Image not found or type unknown

. (Executive Summary & Objective)

MetaRang Frontend Next.js 16 (App Router / Standalone) React 19 Server Actions (src/components/utils/actions.js) API Route Handlers (src/app/**/api/**) (SSO) Supabase Storage (Attack Surface) (SSR/Node/Edge) .

(Bug-Bounty-Grade Code Security Testing) :

Sub-Issue 1 (CI) Sub-Issue 6 . (Unit, Integration, E2E Security Tests) (XSS mXSS JSON-LD Script Breakout SSRF Path Traversal Open Redirect HTTP Parameter Pollution Timing Side-Channel Header/CRLF Injection Cache Poisoning Unrestricted File Upload) . GitHub Actions main (dev) Merge main Merge main . . (@theAwmin)

:

Sub-Issue 1 (Sequential Execution): Sub-Issue 1 (Vitest React Testing Library MSW Playwright) . . . (@theAwmin): (Fail) ( ) ( ) ( ) . (theAwmin) Assignees . (Zero External Network Calls): MSW (Mock Service Worker) Fetch/Request (Redirect 301/302 IP XSS API) . main (Main Branch Merge Gate Only): Branch Protection main dev . . (Master Action Plan & Sub-Issues Checklist) Sub-Issue 1: (Vitest, Playwright, MSW) Merge Gate main ENV PII Sentry

Sub-Issue 2: Sanitization (stripHtml.ts) XSS (Double-Encoding, Numeric/Hex Entities, Unclosed Tags) Rich-Text (quill) JSON-LD Schema Breakout

Sub-Issue 3: Server Actions (src/components/utils/actions.js): SSRF getMainFile Dot-Segment Path Traversal (..) sanitizePathSegment / getSingleVideoData

Sub-Issue 4: API Route Handlers (src/app/**/api/**): Redirect-SSRF URL Parser Confusion (model) SVG Range flag firstpage-video Timing Attack webhook SMTP Header Injection / ReDoS sendEmail

Sub-Issue 5: (SSO) authRedirect.ts (HPP Open Redirect [removed] URI) getAuthData.tsx ReDoS validationAuth.tsx uploadImage.ts

Sub-Issue 6: E2E Playwright (DOM/Reflected XSS HTTP next.config.js src/middleware.ts) main . (Standard Bug Report Template for @theAwmin)

Fail @theAwmin (Assign) :

** :** `[Security-Bug][Phase-X] < />` **Assignee:** @theAwmin **Labels:** `Security`, `bug`, `AppSec`, `Priority: High` ### . (Vulnerability Metadata) - ** (CWE / OWASP):** (CWE-79: Improper Neutralization of Input During Web Page Generation / DOM XSS) - ** (Severity / CVSS v3.1):** (Critical / High / Medium) - ** :** `src/...` (X Y) - ** :** #< > - ** :** `tests/security/phaseX-....test.ts` (: `should reject ...`) ### . (Root Cause Analysis) < > ### . (Proof of Concept - PoC Payload) - ** (Input Payload):** `...` - ** (Actual Vulnerable Behavior):** `...` - ** (Expected Secure Behavior):** `...` ### . (Recommended Remediation) < >

: (AppSec & Bug-Bounty Test Suite) Merge Gate main
: manager of backend
: 3
: 18 30
:
: 1
: 2026.11.14
: 2027.01.21