NullTrace

RISERVATO

VULNERABILITY ASSESSMENT ESTERNO · AVANZATO · EXTERNAL EXPOSURE REVIEW

Sai davvero tutto ciò che il tuo sito mostra all'esterno?

aziendatest.example

ESEMPIO · DATI FITTIZI

CLIENTE	PERIODO DELL'ANALISI	CONSEGNA
Azienda Test (fittizia)	10/11/2026 → 12/11/2026	13/11/2026
PERIMETRO	**LIVELLO**	**ID REPORT**
3 indirizzi	Avanzato	NT-ESEMPIO-AVANZATO

OSSERVAZIONI PER GRAVITÀ · 15 IN TUTTO



2 critico 6 alto 5 medio 2 basso

ESEMPIO

Questo è un esempio con dati fittizi. Il report che riceverai ha la stessa struttura, ma può essere più o meno ricco a seconda di ciò che emerge sul tuo sito.

01 Sintesi

15 osservazioni

5 azioni prioritarie

4 risorse dimenticate raggiungibili

Da fuori si raggiungono un backup del database e la cartella .git del sito: sono le prime cose da togliere. Anche il database, phpMyAdmin e il sito di prova sono aperti a chiunque. Il resto riguarda aggiornamenti e configurazioni. Le cinque azioni della mappa delle priorità risolvono le osservazioni più gravi in circa due giorni di lavoro.

AREA	CRITICO	ALTO	MEDIO	BASSO	INFO
Software e versioni	1	3	1	—	—
HTTPS e cifratura	—	—	1	—	—
Protezioni del browser	—	—	—	1	—
DNS ed email	—	—	1	—	—
Servizi esposti	—	1	—	—	—
Superficie esposta	1	2	2	1	—

02 Mappa delle priorità

Le cinque azioni che riducono di più il rischio, ordinate per impatto e sforzo.



1. **Togli dal sito il backup e la cartella .git**
   Fornitore o IT · 30 minuti · risolve F-01, F-03
2. **Chiudi a internet il database e phpMyAdmin**
   Fornitore o IT · 1 ora · risolve F-05, F-04
3. **Aggiorna il modulo contatti, WordPress, il tema e i plugin**
   Tu o il fornitore · 1-2 ore · risolve F-02, F-13
4. **Porta PHP a una versione supportata**
   Fornitore · Mezza giornata · risolve F-06
5. **Metti il sito di prova dietro una password**
   Fornitore · 30 minuti · risolve F-09

ESEMPIO · DATI FITTIZI

03 Le cinque azioni, passo per passo

01 Togli dal sito il backup e la cartella .git

Chi: Fornitore o IT | Tempo: 30 minuti | Risolve: F-01, F-03

1. Se il backup ti serve ancora, copialo in un posto sicuro fuori dal server.
2. Cancella /backup/db-2025-10.sql.gz dalla cartella pubblica del sito.
3. Blocca nel server l'accesso a file e cartelle nascosti, come .git e .env.
4. Controlla nei log di accesso se il backup è stato scaricato dal 3 ottobre 2025.
5. Se risultano download sconosciuti, cambia le password del database e valuta con il consulente privacy se serve una notifica.

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

COME VERIFICARE CHE È RISOLTO

curl -I https://aziendatest.example/backup/db-2025-10.sql.gz → atteso 404

curl -I https://aziendatest.example/.git/HEAD → atteso 403 o 404

02 Chiudi a internet il database e phpMyAdmin

Chi: Fornitore o IT | Tempo: 1 ora | Risolve: F-05, F-04

1. Imposta MySQL perché ascolti solo in locale (bind-address = 127.0.0.1) e riavvialo.
2. Chiudi la porta 3306 nel firewall del server.
3. Rimuovi phpMyAdmin se non serve; altrimenti limitalo agli IP dell'ufficio.
4. Pianifica il passaggio a MySQL 8.4, la versione con supporto fino al 2032.

