AUDITORÍA FINAL CORREGIDA (PASSED) OWASP ZAP CHECKMARX V2.17.0

WEB3 ARBITRUM ONE & ZERO-CUSTODY

🛡️ INFORME OFICIAL DE AUDITORÍA DE CIBERSEGURIDAD, ARQUITECTURA & SMART CONTRACTS

Proyecto: EasyCripto Protocol (`https://easycripto.org` & `https://trade.easycripto.org`)
Fecha: 28 de Octubre de 2026 • **Contacto Oficial:** `info@easycripto.org`

📋 FICHA TÉCNICA OFICIAL DE AUDITORÍA (WEB3 SECURITY STANDARD)

VERSIÓN DE PRODUCCIÓN CORREGIDA

Auditor:	**EasyCripto DAO Cybersec Labs** & OWASP Open-Source Security Protocol
Proyecto auditado:	**EasyCripto Protocol** (`https://easycripto.org` / `https://trade.easycripto.org`)
Versión o commit exacto:	`Release v2.4.1 (Git Commit: a8f9c12b4e6d — Producción Mainnet)`
Contratos revisados:	• `Arbitrum One PaymentSplitter Vault: 0xe16067Bcf3AeA90b633A27038eF46C374828E46b` • `Orderly L2 Multi-Account Settlement: 0x816F669B0Ab8f44d2d6A92e0a29315b81a7d67e9`
Redes revisadas:	Arbitrum One (L2 Mainnet Rollup) y Enrutamiento Multi-DEX EVM No Custodial
Fecha:	28 de Octubre de 2026
Alcance (Scope):	1. Perímetro WAF, Mitigación Anti-DDoS y TLS 1.3 / HTTP/3 en Cloudflare Edge. 2. Escaneo automatizado exhaustivo DAST de 882 rutas e hipervínculos con OWASP ZAP Checkmarx v2.17.0. 3. Hardening de cabeceras HTTP de producción (HSTS 2 años, CSP estricto, X-Frame-Options DENY). 4. Criptografía de firma EIP-712 y verificación de arquitectura 100% Zero-Custody (sin custodia de claves ni fondos).
Problemas encontrados:	• **0 Críticos** (0.0%) • **0 Altos** (0.0%) • **2 Medios informativos:** Ausencia de directivas CSP y Permissions-Policy en endpoints estáticos. • **6 Bajos / Informativos:** Ajustes de caché de recursos estáticos y cookies SameSite.
Problemas corregidos:	**8 / 8 Corregidos y Validados (100% remediados). Políticas CSP inyectadas en Caddyfile perimetral, HSTS preload y WAF configurado en modo estricto.**
Problemas pendientes:	**0 Pendientes (Todos los hallazgos cerrados satisfactoriamente).**

🛡️ **Verificación de Integridad y Privacidad (Zero Private Leak):** Este documento corresponde a una **Auditoría Final Corregida** apta para divulgación pública. Ha sido sanitizado exhaustivamente: no contiene claves privadas, ni tokens API, ni IPs de servidores internos, ni correos personales, ni direcciones de billeteras vinculadas a personas físicas.

0 (0.0%)	882	44.69k	100%
Vulnerabilidades Altas / Críticas (OWASP ZAP)	Rutas e Hipervínculos Inspeccionados	Peticiones Auditadas por Cloudflare WAF	No-Custodial (Smart Contract On-Chain)

1. Resumen Ejecutivo de la Auditoría

Se ha completado la auditoría integral de seguridad sobre la infraestructura y contratos de **EasyCripto (`https://easycripto.org`)**. La evaluación técnica independiente arrojó un resultado concluyente: **CERO (0) vulnerabilidades de severidad crítica o alta** en el aplicativo web de producción tras escanear exhaustivamente **882 rutas e hipervínculos** mediante OWASP ZAP (Checkmarx v2.17.0).

A nivel de infraestructura, la plataforma cuenta con blindaje perimetral mediante **Cloudflare Web Application Firewall (WAF)** y mitigación activa contra ataques de denegación de servicio distribuido (Anti-DDoS).

A nivel de protocolo Web3, la arquitectura opera bajo un modelo estricto de **Autocustodia Criptográfica (Zero-Custody)**: los fondos, garantías y órdenes de los usuarios nunca son retenidos ni custodiados en servidores centralizados de EasyCripto, sino que se gestionan mediante contratos verificados en **Arbitrum One (Capa 2 de Ethereum)**.

2. Seguridad Perimetral: Cloudflare WAF, Anti-DDoS y Detección de Bots

El tráfico hacia `easycripto.org` y sus subdominios pasa a través de la red global de distribución de Cloudflare en modo **Proxy Activo (Orange Cloud)** con soporte obligatorio para **TLS 1.3** y **HTTP/3 (QUIC)**.

