NullTrace

CONFIDENTIAL

EXTERNAL VULNERABILITY ASSESSMENT · ADVANCED · EXTERNAL EXPOSURE REVIEW

Do you know everything your website shows to the outside world?

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	Advanced	NT-SAMPLE-ADVANCED

FINDINGS BY SEVERITY · 15 IN TOTAL



2 critical **6** high **5** medium **2** 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

15
findings

5
priority actions

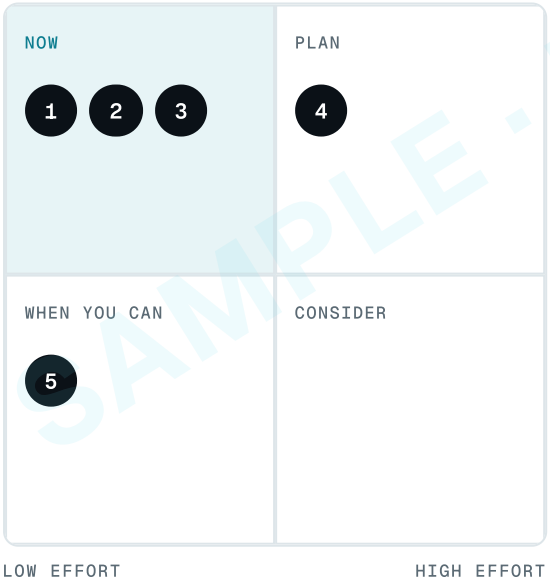
4
forgotten resources reachable

From outside, a database backup and the site's .git folder can be reached: they are the first things to remove. The database, phpMyAdmin and the test site are also open to anyone. The rest concerns updates and configuration. The five actions in the priority map solve the most serious findings in about two days of work.

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	—	—	—
Exposed surface	1	2	2	1	—

02 Priority map

The five actions that reduce risk the most, ordered by impact and effort.



1. **Remove the backup and the .git folder from the site**
   Provider or IT · 30 minutes · solves F-01, F-03
2. **Close the database and phpMyAdmin to the internet**
   Provider or IT · 1 hour · solves F-05, F-04
3. **Update the contact form, WordPress, the theme and the plugins**
   You or your provider · 1-2 hours · solves F-02, F-13
4. **Move PHP to a supported version**
   Provider · Half a day · solves F-06
5. **Put the test site behind a password**
   Provider · 30 minutes · solves F-09

SAMPLE · FICTITIOUS DA

03 The five actions, step by step

01 Remove the backup and the .git folder from the site

Who: Provider or IT | Time: 30 minutes | Solves: F-01, F-03

1. If you still need the backup, copy it to a safe place outside the server.
2. Delete /backup/db-2025-10.sql.gz from the site's public folder.
3. Block access on the server to hidden files and folders, such as .git and .env.
4. Check the access logs for downloads of the backup since 3 October 2025.
5. If there are unknown downloads, change the database passwords and ask your privacy adviser whether a notification is needed.

```
location ~ /\.(?!well-known) { deny all; }
location ^~ /backup/ { deny all; }
```

> **HOW TO CHECK IT IS FIXED**
>
> curl -I https://aziendatest.example/backup/db-2025-10.sql.gz → expected 404
>
> curl -I https://aziendatest.example/.git/HEAD → expected 403 or 404

02 Close the database and phpMyAdmin to the internet

Who: Provider or IT | Time: 1 hour | Solves: F-05, F-04

1. Set MySQL to listen locally only (bind-address = 127.0.0.1) and restart it.
2. Close port 3306 in the server firewall.
3. Remove phpMyAdmin if it is not needed; otherwise limit it to the office IPs.
4. Plan the move to MySQL 8.4, the version supported until 2032.

> **HOW TO CHECK IT IS FIXED**
>
> nmap -p 3306 aziendatest.example → expected closed or filtered
>
> curl -I https://aziendatest.example/phpmyadmin/ → expected 403 or 404

03 Update the contact form, WordPress, the theme and the plugins

Who: You or your provider | Time: 1-2 hours | Solves: F-02, F-13

1. Make a full backup and store it outside the site.
2. Try the updates on the test site, not on the real one.
3. Update in this order: Contact Form 7, WordPress, theme, other plugins.
4. Check that the contact form sends and the main pages display correctly.

