Security Assessment Report

Target: hackura.store
Generated: 2026-01-02 18:10 UTC

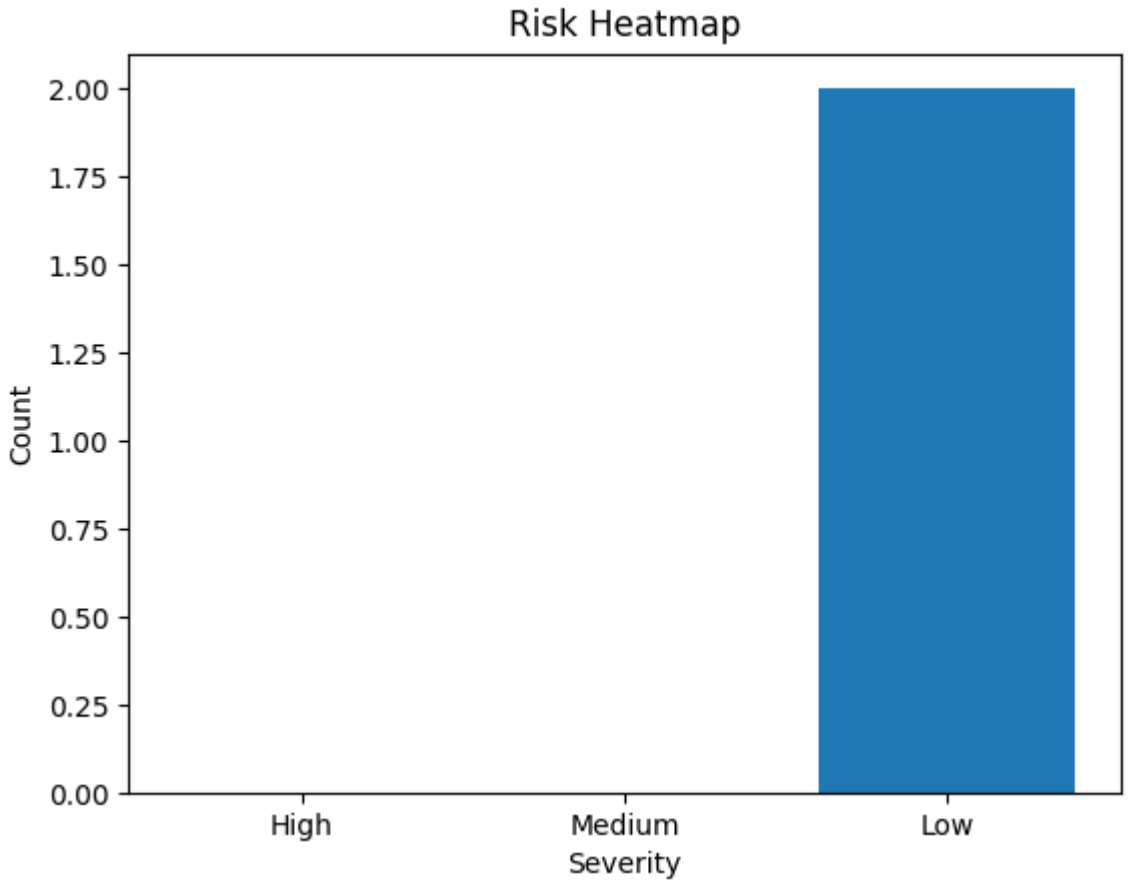
Executive Summary

This report presents the results of a non-intrusive security assessment conducted using automated discovery and analysis tools. The goal is to identify exposed services, observable technologies, and common security weaknesses.

Executive Risk Score: **4.25 / 10**

The Executive Risk Score represents the overall security posture of the target, considering severity, likelihood, and confidence of findings. Scores above **7.0** indicate a high priority for remediation.

Risk Heatmap



Technical Findings

Medium

Finding	Severity	CVSS	CVSS Vector	Confidence	Evidence
General Security Observation	MEDIUM	6.5	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N	0.62	Host is reachable via ICMP
General Security Observation	MEDIUM	6.5	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N	0.62	Host is reachable via ICMP
General Security Observation	MEDIUM	6.5	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N	0.62	Host is reachable via ICMP
General Security Observation	MEDIUM	6.5	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N	0.68	□[1m□[34mhttp://hackura.store[Permanent Redirect] □[1mCountry□[0m[□[0m□[22mU STATES□[0m][□[1m□[31mUS□[0 □[1mHTTPServer□[0m[□[1m□[3 □[1mIP□[0m[□[0m□[22m216.198 □[1mRedirectLocation□[0m[□[0 hackura.store/□[0m]
Publicly Accessible HTTP Service Detected	MEDIUM	6.5	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N	0.68	□[1m□[34mhttps://hackura.store Temporary Redirect] □[1mCountry□[0m[□[0m□[22mU STATES□[0m][□[1m□[31mUS□[0 □[1mHTTPServer□[0m[□[1m□[3 □[1mIP□[0m[□[0m□[22m216.198 □[1mRedirectLocation□[0m[□[0 www.hackura.store/□[0m], □[1m Transport-Security□[0m[□[0m□[age=63072000□[0m],

					[1mUncommonHeaders[0m[vercel-id[0m]
Publicly Accessible HTTP Service Detected	MEDIUM	6.5	CVSS:3.1/ AV:N/ AC:H/ PR:L/ UI:R/S:U/ C:L/I:L/ A:N	0.68	[1m[34mhttps://hackura.store Temporary Redirect] [1mCountry[0m[[0m[22mU STATES[0m][[1m[31mUS[0 [1mHTTPServer[0m[[1m[3 [1mIP[0m[[0m[22m216.198 [1mRedirectLocation[0m[[0 www.hackura.store/[0m], [1m Transport-Security[0m[[0m[age=63072000[0m], [1mUncommonHeaders[0m[vercel-id[0m]
Publicly Accessible HTTP Service Detected	MEDIUM	6.5	CVSS:3.1/ AV:N/ AC:H/ PR:L/ UI:R/S:U/ C:L/I:L/ A:N	0.68	[1m[34mhttps://www.hackura [200 OK] [1mCountry[0m[[0m[22mU STATES[0m][[1m[31mUS[0 [1mHTML5[0m, [1mHTTPServer[0m[[1m[3 [1mIP[0m[[0m[22m216.198 [1mScript[0m, [1mStrict-Tra Security[0m[[0m[22mmax-age=63072000[0m], [1mTitle[0m[[1m[33mHack [1mUncommonHeaders[0m[matched-path,x-vercel-cache,x id[0m], [1mX-Powered-By[0m[[0m[22mNext.js[0m

AI-Generated Remediation Roadmap

The following remediation guidance was generated to assist technical and non-technical stakeholders in prioritizing corrective actions.

```
AI remediation unavailable: 400 Client Error: Bad Request for url: http
```

Risk Acceptance

Any risks not immediately remediated should be formally accepted by business stakeholders after evaluating operational impact, likelihood of exploitation, and regulatory requirements.

Consultant Sign-Off

This assessment was conducted for educational and defensive purposes using RedSentinel.

Assessor: _____
Date: _____

Generated by RedSentinel – AI-Assisted Security Analysis