NullTrace

RISERVATO

VULNERABILITY ASSESSMENT ESTERNO · PRO · EXTERNAL SECURITY REVIEW

Il tuo sito è configurato per proteggerti?

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	Pro	NT-ESEMPIO-PRO

OSSERVAZIONI PER GRAVITÀ · 9 IN TUTTO



1 critico **4** alto **3** medio **1** 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

9
osservazioni

4
aree di configurazione verificate

7
CVE potenzialmente pertinenti

Il punto più urgente è il modulo contatti, in una versione con una falla critica nota. Sul fronte della configurazione il database risponde da internet, la cifratura accetta versioni ritirate e le email false a nome del dominio non vengono bloccate. Quasi tutto si risolve con aggiornamenti e poche righe di configurazione.

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	—	—	—

02 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

03 Osservazioni

Dalla più grave. «Potenziale» vuol dire dedotta dalla versione dichiarata, da confermare con il fornitore.

CRITICO POTENZIALE Contact Form 7 5.3.1 F-01

Il modulo contatti usa una versione con una falla critica nota

PERCHÉ CONTA

Il modulo contatti è aperto a chiunque. In questa versione un file con un nome costruito ad arte poteva superare i controlli e finire sul server.

PER IL TUO IT

Versione 5.3.1 rilevata dal parametro ver= dei file del plugin. CVE-2020-35489 (CVSS 10.0): caricamento di file non controllato, corretto nella 5.3.2. La deduzione si basa sulla versione: conferma lato server e aggiorna.

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

CVE-2020-35489 · CVSS 10.0

Prova: GET /wp-content/plugins/contact-form-7/includes/js/index.js?ver=5.3.1 → 200
Riferimenti: NVD CVE-2020-35489

ALTO OSSERVATO MySQL 8.0.28 · porta 3306 F-02

Il database MySQL, senza più supporto, risponde da internet

PERCHÉ CONTA

Il database contiene i dati del sito e dei clienti. Oggi chiunque può tentare di collegarsi e provare password, e la versione non riceve più correzioni.

PER IL TUO IT

Porta 3306/tcp aperta su 203.0.113.10, MySQL 8.0.28 (ramo fuori supporto dal 30/04/2026). Serve solo all'applicazione: limita l'ascolto a localhost e pianifica il passaggio a 8.4 LTS.

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

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

ALTO OSSERVATO PHP 7.4.33 F-03

PHP 7.4 non riceve aggiornamenti di sicurezza da novembre 2022

PERCHÉ CONTA

Ogni falla di PHP scoperta dopo novembre 2022 resta aperta per sempre su questa versione. È una serratura che il produttore non sostituisce più.

PER IL TUO IT

Header X-Powered-By: PHP/7.4.33. Il ramo 7.4 è fuori supporto dal 28/11/2022. Pianifica il passaggio a 8.3 o 8.4: verifica tema e plugin in staging, poi aggiorna il pool PHP-FPM.

```
sudo apt install php8.3-fpm php8.3-mysql
# nel blocco server di nginx:
fastcgi_pass unix:/run/php/php8.3-fpm.sock;
```

Prova: x-powered-by: PHP/7.4.33 **Riferimenti:** php.net/supported-versions

ESEMPIO · DATI FITTIZI

ALTO POTENZIALE OpenSSH 8.9p1 (Ubuntu) F-04

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-05

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-06

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-07

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 POTENZIALE WordPress 6.1.1 · jQuery 1.12.4 F-08

WordPress e jQuery non sono aggiornati (4 falle note)

PERCHÉ CONTA

Sono le parti del sito che i visitatori usano ogni giorno. Le versioni installate hanno falle note, corrette da anni, che in certi casi permettono di inserire codice nelle pagine.

PER IL TUO IT

Meta generator WordPress 6.1.1 (CVE-2023-2745, CVSS 6.1); jquery.min.js?ver=1.12.4 (tre CVE, CVSS 6.1, corrette in 3.5.0). Aggiorna core e tema; rimuovi jquery-migrate se non serve.

```
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

Prova: <meta name="generator" content="WordPress 6.1.1"> · jquery.min.js?ver=1.12.4

Riferimenti: NVD CVE-2023-2745 · NVD CVE-2020-11022

BASSO OSSERVATO Header di sicurezza F-09

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

04 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

05 In breve

- Il server dichiara nome e versione del software negli header Server e X-Powered-By: nascondili (server_tokens off; expose_php = Off).
- La porta SSH 22 risponde a tutto internet: limitala agli IP di amministrazione.

06 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