B revobits.com

Protected, but with gaps worth closing

The site sends none of the standard browser protections.

External exposure check of revobits.com · 27 November 2026 · graded on severity, not on the number of findings

What needs attention

ISSUE

Your website skips standard free protections

Your site sends none of the standard instructions that tell browsers to protect your visitors. They cost nothing and defend against common attacks (technical names: HSTS, Content-Security-Policy, X-Content-Type-Options).

What to do: Add the standard security response headers to your web server configuration. They are free and take one change.

WARNING

Your server tells attackers what software it runs

It announces "Apache/2.4.52 (Ubuntu)" to everyone. Attackers use this to pick matching break-in tools. Hiding it is a quick fix.

What to do: Turn off the version number in your web server signature so it no longer advertises exactly what it runs.

What is already in order

✓ Sending email in your name is restricted · Impersonation of your company is blocked · Website encryption is valid · Visitors are moved to the encrypted site

This is a passive check: it reads public DNS records, the TLS certificate and the headers the site already sends to every visitor. Nothing was attacked and nothing was logged into. It describes the surface only — exposed services, breached staff accounts and web-application weaknesses need a full assessment.

Checked by **Storm Outpost** · stormoutpost.com/check/revobits-com-4cb643a2 · re-check any time to confirm a fix worked.