# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://addi.ehu.es | Checks | 9 pruebas |
| Dominio | addi.ehu.es | Hallazgos | 51 totales |
| Fecha | 16 de septiembre de 2026 a las 18:04 | Problemas | 12 detectados |

C

72/100

puntos de seguridad

## RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio arroja una puntuación de 72/100 con una calificación de grado C. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 5 resultaron satisfactorias, 2 generaron advertencias y 2 finalizaron con fallos críticos. Aunque la cifrado de transporte es válido, se han detectado deficiencias importantes en la configuración de cabeceras y en la protección de las sesiones de usuario. Por tanto, el sitio se considera vulnerable a ataques de interceptación de datos y manipulación de contenido debido a la falta de políticas de seguridad modernas.

## Resumen de Riesgos

| 0 | 4 | 6 | 2 | 39 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 143 dias |
| Cabeceras de Seguridad | 55 | AVISO | 4/6 presentes. Faltan: Content-Security-Policy, ... |
| Redireccion HTTPS | 70 | AVISO | HTTP redirige a HTTPS pero falta HSTS |
| 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 | 33 | FALLO | JSESSIONID: falta Secure; JSESSIONID: falta Same... |
| Contenido Mixto | 20 | FALLO | 12 recursos HTTP en pagina HTTPS |
| Robots.txt y Sitemap | 100 | OK | robots.txt y sitemap.xml presentes |
| Puertos Abiertos | 100 | OK | 2 puerto(s) abierto(s), todos esperados |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 143 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  143 dias restantes (expira: 2027-02-06T18:12:29.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-22T18:12:30.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

## Cabeceras de Seguridad — 55/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido

- INFO **X-Frame-Options**
  Presente: DENY
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: geolocation=(), microphone=()

## Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://addi.ehu.es/
- 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

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
- BAJO **Meta generator**
  Expone: DSpace 6.4

## 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 — 33/100

Estado: FALLO

JSESSIONID: falta Secure; JSESSIONID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: JSESSIONID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: JSESSIONID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: JSESSIONID — SameSite**
  Falta SameSite — Vulnerable a CSRF

## Contenido Mixto — 20/100

Estado: FALLO

12 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://addi.ehu.es:80/open-search/description.xml
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.ehu.es
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://addi.ehu.es:80/?locale-attribute=en
- MEDIO **href (link/stylesheet)**
  ...y 9 mas del mismo tipo

## Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (3206 bytes)
- INFO **Reglas robots.txt**
  16 Disallow, 2 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://addi.ehu.eus/sitemap
- 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**

[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que permite ataques de degradación de protocolo y conexiones inseguras.
[HIGH] Cookie JSESSIONID - Flag Secure: La cookie de sesión carece del atributo Secure, permitiendo que la identificación del usuario se transmita por canales no cifrados.
[MEDIUM] Cookie JSESSIONID - Flag SameSite: La falta de esta configuración expone a los usuarios a ataques de falsificación de solicitud en sitios cruzados o CSRF.
[MEDIUM] Contenido Mixto: Se detectaron 12 recursos, como hojas de estilo y enlaces, que cargan mediante HTTP dentro de la página HTTPS, comprometiendo la integridad del sitio.
[MEDIUM] Robots.txt - Bloqueo total y exposición: El archivo prohíbe el rastreo completo del sitio y menciona la ruta config, lo que revela información sobre la estructura interna.
[LOW] Meta generator: El sitio expone públicamente que utiliza DSpace 6.4, lo que facilita a un atacante buscar exploits específicos para esa versión.