GALAXEOS

RAPPORT POUR

Bilan de sécurité de votre domaine

exemple-sa.ch

Date de l'analyse : 20.11.2026 10:30 (Europe/Zurich)



NOTE GLOBALE

Niveau correct, mais plusieurs points méritent votre attention prochainement.

Synthèse

DOMAINE VÉRIFIÉ	NOTE	POINTS À CORRIGER
Certificat du site	A	0
Chiffrement des connexions (TLS)	C	1
Connexion sécurisée (HTTPS)	B	1
En-têtes de sécurité et informations exposées	D	4
Sécurité des e-mails	D	3
Configuration DNS	C	2
Réputation (listes noires)	A	0
Fichiers sensibles exposés	D	1

Constats par gravité

0	2	6	4	2	10
CRITIQUE	ÉLEVÉ	MOYEN	FAIBLE	INFO	OK

Les 3 priorités

1. ÉLEVÉ **Aucune politique DMARC** · Sécurité des e-mails
Comment corriger : Publiez _dmarc.exemple-sa.ch : « v=DMARC1; p=none; rua=mailto:… », puis passez à quarantine/reject.

2. ÉLEVÉ **Fichier sensible accessible : /.git/HEAD** · Fichiers sensibles exposés
Comment corriger : Supprimez le fichier du serveur ou bloquez son accès, puis changez les mots de passe concernés.

3. MOYEN **Anciennes versions TLS 1.0/1.1 encore acceptées** · Chiffrement des connexions (TLS)
Comment corriger : Désactivez TLS 1.0 et 1.1 ; gardez TLS 1.2 et 1.3.

A Certificat du site

Le certificat prouve à vos visiteurs qu'ils sont bien sur votre site. S'il expire ou est mal configuré, les navigateurs affichent une alerte qui fait fuir les clients.

Ce qui est en ordre

- ✓ Certificat valide et reconnu `issuer=R11 (Let's Encrypt) · cert_valid`
- ✓ Expiration lointaine `expires in 74 days · cert_expiry_ok`
- ✓ Clé de chiffrement robuste `EC 256 bits · cert_key`

C Chiffrement des connexions (TLS)

Le chiffrement protège les données échangées entre vos visiteurs et votre site. Les anciennes versions ont des failles connues et devraient être désactivées.

Points d'attention

MOYEN **Anciennes versions TLS 1.0/1.1 encore acceptées**

Ces versions ont des faiblesses connues et ne sont plus acceptées par les navigateurs récents.

Comment corriger : Désactivez TLS 1.0 et 1.1 ; gardez TLS 1.2 et 1.3.

```
Constat technique : TLSv1.0, TLSv1.1 accepted
id: tls_legacy
```

Ce qui est en ordre

- ✓ Méthodes de chiffrement solides `AEAD + PFS · tls_ciphers_ok`
- ✓ TLS 1.3 disponible `TLSv1.3 · tls_versions_ok`

B Connexion sécurisée (HTTPS)

Ces réglages obligent les navigateurs à toujours utiliser la connexion sécurisée. Ils évitent qu'un visiteur soit piégé sur une version non chiffrée de votre site.

Points d'attention

FAIBLE **Protection HSTS de courte durée**

Le navigateur n'est obligé d'utiliser HTTPS que pendant une courte période.

Comment corriger : Augmentez max-age à au moins 6 mois (15552000).

```
Constat technique : max-age=86400
id: hsts_short
```

Ce qui est en ordre

✓ Redirection automatique vers HTTPS `http://exemple-sa.ch/ -> 301 https://exemple-sa.ch/ · https_redirect`

D En-têtes de sécurité et informations exposées

Ces réglages discrets du serveur indiquent au navigateur comment protéger vos visiteurs. Ils évitent aussi de dévoiler des informations utiles à un attaquant.

Points d'attention

MOYEN **Le site peut être intégré dans une autre page**

Un site malveillant pourrait afficher le vôtre de façon invisible pour piéger vos visiteurs.

Comment corriger : Ajoutez « frame-ancestors 'self' » à la CSP ou X-Frame-Options: SAMEORIGIN.

```
Constat technique : no XFO, no CSP
id: clickjacking
```

MOYEN **Version exacte du CMS visible**

Une version visible permet de chercher facilement des failles connues.

Comment corriger : Mettez WordPress à jour et masquez le générateur.

```
Constat technique : meta generator: WordPress 6.2.1
id: cms_version
```

MOYEN **Cookies sans protections**

Certains cookies peuvent être lus par des scripts ou envoyés sans chiffrement.

Comment corriger : Ajoutez Secure, HttpOnly et SameSite aux cookies.

```
Constat technique : PHPSESSID: missing Secure, HttpOnly
id: cookie_flags
```

FAIBLE **Pas de fichier security.txt**

Personne ne sait comment vous signaler un problème de sécurité.

Comment corriger : Publiez /.well-known/security.txt avec une adresse de contact.

```
Constat technique : 404
id: securitytxt_missing
```

D Sécurité des e-mails

Ces enregistrements empêchent des inconnus d'envoyer des e-mails en votre nom. Sans eux, vos clients peuvent recevoir de fausses factures qui semblent venir de vous.

Points d'attention

ÉLEVÉ **Aucune politique DMARC**

Sans DMARC, les faux e-mails à votre nom (hameçonnage) ne sont pas bloqués et vous n'en êtes pas informé.

