Rustler Recon

Your local reconnaissance assistant. It shows what a website, an API or a server exposes to the internet, with no exploits, no vulnerability payloads and no state-changing requests.

Windows · runs locally | Single and multi target | Observation only | Results stay local | Pilot phase · selected test users

What it covers

Public sources and domain

robots.txt, sitemap.xml, DNS, WHOIS, ASN, Wayback and public email patterns, partly from third-party sources.

Network inventory

Common ports or your own list, certificates, protocol versions, cipher strength, subdomains and virtual hosts.

Web reconnaissance

A scope-bound crawler, directory discovery, header and cookie checks, technology and CMS detection, screenshots.

APIs and cloud

OpenAPI and Swagger, GraphQL introspection with fixed queries, SOAP, API routes and cloud storage candidates.

Projects, Dash and reports

Import many targets, scan up to five in parallel and review everything in Rustler Dash or a one-click HTML report.

Local and data-minimal

Results stay on your machine, secrets are redacted and no telemetry goes to KintsuKai. Traffic can go through Burp or another proxy.

How it works

1. **Enter a target**
   A domain, IP or URL, or import many targets at once.
2. **Pick a profile**
   Guided Safe Recon, Extended Recon or your own module set.
3. **Start the scan**
   Rustler collects observations and shows live progress.
4. **Read the results**
   Review them in Rustler Dash or the HTML report, never as confirmed.

A clear product boundary

Rustler Recon does

- ✓ Authorized discovery and inventory requests
- ✓ GET, HEAD and OPTIONS plus fixed GraphQL queries
- ✓ DNS, TLS, port, web, API and cloud inventory
- ✓ Review signals with traceable provenance
- ✓ Redacted, data-minimal result storage

Rustler Recon does not

- ✗ Run exploits or send vulnerability payloads
- ✗ Send state-changing requests such as PUT or DELETE
- ✗ Check logins or passwords
- ✗ Run callback or OAST tests
- ✗ Claim that a vulnerability is confirmed

Coming next

Three extensions are planned for later versions. Priorities can shift with pilot feedback, so we do not promise dates.

Web overview

A web-based overview that lets you work with Rustler in a single click.

Known-vulnerability matching

Selected results compared with public sources such as CVE, as review hints for a human to verify.

Better reports and documents

A more capable report and a variant that helps manage reports and documents.

Pilot phase. Rustler Recon 0.9 is not generally available yet and is provided only to selected test users. It sends real, visible requests to the target, so scan only systems you own or may test with written permission. Ask for pilot access at **kintsukai4contact@gmail.com**.