Kayvrn Security Report

Executive Summary

The scan of yourdomain.io found 132 issues (grade F), including 1 critical and 25 high findings requiring immediate attention. 2 CVE-linked findings are confirmed reachable — a direct HTTP probe verified the affected service is accessible. Technologies detected: Cloudflare WAF / CDN, Cloudflare WAF / CDN, Nginx, Cloudflare WAF / CDN. 50 previously-reported issues resolved.

Security Posture

F

132 total findings

Severity	Count
Critical	1
High	25
Medium	0
Low	0
Info	106

Change	
+ Introduced	0
✓ Closed	50
~ Still open	132

Scan Details

Domain	yourdomain.io	**Scan ID**	6cdb5c79-6287-4cfa-8126-edc3e1197139
Trigger	Manual	**Completed**	16 Jun 2026, 20:30 UTC
Organisation	88202812-14e7-46b5-afc8-cfb85348725e	**Scheduled for**	—

Public Surface Discovered

Internet-facing assets 3 public hosts Kayvrn can reach	**Subdomains** 2 discovered
DNS records 12 mapped (A, AAAA, MX, TXT…)	**Web endpoints** 43 reachable pages & routes
Security certificates 2 (valid…)	**WAF / CDN** Cloudflare — traffic is filtered before reaching your servers

What The Internet Can See

A summary of what is publicly observable about your attack surface. Items in the clean list passed all checks — maintain them. Items requiring attention are counted by priority tier.

Publicly Visible

No issues found — ensure these remain correctly configured.

- ✓ Valid TLS certificates
- ✓ TLS 1.2 / TLS 1.3 enabled
- ✓ HTTPS available
- ✓ WAF / CDN protection detected: cloudflare (0.9 confidence) — signals: server:cloudflare, cf-ray:present
- ✓ No subdomain takeover detected

- ✓ No exposed databases detected
- ✓ No exposed Kubernetes API detected
- ✓ No exposed Docker API detected
- ✓ No exposed Redis detected
- ✓ No exposed MongoDB detected
- ✓ No exposed Elasticsearch detected
- ✓ No exposed SMB services detected
- ✓ No exposed RDP services detected
- ✓ No exposed VNC services detected
- ✓ No confirmed SSRF identified
- ✓ No confirmed XXE identified
- ✓ No confirmed command injection identified
- ✓ No confirmed deserialisation identified
- ✓ No confirmed authentication bypass identified
- ✓ No confirmed privilege escalation identified
- ✓ No publicly accessible storage buckets detected
- ✓ No publicly accessible source maps detected
- ✓ No parked domains detected

Publicly Visible Requiring Attention

FIX NOW	5
INVESTIGATE	87

Technology Detected

Software detected on your attack surface. Items with a CVE count have associated known-vulnerability findings.

Product	Version	Confidence	Asset	CVEs
Cloudflare WAF / CDN	CDN / WAF	90% response headers	https://yourdomain.io/	—
Cloudflare WAF / CDN	CDN / WAF	90% response headers	https://app-api.yourdomain.io/	—
Nginx	1.28.3	—	https://app-api.yourdomain.io/	—
Cloudflare WAF / CDN	CDN / WAF	90% response headers	https://app.yourdomain.io/	—
Nginx	1.28.3	—	https://yourdomain.io/	—

Attack Paths

The attack-path engine ran a bounded graph search (up to 6 hops) over your asset inventory, connecting internet-exposed nodes to active high or critical findings. Paths are scored: **exploit maturity × reachability × blast radius**. Score 1.0 = maximum exposure. Direct paths (0 hops) mean the vulnerable asset is directly reachable from the internet without traversal.