COME VERIFICARE CHE È RISOLTO

nmap -p 3306 aziendatest.example → atteso closed o filtered

curl -I https://aziendatest.example/phpmyadmin/ → atteso 403 o 404

03 Aggiorna il modulo contatti, WordPress, il tema e i plugin

Chi: Tu o il fornitore | Tempo: 1-2 ore | Risolve: F-02, F-13

1. Fai un backup completo e salvalo fuori dal sito.
2. Prova gli aggiornamenti sul sito di prova, non su quello vero.
3. Aggiorna nell'ordine: Contact Form 7, WordPress, tema, altri plugin.
4. Controlla che il modulo contatti invii e che le pagine principali si vedano bene.

COME VERIFICARE CHE È RISOLTO

Nel codice della home non compaiono più «ver=5.3.1» né «jquery … ver=1.12.4»

ESEMPIO · DATI FITTIZI

04 Porta PHP a una versione supportata

Chi: Fornitore | Tempo: Mezza giornata | Risolve: F-06

1. Chiedi all'hosting di attivare PHP 8.3 o 8.4.
2. Prova il sito di prova con la nuova versione e annota cosa non funziona.
3. Correggi tema e plugin incompatibili, poi passa il sito vero alla nuova versione.
4. Nascondi la versione di PHP impostando expose_php = Off.

> **COME VERIFICARE CHE È RISOLTO**
>
> `curl -I https://aziendatest.example/ → nessun header X-Powered-By`

05 Metti il sito di prova dietro una password

Chi: Fornitore | Tempo: 30 minuti | Risolve: F-09

1. Proteggi staging.aziendatest.example con una password o con una lista di IP.
2. Aggiungi l'header X-Robots-Tag: noindex a tutte le pagine del sito di prova.
3. Se compare già su Google, chiedi la rimozione da Search Console.

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

> **COME VERIFICARE CHE È RISOLTO**
>
> `curl -I https://staging.aziendatest.example/ → atteso 401`

04 Superficie esposta

Cosa risponde da internet oltre alle pagine del sito.

INDIRIZZO	COSA RISPONDE	STATO
staging.aziendatest.example	Copia di prova del sito, senza password	PRESENTE
/backup/db-2025-10.sql.gz	Backup del database, 48 MB	PRESENTE
/.git/	Storico del codice del sito	PRESENTE
/phpmyadmin/	Pannello di gestione del database	PRESENTE
porta 3306	Database MySQL	OSSERVATO
porta 22	Accesso remoto SSH	OSSERVATO
/xmlrpc.php	Interfaccia remota di WordPress, attiva	OSSERVATO
/readme.html	File che rivela la versione di WordPress	OSSERVATO

ESEMPIO · DATI FITTIZI

SERVIZI ESTERNI COLLEGATI

SERVIZIO	A COSA SERVE	DOVE SI VEDE
Google Analytics 4	Statistiche delle visite	script nella pagina
Google Maps	Mappa nella pagina contatti	script nella pagina
Mailchimp	Iscrizione alla newsletter	modulo nella pagina
mailprovider.example	Posta aziendale	record MX
Let's Encrypt	Certificato HTTPS	certificato del sito

05 Tecnologie rilevate

CATEGORIA	TECNOLOGIA	VERSIONE	STATO	DOVE SI VEDE
Server web	**nginx**	1.18.0	OBSOLETA	header Server
Sistema operativo	**Ubuntu**	22.04 LTS	SUPPORTATA	banner SSH e header
Linguaggio	**PHP**	7.4.33	SENZA SUPPORTO	header X-Powered-By
CMS	**WordPress**	6.1.1	OBSOLETA	meta generator
Plugin	**Contact Form 7**	5.3.1	OBSOLETA	file del plugin (?ver=)
Plugin	**Yoast SEO**	20.1	OBSOLETA	commento nel codice HTML
Libreria JavaScript	**jQuery**	1.12.4	OBSOLETA	file della libreria (?ver=)
Database	**MySQL**	8.0.28	SENZA SUPPORTO	porta 3306
Accesso remoto	**OpenSSH**	8.9p1	DA VERIFICARE	porta 22
Certificato HTTPS	**Let's Encrypt**	–	VALIDO	valido fino al 20/01/2027
Statistiche	**Google Analytics 4**	–	SERVIZIO ESTERNO	script nella pagina
Newsletter	**Mailchimp**	–	SERVIZIO ESTERNO	modulo di iscrizione

ESEMPIO · DATI FITTIZI

06 Altre osservazioni, in dettaglio

Le osservazioni non coperte dalle cinque azioni, dalla più grave.