> **HOW TO CHECK IT IS FIXED**
>
> The home page code no longer shows “ver=5.3.1” or “jquery … ver=1.12.4”

SAMPLE · FICTITIOUS DA

04 Move PHP to a supported version

Who: Provider | Time: Half a day | Solves: F-06

1. Ask your hosting provider to enable PHP 8.3 or 8.4.
2. Try the test site with the new version and note what does not work.
3. Fix incompatible theme and plugins, then move the real site to the new version.
4. Hide the PHP version by setting expose_php = Off.

> HOW TO CHECK IT IS FIXED
>
> curl -I https://aziendatest.example/ → no X-Powered-By header

05 Put the test site behind a password

Who: Provider | Time: 30 minutes | Solves: F-09

1. Protect staging.aziendatest.example with a password or an IP allow-list.
2. Add the X-Robots-Tag: noindex header to every page of the test site.
3. If it already shows on Google, request removal in Search Console.

```
auth_basic "Restricted area";
auth_basic_user_file /etc/nginx/.htpasswd;
add_header X-Robots-Tag "noindex, nofollow" always;
```

> HOW TO CHECK IT IS FIXED
>
> curl -I https://staging.aziendatest.example/ → expected 401

04 Exposed surface

What responds from the internet besides the website's pages.

ADDRESS	WHAT RESPONDS	STATUS
staging.aziendatest.example	Test copy of the site, with no password	PRESENT
/backup/db-2025-10.sql.gz	Database backup, 48 MB	PRESENT
/.git/	History of the site's code	PRESENT
/phpmyadmin/	Database management panel	PRESENT
port 3306	MySQL database	OBSERVED
port 22	SSH remote access	OBSERVED
/xmlrpc.php	WordPress remote interface, enabled	OBSERVED
/readme.html	File that reveals the WordPress version	OBSERVED

SAMPLE FICTITIOUS D

CONNECTED EXTERNAL SERVICES

SERVICE	WHAT IT IS FOR	WHERE IT SHOWS
Google Analytics 4	Visit statistics	script in the page
Google Maps	Map on the contact page	script in the page
Mailchimp	Newsletter sign-up	form in the page
mailprovider.example	Company email	MX record
Let's Encrypt	HTTPS certificate	site certificate

05 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 DA

06 Other findings, in detail

The findings not covered by the five actions, most severe first.

HIGH POTENTIAL OpenSSH 8.9p1 (Ubuntu) F-07

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-08

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-10

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 DA

MEDIUM OBSERVED DNS · DMARC and SPF F-11

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 OBSERVED azt theme · functions.php F-12

An error message shows the server's internal paths

WHY IT MATTERS

An error message shows anyone how the server's folders are organised. It is not harmful in itself, but it helps whoever is preparing an attack.

FOR YOUR IT TEAM

The theme's functions.php responds 500 with a PHP Warning showing the path /var/www/aziendatest/releases/2025-10/. Turn off display_errors in production and fix the undefined variable.

```
; production php.ini
display_errors = Off
log_errors = On
```

Evidence: PHP Warning: Undefined variable $opts in /var/www/aziendatest/… on line 214

References: OWASP WSTG-ERRH-01

LOW OBSERVED Security headers F-14

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 D/

LOW OBSERVED Google Maps JavaScript API F-15

A Google API key is in the page's code

WHY IT MATTERS

Google Maps keys are meant to sit in the page, but they must be limited to your domain: otherwise someone can use them at your expense.

FOR YOUR IT TEAM

Key AIza[redacted] in the map script on the home page. We did not use it. Check in the Google Cloud Console that it is limited to the *.aziendatest.example referrers and to the Maps APIs only.

Evidence: maps.googleapis.com/maps/api/js?key=AIza[redacted]

References: Google Maps Platform: API key best practices

07 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

08 In brief

- xmlrpc.php is enabled: if no app or service needs it, turn it off.
- /readme.html reveals the WordPress version: delete it after every update.
- The server declares the software name and version in the Server and X-Powered-By headers.

SAMPLE · FICTITIOUS DA

09 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 D