EXTERNAL VULNERABILITY ASSESSMENT · PRO · EXTERNAL SECURITY REVIEW

Is your website configured to protect your business?

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	Pro	NT-SAMPLE-PRO

FINDINGS BY SEVERITY · 9 IN TOTAL



1 critical **4** high **3** medium **1** low

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

9 findings

4 configuration areas checked

7 CVEs that may apply

The most urgent point is the contact form, in a version with a known critical flaw. On the configuration side, the database answers from the internet, encryption accepts retired versions and fake emails in the domain's name are not blocked. Almost everything is solved with updates and a few lines of configuration.

AREA	CRITICAL	HIGH	MEDIUM	LOW	INFO
Software and versions	1	3	1	—	—
HTTPS and encryption	—	—	1	—	—
Browser protections	—	—	—	1	—
DNS and email	—	—	1	—	—
Exposed services	—	1	—	—	—

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Web server	**nginx**	1.18.0	OUTDATED	Server header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CMS	**WordPress**	6.1.1	OUTDATED	meta generator
Plugin	**Contact Form 7**	5.3.1	OUTDATED	plugin files (?ver=)
Plugin	**Yoast SEO**	20.1	OUTDATED	comment in the HTML code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

SAMPLE · FICTITIOUS DATA

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

WHY IT MATTERS

The contact form is open to anyone. In this version a file with a crafted name could get past the checks and end up on the server.

FOR YOUR IT TEAM

Version 5.3.1 detected from the ver= parameter of the plugin files. CVE-2020-35489 (CVSS 10.0): unrestricted file upload, fixed in 5.3.2. The inference is based on the version: confirm on the server and update.

```
wp plugin update contact-form-7
wp plugin get contact-form-7--field=version
```

CVE-2020-35489 · CVSS 10.0

Evidence: GET /wp-content/plugins/contact-form-7/includes/js/index.js?ver=5.3.1 → 200

References: NVD CVE-2020-35489

HIGH OBSERVED MySQL 8.0.28 · port 3306 F-02

The MySQL database, no longer supported, answers from the internet

WHY IT MATTERS

The database holds the site's and the customers' data. Right now anyone can try to connect and guess passwords, and the version no longer gets fixes.

FOR YOUR IT TEAM

Port 3306/tcp open on 203.0.113.10, MySQL 8.0.28 (branch unsupported since 30 Apr 2026). Only the application needs it: bind it to localhost and plan the move to 8.4 LTS.

```
# /etc/mysql/mysql.conf.d/mysqld.cnf
bind-address = 127.0.0.1
# and in the firewall:
sudo ufw deny 3306/tcp
```

Evidence: 3306/tcp open mysql MySQL 8.0.28-0ubuntu0.22.04.1 **References:** dev.mysql.com: security guidelines

HIGH OBSERVED PHP 7.4.33 F-03

PHP 7.4 has had no security updates since November 2022

WHY IT MATTERS

Every PHP flaw found after November 2022 stays open for good on this version. It is a lock the manufacturer no longer replaces.

FOR YOUR IT TEAM

X-Powered-By header: PHP/7.4.33. The 7.4 branch has been unsupported since 28 Nov 2022. Plan the move to 8.3 or 8.4: check theme and plugins on staging, then update the PHP-FPM pool.

```
sudo apt install php8.3-fpm php8.3-mysql
# in the nginx server block:
fastcgi_pass unix:/run/php/php8.3-fpm.sock;
```

Evidence: x-powered-by: PHP/7.4.33 **References:** php.net/supported-versions

SAMPLE · FICTITIOUS DATA

HIGH POTENTIAL OpenSSH 8.9p1 (Ubuntu) F-04

OpenSSH declares a version affected by a known flaw

WHY IT MATTERS

SSH is the door administrators use to get into the server. On this version, under certain conditions, someone could get in without a password. The fix may already be there: it needs checking.

FOR YOUR IT TEAM

Banner OpenSSH_8.9p1 Ubuntu-3ubuntu0.6. CVE-2024-6387 (regreSSHion, CVSS 8.1) affects 8.5p1–9.7p1; Ubuntu fixed it in 1:8.9p1-3ubuntu0.10 (USN-6859-1). Update and limit port 22 to admin IPs.

```
sudo apt update && sudo apt install--only-upgrade openssh-server
dpkg -l openssh-server   # expected: 1:8.9p1-3ubuntu0.10 or later
```

CVE-2024-6387 · CVSS 8.1

Evidence: 22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 **References:** NVD CVE-2024-6387 · Ubuntu USN-6859-1

HIGH POTENTIAL nginx 1.18.0 (Ubuntu) F-05

nginx 1.18.0 falls within a known DNS resolver flaw

WHY IT MATTERS

The web server is the first program that answers visitors. This flaw is triggered only by a specific configuration: the real risk may be low.