#	Severity	Score	Hops	Attack scenario
1	CRITICAL	**0.70** EM 0.70 × R 1.00 × BR 1.00	1	netdata-dev.monitor.yourdomain.io → https://netdata-dev.monitor.yourdomain.io/: cors.credentialed_access_confirmed netdata-dev.monitor.yourdomain.io → https://netdata-dev.monitor.ap…
2	HIGH	**0.45** EM 0.45 × R 1.00 × BR 1.00	1	app.yourdomain.io → https://app.yourdomain.io/: open_redirect.dom_based app.yourdomain.io → https://app.yourdomain.io/
3	HIGH	**0.45** EM 0.45 × R 1.00 × BR 1.00	1	dev.yourdomain.io → https://dev.yourdomain.io/: open_redirect.dom_based dev.yourdomain.io → https://dev.yourdomain.io/
4	HIGH	**0.45** EM 0.45 × R 1.00 × BR 1.00	1	dev-api.yourdomain.io → https://dev-api.yourdomain.io/: open_redirect.dom_based dev-api.yourdomain.io → https://dev-api.yourdomain.io/
5	HIGH	**0.45** EM 0.45 × R 1.00 × BR 1.00	Direct	https://yourdomain.io/ (direct exposure): open_redirect.dom_based https://yourdomain.io/
6	HIGH	**0.45** EM 0.45 × R 1.00 × BR 1.00	1	portainer-dev.monitor.yourdomain.io → https://portainer-dev.monitor.yourdomain.io/: open_redirect.dom_based portainer-dev.monitor.yourdomain.… → https://portainer-dev.monitor.…
7	HIGH	**0.45** EM 0.45 × R 1.00 × BR 1.00	1	dozzle-dev.monitor.yourdomain.io → https://dozzle-dev.monitor.yourdomain.io/: debug.env_exposed dozzle-dev.monitor.yourdomain.io → https://dozzle-dev.monitor.app…
8	HIGH	**0.45** EM 0.45 × R 1.00 × BR 1.00	1	devapp.yourdomain.io → https://devapp.yourdomain.io/: open_redirect.dom_based devapp.yourdomain.io → https://devapp.yourdomain.io/
9	HIGH	**0.45** EM 0.45 × R 1.00 × BR 1.00	1	app-api.yourdomain.io → https://app-api.yourdomain.io/: open_redirect.dom_based app-api.yourdomain.io → https://app-api.yourdomain.io/

Things That Need Attention

Report scope — 21 additional high-severity findings detected but not shown. This PDF covers confirmed issues for **yourdomain.io** and its directly registered assets. The full scan found **26 high or critical** issues across all discovered subdomains — findings on other subdomains require dashboard access to view. Sign in at **app.kayvrn.com** for the complete picture.

FIX NOW 5 findings

Host	Rule / Evidence	Asset	Message & Impact
yourdomain.io	cache.deception_confirmed cache_poisoning	https://yourdomain.io/account/kayvrn-cache-test.css	Web cache deception confirmed at `/account`: appending `/kayvrn-cache-test.css` to a sensitive path returned HTTP 200 with caching headers (cache_hit=True, is_cacheable=True). CONFIRMED: anonymous unauthenticated client retrieved the cached response — private data is publicly accessible. A cache layer may store this private-looking response and serve it to unauthenticated users who request the same URL. **[STRONG SIGNAL]** **Impact:** Cache poisoning lets an attacker store a malicious response in a shared cache, delivering it to every subsequent user who requests the same resource. **Fix:** Ensure cache keys include all request headers that influence the response. Add Cache-Control: no-store to responses containing user-specific data. Audit CDN/proxy cache key configu… *url: https://yourdomain.io/account/kayvrn-cache-test.css · status_code: 200*
yourdomain.io	http_smuggling.cl0_confirmed http_smuggling	https://yourdomain.io/	HTTP request smuggling CL.0 confirmed at `https://yourdomain.io/`: a POST with `Content-Length: 0` and a non-empty body caused the follow-up victim request to receive HTTP 405 (anomalous), indicating the server read the smuggled body as the start of the next request. **[STRONG SIGNAL]** **Impact:** HTTP request smuggling lets an attacker poison the request queue shared between a front-end proxy and back-end server, enabling cache poisoning, session hijacking, bypassing access… **Fix:** Ensure your front-end proxy and back-end servers agree on how Content-Length and Transfer-Encoding headers are parsed. Upgrade to HTTP/2 end-to-end where possible, as it is not sus… *host: yourdomain.io · port: 443*
app-api.	open_redirect.dom_based open_redirect	https://app-api.yourdomain.io/login?next=https://evil.kayvrn-canary.invalid/	DOM-based open redirect at `https://app-api.yourdomain.io/login?next=https://evil.kayvrn-canary.invalid/`: after page load, client-side JavaScript navigated the browser to `https://evil.kayvrn-canary.invalid/`. This is a confirmed JS-driven redirect that bypasses server-side redirect validation. **[BROWSER CONFIRMED]** **Impact:** An open redirect allows attackers to craft URLs on your domain that silently forward users to malicious sites — enabling phishing, OAuth token theft, and bypassing referrer-based a… **Fix:** Validate all redirect targets against an allowlist of trusted destinations. Never construct redirect URLs from unvalidated user input. Use relative paths where possible, and return…
app.	open_redirect.dom_based open_redirect	https://app.yourdomain.io/login?next=https://evil.kayvrn-canary.invalid/	DOM-based open redirect at `https://app.yourdomain.io/login?next=https://evil.kayvrn-canary.invalid/`: after page load, client-side JavaScript navigated the browser to `https://evil.kayvrn-canary.invalid/`. This is a confirmed JS-driven redirect that bypasses server-side redirect validation. **[BROWSER CONFIRMED]** **Impact:** An open redirect allows attackers to craft URLs on your domain that silently forward users to malicious sites — enabling phishing, OAuth token theft, and bypassing referrer-based a… **Fix:** Validate all redirect targets against an allowlist of trusted destinations. Never construct redirect URLs from unvalidated user input. Use relative paths where possible, and return…