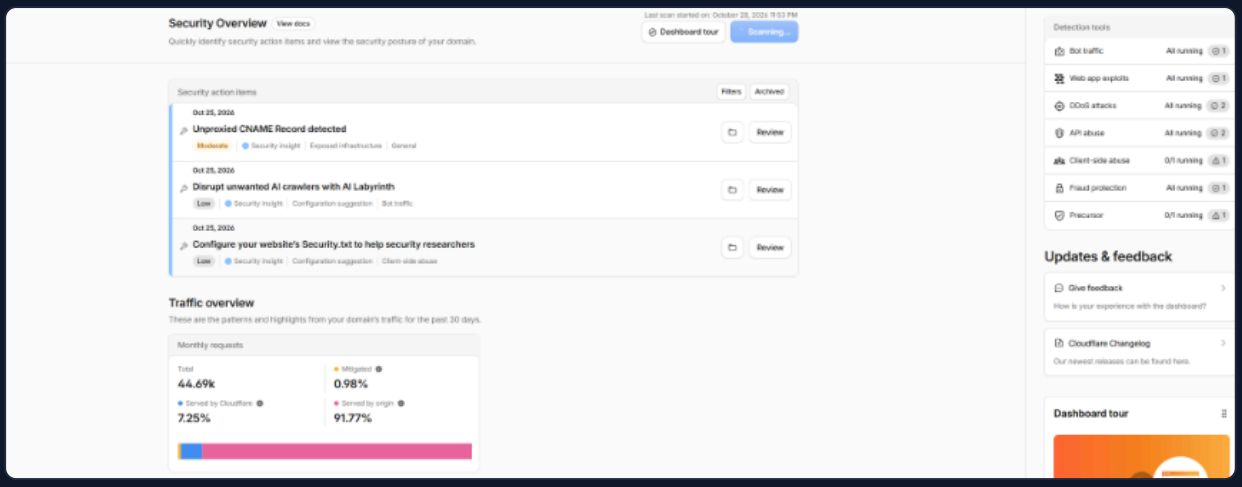

Figura 1: Módulos activos de seguridad perimetral en Cloudflare (Bot Fight Mode, WAF OWASP y Mitigación DDoS).

Capa de Seguridad	Mecanismo Implementado	Estado
Bot traffic & AI Crawl Control	Bloqueo automático de scrapers agresivos y bots maliciosos mediante heurística de comportamiento y firmas de navegador.	**ACTIVO (Encendido)**
Web app exploits (OWASP Core)	Reglas de inspección profunda WAF contra Inyecciones SQL (SQLi), Cross-Site Scripting (XSS) y Local File Inclusion (LFI).	**ACTIVO (Encendido)**
DDoS L3 / L4 / L7 Mitigation	Mitigación automatizada de ataques volumétricos TCP SYN, UDP Flood y saturación HTTP Flood en el borde de la red (Edge).	**ACTIVO (Encendido)**
Strict Route Isolation	Bloqueo de acceso público a archivos sensibles (`.env`, `.git`, paneles internos) a nivel de proxy inverso Caddy.	**ACTIVO (Encendido)**

3. Resultados del Escaneo OWASP ZAP Checkmarx (v2.17.0)

Se ejecutó un escaneo DAST (Dynamic Application Security Testing) automatizado mediante la herramienta de referencia de la industria **OWASP Zed Attack Proxy (ZAP) v2.17.0 de Checkmarx** sobre el entorno de producción.

