

EVALUACIÓN DE SEGURIDAD

northwind-retail.example

Health Check · evaluación externa y autorizada · realizada el 23 de octubre de 2026 por Ionuț-Robert Sandu

!

Exposición crítica

Uno o más problemas permiten a un atacante tomar el control o extraer datos. Corrige los elementos críticos antes que nada.

CRÍTICO	ALTO	MEDIO	BAJO	TOTAL
2	3	6	4	17

Qué corregir primero

- CRÍTICO

MySQL database exposed to the internet `admin.northwind-retail.example:3306`
Bind MySQL to localhost or a private network and block 3306 at the firewall. Rotate database credentials.
- CRÍTICO

PHP-CGI argument injection (actively exploited) `https://api.northwind-retail.example`
Update PHP to 8.3.8 / 8.2.20 / 8.1.29 or later immediately, or apply your distribution's patched package.
- ALTO

Grafana reachable with default admin login `https://grafana.northwind-retail.example`
Change the admin password, disable default accounts, and put Grafana behind SSO or a VPN.
- ALTO

Exposed .git directory `https://www.northwind-retail.example/.git/config`
Block access to /.git in the web server and remove the directory from the web root.
- ALTO

Dangling DNS — possible subdomain takeover `staging-old.northwind-retail.example`
Remove the dangling DNS record, or reclaim the resource it points to.
- MEDIO

SQL injection in product search `https://shop.northwind-retail.example/search?q=`
Use parameterized queries / prepared statements and validate input. Review the endpoint for data exposure.

Superficie de ataque

Subdominios descubiertos	12
Hosts activos sondeados	3
Puertos / servicios abiertos	22/ssh, 80/http, 443/https, 3000/grafana, 3306/mysql
Tecnologías identificadas	nginx, PHP, WordPress, jQuery, Grafana
Autenticación de correo	SPF presente · DMARC ausente · DNSSEC inactivo
Formularios / puntos de entrada	9
Secretos expuestos en el código	2
Superficie de API (OpenAPI)	Encontrado

Subdominios en el alcance

`www.northwind-retail.example``shop.northwind-retail.example``api.northwind-retail.example`

`staging.northwind-retail.example``staging-old.northwind-retail.example`

`admin.northwind-retail.example``vpn.northwind-retail.example``mail.northwind-retail.example`

`grafana.northwind-retail.example``git.northwind-retail.example``cdn.northwind-retail.example`

`assets.northwind-retail.example`

Reputación y listas de bloqueo

Si cada objetivo está marcado por malware o phishing (inteligencia de Cloudflare, y URLhaus cuando está disponible), y si las direcciones de sus servidores de correo y web aparecen en listas públicas de bloqueo de spam.

northwind-retail.example EN LISTA DE BLOQUEO
203.0.113.11 (mail server) en UCEPROTECT L1

Hallazgos (17)

Crítico — 2

CRÍTICO

F-01

Vulnerability scan

MySQL database exposed to the internet

admin.northwind-retail.example:3306

The MySQL service on admin.northwind-retail.example accepts connections from any address on port 3306. An exposed database is a direct route to full data theft and ransomware.

Remediación. Bind MySQL to localhost or a private network and block 3306 at the firewall. Rotate database credentials.

PHP-CGI argument injection (actively exploited)

`https://api.northwind-retail.example`

The API runs a PHP version affected by CVE-2024-4577, an argument-injection flaw that allows remote code execution and is being exploited in the wild.

Remediación. Update PHP to 8.3.8 / 8.2.20 / 8.1.29 or later immediately, or apply your distribution's patched package.

[CVE-2024-4577](#) · [CVE-2024-4577](#)

Alto — 3

Grafana reachable with default admin login

`https://grafana.northwind-retail.example`

The Grafana instance accepts the default admin/admin credentials, exposing dashboards and data sources — and often database passwords stored in them.

Remediación. Change the admin password, disable default accounts, and put Grafana behind SSO or a VPN.

Exposed .git directory

`https://www.northwind-retail.example/.git/config`

The .git directory is served publicly. Attackers can download the full source code and any secrets committed to it.

Remediación. Block access to /.git in the web server and remove the directory from the web root.

Dangling DNS — possible subdomain takeover

`staging-old.northwind-retail.example`

staging-old.northwind-retail.example points to a decommissioned cloud host that is no longer claimed. An attacker can register it and serve content from your domain.

Remediación. Remove the dangling DNS record, or reclaim the resource it points to.

