EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://app.thefuturepick.com/	Checks	9 pruebas
Dominio	app.thefuturepick.com	Hallazgos	44 totales
Fecha	16 de junio de 2026 a las 23:12	Problemas	10 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras la auditoría de seguridad realizada a app.thefuturepick.com, el sitio ha obtenido una puntuación de 80/100, lo que corresponde a una nota B. El análisis se basó en 9 comprobaciones pasivas, de las cuales 7 resultaron satisfactorias y 2 presentaron fallos relacionados con la configuración del servidor y la indexación. Se concluye que el sitio es generalmente estable en su cifrado de datos, pero se mantiene vulnerable ante ataques dirigidos al navegador del usuario debido a la ausencia de políticas de seguridad esenciales. La postura actual es de riesgo moderado, requiriendo ajustes técnicos para alcanzar un nivel de protección profesional.

Resumen de Riesgos

0	2	7	1	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 76 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	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 76 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  76 dias restantes (expira: 2026-08-31T23:22:41.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-02T23:22:42.000Z
- 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: Vercel — 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=63072000
- 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 308 redirige a https://app.thefuturepick.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 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

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

- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- 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

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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] Content-Security-Policy: Falta esta directiva, lo que permite la ejecución de scripts no autorizados y aumenta el riesgo de ataques XSS.
[HIGH] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking.
[MEDIUM] X-Content-Type-Options: El servidor no previene el sniffing de tipos MIME, permitiendo que el navegador interprete archivos de forma insegura.

[MEDIUM] Referrer-Policy: No se controla la información de referencia enviada en las peticiones, lo que podría exponer datos de navegación a terceros.
[MEDIUM] Permissions-Policy: No se restringe el acceso a funciones del hardware del usuario como la cámara o el micrófono a través del navegador.
[MEDIUM] Archivos /readme.html y /README.txt: Estos documentos son accesibles públicamente y podrían revelar información técnica sensible sobre el software base.
[MEDIUM] Paneles de login expuestos: Las rutas /wp-login.php y /user/login están abiertas al público, facilitando ataques de fuerza bruta contra las credenciales.
[LOW] Server header expuesto: La cabecera Server revela el uso de Vercel, lo que proporciona pistas sobre la infraestructura a potenciales atacantes.
[LOW] Robots.txt y Sitemap faltantes: La carencia de estos archivos impide una gestión adecuada del rastreo de buscadores y la indexación del contenido.