The Good, the Bad and npx

Get hacked with npm run

Василий Ванчук

Василий Ванчук

Ведущий эксперт

Friends
are welcome

@ vvscode

Василий Ванчук

Ведущий эксперт

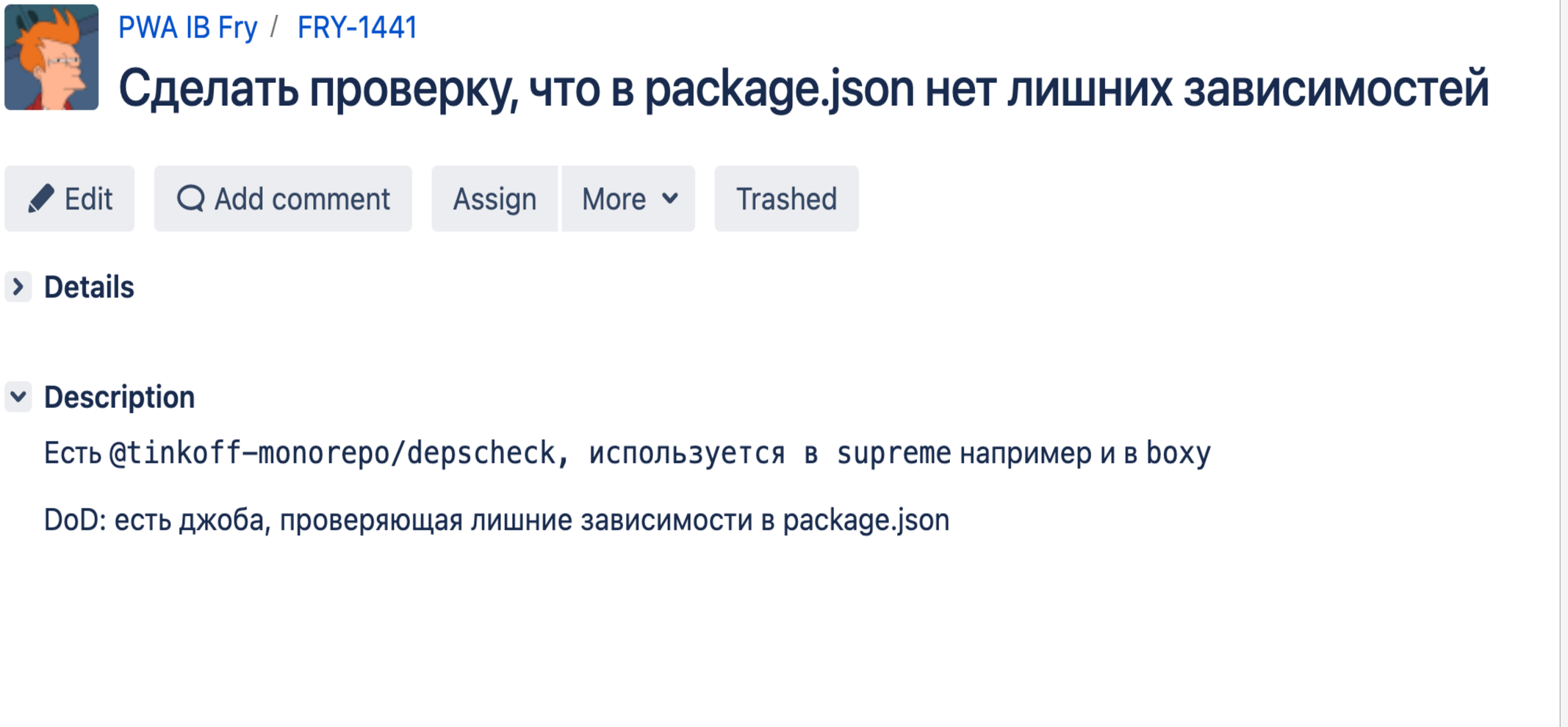
- Пишу на JS последние 12 лет
- Помню bower.js
- В юношестве читал Хакер и криптовал малварь