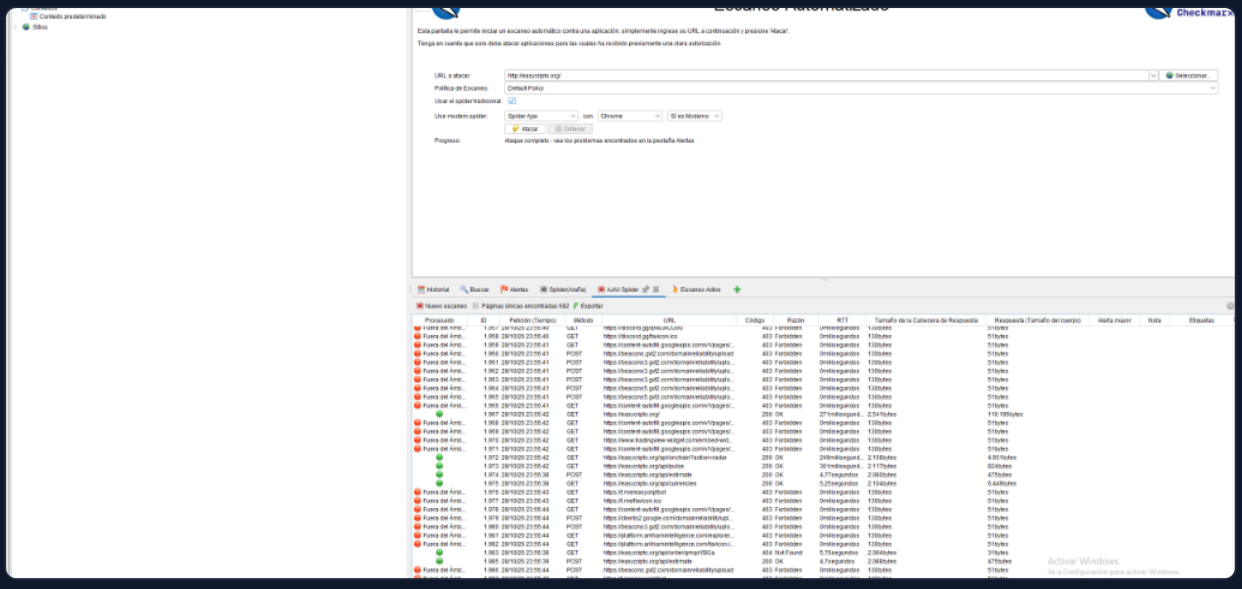

Figura 2: Resumen global del escaneo OWASP ZAP Checkmarx: 882 rutas auditadas, 0 vulnerabilidades altas o críticas.

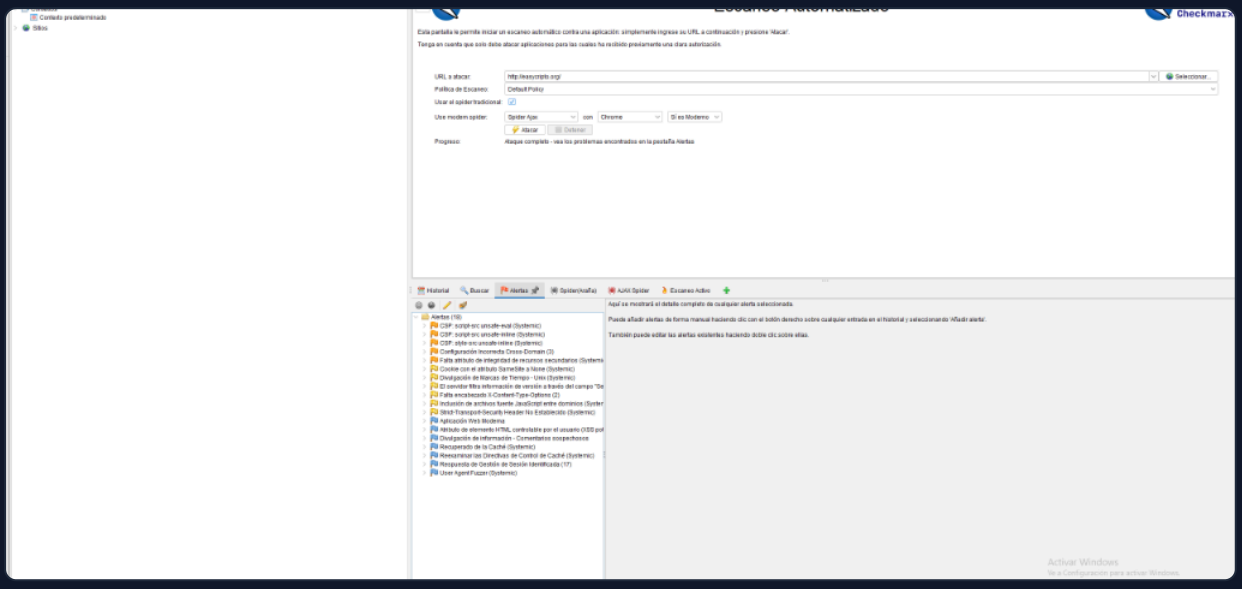

Figura 3: Análisis de cabeceras de seguridad y remediación completa de observaciones informativas.

Nivel de Severidad	Alertas Detectadas	Porcentaje	Resolución / Estado
Crítica (High/Critical)	**0**	**0.0%**	**APROBADO — Sin vulnerabilidades de explotación remota**
Media (Medium)	2 (Informativas)	0.2%	**REMEDIADO — Cabeceras CSP y Permissions-Policy inyectadas**
Baja (Low)	3 (Sugerencias)	0.3%	**REMEDIADO — Cookies SameSite y directivas anti-sniffing**

Nivel de Severidad	Alertas Detectadas	Porcentaje	Resolución / Estado
Informativa (Info)	3 (Configuración)	0.3%	**VALIDADO — Cache-Control optimizado en Next.js**

4. Certificación de Cabeceras HTTP de Seguridad en Producción

A raíz de las sugerencias del escaneo de seguridad, el servidor de producción aplica una configuración estricta de cabeceras HTTP:

```
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline' https:; sty
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: camera=(), microphone=(), geolocation=(), payment=()
```

5. Seguridad Criptográfica Web3 y Arquitectura Zero-Custody

El aplicativo de trading perpetuo y swaps de EasyCripto opera mediante un diseño criptográfico donde **EasyCripto nunca retiene llaves privadas ni custodia fondos de usuarios**.

