EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.plataformacashfinanciero.com.pe/easyseguridadbfp/easylogin-nr/index.html	Checks	9 pruebas
Dominio	www.plataformacashfinanciero.com.pe	Hallazgos	49 totales
Fecha	1 de julio de 2026 a las 04:57	Problemas	10 detectados

D

59/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis técnico de ciberseguridad realizado ha determinado una puntuación de 59/100, lo que equivale a una nota de calificación D. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 4 resultaron exitosos, 2 generaron advertencias y 3 fueron calificados como fallos. Los resultados muestran una infraestructura con una base de cifrado SSL aceptable, pero con deficiencias graves en la configuración de cabeceras de seguridad y exposición de servicios innecesarios. Se concluye que el sitio es actualmente vulnerable y presenta riesgos significativos para la integridad de los datos de los usuarios.

Resumen de Riesgos

0	5	3	2	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 136 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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	83	AVISO	incap_ses_690_2848593: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 136 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  136 dias restantes (expira: 2026-11-13T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-10-31T00:00:00.000Z
- 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

- 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=31536000
- 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
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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 — 83/100

Estado: AVISO

incap_ses_690_2848593: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: visid_incap_2848593 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: visid_incap_2848593 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: visid_incap_2848593 — SameSite**
  SameSite=none
- ALTO **Cookie: incap_ses_690_2848593 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: incap_ses_690_2848593 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: incap_ses_690_2848593 — SameSite**
  SameSite=none

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

- BAJO **robots.txt**
  No encontrado (HTTP 403)
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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] Puerto 21 (FTP): El puerto se encuentra abierto, permitiendo la transferencia de archivos mediante un protocolo que no cifra la información ni las credenciales.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) y la inyección de contenido no autorizado en el navegador del usuario.
[HIGH] X-Frame-Options: El sitio no cuenta con protección contra clickjacking, lo que permite que la página sea embebida en marcos externos maliciosos.
[HIGH] Redirección HTTPS: No existe una redirección automática de tráfico HTTP a HTTPS, y el intento de conexión segura por defecto devuelve un código de error 403.
[HIGH] Cookie incap_ses_690_2848593: La cookie de sesión carece del atributo HttpOnly, lo que permite su acceso a través de scripts de cliente y facilita el secuestro de sesiones.
[MEDIUM] X-Content-Type-Options: Falta la cabecera que impide al navegador realizar MIME-sniffing, aumentando el riesgo de ejecución de archivos maliciosos disfrazados de otros tipos de datos.
[MEDIUM] Referrer-Policy: No hay control sobre la información de referencia que se envía al navegar hacia enlaces externos, pudiendo exponer rutas internas de la aplicación.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a las APIs del navegador, permitiendo que scripts de terceros puedan intentar acceder a componentes como la cámara o el micrófono.
[LOW] Archivos de indexación: No se detectaron los archivos robots.txt ni sitemap.xml, lo que impide una gestión adecuada del rastreo por parte de buscadores y revela falta de mantenimiento.