yourdomain.io	open_redirect.dom_based open_redirect	https://yourdomain.io/login?next=https://evil.kayvrn-canary.invalid/	DOM-based open redirect at `https://yourdomain.io/login?next=https://evil.kayvrn-canary.invalid/`: after page load, client-side JavaScript navigated the browser to `https://evil.kayvrn-canary.invalid/`. This is a confirmed JS-driven redirect that bypasses server-side redirect validation. **[BROWSER CONFIRMED]** **Impact:** An open redirect allows attackers to craft URLs on your domain that silently forward users to malicious sites — enabling phishing, OAuth token theft, and bypassing referrer-based a… **Fix:** Validate all redirect targets against an allowlist of trusted destinations. Never construct redirect URLs from unvalidated user input. Use relative paths where possible, and return…

INVESTIGATE 30 findings

Host	Rule / Evidence	Asset	Message & Impact
yourdomain.io	email.mailbox_takeover_risk email	yourdomain.io	`yourdomain.io` routes mail through a free consumer provider (`yourdomain-io.mail.protection.outlook.com`) without DMARC enforcement. If the account at that provider is deleted or expires, anyone can register it and receive all inbound mail for your domain — including password-reset emails. **[INVESTIGATE]** **Impact:** Email exposure increases phishing and spam risk and may indicate misconfigured DMARC/SPF/DKIM records. **Fix:** Configure SPF, DKIM, and DMARC records with a reject policy. Avoid publishing email addresses in public-facing HTML.
yourdomain.io ×2 hosts	cloud.public_container_image cloud	https://yourdomain.io/v2/	Container registry endpoint detected at `yourdomain.io/v2/` (HTTP 200, type: docker_registry_v2). Registry is publicly accessible — enumerate images. **[INVESTIGATE]** **Impact:** Publicly exposed container registries or cloud-native endpoints can reveal internal image layers, environment variables, build secrets, and service credentials embedded in Docker i… **Fix:** Restrict container registry access to authenticated pull only. Audit Docker image layers for embedded secrets using tools such as Trivy or truffleHog. Rotate any credentials found.… Also affects: yourdomain.io/v1/search
yourdomain.io	repo.package_registry_exposed cloud	https://yourdomain.io/v2/	Docker Registry package registry detected at `https://yourdomain.io/v2/` (HTTP 200). Exposed registries leak internal package names and versions, and may enable dependency-confusion or supply-chain attacks. **[INVESTIGATE]** **Impact:** Publicly exposed container registries or cloud-native endpoints can reveal internal image layers, environment variables, build secrets, and service credentials embedded in Docker i… **Fix:** Restrict container registry access to authenticated pull only. Audit Docker image layers for embedded secrets using tools such as Trivy or truffleHog. Rotate any credentials found.… *url: https://yourdomain.io/v2/ · status_code: 200*
yourdomain.io	email.high_spoofability_score email	yourdomain.io	`yourdomain.io` has a spoofability score of 100/100. This composite score reflects missing or weak SPF/DMARC/DKIM controls. Attackers can forge emails appearing to come from your domain with low risk of detection. **[INVESTIGATE]** **Impact:** Email exposure increases phishing and spam risk and may indicate misconfigured DMARC/SPF/DKIM records. **Fix:** Configure SPF, DKIM, and DMARC records with a reject policy. Avoid publishing email addresses in public-facing HTML.
yourdomain.io ×2 hosts	xss.js_sink_innerhtml xss	https://yourdomain.io/	JavaScript sink `innerhtml` detected in `https://yourdomain.io/_next/static/chunks/0m_p1bxtorv5i.js` at line ~1. innerHTML assignment found in JavaScript. If user-controlled data flows to this sink, it executes as HTML and enables stored or reflected XSS. Code context: `),a.onerror=r):n&&(a.innerHTML=n.children,setTimeout(e)),document.head.` **[INVESTIGATE]** **Impact:** Cross-site scripting allows injection of arbitrary JavaScript into your pages, enabling session hijacking, credential theft, keylogging, and defacement for any user who visits the … **Fix:** Apply context-aware output encoding (HTML, JS, URL) at every output point. Implement a strict Content-Security-Policy that disallows inline scripts. Use framework-level auto-escapi… Also affects: app.yourdomain.io/