ALTO · POTENZIALE · OpenSSH 8.9p1 (Ubuntu) F-07

OpenSSH dichiara una versione colpita da una falla nota

PERCHÉ CONTA

SSH è la porta da cui gli amministratori entrano nel server. Su questa versione, in certe condizioni, si potrebbe entrare senza password. La correzione potrebbe già esserci: va verificato.

PER IL TUO IT

Banner OpenSSH_8.9p1 Ubuntu-3ubuntu0.6. CVE-2024-6387 (regreSSHion, CVSS 8.1) colpisce 8.5p1–9.7p1; Ubuntu l'ha corretta in 1:8.9p1-3ubuntu0.10 (USN-6859-1). Aggiorna e limita la porta 22 agli IP di amministrazione.

```
sudo apt update && sudo apt install--only-upgrade openssh-server
dpkg -l openssh-server   # atteso: 1:8.9p1-3ubuntu0.10 o successiva
```

CVE-2024-6387 · CVSS 8.1

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

ALTO · POTENZIALE · nginx 1.18.0 (Ubuntu) F-08

nginx 1.18.0 rientra in una falla nota del resolver DNS

PERCHÉ CONTA

Il server web è il primo programma che risponde ai visitatori. Questa falla si attiva solo con una configurazione particolare: il rischio reale potrebbe essere basso.

PER IL TUO IT

Server: nginx/1.18.0 (Ubuntu). CVE-2021-23017 (CVSS 7.7) riguarda il resolver interno. Se la direttiva resolver non è usata il rischio è teorico: aggiorna comunque il pacchetto.

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

CVE-2021-23017 · CVSS 7.7

Prova: server: nginx/1.18.0 (Ubuntu) **Riferimenti:** NVD CVE-2021-23017

MEDIO · OSSERVATO · HTTPS · porta 443 F-10

Il sito accetta ancora TLS 1.0 e TLS 1.1

PERCHÉ CONTA

Sono versioni della cifratura di oltre vent'anni fa, ritirate dai browser. Tenerle attive non serve ai visitatori e lascia aperta una strada più debole.

PER IL TUO IT

TLS 1.0 e 1.1 offerti, TLS 1.3 non offerto. I due protocolli sono deprecati da RFC 8996. Lascia attivi solo TLS 1.2 e 1.3.

```
# nel blocco server di nginx
ssl_protocols TLSv1.2 TLSv1.3;
```

Prova: TLS 1 offered (deprecated) · TLS 1.1 offered (deprecated) · TLS 1.3 not offered **Riferimenti:** RFC 8996

ESEMPIO · DATI FITTIZI

MEDIO OSSERVATO DNS · DMARC e SPF F-11

Le email false a nome del tuo dominio non vengono bloccate

PERCHÉ CONTA

DMARC dice agli altri server cosa fare con le email che fingono di essere tue. Ora è impostato solo per osservare: un'email falsa a nome dell'azienda può arrivare ai clienti.

PER IL TUO IT

_dmarc: v=DMARC1; p=none, senza indirizzo rua per i report. SPF termina con ~all. Attiva i report, verifica le fonti legittime, poi passa a p=quarantine e infine a p=reject.

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

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

MEDIO OSSERVATO tema azt · functions.php F-12

Un errore mostra i percorsi interni del server

PERCHÉ CONTA

Un messaggio d'errore mostra a chiunque come sono organizzate le cartelle del server. Non è un danno in sé, ma aiuta chi prepara un attacco.

