

TRUST REPORT

seolinkmap.com

https://seolinkmap.com/mcp

Scanned May 4, 2026 · 03:34 UTC



VERDICT REVIEW

Score **92** / 100
Risk **HIGH**
Tier Public handshake

TOOLS

0

RISK SURFACE

0R · 0W · 0D

RULES PASSED

28/31

AUTH

Anonymous

WHY THIS VERDICT

- 01 Server accepted a cross-origin POST (status 200) ? DNS-rebinding mitigation missing
- 02 Server does not advertise HSTS
- 03 tools/list did not return an array

CATEGORY BREAKDOWN

Trust dimensions

Each dimension shows percent of contributing rule weight earned.



RULE FINDINGS

All rules evaluated

Failing rules are listed first, ordered by severity. Weight reflects the rule's contribution to the score.

FAIL	Server validates the Origin header	HIGH · w8
FAIL	Server advertises HTTP Strict-Transport-Security	LOW · w3
FAIL	tools/list returned a tool array	INFO · w1
PASS	No code-execution tools in the public surface	CRITICAL · w14
PASS	No credential-access tools in the public surface	CRITICAL · w12
PASS	Server identity does not match a known security advisory	CRITICAL · w12
PASS	No filesystem-write tools in the public surface	CRITICAL · w10
PASS	No admin-control tools in the public surface	CRITICAL · w10
PASS	Server uses HTTPS	HIGH · w10
PASS	No destructive tools in the public surface	HIGH · w8
PASS	No unconstrained prompt-injection vectors	HIGH · w8
PASS	TLS handshake completes with a trusted certificate	HIGH · w8
PASS	No credentials in the endpoint URL	HIGH · w6
PASS	Resource URIs do not advertise risky targets	HIGH · w6
PASS	Tool annotations are consistent with the surface	HIGH · w6
PASS	No prompt-manipulation patterns in tool descriptions	HIGH · w6
PASS	Auth-discovery metadata URLs are HTTPS and publicly routable	HIGH · w6
PASS	Authorization server advertises PKCE with S256	HIGH · w6
PASS	No insecure grant types advertised	HIGH · w6
PASS	No financial-action tools in the public surface	HIGH · w6

RULE FINDINGS (continued)

PASS	Authorization server issuers are HTTPS	HIGH · w6
PASS	No outbound-messaging tools in the public surface	HIGH · w4
PASS	No outbound network-access tools in the public surface	HIGH · w4
PASS	All tools declare an input schema	MEDIUM · w6
PASS	No injection vectors in initialize.instructions	MEDIUM · w5
PASS	No description-borne injection vectors	MEDIUM · w5
PASS	Tool surface does not mention PII	MEDIUM · w5
PASS	TLS 1.2 or newer is negotiated	MEDIUM · w5
PASS	No secret material leaked in observed metadata	MEDIUM · w5
PASS	Auth-required server advertises discovery metadata	MEDIUM · w5
PASS	Tool surface unchanged since the previous scan	MEDIUM · w5
PASS	No injection vectors in resource or prompt entries	MEDIUM · w5
PASS	Sampled resource contents contain no injection vectors	MEDIUM · w5
PASS	Endpoint hostname is reachable from the public internet	MEDIUM · w4
PASS	Destructive tools positively declare destructiveHint	MEDIUM · w4
PASS	Probe walked the full tool surface (pagination not truncated)	MEDIUM · w4
PASS	Server identity claim matches transport identity	MEDIUM · w4
PASS	Tool input schemas are structurally well-formed	MEDIUM · w4
PASS	No new tools added since the previous scan	MEDIUM · w4
PASS	Existing tool descriptions are unchanged since the previous scan	MEDIUM · w4
PASS	Auth-required server advertises RFC 9728 protected-resource met?	MEDIUM · w4
PASS	Tool descriptions do not collide with other registered servers	MEDIUM · w4

RULE FINDINGS (continued)

PASS	Active probe: read-only tools honor their declared schema	MEDIUM · w4
PASS	Server advertises the latest published version of its upstream ?	MEDIUM · w4
PASS	All tools have descriptions	LOW · w4
PASS	Server advertises an MCP protocol version	LOW · w3
PASS	Authorization server metadata is parseable	LOW · w3
PASS	Authorization server advertises a token endpoint	LOW · w2
PASS	Authorization server advertises a JWKS URI	LOW · w2
PASS	Tool names are ASCII identifier-shaped	LOW · w2
PASS	Tool input schemas have bounded shape	LOW · w2
PASS	Tool descriptions are within the size bound	LOW · w2
PASS	TLS certificate has at least 14 days until expiry	LOW · w2
PASS	No two tools share an identical description	LOW · w2
PASS	Tool count is reasonable	LOW · w2
PASS	Server identifies itself	INFO · w2
PASS	Probe redirects are within the safe bound	INFO · w1
PASS	Probe completed within a reasonable wall-clock budget	INFO · w1
PASS	Server advertises a version string	INFO · w1
PASS	Probe response size is within the safe bound	INFO · w1
PASS	Probe response content-type was acceptable	INFO · w1