EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://quiz.dressly.world/es/fb-shop-amazon-personalized-plan-hp/Offer?utm_source=facebook&utm_term=120249980916370675&utm_content=120249980921960675&utm_id=120249980914560675&utm_placement=Facebook_Mobile_Reels&utm_platform=fb&utm_medium=paid&utm_campaign=120249980914560675&device_id=303f854b-c97f-44f3-a096-b3e409e56d0d&user_id=d9enjb9bqnk0008n3yy0	Checks	9 pruebas
Dominio	quiz.dressly.world	Hallazgos	43 totales
Fecha	19 de julio de 2026 a las 23:14	Problemas	9 detectados

B

76/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio web ha arrojado una puntuacion de 76/100, lo que otorga una calificacion final de nota B. Se ejecutaron un total de 9 checks pasivos, obteniendo como resultado 6 validaciones correctas, 1 advertencia por configuracion de puertos y 2 fallos criticos en la seguridad de cabeceras y archivos de informacion. La infraestructura cuenta con un cifrado SSL robusto y redireccion automatica a HTTPS, lo que protege la transmision de datos. Sin embargo, la ausencia de politicas de seguridad modernas en el servidor deja el sitio expuesto a ataques de inyeccion y suplantacion. En conclusion, el sitio es moderadamente seguro pero vulnerable frente a ataques dirigidos a nivel de aplicacion y navegador.

Resumen de Riesgos

0	2	6	1	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 34 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 34 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  34 dias restantes (expira: 2026-08-22T18:16:32.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-24T17:16:39.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://account.dressly.world/plan
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: La ausencia de esta cabecera impide restringir las fuentes de contenido permitidas, facilitando ataques de inyeccion de codigo XSS.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es vulnerable a clickjacking, permitiendo que atacantes carguen la web en marcos invisibles para engañar al usuario.
[MEDIUM] X-Content-Type-Options: Falta la directiva que evita que el navegador realice sniffing de tipos MIME, lo que podria ejecutar archivos maliciosos disfrazados de otros formatos.
[MEDIUM] Referrer-Policy: No existe control sobre la informacion de procedencia enviada en las peticiones, lo que puede filtrar URLs privadas a sitios de terceros.

[MEDIUM] Permissions-Policy: No se limitan las capacidades del navegador, permitiendo potencialmente el acceso a camaras, microfonos o geolocalizacion sin una politica definida.
[MEDIUM] Archivos /readme.html y /README.txt: Estos archivos son accesibles publicamente y pueden revelar informacion sensible sobre el despliegue o la configuracion del sistema.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detecto un puerto de servidor alternativo abierto, lo cual aumenta la superficie de ataque y puede exponer servicios no protegidos.
[LOW] Server header expuesto: La respuesta del servidor revela explicitamente el uso de Cloudflare, permitiendo a los atacantes acotar sus tecnicas de explotacion.