@ vvscode

Friends are welcome

Введение

Задача на расчистку зависимостей



PWA IB Fry / FRY-1441

Сделать проверку, что в package.json нет лишних зависимостей

Edit | Add comment | Assign | More | Trashed

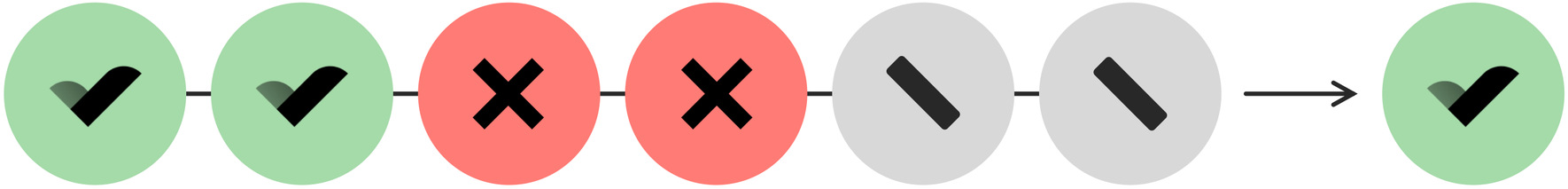
Details

Description

Есть `@tinkoff-monorepo/depscheck`, используется в supreme например и в boxy

DoD: есть джоба, проверяющая лишние зависимости в package.json

Проект стал чище. Но...



Incorrect work on Linux (`Error:` resolve `must be run directly as an executable`)

#316 by vvscode was closed on Sep 15, 2023

`npx resolve` errors

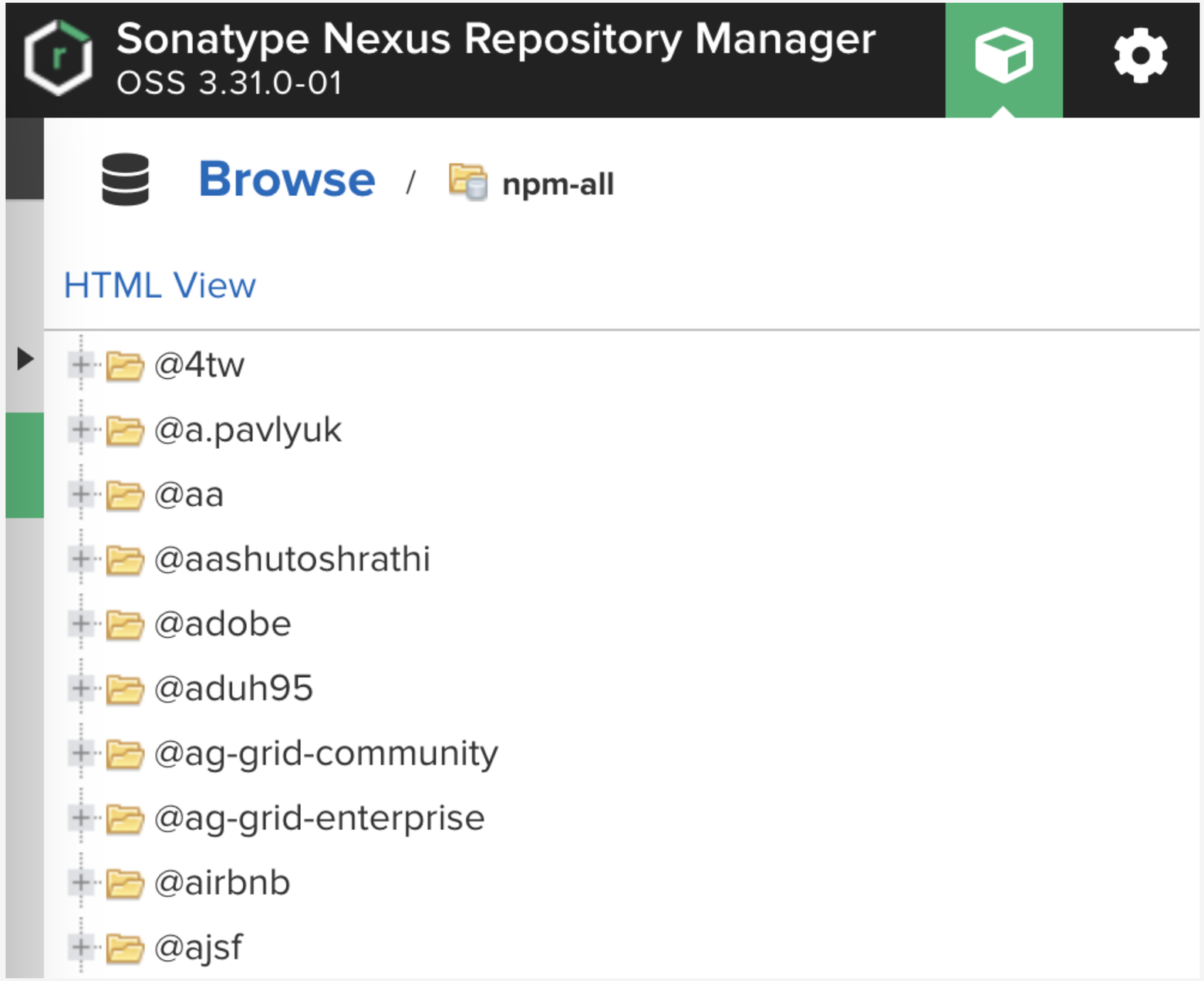
#315 by vvscode was closed on Sep 14, 2023