FOR YOUR IT TEAM

Server: nginx/1.18.0 (Ubuntu). CVE-2021-23017 (CVSS 7.7) affects the built-in resolver. If the resolver directive is not used the risk is theoretical: update the package anyway.

```
grep -R "resolver" /etc/nginx/
sudo apt install--only-upgrade nginx
```

CVE-2021-23017 · CVSS 7.7

Evidence: server: nginx/1.18.0 (Ubuntu) **References:** NVD CVE-2021-23017

MEDIUM OBSERVED HTTPS · port 443 F-06

The site still accepts TLS 1.0 and TLS 1.1

WHY IT MATTERS

These encryption versions are over twenty years old and browsers have dropped them. Keeping them on does not help visitors and leaves a weaker path open.

FOR YOUR IT TEAM

TLS 1.0 and 1.1 offered, TLS 1.3 not offered. Both protocols are deprecated by RFC 8996. Keep only TLS 1.2 and 1.3 enabled.

```
# in the nginx server block
ssl_protocols TLSv1.2 TLSv1.3;
```

Evidence: TLS 1 offered (deprecated) · TLS 1.1 offered (deprecated) · TLS 1.3 not offered **References:** RFC 8996

SAMPLE · FICTITIOUS DATA

MEDIUM OBSERVED DNS · DMARC and SPF F-07

Fake emails in your domain's name are not blocked

WHY IT MATTERS

DMARC tells other servers what to do with emails pretending to be yours. Right now it is set to observe only: a fake email in the company's name can reach your customers.

FOR YOUR IT TEAM

_dmarc: v=DMARC1; p=none, with no rua address for reports. SPF ends with ~all. Turn on reports, check the legitimate senders, then move to p=quarantine and finally to p=reject.

```
_dmarc.aziendatest.example. TXT "v=DMARC1; p=quarantine; rua=mailto:dmarc@aziendatest.example"
```

Evidence: _dmarc.aziendatest.example TXT "v=DMARC1; p=none" **References:** RFC 7489

MEDIUM POTENTIAL WordPress 6.1.1 · jQuery 1.12.4 F-08

WordPress and jQuery are not up to date (4 known flaws)

WHY IT MATTERS

These are the parts of the site visitors use every day. The installed versions have known flaws, fixed years ago, that in some cases allow code to be injected into pages.

FOR YOUR IT TEAM

Meta generator WordPress 6.1.1 (CVE-2023-2745, CVSS 6.1); jquery.min.js?ver=1.12.4 (three CVEs, CVSS 6.1, fixed in 3.5.0). Update core and theme; remove jquery-migrate if not needed.

```
wp core update
wp theme update--all && wp plugin update--all
```

CVE-2023-2745 · CVSS 6.1 | CVE-2019-11358 · CVSS 6.1 | CVE-2020-11022 · CVSS 6.1 | CVE-2020-11023 · CVSS 6.1

Evidence: <meta name="generator" content="WordPress 6.1.1"> · jquery.min.js?ver=1.12.4
References: NVD CVE-2023-2745 · NVD CVE-2020-11022

LOW OBSERVED Security headers F-09

The protections the site asks of the browser are missing

WHY IT MATTERS

These are instructions the site sends to the browser, such as “always use HTTPS” or “do not show me inside other sites”. Without them, the browser cannot help protect visitors.

FOR YOUR IT TEAM

Strict-Transport-Security, Content-Security-Policy, X-Frame-Options and Referrer-Policy are missing. Add HSTS and the other headers; prepare the CSP in Report-Only mode before enforcing it.

```
add_header Strict-Transport-Security "max-age=31536000" always;
add_header X-Frame-Options "SAMEORIGIN" always;
add_header Referrer-Policy "strict-origin-when-cross-origin" always;
add_header Content-Security-Policy-Report-Only "default-src 'self'" always;
```

Evidence: Strict Transport Security not offered · Content-Security-Policy--
References: OWASP Secure Headers Project

SAMPLE · FICTITIOUS DA

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

- The server declares the software name and version in the Server and X-Powered-By headers: hide them (server_tokens off; expose_php = Off).
- SSH port 22 answers the whole internet: limit it to admin IPs.

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