



RAPPORT D'EXEMPLE · DONNÉES FICTIVES

Constats illustratifs sur example.com. Ce document ne décrit ni un scan réel ni un incident de sécurité réel.

ÉVALUATION AUTOMATISÉE

Rapport de sécurité

Application web

example.com



Date du scan	Mode
2026-10-29	Comprehensive

Synthèse

2 résultats de gravité critique ou élevée.

<div>5</div> <div>résultats établis</div> <div>3 confirmés · 2 observés</div>	<div>62/100</div> <div>Score de sécurité</div>
---	--

Répartition par gravité

<div>1</div> <div>Critique</div>	<div>1</div> <div>Élevée</div>	<div>1</div> <div>Moyenne</div>	<div>1</div> <div>Faible</div>	<div>1</div> <div>Informative</div>
----------------------------------	--------------------------------	---------------------------------	--------------------------------	-------------------------------------

1 — Vulnérabilités potentielles — à vérifier
1 signalement à examiner, hors totaux par gravité et score de sécurité.
[Consulter les descriptions, les localisations et les éléments observés](#)

Priorités de traitement

- 01

Sauvegarde de données utilisateurs exposée
Confirmée · Critique
- 02

Exécution de JavaScript dans le formulaire de recherche
Confirmée · Élevée

Consultez les preuves et les recommandations de chaque fiche.

Couverture et limites
2 limites de couverture — Erreur réseau : 1 · Scan réalisé sans identifiants : 1
Le périmètre et les limites sont détaillés dans les pages suivantes. Le score ne garantit pas la sécurité de l'application.

Contexte de l'évaluation

RedSparta — sample report

Ce rapport couvre une évaluation de sécurité automatisée de <https://example.com>, exécutée en mode comprehensive le 2026-10-29.

5 vulnérabilité(s) vérifiée(s) retenue(s), dont 2 à traiter en priorité (critique ou élevée).

1 signalement(s) de vulnérabilité potentielle restent à vérifier et sont détaillés dans une section dédiée, hors totaux par gravité et score de sécurité.

À traiter en premier : Sauvegarde de données utilisateurs exposée · Exécution de JavaScript dans le formulaire de recherche.

Niveau de confirmation : 3 confirmée(s) (exploit reproduit), 2 observée(s) (comportement constaté directement), 1 non concluante(s) (pas de preuve rejouable — des pistes à trier, pas des exploits confirmés).

Ce que ce scan n'a pas pu tester

2 limites de couverture — Erreur réseau (1) · Scan réalisé sans identifiants (1)

- **Cible injoignable au niveau réseau** — 1 occurrence
<https://example.com/legacy>
- **Scan sans identifiants : la surface derrière la connexion n'a pas été testée** — 1 occurrence

Vue d'ensemble des résultats

#	Intitulé	Gravité	CVSS	CWE	OWASP	Niveau de confirmation
1	Sauvegarde de données utilisateurs exposée Vulnérabilités confirmées	Critique	9.1	CWE-530	A05:2021	Confirmée
2	Exécution de JavaScript dans le formulaire de recherche Vulnérabilités confirmées	Élevée	—	CWE-79	A03:2021	Confirmée
3	Redirection vers une destination externe non contrôlée Vulnérabilités confirmées	Moyenne	—	CWE-601	A01:2021	Confirmée
4	Politique Content-Security-Policy absente Observations et durcissement	Faible	—	CWE-693	A05:2021	Observée
5	Identification du serveur dans un en-tête HTTP Observations et durcissement	Informative	—	CWE-200	A05:2021	Observée



Détail des vulnérabilités · FICHE 01

Vulnérabilités confirmées

Sauvegarde de données utilisateurs exposée

Critique

Confirmée

Ouvert

CVSS 9.1 CWE-530 OWASP A05:2021

Ressource concernée

<https://example.com/backups/users.json>

Détectée le

2026-10-29

Constat et impact

Une sauvegarde JSON est accessible sans authentification. Dans cet exemple fictif, elle contient des données utilisateurs et un jeton API. Le contrôle comparatif renvoie une page introuvable, ce qui distingue le fichier exposé d’une réponse générique.

