GALAXEOS

REPORT FOR

Security check of your domain

exemple-sa.ch

Scan date : 20 November 2026, 10:30 (Europe/Zurich)



OVERALL GRADE

Fair, but several items deserve your attention soon.

Summary

AREA CHECKED	GRADE	ITEMS TO FIX
Website certificate	A	0
Connection encryption (TLS)	C	1
Secure connection (HTTPS)	B	1
Security headers and exposed information	D	4
E-mail security	D	3
DNS configuration	C	2
Reputation (blocklists)	A	0
Exposed sensitive files	D	1

Findings by severity

0	2	6	4	2	10
CRITICAL	HIGH	MEDIUM	LOW	INFO	OK

Top 3 priorities

1. HIGH **No DMARC policy** · E-mail security
How to fix : Publish _dmarc.exemple-sa.ch: "v=DMARC1; p=none; rua=mailto:...", then move to quarantine/reject.

2. HIGH **Sensitive file accessible: /.git/HEAD** · Exposed sensitive files
How to fix : Remove the file from the server or block access to it, then change any affected passwords.

3. MEDIUM **Old TLS 1.0/1.1 still accepted** · Connection encryption (TLS)
How to fix : Disable TLS 1.0 and 1.1; keep TLS 1.2 and 1.3.

A Website certificate

The certificate proves to visitors that they really are on your website. If it expires or is misconfigured, browsers show a warning that drives customers away.

What is in order

- ✓ Valid, trusted certificate `issuer=R11 (Let's Encrypt) · cert_valid`
- ✓ Expiry is far away `expires in 74 days · cert_expiry_ok`
- ✓ Strong encryption key `EC 256 bits · cert_key`

C Connection encryption (TLS)

Encryption protects data exchanged between your visitors and your website. Old versions have known flaws and should be switched off.

Points of attention

MEDIUM **Old TLS 1.0/1.1 still accepted**

These versions have known weaknesses and are no longer accepted by modern browsers.

How to fix : Disable TLS 1.0 and 1.1; keep TLS 1.2 and 1.3.

```
Technical evidence : TLSv1.0, TLSv1.1 accepted
id: tls_legacy
```

What is in order

- ✓ Strong encryption methods `AEAD + PFS · tls_ciphers_ok`
- ✓ TLS 1.3 available `TLSv1.3 · tls_versions_ok`

B Secure connection (HTTPS)

These settings force browsers to always use the secure connection. They prevent visitors from being trapped on an unencrypted version of your site.

Points of attention

LOW **Short HSTS protection**

Browsers are only forced to use HTTPS for a short period.

How to fix : Raise max-age to at least 6 months (15552000).

```
Technical evidence : max-age=86400
id: hsts_short
```

What is in order

✓ Automatic redirect to HTTPS `http://exemple-sa.ch/ -> 301 https://exemple-sa.ch/ · https_redirect`

D Security headers and exposed information

These discreet server settings tell browsers how to protect your visitors. They also avoid revealing details that help an attacker.

Points of attention

MEDIUM **The site can be embedded in another page**
A malicious site could show yours invisibly to trick your visitors.

How to fix : Add "frame-ancestors 'self'" to the CSP or X-Frame-Options: SAMEORIGIN.

```
Technical evidence : no XFO, no CSP
id: clickjacking
```

MEDIUM **Exact CMS version visible**
A visible version makes it easy to look up known flaws.

How to fix : Update WordPress and hide the generator tag.

```
Technical evidence : meta generator: WordPress 6.2.1
id: cms_version
```

MEDIUM **Cookies without protections**
Some cookies can be read by scripts or sent unencrypted.

How to fix : Add Secure, HttpOnly and SameSite to cookies.

```
Technical evidence : PHPSESSID: missing Secure, HttpOnly
id: cookie_flags
```

LOW **No security.txt file**
Nobody knows how to report a security problem to you.

