EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://site2.q10.com/login?ReturnUrl=%2F&aplentId=977c8300-505c-4ab0-beb5-c59...	Escaneado	98ab90faa2
Dominio	site2.q10.com	Hallazgos	52 totales
Fecha	8 de agosto de 2026 a las 14:54	Problemas	9 detectados

B

83/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web ha otorgado una puntuación de 83/100, equivalente a una nota B. Se ejecutaron un total de 9 checks pasivos, resultando en 5 verificaciones exitosas, 3 advertencias y 1 fallo en configuraciones críticas. Aunque la infraestructura de cifrado es robusta, existen carencias importantes en las políticas de seguridad del servidor y en la protección de las cookies. El sitio presenta vulnerabilidades que podrían ser explotadas mediante ataques de intermediarios o manipulación de sesiones. Se concluye que el sitio es moderadamente seguro, pero requiere correcciones inmediatas para mitigar riesgos de nivel alto y medio.

Resumen de Riesgos

0	1	7	1	43
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 74 dias
Cabeceras de Seguridad	60	FALLO	Solo 3/6 presentes. Faltan: X-Frame-Options, Ref...
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	67	AVISO	.ASPXANONYMOUS: falta SameSite; XperiCode.CacheT...
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 74 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  74 dias restantes (expira: 2026-10-21T13:59:44.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-06T13:59:44.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: FALLO

Solo 3/6 presentes. Faltan: X-Frame-Options, Referrer-Policy, Permissions-Policy

- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' blob: https:...

- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubdomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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://site2.q10.com/
- 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

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)
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 67/100

Estado: AVISO

.ASPXANONYMOUS: falta SameSite; XperiCode.CacheTempData.SessionId: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: .ASPXANONYMOUS — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: .ASPXANONYMOUS — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: .ASPXANONYMOUS — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: XperiCode.CacheTempData.SessionId — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: XperiCode.CacheTempData.SessionId — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: XperiCode.CacheTempData.SessionId — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.q10.com/terminoscondiciones

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (26 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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

[ALTA] X-Frame-Options: Esta cabecera de seguridad no está presente, lo que permite que el sitio sea cargado dentro de un iframe y facilita ataques de clickjacking para engañar al usuario.
[MEDIA] Referrer-Policy: La ausencia de esta directiva impide controlar qué información de navegación se comparte con otros dominios al seguir enlaces externos.
[MEDIA] Permissions-Policy: No se han definido restricciones para el uso de APIs del navegador, dejando expuestas funciones como la cámara o el micrófono ante posibles inyecciones.
[MEDIA] Seguridad de Cookies (.ASPXANONYMOUS): Falta el atributo SameSite, lo que vuelve a la cookie vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIA] Seguridad de Cookies (XperiCode.CacheTempData.SessionId): La cookie de sesión carece del atributo SameSite, permitiendo que navegadores envíen información sensible en contextos no seguros.
[MEDIA] Contenido Mixto: Se detectó el recurso http://www.q10.com/terminoscondiciones cargado mediante HTTP, lo cual debilita la integridad de la conexión cifrada HTTPS.
[MEDIA] Ruta /user/login: El panel de acceso está expuesto públicamente, lo que facilita el reconocimiento del sistema y posibles intentos de acceso no autorizado.
[MEDIA] Bloqueo de Rastreo: El archivo robots.txt prohíbe el acceso a todo el sitio, lo que puede interferir con herramientas legítimas de monitoreo de seguridad.
[BAJA] Sitemap.xml: El archivo de mapa del sitio no fue encontrado, dificultando la indexación controlada y la auditoría completa de los endpoints disponibles.