PER IL TUO IT

functions.php del tema risponde 500 con un PHP Warning che riporta il percorso /var/www/aziendatest/releases/2025-10/. Disattiva display_errors in produzione e correggi la variabile non definita.

```
; php.ini di produzione
display_errors = Off
log_errors = On
```

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

Riferimenti: OWASP WSTG-ERRH-01

BASSO OSSERVATO Header di sicurezza F-14

Mancano le protezioni che il sito chiede al browser

PERCHÉ CONTA

Sono istruzioni che il sito manda al browser, come «usa sempre HTTPS» o «non mostrarmi dentro altri siti». Senza, il browser non può aiutare a proteggere i visitatori.

PER IL TUO IT

Assenti Strict-Transport-Security, Content-Security-Policy, X-Frame-Options e Referrer-Policy. Introduci HSTS e gli altri header; prepara la CSP in modalità Report-Only prima di applicarla.

```
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;
```

Prova: Strict Transport Security not offered · Content-Security-Policy--

Riferimenti: OWASP Secure Headers Project

ESEMPIO · DATI FITTIZI

BASSO OSSERVATO Google Maps JavaScript API F-15

Una chiave API di Google è nel codice della pagina

PERCHÉ CONTA

Le chiavi di Google Maps sono fatte per stare nella pagina, ma vanno limitate al tuo dominio: altrimenti qualcuno può usarle a tue spese.

PER IL TUO IT

Chiave AIza[oscurato] nello script della mappa in home. Non l'abbiamo usata. Verifica nella Google Cloud Console che sia limitata ai referrer *.aziendatest.example e alle sole API Maps.

Prova: maps.googleapis.com/maps/api/js?key=AIza[oscurato]

Riferimenti: Google Maps Platform: API key best practices

07 Falle note (CVE) potenzialmente pertinenti

Dedotte dalle versioni dichiarate: non sono vulnerabilità confermate. Punteggi CVSS da NVD.

COMPONENTE	CVE	CVSS	COSA RIGUARDA	CORRETTA IN
Contact Form 7 5.3.1	CVE-2020-35489	10.0	Caricamento di file pericolosi tramite il modulo	5.3.2
OpenSSH 8.9p1 (Ubuntu)	CVE-2024-6387	8.1	Accesso remoto senza password, in condizioni particolari	Ubuntu USN-6859-1
nginx 1.18.0	CVE-2021-23017	7.7	Errore di memoria nel resolver DNS interno	1.20.1
WordPress 6.1.1	CVE-2023-2745	6.1	Caricamento di file di traduzione arbitrari	6.2.1
jQuery 1.12.4	CVE-2019-11358	6.1	Modifica degli oggetti JavaScript (prototype pollution)	3.4.0
	CVE-2020-11022	6.1	Esecuzione di codice da HTML non fidato	3.5.0
	CVE-2020-11023	6.1	Esecuzione di codice da HTML con elementi option	3.5.0

08 In breve

- xmlrpc.php è attivo: se non usi app o servizi che lo richiedono, disattivalo.
- /readme.html rivela la versione di WordPress: cancellalo dopo ogni aggiornamento.
- Il server dichiara nome e versione del software negli header Server e X-Powered-By.

ESEMPIO · DATI FITTIZI

09 Perimetro, metodo e limiti

Perimetro

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

Metodo

Analisi esterna «black box», dal 10/11/2026 al 12/11/2026: solo ciò che è visibile da internet, senza credenziali, con verifiche non distruttive. Nessun exploit, nessun test di carico, nessun file esposto aperto o scaricato.

Limiti

- Non garantisce che il sito sia sicuro, né che non ci saranno attacchi in futuro.
- Fotografa il sito nelle date indicate: un aggiornamento o un plugin nuovo cambiano il quadro.
- Copre solo il perimetro concordato: rete interna, computer dell'ufficio ed email del personale restano fuori.
- Non corregge: le correzioni le applichi tu o il tuo fornitore, seguendo il report.

DOMANDE SUL REPORT

Per 14 giorni di calendario puoi scriverci a **reports@nulltrace.systems**. La prima risposta nel merito arriva entro 3 giorni lavorativi.

Questo è un esempio con dati fittizi. Il report che riceverai ha la stessa struttura, ma può essere più o meno ricco a seconda di ciò che emerge sul tuo sito.

ESEMPIO · DATI FITTIZI