EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://equipo.com.uy/	Checks	9 pruebas
Dominio	equipo.com.uy	Hallazgos	52 totales
Fecha	28 de julio de 2026 a las 13:06	Problemas	20 detectados

D

45/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio equipo.com.uy arroja un resultado crítico con una puntuación de 45/100 y una nota de calificación D. La auditoría se basó en 9 checks pasivos, de los cuales solo 4 resultaron correctos, mientras que se detectaron 1 advertencia y 4 fallos de seguridad de alto impacto. Los hallazgos principales revelan una infraestructura desactualizada y una configuración de servidor deficiente que no implementa medidas básicas de protección contra ataques web. Debido a la exposición de versiones de software obsoletas y la falta de cifrado forzado, se concluye que el sitio es actualmente vulnerable a ataques de inyección, interceptación de datos y secuestro de sesiones.

Resumen de Riesgos

0	6	11	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	70	AVISO	Certificado expira en 29 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 3.3.9 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	19 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 70/100

Estado: AVISO

Certificado expira en 29 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- MEDIO **Dias hasta expiracion**
  29 dias restantes (expira: 2026-08-26T16:19:13.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-28T16:19:14.000Z
- 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: Apache — 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
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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 4.0.5; features: additional_custom_breakpoints; settings: css_print_method-internal, google_font-enabled, font_display-swap
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 3.3.9 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 3.3.9 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 — 100/100

Estado: OK

No se encontraron cookies

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

Contenido Mixto — 20/100

Estado: FALLO

19 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://equipo.com.uy/wp-content/uploads/2025/11/Tem-banner.p...
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://equipo.com.uy/wp-content/uploads/2025/11/mabe_728-x-9...
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://equipo.com.uy/wp-content/uploads/2025/10/logos-marcas...
- MEDIO **src (script/img/iframe)**
  ...y 14 mas del mismo tipo
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://equipo.com.uy/wp-content/uploads/2026/05/WhatsApp-Ima...

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (316 bytes)
- INFO **Reglas robots.txt**
  6 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://equipo.com.uy/wp-sitemap.xml
- 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] WordPress version: La versión 3.3.9 se encuentra expuesta públicamente, permitiendo a atacantes buscar vulnerabilidades conocidas (CVEs) específicas para este software antiguo.
[HIGH] Content-Security-Policy: Falta esta cabecera esencial para prevenir ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: Ausencia de protección contra ataques de clickjacking, lo que permite que el sitio sea cargado dentro de marcos externos no autorizados.
[HIGH] Strict-Transport-Security: No se ha configurado la cabecera HSTS, impidiendo que el navegador fuerce conexiones seguras en futuras visitas.
[HIGH] HTTP a HTTPS redirección: El sitio no redirige automáticamente el tráfico inseguro HTTP a HTTPS, devolviendo un código 200 que permite comunicaciones no cifradas.
[MEDIUM] Contenido Mixto: Se detectaron 19 recursos, como imágenes y scripts, que se cargan mediante HTTP dentro de una página HTTPS, comprometiendo la seguridad global del cifrado.
[MEDIUM] X-Content-Type-Options: Falta esta directiva para evitar que los navegadores realicen MIME-type sniffing y ejecuten archivos con formatos incorrectos.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a otros sitios al navegar desde el dominio analizado.
[MEDIUM] Permissions-Policy: El sitio no restringe el uso de APIs sensibles del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y facilita información sobre la instalación y versión del CMS a posibles atacantes.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es visible para cualquier usuario de internet, facilitando ataques de fuerza bruta.
[LOW] Server header expuesto: La cabecera del servidor revela el uso de Apache, proporcionando pistas sobre la tecnología subyacente para ataques dirigidos.
[LOW] Meta generator: La etiqueta meta expone detalles técnicos de Elementor 4.0.5 y sus configuraciones internas.
[LOW] Ruta sensible en robots.txt: Se incluye una referencia directa a la ruta "admin", indicando a los rastreadores y atacantes dónde se encuentran áreas restringidas.
[WARN] SSL/TLS: El certificado de seguridad actual expira en 29 días, lo que representa un riesgo de interrupción del servicio a corto plazo.