Les données exposées peuvent faciliter la réutilisation de secrets et des attaques sur les comptes concernés.

Preuve observée

Extraits des éléments observés · données sensibles masquées

```
GET /backups/users.json (anonyme)
HTTP/1.1 200
Content-Type: application/json

{
  "api_token": "[REDACTED]",
  "users": [{ "email": "[REDACTED]" }]
}

Contrôle : /backups/nonexistent-control.json -> 404
```

Niveau de confirmation : Confirmée · Rejeu probant

Correction recommandée

Remédiation

01

Supprimer l'accès public

Retirer les exports de la racine web et bloquer /backups/.

02

Sécuriser le stockage

Conserver les sauvegardes dans un espace à accès restreint.

03

Renouveler les secrets exposés

Révoquer le jeton et examiner les accès aux comptes concernés.

Vérification après correction

Appliquez la correction, puis lancez un retest et examinez les nouvelles preuves. Une modification n’est considérée comme corrigée qu’après vérification.



FICHE 02

Vulnérabilités confirmées

Exécution de JavaScript dans le formulaire de recherche

Élevée

Confirmée

Ouvert

CWE-79 OWASP A03:2021

Ressource concernée

<https://example.com/search?q=demo-marker>

Détectée le

2026-10-29

Constat et impact

La valeur du paramètre q est réinjectée dans la page sans encodage adapté. Dans le scénario de démonstration, un marqueur JavaScript inoffensif s'exécute dans le navigateur lors du rejeu.

Un lien préparé pourrait exécuter du code dans le contexte du navigateur de la victime. Aucun accès à un compte réel n'est illustré ici.

Preuve observée

Extraits des éléments observés · données sensibles masquées

```
GET /search?q=[DEMONSTRATION INPUT]
Rejeu navigateur : marqueur rs-demo-xss exécuté
Second rejeu : même marqueur exécuté
Contrôle en texte brut : aucune exécution de script
```

Niveau de confirmation : Confirmée · Rejeu probant

Correction recommandée

Remédiation

- 01 Encoder les valeurs selon leur contexte HTML.
- 02 Supprimer les insertions HTML non nécessaires et utiliser des API de texte.
- 03 Ajouter une politique CSP adaptée en défense complémentaire.

Vérification après correction

Appliquez la correction, puis lancez un retest et examinez les nouvelles preuves. Une modification n'est considérée comme corrigée qu'après vérification.



FICHE 03

Vulnérabilités confirmées

Redirection vers une destination externe non contrôlée

Moyenne

Confirmée

Ouvert

CWE-601 OWASP A01:2021

Ressource concernée

<https://example.com/redirect?next=https%3A%2F%2Fexample.org>

Détectée le

2026-10-29

Constat et impact

Le point d'entrée de redirection accepte une destination externe. La réponse de démonstration contient un en-tête Location vers le domaine réservé example.org, sans restriction d'origine.

Un lien utilisant le domaine de confiance pourrait rediriger un visiteur vers une page trompeuse.

Preuve observée

Extraits des éléments observés · données sensibles masquées

```
GET /redirect?next=https%3A%2F%2Fexample.org
HTTP/1.1 302
Location: https://example.org

Contrôle : next=/account -> Location: /account
Aucune requête envoyée vers la destination externe.
```

Niveau de confirmation : Confirmée · Rejeu probant

Correction recommandée

Remédiation

- 01 Accepter uniquement des chemins relatifs ou une liste explicite de destinations.
- 02 Rejeter les origines externes après normalisation de l'URL.
- 03 Tester les variantes encodées et les URL relatives au protocole.

Vérification après correction

Appliquez la correction, puis lancez un retest et examinez les nouvelles preuves. Une modification n'est considérée comme corrigée qu'après vérification.