Когда ошибки кончились

Пайплайн вместо того чтобы упасть, просто завис

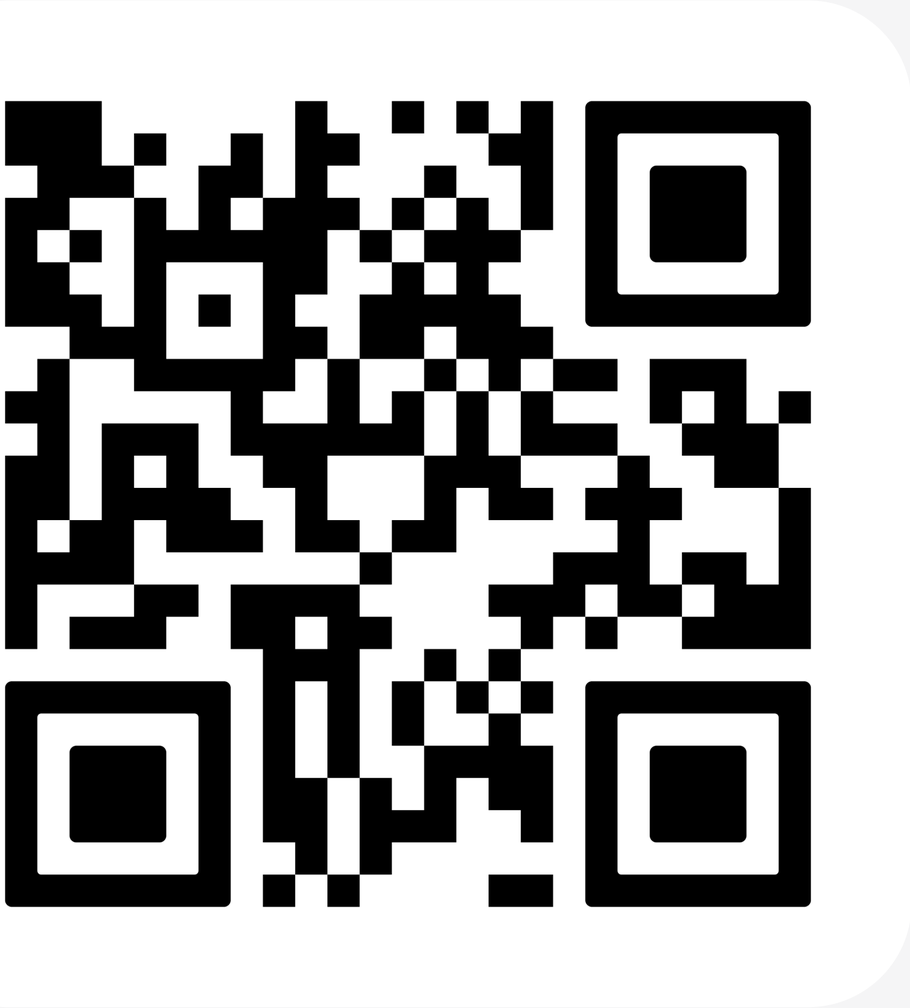
«Вместе с водой выплеснуть и ребенка»

Захотел посмотреть, как часто такое происходит



Пара часов на анализ

Мало



Минутка теории

node_modules/.bin

npm exec / npm run

npm exec / npm run

bin

A lot of packages have one or more executable files that they'd like to install into the PATH. npm makes this pretty easy (in fact, it uses this feature to install the "npm" executable.)

directories.bin

If you specify a `bin` directory in `directories.bin`, all the files in that folder will be added.

