EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.mediafire.com/file/4zhqzh05fseo6l9/ULTRAKILL.Build.22195083.zip/file	9 pruebas	
Dominio	www.mediafire.com	Hallazgos	57 totales
Fecha	30 de junio de 2026 a las 05:22	Problemas	19 detectados

D

56/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha resultado en una puntuación de 56/100, lo que equivale a una calificación de grado D. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 3 resultaron satisfactorios, 3 generaron advertencias y 3 fueron fallos críticos. Se detectaron deficiencias importantes en la implementación de cabeceras de seguridad y en la configuración de la privacidad de las cookies. Debido a la falta de cifrado forzado y la ausencia de políticas contra inyección de código, el sitio se clasifica actualmente como vulnerable.

Resumen de Riesgos

0	7	10	2	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 31 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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	42	FALLO	ukey: falta Secure; ukey: falta SameSite; 4zkl: ...
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 31 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  31 dias restantes (expira: 2026-07-30T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-08-05T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, 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
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=0
- 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 403 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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

Seguridad de Cookies — 42/100

Estado: FALLO

ukey: falta Secure; ukey: falta SameSite; 4zkl: falta Secure; 4zkl: falta SameSite; conv_tracking_data-2: falta HttpOnly; conv_tracking_data-2: falta Secure; conv_tracking_data-2: falta SameSite

- INFO **Cookies detectadas**
  4 cookie(s) encontrada(s)
- INFO **Cookie: ukey — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: ukey — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: ukey — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: 4zkl — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: 4zkl — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: 4zkl — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: conv_tracking_data-2 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: conv_tracking_data-2 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: conv_tracking_data-2 — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: __cf_bm — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __cf_bm — SameSite**
  SameSite=none

Contenido Mixto — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://blog.mediafire.com/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://blog.mediafire.com/

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (212 bytes)
- INFO **Reglas robots.txt**
  9 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 — 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 permite ataques de Cross-Site Scripting (XSS) e inyección de datos maliciosos.
[HIGH] Redirección HTTPS: El sitio no redirige el tráfico inseguro HTTP a HTTPS, devolviendo un error 403, lo que expone la comunicación.
[HIGH] HSTS (Strict-Transport-Security): No está configurado, impidiendo que el navegador obligue a usar conexiones seguras en futuras visitas.
[HIGH] Cookies sin flag Secure: Las cookies ukey, 4zkl y conv_tracking_data-2 pueden ser transmitidas por canales no cifrados.
[HIGH] Cookie sin flag HttpOnly: La cookie conv_tracking_data-2 es accesible mediante scripts del lado del cliente, facilitando el robo de sesión.
[MEDIUM] X-Content-Type-Options: Falta esta protección, permitiendo que el navegador realice sniffing de tipos MIME y ejecute archivos peligrosos.
[MEDIUM] Referrer-Policy: No existe una política definida, lo que puede filtrar información sensible en las cabeceras de navegación.
[MEDIUM] Permissions-Policy: La falta de esta cabecera no restringe el acceso del sitio a funciones del navegador como cámara o micrófono.
[MEDIUM] Cookies sin flag SameSite: Las cookies de la sesión no tienen restricciones de origen, lo que hace al sitio vulnerable a ataques CSRF.
[MEDIUM] Contenido Mixto: Se identificaron 2 recursos (hojas de estilo del blog) cargándose mediante HTTP en una página HTTPS.
[MEDIUM] Puerto 8080 abierto: La detección de un puerto alternativo HTTP-Alt abierto representa un vector de ataque adicional.
[MEDIUM] Robots.txt restrictivo: El archivo bloquea el acceso a todo el contenido mediante Disallow: /, ocultando el sitio a auditorías y buscadores.
[LOW] Server Header expuesto: La cabecera revela el uso de infraestructura de Cloudflare, proporcionando información útil para un atacante.
[LOW] Sitemap.xml faltante: La ausencia de este archivo dificulta la indexación y el análisis estructurado del sitio.