FICHE 04

Observations et durcissement

Politique Content-Security-Policy absente

Faible

Observée

Ouvert

CWE-693 OWASP A05:2021

Ressource concernée

<https://example.com/>

Détectée le

2026-10-29

Constat et impact

Les réponses HTML contrôlées ne portent pas d'en-tête Content-Security-Policy. Cette observation décrit une mesure de durcissement absente ; elle ne démontre pas à elle seule une exécution de code.

Une politique CSP peut limiter certaines conséquences d'une injection de contenu. Elle complète les corrections applicatives.

Preuve observée

Extraits des éléments observés · données sensibles masquées

```
GET / -> 200 text/html
Content-Security-Policy: absent
```

```
GET /contact -> 200 text/html
Content-Security-Policy: absent
```

Niveau de confirmation : Observée · Observation HTTP

Correction recommandée

Remédiation

- 01 Recenser les sources de scripts et de styles nécessaires.
- 02 Déployer une politique en mode Report-Only et examiner les violations.
- 03 Activer progressivement la politique validée.

Vérification après correction

Appliquez la correction, puis lancez un retest et examinez les nouvelles preuves. Une modification n'est considérée comme corrigée qu'après vérification.



FICHE 05

Observations et durcissement

Identification du serveur dans un en-tête HTTP

Informative

Observée

Ouvert

CWE-200 OWASP A05:2021

Ressource concernée

https://example.com/

Détectée le

2026-10-29

Constat et impact

Une réponse publique révèle le nom du serveur web. Le nom du logiciel ne prouve ni une version vulnérable ni une exploitation possible.

Cette information peut faciliter la reconnaissance technique. Sa suppression reste une mesure de durcissement.

Preuve observée

Extraits des éléments observés · données sensibles masquées

```
GET /  
HTTP/1.1 200  
Server: nginx
```

Niveau de confirmation : Observée · Observation HTTP

Correction recommandée

Remédiation

- 01 Réduire les informations techniques renvoyées par le serveur.
- 02 Vérifier la configuration du reverse proxy.
- 03 Maintenir les composants à jour, indépendamment des en-têtes exposés.

Vérification après correction

Appliquez la correction, puis lancez un retest et examinez les nouvelles preuves. Une modification n'est considérée comme corrigée qu'après vérification.



FICHE 06

Vulnérabilités potentielles — à vérifier · Le moteur n’a pu ni confirmer ni écarter ces résultats. Leurs descriptions, localisations et éléments observés sont conservés pour permettre une vérification complémentaire. Ils restent exclus des totaux par gravité et du score de sécurité.

Contrôle d’accès à examiner sur les exports

Elevée

Non concluante

Ouvert

CWE-639 OWASP A01:2021

Ressource concernée
https://example.com/exports/42

Détectée le
2026-10-29

Constat et impact

Deux références d’export produisent des réponses différentes. Faute de second compte de test, il n’a pas été possible de vérifier si un utilisateur pouvait accéder à l’export d’un autre utilisateur.

Une exposition entre comptes reste une hypothèse à vérifier. Aucune donnée d’un autre utilisateur n’a été obtenue dans cet exemple.

Preuve observée

Extraits des éléments observés · données sensibles masquées

GET /exports/42 -> 403
GET /exports/43 -> 404

Ces réponses différentes ne prouvent pas un accès non autorisé.
Comparaison avec un second compte : non effectuée.

Niveau de confirmation : Non concluante · Comparaison incomplète · Non vérifié

Pourquoi la vérification reste non concluante
Les éléments disponibles ne suffisent pas à démontrer l’exploitation signalée.

Correction recommandée

Remédiation

- 01 Préparer deux comptes de test avec des droits distincts.
- 02 Contrôler côté serveur la propriété de chaque export.
- 03 Rejouer le scénario avec les deux sessions et comparer les résultats.

Vérification après correction
Appliquez la correction, puis lancez un retest et examinez les nouvelles preuves. Une modification n’est considérée comme corrigée qu’après vérification.