yourdomain.io	dns.missing_caa dns	yourdomain.io	No CAA record on `yourdomain.io`. Without a Certification Authority Authorisation record any public CA can issue a certificate for your domain. Add a CAA record to pin permitted issuers (e.g. `0 issue "letsencrypt.org"`). **[INVESTIGATE]** **Impact:** DNS misconfigurations can lead to traffic hijacking, subdomain takeover, or disruption of service availability. **Fix:** Audit DNS records for stale or dangling entries. Enable DNSSEC. Restrict zone transfers to authorised secondaries only.
yourdomain.io	email.dmarc.monitor_only email	_dmarc	DMARC is set to `p=none`. The policy is monitor-only — receivers do NOT take action on spoofed mail. Move to `p=quarantine` once you've reviewed your `rua=` reports for a few weeks. Additionally, no `rua=` aggregate reporting address is set — you will receive no DMARC reports and cannot monitor SPF/DKIM alignment. **[INVESTIGATE]** **Impact:** Email exposure increases phishing and spam risk and may indicate misconfigured DMARC/SPF/DKIM records. **Fix:** Configure SPF, DKIM, and DMARC records with a reject policy. Avoid publishing email addresses in public-facing HTML.
yourdomain.io	email.missing_mta_sts email	_mta-sts.yourdomain.io	No MTA-STS record at `_mta-sts.<domain>`. MTA-STS (RFC 8461) prevents SMTP downgrade attacks by publishing a strict TLS policy for inbound mail. Without it, intermediate mail servers can silently strip TLS and deliver mail in plaintext. **[INVESTIGATE]** **Impact:** Email exposure increases phishing and spam risk and may indicate misconfigured DMARC/SPF/DKIM records. **Fix:** Configure SPF, DKIM, and DMARC records with a reject policy. Avoid publishing email addresses in public-facing HTML.
app-api. **×2 hosts**	error_disclosure.framework_version error_disclosure	https://app-api.yourdomain.io/	Server reveals `Nginx 1.28.3` in an error page triggered by: `invalid method NOTAVERB`. Version disclosure allows attackers to target known CVEs for the exact framework release. **[INVESTIGATE]** **Impact:** Framework or server version disclosure in error pages gives attackers a precise target for known CVEs, reducing the effort required to identify and exploit version-specific vulnera… **Fix:** Suppress framework and server version strings in error pages, response headers (Server, X-Powered-By), and HTTP 404/500 pages. Configure your web server and application framework t… Also affects: yourdomain.io/
yourdomain.io	clickjacking.frameable http	https://yourdomain.io/login	Sensitive page `/login` can be embedded in an iframe: no X-Frame-Options header and no CSP frame-ancestors directive. An attacker can load this page in a hidden iframe and trick a victim into interacting with it — credential phishing, forced clicks, or account-linking attacks. **[INVESTIGATE]** **Impact:** Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. **Fix:** Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable directory listing.
yourdomain.io	http.exposed_composer_json http	https://yourdomain.io/composer.json	`composer.json` is publicly accessible — exposes PHP dependency list and version ranges, aiding targeted exploitation. **[INVESTIGATE]** **Impact:** Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. **Fix:** Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable directory listing. *status_code: 200*

yourdomain.io	http.exposed_package_json http	https://yourdomain.io/package.json	`package.json` is publicly accessible — exposes Node.js dependency list and version ranges. **[INVESTIGATE]** **Impact:** Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. **Fix:** Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable directory listing. *status_code: 200*
yourdomain.io ×2 hosts	http.missing_csp http	https://yourdomain.io/	No Content-Security-Policy header. Without CSP, browsers have no policy for blocking injected scripts (XSS), mixed content, or unwanted framing. **[INVESTIGATE]** **Impact:** Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. **Fix:** Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable directory listing. *url: https://yourdomain.io/ · expected_header: Content-Security-Policy* Also affects: app.yourdomain.io/
yourdomain.io ×2 hosts	http.missing_hsts http	https://yourdomain.io/	https://yourdomain.io/ returned 200 but no Strict-Transport-Security header — browsers may downgrade to HTTP on first visit. **[INVESTIGATE]** **Impact:** Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. **Fix:** Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable directory listing. *url: https://yourdomain.io/ · expected_header: Strict-Transport-Security* Also affects: www.yourdomain.io/
yourdomain.io	http.missing_x_frame_options http	https://yourdomain.io/	No X-Frame-Options header and no CSP frame-ancestors directive. The page can be embedded in an iframe, enabling clickjacking attacks. **[INVESTIGATE]** **Impact:** Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. **Fix:** Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable directory listing. *url: https://yourdomain.io/ · expected_header: X-Frame-Options*
app. ×21 hosts	rate_limit.too_permissive rate_limit	https://app.yourdomain.io/auth/login	Rate limiting on `/auth/login` (auth login) at https://app.yourdomain.io could not be confirmed: 15 rapid requests were sent — exceeding the OWASP API Security Top 10 (API4) recommended threshold of ≤10 failed attempts — and no 429 response was received. No X-RateLimit-* response headers were observed either, so it is not possible to confirm whether a limiter exists with a higher threshold or no limiter is present at all. Ensure rate limiting is enforced after ≤10 attempts and applied globally across all instances (shared Redis/database backend, not per-instance in-memory storage). **[INVESTIGATE]** **Impact:** Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force attacks, leading to account compromise at scale. **Fix:** Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or sliding-window algorithm. Return HTTP 429 with a Retry-Afte… *endpoint: /auth/login* Also affects: app.yourdomain.io/login, app.yourdomain.io/auth/token, app.yourdomain.io/oauth/token, app.yourdomain.io/v1/auth/login +16 more

