majhenlabs

Security report

example-company.com

Date: 20 July 2026

Overview: 8 findings

2 high | 3 medium | 1 low | 2 info

Findings

A database or similar service is directly reachable from the internet

HIGH

`3306/tcp — MySQL`

These are services that hold data and are not meant for the public internet — the site reaches them from the inside, on the same server.

Why this is the most serious finding in this report: some of these services historically have NO password until someone explicitly sets one (Redis, MongoDB, Elasticsearch, Memcached). Whoever finds them open can often read and delete them without a single password. The bots that hunt for them sweep the whole internet continuously — it isn't a question of whether they'll arrive, but when.

We only checked whether the port was open. We did not try to connect or read anything.

Fix:

Close them off from the internet. They should listen only on 127.0.0.1 (if they're on the same server as the site), or a firewall should allow access only from the IP address that needs them. MySQL: bind-address = 127.0.0.1. PostgreSQL: listen_addresses = 'localhost'. Redis/MongoDB: bind 127.0.0.1 and always a password.

If something here is public on purpose because it connects from another location — then it needs a firewall that admits only that address, and an encrypted connection. That's no longer a click in a panel.

Plugin Contact Form 7 5.7.1 — Contact Form 7 < 5.8.2 — Authenticated (Editor+) Arbitrary File Upload

HIGH

CVE-2023-6449 · CVSS 8.8

The Contact Form 7 plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in versions up to, and including, 5.8.1. This makes it possible for authenticated attackers, with editor-level access and above, to upload arbitrary files on the affected site's server, which may make remote code execution possible.

Weakness type: Unrestricted Upload of File with Dangerous Type.

Fix:

Update Contact Form 7 to version 5.8.2 or later. In wp-admin: Plugins → Installed Plugins → find Contact Form 7 → Update. Before updating, back up your database and files. After updating, open the home page and one sub-page to check that nothing broke.

The domain has no DMARC record — anyone can send mail in your name

MEDIUM

DMARC tells the recipient's server what to do with mail that claims to come from your domain but fails the check. Without it, that decision is left to the recipient and most often means: let it through.

In practice: someone puts your address as the sender and emails an invoice to your customer with their own bank details. The mail looks like yours because it SAYS it's yours. No breach of the site is needed — it's enough that the domain has no DMARC.

A limitation, to avoid misunderstanding: DMARC protects YOUR domain from forgery. It doesn't stop mail sent from someone else's address where only the display name reads as yours, and it doesn't protect against look-alike domains.

Fix:

Add a TXT record where your DNS is (usually at the domain registrar):

```
name: _dmarc.example-company.com
type: TXT
value: v=DMARC1; p=none; rua=mailto:postmaster@example-company.com
```

Do NOT jump straight to p=reject. The order is deliberate: start with p=none, read the rua reports for two to three weeks and find every legitimate sender, then move to p=quarantine, and finally p=reject. Whoever skips those steps and goes straight to p=reject shuts off their own outgoing invoices.

Plugin Elementor 3.18.0 — Elementor <= 3.18.1 — Authenticated (Contributor+) Stored Cross-Site Scripting

MEDIUM

CVE-2023-47505 · CVSS 6.4

The Elementor Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via uploaded SVG files in versions up to, and including, 3.18.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.

Weakness type: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

Fix:

Update Elementor to version 3.18.2 or later. In wp-admin: Plugins → Installed Plugins → find Elementor → Update. Before updating, back up your database and files.

Remote-access services are open to the internet

MEDIUM

```
21/tcp — FTP
```

FTP and Telnet transmit the username and password in readable form — anyone anywhere along the path can read them. RDP, VNC and SMB are favourite targets of automated password guessing, and occasionally have vulnerabilities that don't even need a password.

This isn't a finding that someone got in. The finding is that the door exists and anyone can try to open it, as many times as they like.

Fix:

Replace FTP with SFTP (it runs over SSH, port 22) — with most hosting that's already available and you just need to stop using the old FTP. Telnet has no justification in any scenario; turn it off. RDP and VNC should not be directly on the internet. The right approach is to allow them only through a VPN, or to let a firewall admit only the IP addresses you actually connect from.

No protection against embedding the page in someone else's frame (clickjacking)

LOW

Without this, anyone can load your page into an invisible frame on their own, cover it with their own content, and get a visitor to click something they think is theirs but is actually yours.

Exploitability is limited in practice and requires the user to visit the attacker's page. For a site with no login and no one-click actions, this is mostly theory — we list it because the fix is trivial.

Fix:

Add one of these to all responses:

```
X-Frame-Options: SAMEORIGIN
```

or, if you already use CSP: Content-Security-Policy: frame-ancestors 'self'. If you DO embed the site somewhere on purpose (for example a widget at a partner), replace 'self' with exactly that domain.

5 of 23 checked ports are open

INFO

```
21/tcp — FTP
80/tcp — HTTP
443/tcp — HTTPS
587/tcp — SMTP (submission)
3306/tcp — MySQL
```

We checked around twenty well-known ports, not all of them. An open port by itself is not a problem — SSH, SMTP and the like belong there.

An important limitation: we checked the IP the domain points to. If the site is behind a CDN or proxy, that's their server, not yours — in which case this list describes them.

Fix:

There's nothing to fix until the list is read. For each port, ask yourself whether it needs to be reachable by the whole internet or only by you.

No Content-Security-Policy header

INFO

CSP is a list of sources a page is allowed to load scripts and styles from. When it exists and is well written, it makes XSS harder to exploit.

This is NOT a vulnerability. A missing CSP doesn't mean the site has a hole — it means it's missing one layer of defence in depth. The vast majority of sites don't have it, which is why we list it as information, not a problem. If someone gives you an 'F' for this, they're selling you fear.

Fix:

For an existing site, CSP isn't written from memory: too strict a list breaks your own scripts, analytics and embeds, while too loose a one does nothing. The approach is to start with Content-Security-Policy-Report-Only, collect the reports, and only then switch on the real one. This is a job for a person and it isn't urgent.

Robert Majhen, MajhenLabs