en mode bloquant.

CORRECTIF RAPIDE **Inclus dans le correctif rapide**

HSTS absent

MOYEN

Sans l'en-tête Strict-Transport-Security, le navigateur ne retient pas que le site doit être chargé uniquement en HTTPS. La première requête peut être interceptée et rétrogradée en HTTP.

CORRECTIF Envoyer `Strict-Transport-Security: max-age=31536000; includeSubDomains`.

CORRECTIF RAPIDE **Inclus dans le correctif rapide**

Version logicielle visible (nginx/1.18.0)

FAIBLE

La version exacte figure dans un en-tête ou dans le code source de la page. Les attaquants s'en servent pour chercher des failles adaptées.

CORRECTIF Masquer les indications de version (par exemple `server_tokens off` sous nginx, supprimer la balise generator) et appliquer les mises à jour rapidement.

PREUVE `nginx/1.18.0`

CORRECTIF RAPIDE **Inclus dans le correctif rapide**

Cookie « shop_session » sans SameSite

FAIBLE

Sans attribut SameSite, la protection contre les requêtes intersites (CSRF) dépend du comportement par défaut du navigateur.

CORRECTIF Définir `SameSite=Lax` (ou `Strict`).

PREUVE `shop_session`

CORRECTIF RAPIDE **Inclus dans le correctif rapide**

X-Content-Type-Options absent

FAIBLE

Les navigateurs peuvent deviner le type de contenu ; des fichiers téléversés ou tiers risquent alors d'être exécutés comme script.

CORRECTIF Envoyer `X-Content-Type-Options: nosniff`.

CORRECTIF RAPIDE **Inclus dans le correctif rapide**

Pas d'enregistrement DMARC pour beispiel-shop.example

FAIBLE

Les serveurs destinataires ne savent pas comment traiter les e-mails falsifiés à votre nom ; l'hameçonnage avec votre domaine passe plus facilement inaperçu.

CORRECTIF Publier un enregistrement TXT `_dmarc.beispiel-shop.example` avec `v=DMARC1; p=quarantine; rua=mailto:…`.

PREUVE `beispiel-shop.example`

CORRECTIF RAPIDE **Inclus dans le correctif rapide**

Pas de contact sécurité (security.txt)

REMARQUE

Qui découvre une vulnérabilité ne sait pas où la signaler. Le Cyber Resilience Act impose ce canal de signalement aux fabricants de produits numériques.

CORRECTIF Publier `/.well-known/security.txt` avec `Contact:` et `Expires:` (RFC 9116).

CORRECTIF RAPIDE **Inclus dans le correctif rapide**

Agir immédiatement

Les fichiers internes accessibles publiquement ne relèvent pas du correctif rapide : les bloquer ne suffit pas, tous les identifiants qu'ils contiennent doivent être considérés comme connus et remplacés. Nous intervenons le même jour ouvré – contactez-nous.

Nous corrigeons cela pour vous

8 des 9 constats de ce test peuvent être corrigés par configuration. Nous nous en chargeons avec le correctif rapide : jusqu'à 6 constats sur ce domaine, nouveau test et nouvelle note inclus.

Prix forfaitaire 390 € HT (TVA en sus), chaque constat supplémentaire 60 €. Réservé aux professionnels. Si vous commandez un audit d'application, de code ou complet dans les 30 jours suivant la date de facture, nous en déduisons l'intégralité des 390 €.

CE DONT NOUS AVONS BESOIN DE VOTRE PART

- → Un accès à l'hébergement, au CDN ou au serveur web (par exemple Vercel, Cloudflare, nginx) – ou un accès en écriture au dépôt si la configuration s'y trouve.
- → Un accès à la gestion DNS et la liste de tous les services qui envoient des e-mails en votre nom (bureautique, newsletter, CRM, boutique).
- → Une adresse de contact pour les signalements de sécurité.
- → Une autorisation écrite pour les modifications. Le résultat ne porte que sur la configuration visible de l'extérieur.

Répondez simplement à notre e-mail.

Comment menons-nous nos audits de sécurité ?

Quatre niveaux, chacun s'appuyant sur le précédent : outils, agents IA en parallèle et contre-vérification de chaque constat. En savoir plus : audit.viewconic.de/fr/methodologie/

QU'EST-CE QUI EST VÉRIFIÉ ?	CE RAPPORT TEST DE SÉCURITÉ	AUDIT D'APPLICATION	RECOMMANDÉ AUDIT DE CODE	AUDIT COMPLET
Chiffrement, en-têtes de sécurité, DNS e-mail	●	●	◐	●
Fichiers exposés et versions	●	●	◐	●
Connexion, sessions et limites de débit	–	●	●	●
Droits d'accès : A voit-il les données de B ?	–	●	●	●
Injection et API non protégées	–	●	●	●
Secrets et clés dans le code	–	–	●	●
Dépendances avec CVE connues	◐	–	●	●
Qualité du code, supply chain, CI/CD	–	–	●	●
Constats du code démontrés dans l'application	–	–	–	●
PRIX	gratuit	490 €	890 €	1 690 €
LIVRAISON	2 heures	3 jours ouvrés	5 jours ouvrés	10 jours ouvrés
		Détails →	Réserver →	Détails →

● vérifié · ◐ en partie · – non vérifié · prix HT

PROCHAINES ÉTAPES

NOTRE RECOMMANDATION POUR BEISPIEL-SHOP.EXAMPLE

Audit de code

Un fichier au contenu vraisemblablement confidentiel est accessible depuis l'extérieur. L'audit de code détermine quels identifiants sont concernés et à quels autres endroits du code ils figurent – en 24 heures avec l'option Express.

890 € HT · rapport en 5 jours ouvrés

Réserver l'audit de code →

Ce que couvre l'audit de code

1
Choisir une offre
En ligne ou en répondant à notre e-mail.

2
Remettre les accès
En toute sécurité, via un lien personnel.

3
Recevoir le rapport
Avec plan d'action, et restitution sur demande.

Des questions ?

Nous examinons volontiers votre résultat avec vous.

Prendre rendez-vous →

NOTRE MÉTHODE

Passive, comme un navigateur : TLS, page d'accueil, chemins de fichiers connus, DNS. Ni connexion, ni formulaire, ni attaque. Versions comparées à endoflife.date et OSV (produit et version uniquement).

Notre propre évaluation de la configuration visible de l'extérieur, pas de l'application dans son ensemble. 100 points moins une déduction par constat (élevé 35, moyen 12, faible 4) ; critique donne F, élevé au mieux D. A très bon, B bon, C/D actions requises, E/F insuffisant.

Ni ce test ni nos audits ne remplacent un test d'intrusion manuel. Prestataire et cocontractant : Viewconic GmbH.

Viewconic GmbH
Ammerseestr. 23
82131 Gauting

d.kreutzer@viewconic.de
www.viewconic.de

AG München, HRB 257528
N° TVA DE331830665
Gérant : David Kreutzer