Comment corriger : Publiez _dmarc.exemple-sa.ch : « v=DMARC1; p=none; rua=mailto:… », puis passez à quarantine/reject.

```
Constat technique : _dmarc.exemple-sa.ch: NXDOMAIN
id: dmarc_missing
```

MOYEN **Règle SPF trop permissive**

La règle se termine par « ?all » : n'importe qui peut envoyer des e-mails en votre nom.

Comment corriger : Terminez l'enregistrement SPF par « -all » ou « ~all ».

```
Constat technique : v=spf1 include:_spf.mail-exemple.net ?all
id: spf_neutral
```

FAIBLE **Pas de MTA-STS**

Le chiffrement des e-mails entrants n'est pas imposé.

Comment corriger : Publiez une politique MTA-STS.

```
Constat technique : _mta-sts: none
id: mtasts_missing
```

Ce qui est en ordre

✓ Serveurs de messagerie trouvés `10 mx1.mail-exemple.net · mx_ok`

NON VÉRIFIÉ **Signature DKIM non trouvée**

Aucun sélecteur courant trouvé ; DKIM peut exister sous un autre nom.

```
id: dkim_unknown · selectors tried: 12
```

NON VÉRIFIÉ **Chiffrement du serveur e-mail non testé**

Le port 25 n'a pas pu être joint depuis notre réseau ; cela ne signifie pas un défaut.

```
id: starttls_untested · mx1.mail-exemple.net:25 timeout
```

C Configuration DNS

Le DNS est l'annuaire qui relie votre nom de domaine à vos serveurs. Le protéger évite qu'on détourne vos visiteurs ou vos e-mails.

Points d'attention

MOYEN **DNSSEC non activé**

Les réponses DNS ne sont pas signées et pourraient être falsifiées.

Comment corriger : Activez DNSSEC chez votre registraire / hébergeur DNS.

```
Constat technique : no DS record
id: dnssec_missing
```

FAIBLE **Pas d'enregistrement CAA**

N'importe quelle autorité peut émettre un certificat pour votre domaine.

Comment corriger : Ajoutez un enregistrement CAA pour votre autorité de certification.

```
Constat technique : CAA: none
id: caa_missing
```

Ce qui est en ordre

✓ Serveurs DNS redondants `ns1.dns-exemple.net, ns2.dns-exemple.net · ns_ok`

A Réputation (listes noires)

Nous vérifions que votre domaine et votre serveur ne figurent pas sur des listes noires. Une inscription peut bloquer vos e-mails et faire fuir vos visiteurs.

Ce qui est en ordre

- ✓ Domaine absent des listes noires `Spamhaus DBL · dbl_clean`
- ✓ Adresse du serveur absente des listes noires `Spamhaus ZEN 192.0.2.10 · zen_clean`

D Fichiers sensibles exposés

Nous cherchons quelques fichiers sensibles oubliés sur le serveur (sauvegardes, configuration). Ils peuvent révéler des mots de passe ou des données clients.

Points d'attention

ÉLEVÉ **Fichier sensible accessible : /.git/HEAD**

N'importe qui peut télécharger ce fichier ; il peut contenir des mots de passe, du code ou des données.

Comment corriger : Supprimez le fichier du serveur ou bloquez son accès, puis changez les mots de passe concernés.

```
Constat technique : /.git/HEAD
id: exposed__git_HEAD
```

Ce que nous n'avons pas pu vérifier

Par honnêteté, voici les points qui n'ont pas été testés ou dont le résultat est incertain. Ils ne sont pas comptés dans la note.

NON VÉRIFIÉ **Signature DKIM non trouvée** · Sécurité des e-mails
Aucun sélecteur courant trouvé ; DKIM peut exister sous un autre nom.
`selectors tried: 12`

NON VÉRIFIÉ **Chiffrement du serveur e-mail non testé** · Sécurité des e-mails
Le port 25 n'a pas pu être joint depuis notre réseau ; cela ne signifie pas un défaut.
`mx1.mail-exemple.net:25 timeout`

Ce que Galaxeos peut faire pour vous

Nous traduisons ce rapport en actions concrètes, à votre rythme et sans jargon.

Galaxeos Orbit — informatique gérée

Nous surveillons et entretenons votre domaine, votre site et vos e-mails en continu : certificats, mises à jour, réglages de sécurité, alertes. Idéal pour : **Chiffrement des connexions (TLS), Connexion sécurisée (HTTPS), En-têtes de sécurité et informations exposées**.

Galaxeos Launch — projet ponctuel

Une intervention unique, au prix convenu d'avance, pour corriger les points de ce rapport. Idéal pour : **Chiffrement des connexions (TLS), En-têtes de sécurité et informations exposées, Sécurité des e-mails, Configuration DNS, Fichiers sensibles exposés**.

Contact

Galaxeos SàRL · Gland
info@galaxeos.net · +41 21 552 24 05
https://galaxeos.net/contact/

Planifier un appel →

À propos de ce rapport. Ce bilan est une vérification passive, à un instant donné, des informations visibles publiquement sur votre domaine (site web, DNS, e-mail). Ce n'est pas un test d'intrusion. Il ne garantit pas l'absence d'autres failles et ne remplace pas un audit complet. Les résultats peuvent évoluer dès qu'un réglage change. (scanner v0.3.0)