EXTERNAL VULNERABILITY ASSESSMENT · ESSENTIAL · TECHNOLOGY & CVE REPORT

Do you really know what powers your website?

aziendatest.example

SAMPLE · FICTITIOUS DATA

CLIENT	ASSESSMENT PERIOD	DELIVERED
Azienda Test (fictitious)	10 Nov 2026 → 12 Nov 2026	13 Nov 2026
SCOPE	**TIER**	**REPORT ID**
3 addresses	Essential	NT-SAMPLE-ESSENTIAL

FINDINGS BY SEVERITY · 7 IN TOTAL



1 critical **4** high **2** medium

SAMPLE

This is a sample with fictitious data. Your report will have the same structure, but it may be more or less detailed depending on what we find on your website.

01 Summary

12
technologies detected

7
outdated or unsupported

7
CVEs that may apply

The site uses several outdated components. The most urgent point is the contact form plugin, in a version with a known critical flaw. PHP and MySQL no longer get fixes from the vendor. The CVEs are inferred from the declared versions: confirm them with your provider, who sometimes applies fixes without changing the version number.

02 Technologies detected

CATEGORY	TECHNOLOGY	VERSION	STATUS	WHERE IT SHOWS
Web server	**nginx**	1.18.0	OUTDATED	Server header
Operating system	**Ubuntu**	22.04 LTS	SUPPORTED	SSH banner and headers
Language	**PHP**	7.4.33	UNSUPPORTED	X-Powered-By header
CMS	**WordPress**	6.1.1	OUTDATED	meta generator
Plugin	**Contact Form 7**	5.3.1	OUTDATED	plugin files (?ver=)
Plugin	**Yoast SEO**	20.1	OUTDATED	comment in the HTML code
JavaScript library	**jQuery**	1.12.4	OUTDATED	library file (?ver=)
Database	**MySQL**	8.0.28	UNSUPPORTED	port 3306
Remote access	**OpenSSH**	8.9p1	TO VERIFY	port 22
HTTPS certificate	**Let's Encrypt**	–	VALID	valid until 20 Jan 2027
Analytics	**Google Analytics 4**	–	EXTERNAL SERVICE	script in the page
Newsletter	**Mailchimp**	–	EXTERNAL SERVICE	sign-up form

03 Findings

Most severe first. “Potential” means inferred from the declared version, to be confirmed with your provider.

CRITICAL POTENTIAL Contact Form 7 5.3.1 F-01

The contact form runs a version with a known critical flaw

WHAT IT MEANS This version of the contact form plugin is one of those that allowed dangerous files to be uploaded to the site.

WHAT TO DO Update Contact Form 7 to the latest version from the WordPress dashboard. The flaw is fixed from 5.3.2 onwards.

CVE-2020-35489 · CVSS 10.0

SAMPLE · FICTITIOUS DA

HIGH OBSERVED PHP 7.4.33 F-02

PHP 7.4 has had no security updates since November 2022

WHAT IT MEANS The language the site runs on is no longer fixed: flaws found after 2022 stay open.

WHAT TO DO Ask your hosting provider to move to PHP 8.3 or 8.4, after a trial on the test site.

HIGH OBSERVED MySQL 8.0.28 F-03

MySQL 8.0 has had no updates since April 2026

WHAT IT MEANS The site's database runs a version the vendor no longer fixes.

WHAT TO DO Plan the move to MySQL 8.4, the long-term support version, with your provider.

HIGH POTENTIAL OpenSSH 8.9p1 (Ubuntu) F-04

OpenSSH declares a version affected by a known flaw

WHAT IT MEANS The server's remote access version is among the affected ones, unless the provider has applied the fix.

WHAT TO DO Ask your provider to update the server packages: Ubuntu has fixed the flaw on 22.04 too.

CVE-2024-6387 · CVSS 8.1

HIGH POTENTIAL nginx 1.18.0 (Ubuntu) F-05

nginx 1.18.0 falls within a known DNS resolver flaw

WHAT IT MEANS The web server version is affected only if it uses its built-in DNS resolution: this needs checking.

WHAT TO DO Update nginx with the distribution packages and check whether the configuration uses the resolver directive.

CVE-2021-23017 · CVSS 7.7

MEDIUM POTENTIAL WordPress 6.1.1 F-06

WordPress 6.1.1 is many versions behind

WHAT IT MEANS The software that runs the site is not up to date and includes at least one known flaw, fixed long ago.

WHAT TO DO Update WordPress to the latest version from the dashboard, after a backup and a trial on the test site.

CVE-2023-2745 · CVSS 6.1

MEDIUM POTENTIAL jQuery 1.12.4 F-07

The jQuery 1.12.4 library has three known flaws

WHAT IT MEANS A library used by the pages has known flaws that, in some cases, allow code to be injected into the page.

WHAT TO DO Update the theme and the plugins that load it: recent versions use jQuery 3.5 or later.

CVE-2019-11358 · CVSS 6.1 CVE-2020-11022 · CVSS 6.1 CVE-2020-11023 · CVSS 6.1

SAMPLE · FICTITIOUS D

04 Known flaws (CVE) that may apply

Inferred from the declared versions: these are not confirmed vulnerabilities. CVSS scores from NVD.

COMPONENT	CVE	CVSS	WHAT IT AFFECTS	FIXED IN
Contact Form 7 5.3.1	CVE-2020-35489	10.0	Upload of dangerous files through the form	5.3.2
OpenSSH 8.9p1 (Ubuntu)	CVE-2024-6387	8.1	Remote access without a password, under specific conditions	Ubuntu USN-6859-1
nginx 1.18.0	CVE-2021-23017	7.7	Memory error in the built-in DNS resolver	1.20.1
WordPress 6.1.1	CVE-2023-2745	6.1	Loading of arbitrary translation files	6.2.1
jQuery 1.12.4	CVE-2019-11358	6.1	Tampering with JavaScript objects (prototype pollution)	3.4.0
	CVE-2020-11022	6.1	Code execution from untrusted HTML	3.5.0
	CVE-2020-11023	6.1	Code execution from HTML with option elements	3.5.0

05 In brief

- Yoast SEO 20.1 is several versions behind: no known flaw is attributed to this version.

06 Scope, method and limits

Scope

- `aziendatest.example`
- `www.aziendatest.example`
- `staging.aziendatest.example`

Method

External “black box” assessment, from 10 Nov 2026 to 12 Nov 2026: only what is visible from the internet, with no credentials and non-destructive checks. No exploits, no load testing, no exposed file opened or downloaded.

Limits

- It does not guarantee that the site is secure, or that there will be no attacks in the future.
- It captures the site on the dates shown: an update or a new plugin changes the picture.
- It covers only the agreed scope: internal network, office computers and staff email stay out.
- It does not fix anything: you or your provider apply the fixes, following the report.

QUESTIONS ABOUT THE REPORT

For 14 calendar days you can email us at **reports@nulltrace.systems**. The first substantive reply comes within 3 business days.

This is a sample with fictitious data. Your report will have the same structure, but it may be more or less detailed depending on what we find on your website.

SAMPLE · FICTITIOUS DA