

Forum:[Hack Forums](#)

Thread: [\[opensource\] I created a workflow for Pen testing Code Review agents on Pull requests](#)

jkshenawy22 - April 19, 2026, 5:03 pm

Hello peer developers,

I'm sharing a workflow I built over the past few weeks that has made our pull request security reviews more consistent and more actionable.

ThinkReview is a browser extension that works across Git platforms (Gitlab, Github , azure devops and Bitbucket)and runs a custom review checklist based on what your team cares about, such as OWASP guidance and your internal secure coding standards.

Example: a pentesting-focused review agent

In this example, I created a review agent focused on pentesting.

Define the agent's goal and scope (what kinds of issues it should look for).

Provide a reference the agent should follow, such as STRIKE Graph best practices

You can create up to 10 review agents

Run the review on a PR and get findings mapped back to the reference.

The project is open source on Github and is available on chrome store and firefox addons
Just google ThinkReview extension

Lookin forward to your feedback , any questions would love to hear

jkshenawy22 - August 29, 2026, 12:06 pm

Hey everyone, I work on an AI code review tool called ThinkReview, and we recently got our Model Context Protocol (MCP) server listed on the official MCP registry.

I thought this might be relevant for anyone here experimenting with Claude Code, Cursor, or GitHub Copilot. Instead of wrapping it in an npm package like most local tools, we built it as a hosted Streamable HTTP endpoint.

Your client just points to `mcp.thinkreview.dev/v1` and handles auth via OAuth or a bearer token.

Once connected, it exposes a `Code review_url_code` tool. You can feed it a pull request or merge request URL from GitHub, GitLab, Azure DevOps, or Bitbucket, and the AI agent can trigger a review directly from your terminal or IDE.

Getting on the main metadata catalog at registry.modelcontextprotocol.io helps with discovery, though it's worth noting that GitHub's specific MCP marketplace is still a separate, manually curated beast we're waiting on.

If anyone is trying to figure out how to register a remote MCP server without dealing with npm packages, we documented the process and the registry update [here](#)

Happy to answer any questions about setting up remote MCP endpoints or handling the HTTP transport layer.

PremiumJoe - August 29, 2026, 11:45 pm

I'm not an admin or staff member here, but I can say that your post is a bit misplaced. There are better sections for your message than "News and Happenings", where like-minded people can find it and respond. Try the programming section, that's much better.

Just trying to help.

(Edited a spelling mistake)

jkshenawy22 - August 30, 2026, 1:42 am

(Aug 29, 2026 11:45 PM)PremiumJoe Wrote: [\[CITE\]](#) I'm not an admin or staff member here, but I can say that your post is a bit misplaced. There are better sections for your message than "News and Happenings", where like-minded people can find it and respond. Try the programming section, that's much better.

Just trying to help.

(Edited a spelling mistake)

will do next time - thanks