EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://aequorahotels.com	Checks	9 pruebas
Dominio	aequorahotels.com	Hallazgos	53 totales
Fecha	20 de abril de 2026 a las 14:27	Problemas	19 detectados

D

55/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada arroja una puntuación de 55/100 con una calificación de grado D. Se ejecutaron 9 checks pasivos que resultaron en 4 conformes, 1 advertencia y 4 fallos críticos. Se han identificado debilidades importantes en la configuración de cabeceras de seguridad, protección de cookies y exposición de versiones del sistema. El análisis concluye que el sitio es actualmente vulnerable y requiere intervenciones inmediatas para proteger la integridad de los usuarios.

Resumen de Riesgos

0	6	10	3	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 80 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 183 expuesta, WordPress 2 expuesta
Seguridad de Cookies	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
Contenido Mixto	20	FALLO	6 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 80 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  80 dias restantes (expira: 2026-07-09T13:20:51.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-10T13:20:52.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

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

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

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- 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://aequorahotels.com/
- 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
- BAJO **Meta generator**
  Expone: Elementor 4.0.1; features: e_font_icon_svg, additional_custom_breakpoints; settings: css_print_method-external, google_font-enabled, font_display-swap
- INFO **Tecnologias detectadas**
  Next.js, Astro

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 183 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 183 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

Seguridad de Cookies — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- 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

Contenido Mixto — 20/100

Estado: FALLO

6 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://aequorahotels.com/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://aequorahotels.com/en/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://aequorahotels.com/fr/
- MEDIO **href (link/stylesheet)**
  ...y 3 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (121 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://aequorahotels.com/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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] X-Frame-Options: La ausencia de esta cabecera permite ataques de clickjacking, donde un atacante puede cargar el sitio en un iframe invisible para engañar al usuario.
[HIGH] Strict-Transport-Security: No se implementa HSTS, lo que permite ataques de degradación de protocolo (SSL Stripping) al no forzar HTTPS en el navegador.
[HIGH] WordPress versión expuesta: Se detectó públicamente la versión 183 y 2, facilitando que atacantes identifiquen y exploten vulnerabilidades conocidas (CVEs).
[HIGH] Cookie PHPSESSID (HttpOnly/Secure): La falta de estas banderas permite que la sesión sea robada mediante scripts maliciosos (XSS) o interceptada en conexiones no seguras.
[MEDIUM] X-Content-Type-Options: Al no estar configurada, el navegador puede intentar interpretar archivos como un tipo de contenido distinto, permitiendo la ejecución de scripts camuflados.
[MEDIUM] Contenido Mixto: Existen 6 recursos que cargan mediante HTTP dentro de la página segura, lo que compromete la seguridad global del cifrado SSL.
[MEDIUM] Acceso a /readme.html y /wp-login.php: Estos archivos y rutas administrativas están expuestos, revelando detalles técnicos y permitiendo intentos de acceso no autorizados.
[MEDIUM] Cookie PHPSESSID (SameSite): La ausencia de esta bandera hace que la sesión sea susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Referrer-Policy: No existe una política definida para controlar cuánta información de procedencia se envía a terceros al hacer clic en enlaces.
[MEDIUM] Permissions-Policy: Falta una política que restrinja el acceso de las APIs del navegador a funciones sensibles como la cámara o el micrófono.
[LOW] Server header expuesto: El encabezado revela el uso de nginx, proporcionando información útil para que un atacante refine sus vectores de ataque.
[LOW] Meta generator expuesto: El código fuente detalla el uso de Elementor 4.0.1 y configuraciones específicas de fuentes y breakpoints.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa al directorio admin, señalando áreas restringidas que no deberían ser indexadas ni sugeridas.