app-api. ×2 hosts	debug.metrics_endpoint_exposed source_map	https://app-api.yourdomain.io/api/metrics	Prometheus metrics endpoint exposed at `/api/metrics`. Metrics expose service internals: request rates, error rates, latency histograms, and often infrastructure hostnames and dependency addresses. **[INVESTIGATE]** **Impact:** Exposed environment files, Git metadata, or source maps can reveal API keys, database credentials, internal architecture, and application source code — directly enabling targeted a… **Fix:** Remove or restrict access to .env files, .git directories, and JavaScript source maps on production servers. Use your web server to return 403/404 for these paths. Rotate any crede… Also affects: app.yourdomain.io/api/metrics
yourdomain.io ×2 hosts	xss.js_sink_location_assign xss	https://yourdomain.io/	JavaScript sink `location_assign` detected in `https://apfora.io/_next/static/chunks/0dgq26a5_oy.a.js` at line ~1. location.href / location.replace / location.assign assignment found. If user-controlled, enables open redirect and javascript: URI injection. Code context: `hard navigation",e),window.location.href=window.next.__pendingUrl.toString(),!0)` **[INVESTIGATE]** **Impact:** Cross-site scripting allows injection of arbitrary JavaScript into your pages, enabling session hijacking, credential theft, keylogging, and defacement for any user who visits the … **Fix:** Apply context-aware output encoding (HTML, JS, URL) at every output point. Implement a strict Content-Security-Policy that disallows inline scripts. Use framework-level auto-escapi… Also affects: app.yourdomain.io/
yourdomain.io	email.missing_tls_rpt email	_smtp._tls	No TLS-RPT record at `_smtp._tls.<domain>`. TLS Reporting (RFC 8460) lets SMTP senders report TLS negotiation failures to you. Without it, you are blind to TLS downgrade attacks and MTA-STS policy misconfigurations. **[INVESTIGATE]** **Impact:** Email exposure increases phishing and spam risk and may indicate misconfigured DMARC/SPF/DKIM records. **Fix:** Configure SPF, DKIM, and DMARC records with a reject policy. Avoid publishing email addresses in public-facing HTML.
yourdomain.io	email.spf.softfail email	@	SPF ends in `~all` (soft-fail). Receivers may still accept spoofed mail with a 'suspicious' flag. The recommended end state is `-all` (hard-fail) once you've confirmed your legitimate senders are listed. **[INVESTIGATE]** **Impact:** Email exposure increases phishing and spam risk and may indicate misconfigured DMARC/SPF/DKIM records. **Fix:** Configure SPF, DKIM, and DMARC records with a reject policy. Avoid publishing email addresses in public-facing HTML.
yourdomain.io ×2 hosts	http.missing_coep http	https://yourdomain.io/	No Cross-Origin-Embedder-Policy header. Without COEP the page cannot safely use `SharedArrayBuffer` and is exposed to Spectre-class side-channel attacks. **[INVESTIGATE]** **Impact:** Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. **Fix:** Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable directory listing. *url: https://yourdomain.io/ · expected_header: Cross-Origin-Embedder-Policy* Also affects: app.yourdomain.io/
yourdomain.io ×2 hosts	http.missing_coop http	https://yourdomain.io/	No Cross-Origin-Opener-Policy header. Opener-based leakage allows a page you linked to navigate back to your origin or probe your window object. **[INVESTIGATE]** **Impact:** Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. **Fix:** Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable directory listing. *url: https://yourdomain.io/ · expected_header: Cross-Origin-Opener-Policy* Also affects: app.yourdomain.io/