Medio — 6

SQL injection in product search

`https://shop.northwind-retail.example/search?q=`

The product search endpoint returns database errors for crafted input, indicating an injectable parameter. Confirmed exploitation is part of the App Pen Test.

Remediación. Use parameterized queries / prepared statements and validate input. Review the endpoint for data exposure.

MEDIO F-07

Configuration & hardening

Weak TLS version supported (TLS 1.0/1.1)

`https://www.northwind-retail.example`

The web server still negotiates TLS 1.0/1.1, which are deprecated and vulnerable to downgrade attacks.

Remediación. Disable TLS 1.0 and 1.1; serve only TLS 1.2 and 1.3.

MEDIO F-08

Configuration & hardening

Weak cipher suite (CBC / RSA key exchange)

`https://www.northwind-retail.example`

The server offers CBC-mode and RSA-key-exchange ciphers without forward secrecy.

Remediación. Prefer ECDHE suites with AES-GCM; remove CBC and static-RSA ciphers.

MEDIO F-09

Configuration & hardening

Content-Security-Policy allows unsafe-inline

`https://www.northwind-retail.example`

The CSP permits inline scripts, which weakens its protection against cross-site scripting.

Remediación. Move to nonce- or hash-based CSP and remove 'unsafe-inline'.

MEDIO F-10

Configuration & hardening

HSTS header missing

`https://shop.northwind-retail.example`

Without HSTS, browsers may connect over plain HTTP first, where traffic can be intercepted.

Remediación. Send Strict-Transport-Security: max-age=31536000; includeSubDomains.

MEDIO F-11

Reputation & blocklists

Mail server 203.0.113.11 on 1 spam blocklist

`northwind-retail.example`

Listed on UCEPROTECT L1. Email sent from this server may land in spam or be rejected.

Remediación. Find what sent spam (a compromised mailbox, form or plugin), fix it, then request delisting on each list.

Bajo — 4

BAJO F-12

Configuration & hardening

DNSSEC not enabled

`https://northwind-retail.example`

DNS answers for this domain cannot be cryptographically verified.

Remediación. Enable DNSSEC at your DNS provider and add the DS record at your registrar.

BAJO F-13

Configuration & hardening

DMARC policy not enforced

`https://northwind-retail.example`

No enforcing DMARC record, so spoofed mail using this domain is not rejected.

Remediación. Publish a DMARC record and move to `p=quarantine` then `p=reject`.

BAJO F-14

Configuration & hardening

Referrer-Policy header missing

`https://www.northwind-retail.example`

Full page addresses can leak to third-party sites through links.

Remediación. Send Referrer-Policy: `strict-origin-when-cross-origin`.

BAJO F-15

Configuration & hardening

Permissions-Policy header missing

`https://www.northwind-retail.example`

Browser features are not restricted, widening the impact of a compromise.

Remediación. Send a Permissions-Policy limiting camera, microphone and geolocation.

Info — 2

INFO F-16

Configuration & hardening

Cache-Control missing on authenticated pages

`https://shop.northwind-retail.example`

Sensitive pages may be cached by browsers or proxies.

Remediación. Send Cache-Control: `no-store` on authenticated responses.

INFO F-17

Configuration & hardening

API token found in client-side JavaScript

`https://https://www.northwind-retail.example`

A token was found in a public JS bundle. Confirm it is not a privileged credential.

Remediación. Move secrets server-side and rotate the exposed token.

Alcance y método

Fue una **health check externo de caja negra** de `northwind-retail.example`, autorizada por el cliente. Cartografiamos la superficie de ataque como lo haría un atacante —sin credenciales ni acceso interno— usando nuestra cadena de herramientas ofensiva (descubrimiento de subdominios, escaneo de puertos y servicios, análisis de TLS y cabeceras, fingerprinting de tecnologías y un análisis de vulnerabilidades con Nuclei y OpenVAS), con cada hallazgo revisado por un ingeniero de seguridad.

Módulos ejecutados: `whois`, `subdomain_discovery`, `dns_resolution`, `shodan_enrich`, `port_scan`, `nmap_scan`, `tlx`, `http_probe`, `resource_enum`, `vuln_scan`. Los hallazgos reflejan el estado de los objetivos en el momento del escaneo. Una

evaluación externa no puede garantizar que no exista ninguna vulnerabilidad; refleja lo que es accesible y comprobable desde Internet dentro del alcance acordado. No se realizaron pruebas de denegación de servicio ni destructivas.

RiskBits Check · check.riskbits.net · Preparado el 23 de octubre de 2026 · Ionuț-Robert Sandu · Confidencial — para el cliente indicado arriba.