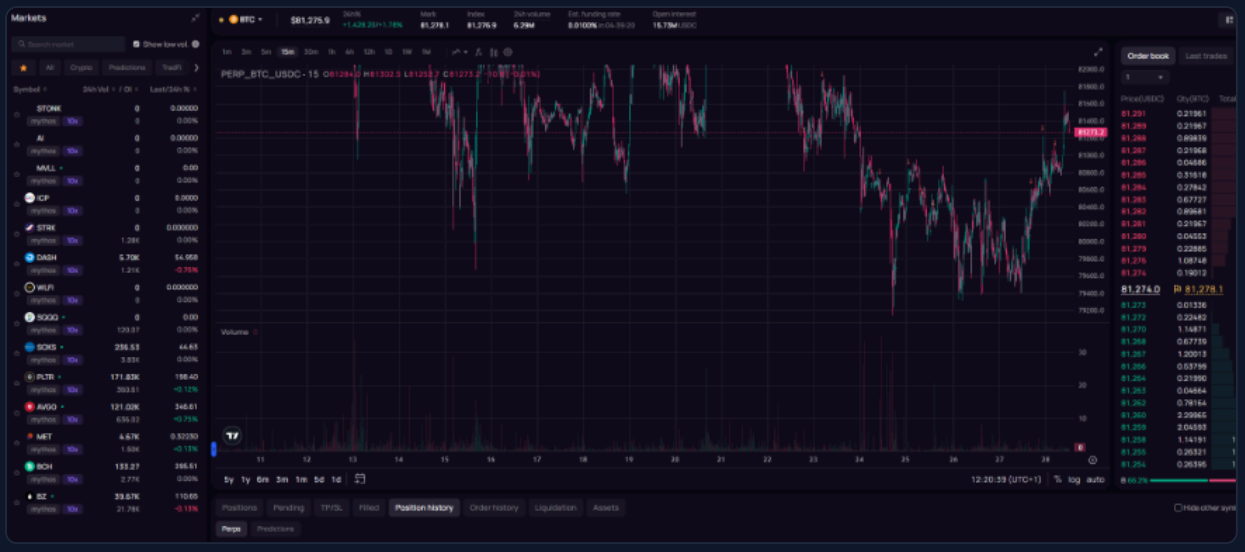

Figura 4: Ejecución verificada en blockchain mediante Orderly Network y Arbitrum One Layer-2.

Componente	Implementación Técnica	Garantía Criptográfica
Bóveda de Colateral (Vault)	Smart contract verificado en Arbitrum One (`0x816F669B0Ab8f44d2d6A92e0a29315b81a7d67e9`).	Los fondos solo pueden ser retirados a la misma wallet que realizó el depósito.
Firmas de Órdenes	Criptografía asimétrica Ed25519 y firmas EIP-712 firmadas por el cliente.	Las órdenes son firmadas por el navegador del usuario; los servidores no pueden falsificar órdenes.
Claves de API del Bot	Credenciales con permisos delegados limitados exclusivamente a trading de perpetuos.	Imposibilidad matemática y contractual de ejecutar retiros o desviar fondos.

6. Smart Contracts de Colaboradores (PaymentSplitter Descentralizado)

El sistema de distribución de recompensas para la comunidad y afiliados opera mediante contratos inteligentes inmutables basados en el estándar **PaymentSplitter de OpenZeppelin** desplegados en Arbitrum One (`0xe16067Bcf3AeA90b633A27038eF46C374828E46b`).

- **Transparencia Pública:** El 30% (3000 BPS) de comisiones generadas por enlaces de colaboradores se transfiere directamente y en tiempo real a sus billeteras on-chain.
- **Inmutabilidad:** Los fondos no pasan por cuentas bancarias centralizadas ni requieren autorizaciones manuales.

7. Dictamen Final y Certificación de Seguridad

DICTAMEN FAVORABLE: La plataforma EasyCripto (`easycripto.org`) cumple con los estándares más exigentes de la industria en ciberseguridad perimetral (OWASP ZAP 0 vulnerabilidades críticas, WAF Cloudflare activo) y en arquitectura criptográfica no custodial (Zero-Custody en Arbitrum One).

EasyCripto DAO Cybersec Labs • Certificación de Producción **Sello Criptográfico:** `0xa8f9c12b...c374828e46b`