yourdomain.io	http.missing_referrer_policy http	https://yourdomain.io/	No Referrer-Policy header. Full URLs (including query strings and paths) may leak to third-party origins in the Referer header. **[INVESTIGATE]** **Impact:** Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. **Fix:** Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable directory listing. *url: https://yourdomain.io/ · expected_header: Referrer-Policy*
yourdomain.io	http.missing_x_content_type http	https://yourdomain.io/	No X-Content-Type-Options: nosniff header. MIME-type sniffing can allow browsers to interpret served content as executable script. **[INVESTIGATE]** **Impact:** Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. **Fix:** Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable directory listing. *url: https://yourdomain.io/ · expected_header: X-Content-Type-Options*
yourdomain.io	cmdi.blind_dns_payload_sent cmdi	https://yourdomain.io	Blind CMDi DNS callback payloads sent to https://yourdomain.io: nslookup '6cdb5c7962874cfa8126.165e74461e663cd293b4.oast.pro' injected via 3 paths × 3 parameters. No OOB callback received within the polling window. **[INVESTIGATE]** **Impact:** Command injection gives an attacker direct shell access on your server, enabling full compromise, data exfiltration, and lateral movement to internal systems. **Fix:** Never pass user-supplied input to shell commands. Use language-native APIs instead of shell invocations. If shell execution is unavoidable, use a strict allowlist for every argumen…
yourdomain.io **×2 hosts**	http.missing_corp http	https://yourdomain.io/	No Cross-Origin-Resource-Policy header. Any cross-origin site can embed this resource in an image or script element. **[INVESTIGATE]** **Impact:** Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. **Fix:** Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable directory listing. *url: https://yourdomain.io/ · expected_header: Cross-Origin-Resource-Policy* Also affects: app.yourdomain.io/
yourdomain.io	http.missing_permissions_policy http	https://yourdomain.io/	No Permissions-Policy header. Browser APIs (camera, microphone, geolocation) are not gated; third-party iframes can request them. **[INVESTIGATE]** **Impact:** Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. **Fix:** Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable directory listing. *url: https://yourdomain.io/ · expected_header: Permissions-Policy*
app.	http.x_powered_by_leak http	https://app.yourdomain.io/	X-Powered-By header discloses the runtime stack (Next.js). Remove this header to reduce fingerprinting surface. **[INVESTIGATE]** **Impact:** Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. **Fix:** Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable directory listing.

app-api. ×2 hosts	debug.health_endpoint_exposed source_map	https://app-api.yourdomain.io/healthz	Health/status endpoint exposed at `/healthz`. Health endpoints reveal service state and dependency status, which can help attackers map the technology stack and identify degraded dependencies. **[INVESTIGATE]** **Impact:** Exposed environment files, Git metadata, or source maps can reveal API keys, database credentials, internal architecture, and application source code — directly enabling targeted a… **Fix:** Remove or restrict access to .env files, .git directories, and JavaScript source maps on production servers. Use your web server to return 403/404 for these paths. Rotate any crede… Also affects: app.yourdomain.io/healthz
yourdomain.io	tls.dane_not_configured tls	_443._tcp.yourdomain.io	No DANE/TLSA record at `_443._tcp.yourdomain.io`. DANE (RFC 6698) pins the expected certificate or public key in DNS, preventing MitM even if a rogue CA mis-issues a cert for your domain. **[INVESTIGATE]** **Impact:** Certificate issues can enable man-in-the-middle attacks, connection failures, or browser warnings that erode user trust. **Fix:** Renew the certificate before expiry. Enforce TLS 1.2+ with strong cipher suites, use a trusted CA, and verify the full chain is served. *port: 443*

Credential Monitoring

Email addresses on your breach-monitoring watchlist checked against the Have I Been Pwned (HIBP) breach corpus.

No email addresses are configured for breach monitoring on this domain.

Changes Since Last Scan

Finding lifecycle changes and infrastructure drift detected by comparing this scan to the previous one.

Change	Count	Notes
+ Introduced	0	New findings not seen in any previous scan
✓ Closed	50	Previously open findings no longer detected
~ Still open	132	Findings carried over from prior scan(s)
Critical	1	
High	25	
Info	106	

Resolved Findings

The following findings were no longer detected in this scan.

Sev	Finding	Asset / Impact / Fix
INV	http.missing_corp	https://devapp.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	http.missing_referrer_policy	https://dozzle-dev.monitor.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	http.missing_permissions_policy	https://dev.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	http.missing_coep	https://dev.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	http.missing_coop	https://dev.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	http.missing_corp	https://dev.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	clickjacking.frameable	https://dev.yourdomain.io/login Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable

INV	http.missing_csp	https://devapp.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	http.missing_coop	https://devapp.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	http.missing_hsts	https://dozzle-dev.monitor.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	http.missing_permissions_policy	https://netdata-dev.monitor.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	http.missing_coep	https://netdata-dev.monitor.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	http.missing_referrer_policy	https://dev.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	http.missing_coop	https://netdata-dev.monitor.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	http.missing_corp	https://netdata-dev.monitor.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	http.missing_coep	https://devapp.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable

INV	http.cors_misconfigured	https://netdata-dev.monitor.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	http.missing_x_frame_options	https://dev.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	rate_limit.too_permissive	https://dev.yourdomain.io/api/auth/login Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	rate_limit.too_permissive	https://dev.yourdomain.io/login Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	http.missing_x_frame_options	https://netdata-dev.monitor.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	http.server_header_leak	https://portainer-dev.monitor.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	rate_limit.too_permissive	https://dev.yourdomain.io/api/login Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	rate_limit.too_permissive	https://dev.yourdomain.io/auth/token Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	http.missing_permissions_policy	https://dozzle-dev.monitor.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable

