Two interesting new products for running code in a sandbox today.

Cloudflare launched their Containers product in open beta, and added a new Sandbox library for Cloudflare Workers that can run commands in a "secure, container-based environment":

```
import { getSandbox } from "@cloudflare/sandbox";
const sandbox = getSandbox(env.Sandbox, "my-sandbox");
const output = sandbox.exec("ls", ["-la"]);
```

Vercel shipped a similar feature, introduced in Run untrusted code with Vercel Sandbox, which enables code that looks like this:

```
import { Sandbox } from "@vercel/sandbox";

const sandbox = await Sandbox.create();
await sandbox.writeFiles([
    { path: "script.js", stream: Buffer.from(result.text) },
  ]);
await sandbox.runCommand({
    cmd: "node",
    args: ["script.js"],
    stdout: process.stdout,
    stderr: process.stderr,
});
```

In both cases a major intended use-case is safely executing code that has been created by an LLM.

Posted 26th June 2025 at 1:41 am

Recent articles

- Phoenix.new is Fly's entry into the prompt-driven app development space - 23rd June 2025
- Trying out the new Gemini 2.5 model family - 17th June 2025
- The lethal trifecta for AI agents: private data, untrusted content, and external communication - 16th June 2025

vercel 4 | cloudflare 20 | generative-ai 1211 | ai 1389 | llms 1190 | sandboxing 19

Sponsor & subscribe