EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://integramed.es	Checks	9 pruebas
Dominio	integramed.es	Hallazgos	56 totales
Fecha	21 de abril de 2026 a las 14:56	Problemas	16 detectados

C

70/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis técnico de integramed.es arroja una puntuación de 70/100 con una nota final de C. Durante la auditoría se ejecutaron 9 checks pasivos, resultando en 6 aprobados, 1 advertencia y 2 fallos críticos relacionados con la configuración del servidor. Aunque la infraestructura posee un certificado de cifrado válido, la ausencia de cabeceras de seguridad y la gestión deficiente de cookies representan un riesgo para la integridad de los datos. Se concluye que el sitio es actualmente vulnerable a ataques de suplantación de identidad e inyección de código.

Resumen de Riesgos

0	6	7	3	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 73 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	44	FALLO	PrestaShop-24a5875a6ee9abedf5ce891cd7f77cdd: fal...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 73 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  73 dias restantes (expira: 2026-07-03T04:06:42.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-04T04:06:43.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/7.4.33, PleskLin — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://integramed.es/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- INFO **Tecnologias detectadas**
  Next.js, Astro, PHP/7.4.33, PleskLin

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 44/100

Estado: FALLO

PrestaShop-24a5875a6ee9abedf5ce891cd7f77cdd: falta SameSite; PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite; PrestaShop-24a5875a6ee9abedf5ce891cd7f77cdd: falta SameSite

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- INFO **Cookie: PrestaShop-24a5875a6ee9abedf5ce891cd7f77cdd — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: PrestaShop-24a5875a6ee9abedf5ce891cd7f77cdd — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: PrestaShop-24a5875a6ee9abedf5ce891cd7f77cdd — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: PrestaShop-24a5875a6ee9abedf5ce891cd7f77cdd — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: PrestaShop-24a5875a6ee9abedf5ce891cd7f77cdd — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: PrestaShop-24a5875a6ee9abedf5ce891cd7f77cdd — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (4410 bytes)
- INFO **Reglas robots.txt**
  139 Disallow, 5 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://integramed.es/mod/lgsitemaps/sitemap?name=sitemap_1
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- INFO **Puerto 22 (SSH)**
  Cerrado — Acceso remoto seguro
- INFO **Puerto 23 (Telnet)**
  Cerrado — Acceso remoto sin cifrar

- INFO **Puerto 25 (SMTP)**
  Cerrado — Envio de correo
- INFO **Puerto 80 (HTTP)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — Servidor web seguro
- INFO **Puerto 3306 (MySQL)**
  Cerrado — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- INFO **Puerto 6379 (Redis)**
  Cerrado — Cache Redis sin autenticacion por defecto
- INFO **Puerto 8080 (HTTP-Alt)**
  Cerrado — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Falta de Content-Security-Policy: El sitio no define una política de seguridad de contenido, facilitando ataques de XSS y robo de información.
[HIGH] Falta de X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea embebido en marcos externos, aumentando el riesgo de ataques de clickjacking.
[HIGH] Falta de Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, lo que permite ataques de degradación de protocolo.
[HIGH] Cookie PHPSESSID sin HttpOnly: El identificador de sesión es accesible mediante scripts, facilitando el secuestro de sesiones de usuario.
[HIGH] Cookie PHPSESSID sin flag Secure: La cookie de sesión puede transmitirse por canales no cifrados, comprometiendo la cuenta del usuario.
[MEDIUM] Falta de X-Content-Type-Options: El servidor no previene el rastreo de tipos MIME, lo que podría permitir la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Falta de Referrer-Policy: No se controla qué información de origen se envía a otros sitios, comprometiendo la privacidad de la navegación.
[MEDIUM] Cookie PHPSESSID y PrestaShop sin SameSite: Estas cookies son vulnerables a ataques de falsificación de solicitud en sitios cruzados (CSRF).
[MEDIUM] Bloqueo total en Robots.txt: Se utiliza una directiva que bloquea todo el rastreo del sitio, lo cual puede esconder configuraciones o afectar la visibilidad.
[LOW] Cabecera Server expuesta: Se revela el uso de nginx, proporcionando información útil a atacantes para buscar exploits específicos.
[LOW] Cabecera X-Powered-By expuesta: Se revela el uso de PHP/7.4.33 y Plesk, exponiendo versiones de software potencialmente desactualizadas.
[LOW] Ruta sensible en robots.txt: Se menciona una referencia a "config", lo que orienta a posibles atacantes sobre la estructura interna del servidor.