INV	rate_limit.too_permissive	https://dev.yourdomain.io/oauth/token Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	http.missing_coep	https://dozzle-dev.monitor.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	rate_limit.too_permissive	https://dev.yourdomain.io/api/token Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	http.missing_corp	https://dozzle-dev.monitor.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	rate_limit.too_permissive	https://dev.yourdomain.io/api/users/login Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	rate_limit.too_permissive	https://dev.yourdomain.io/api/v1/user/login Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	http.server_header_leak	https://dozzle-dev.monitor.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	rate_limit.too_permissive	https://dev.yourdomain.io/api/register Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	rate_limit.too_permissive	https://dev.yourdomain.io/api/v2/auth/login Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or

INV	error_disclosure.framework_version	https://dev.yourdomain.io/ Framework or server version disclosure in error pages gives attackers a precise target for known CVEs, reducing the effo Suppress framework and server version strings in error pages, response headers (Server, X-Powered-By), and HTTP 404/500
INV	rate_limit.too_permissive	https://devapp.yourdomain.io/auth/login Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	rate_limit.too_permissive	https://devapp.yourdomain.io/login Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	rate_limit.too_permissive	https://devapp.yourdomain.io/auth/token Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	http.missing_referrer_policy	https://netdata-dev.monitor.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	rate_limit.too_permissive	https://devapp.yourdomain.io/oauth/token Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	rate_limit.too_permissive	https://devapp.yourdomain.io/v1/auth/login Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	rate_limit.too_permissive	https://devapp.yourdomain.io/identity/api/auth/login Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	http.server_header_leak	https://netdata-dev.monitor.yourdomain.io/ Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable

INV	rate_limit.too_permissive	https://dozzle-dev.monitor.yourdomain.io/auth/token Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	rate_limit.too_permissive	https://dozzle-dev.monitor.yourdomain.io/oauth/token Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	clickjacking.frameable	https://netdata-dev.monitor.yourdomain.io/login Misconfigured HTTP services may expose sensitive data, allow session hijacking, or enable cross-site scripting attacks. Apply HTTP security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options). Remove server version banners. Disable
INV	rate_limit.too_permissive	https://dozzle-dev.monitor.yourdomain.io/v1/auth/logi Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	rate_limit.too_permissive	https://dozzle-dev.monitor.yourdomain.io/identity/api Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	rate_limit.too_permissive	https://netdata-dev.monitor.yourdomain.io/auth/login Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or
INV	rate_limit.too_permissive	https://netdata-dev.monitor.yourdomain.io/login Without rate limiting on authentication endpoints an attacker can perform unlimited credential-stuffing or brute-force a Implement rate limiting on all authentication endpoints (login, password reset, OTP verification). Use a token-bucket or

Infrastructure Changes

Asset-level differences between this scan and the previous scan, detected by the infrastructure drift monitor.

Change type	Severity	Asset	Details
DNS IP changed	Info	104.21.87.204	DNS A record for `yourdomain.io` changed from `172.67.145.243` to `104.21.87.204`. · 172.67.145.243 → 104.21.87.204
DNS IP changed	Info	2606:4700:3036::6815:57cc	DNS AAAA record for `yourdomain.io` changed from `2606:4700:3037::ac43:91f3` to `26 · 2606:4700:3037::ac43:91f3 → 2606:4700:3036::6815:57cc

What We Tested

Each probe runs a dedicated set of checks against your domain and all discovered subdomains. Status: ✓ ran cleanly · ■ degraded · ✗ errored · — skipped.

Coverage Summary

Category	Checks	Status
SSL / TLS certificates	25	✓
Email security (SPF, DKIM, DMARC)	24	■
DNS configuration	3	■
Subdomains & exposure	6	✓
Visible ports & services	18	✓
Data breach exposure	2	✓
Vulnerable software (CVE / KEV)	5	■
Abandoned or parked signals	1	✓
Web application headers	34	■
Email sender reputation	5	✓
Third-party scripts	3	✓
Domain reputation & blocklists	6	✓
Asset & config changes	8	✓
DNS rebinding & advanced DNS	6	✓
Cloud & infrastructure probes	24	■
Auth surface & login probes	7	✓
Compromise indicators	20	✓
Web surface & endpoints	8	✓
Injection attacks (XSS, SQLi, NoSQL, XXE, SSTI)	33	■
Authentication & session security	27	✓
CORS, CSRF & request manipulation	17	■
File & path attacks (LFI, uploads, source maps)	26	■
SSRF & server-side injection	11	✓
API & business logic security	18	■
Access control & privilege escalation	14	■