How to fix : Publish /.well-known/security.txt with a contact address.

```
Technical evidence : 404
id: securitytxt_missing
```

D E-mail security

These records stop strangers from sending e-mail in your name. Without them, your customers may receive fake invoices that seem to come from you.

Points of attention

HIGH **No DMARC policy**
Without DMARC, fake e-mails in your name (phishing) are not blocked and you are not told about them.

How to fix : Publish _dmarc.exemple-sa.ch: "v=DMARC1; p=none; rua=mailto:...", then move to quarantine/reject.

```
Technical evidence : _dmarc.exemple-sa.ch: NXDOMAIN
id: dmarc_missing
```

MEDIUM **SPF rule too permissive**
The rule ends with "?all": anyone can send e-mail in your name.

How to fix : End the SPF record with "-all" or "~all".

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

LOW **No MTA-STS**
Encryption of incoming e-mail is not enforced.

How to fix : Publish an MTA-STS policy.

```
Technical evidence : _mta-sts: none
id: mtasts_missing
```

What is in order

✓ Mail servers found `10 mx1.mail-exemple.net · mx_ok`

NOT CHECKED **DKIM signature not found**
No common selector found; DKIM may exist under another name.
`id: dkim_unknown · selectors tried: 12`

NOT CHECKED **Mail server encryption not tested**
Port 25 could not be reached from our network; this does not indicate a flaw.
`id: starttls_untested · mx1.mail-exemple.net:25 timeout`

C DNS configuration

DNS is the directory linking your domain name to your servers. Protecting it prevents your visitors or e-mail from being diverted.

Points of attention

MEDIUM **DNSSEC not enabled**

DNS answers are not signed and could be forged.

How to fix : Enable DNSSEC at your registrar / DNS host.

```
Technical evidence : no DS record
id: dnssec_missing
```

LOW **No CAA record**

Any authority can issue a certificate for your domain.

How to fix : Add a CAA record for your certificate authority.

```
Technical evidence : CAA: none
id: caa_missing
```

What is in order

✓ Redundant DNS servers `ns1.dns-exemple.net, ns2.dns-exemple.net · ns_ok`

A Reputation (blocklists)

We check that your domain and server are not on blocklists. A listing can block your e-mail and scare visitors away.

What is in order

- ✓ Domain not on blocklists `Spamhaus DBL · dbl_clean`
- ✓ Server address not on blocklists `Spamhaus ZEN 192.0.2.10 · zen_clean`

D Exposed sensitive files

We look for a few sensitive files left on the server (backups, configuration). They can reveal passwords or customer data.

Points of attention

HIGH **Sensitive file accessible: /.git/HEAD**

Anyone can download this file; it may contain passwords, code or data.

How to fix : Remove the file from the server or block access to it, then change any affected passwords.

```
Technical evidence : /.git/HEAD
id: exposed__git_HEAD
```

What we could not check

To be transparent, these items were not tested or gave an uncertain result. They do not count towards the grade.

NOT CHECKED **DKIM signature not found** · E-mail security
No common selector found; DKIM may exist under another name.
`selectors tried: 12`

NOT CHECKED **Mail server encryption not tested** · E-mail security
Port 25 could not be reached from our network; this does not indicate a flaw.
`mx1.mail-exemple.net:25 timeout`

What Galaxeos can do for you

We turn this report into concrete actions, at your pace and without jargon.

Galaxeos Orbit — managed IT

We continuously monitor and maintain your domain, website and e-mail: certificates, updates, security settings and alerts. Best for: **Connection encryption (TLS), Secure connection (HTTPS), Security headers and exposed information**.

Galaxeos Launch — one-off project

A single engagement at a price agreed up front to fix the items in this report. Best for: **Connection encryption (TLS), Security headers and exposed information, E-mail security, DNS configuration, Exposed sensitive files**.

Contact

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

Book a call →

About this report. This report is a passive, point-in-time check of information publicly visible about your domain (website, DNS, e-mail). It is not a penetration test. It does not guarantee that no other weaknesses exist and does not replace a full audit. Results may change as soon as a setting changes. (scanner v0.3.0)