Probe Detail

Probe	What it looks for	Status	Evidence Type
tls	SSL / TLS certificates	✓ · Issues found — see findings above	Investigate
tls_posture	SSL / TLS certificates	✓ · All checks passed	
email_mx_probe	Email security (SPF, DKIM, DMARC)	✓ · Issues found — see findings above	
email	Email security (SPF, DKIM, DMARC)	✓ · Issues found — see findings above	Investigate
dns_records	DNS configuration	✓ · Issues found — see findings above	Investigate
dns_advanced	DNS rebinding & advanced DNS	✓ · All checks passed	
ct_log	Subdomains & exposure	✓ · All checks passed	
takeover	Subdomains & exposure	✓ · No applicable targets found	
port_scan	Visible ports & services	✓ · WAF / CDN protected — attack tests cannot reach origin	
hibp	Data breach exposure	✓ · All checks passed	

cve_join	Vulnerable software (CVE / KEV)	✓ · Issues found — see findings above	Validation Confirmed
parked	Abandoned or parked signals	✓ · All checks passed	
http	Web application headers	✓ · Issues found — see findings above	Investigate
email_reputation	Email sender reputation	✓ · All checks passed	
supply_chain	Third-party scripts	✓ · All checks passed	
domain_reputation	Domain reputation & blocklists	✓ · All checks passed	
drift_watchdog	Asset & config changes	✓ · Issues found — see findings above	Investigate
cloud_probe	Cloud & infrastructure probes	✓ · Issues found — see findings above	Investigate
active_validation	Auth surface & login probes	✓ · All checks passed	
strategic_probes	Compromise indicators	✓ · All checks passed	
web_surface	Web surface & endpoints	✓ · All checks passed	
xss_probe	Injection attacks (XSS, SQLi, NoSQL, XXE, SSTI)	✓ · Issues found — see findings above	Investigate
injection_probe	Injection attacks (XSS, SQLi, NoSQL, XXE, SSTI)	✓ · Issues found — see findings above	
xxe_probe	Injection attacks (XSS, SQLi, NoSQL, XXE, SSTI)	✓ · All checks passed	
ssti_probe	Injection attacks (XSS, SQLi, NoSQL, XXE, SSTI)	✓ · All checks passed	
nosql_probe	Injection attacks (XSS, SQLi, NoSQL, XXE, SSTI)	✓ · All checks passed	
auth_probe	Authentication & session security	✓ · All checks passed	
jwt_probe	Authentication & session security	✓ · All checks passed	
session_probe	Authentication & session security	✓ · All checks passed	
twofa_probe	Authentication & session security	✓ · All checks passed	
oauth_probe	Authentication & session security	✓ · All checks passed	
cors_probe	CORS, CSRF & request manipulation	✓ · All checks passed	
csrf_probe	CORS, CSRF & request manipulation	✓ · All checks passed	
open_redirect_probe	CORS, CSRF & request manipulation	✓ · Issues found — see findings above	Browser Confirmed
crlf_probe	CORS, CSRF & request manipulation	✓ · All checks passed	
host_header_probe	CORS, CSRF & request manipulation	✓ · All checks passed	
lfi_probe	File & path attacks (LFI, uploads, source maps)	✓ · All checks passed	
source_map_probe	File & path attacks (LFI, uploads, source maps)	✓ · Issues found — see findings above	Investigate
file_upload_probe	File & path attacks (LFI, uploads, source maps)	✓ · All checks passed	
error_disclosure_probe	File & path attacks (LFI, uploads, source maps)	✓ · Issues found — see findings above	Investigate
ssrf_probe	SSRF & server-side injection	✓ · All checks passed	
cmdi_probe	SSRF & server-side injection	✓ · Issues found — see findings above	Investigate
deserialization_probe	SSRF & server-side injection	✓ · All checks passed	
graphql_probe	API & business logic security	✓ · All checks passed	
rate_limit_probe	API & business logic security	✓ · Issues found — see findings above	Investigate
api_inventory_probe	API & business logic security	✓ · All checks passed	
ws_injection_probe	API & business logic security	✓ · All checks passed	
race_condition_probe	API & business logic security	✓ · All checks passed	
mass_assignment_probe	API & business logic security	✓ · All checks passed	
authz_probe	Access control & privilege escalation	✓ · All checks passed	
default_creds_probe	Access control & privilege escalation	✓ · All checks passed	
prototype_pollution_probe	Access control & privilege escalation	✓ · All checks passed	
cache_poisoning_probe	Access control & privilege escalation	✓ · Issues found — see findings above	Strong Signal

http_smuggling_probe	Access control & privilege escalation	✓ · Issues found — see findings above	Strong Signal
email_injection_probe	CORS, CSRF & request manipulation	✓ · All checks passed	
postmessage_probe	Access control & privilege escalation	✓ · All checks passed	
eol_probe	Vulnerable software (CVE / KEV)	■ · 1 error(s), partial results	

Generated for yourdomain.io · 2026-06-16 20:31 UTC · Full evidence and history at your Kayvrn dashboard.