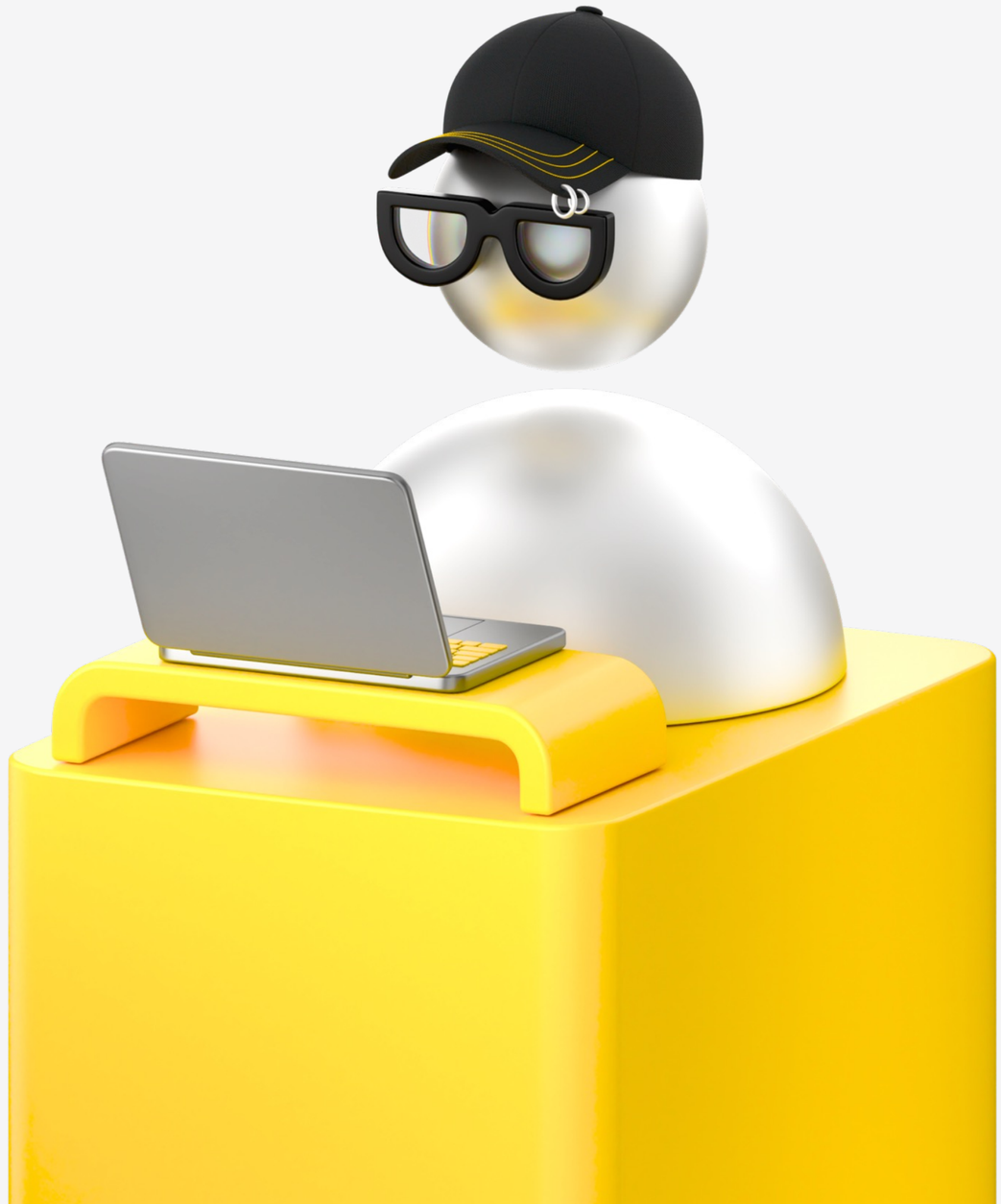
Просмотр скриптов

```
➜  hubert git:(master) ls -la node_modules/.bin
total 0
drwxr-xr-x@  148 v.vanchuk  staff   4736 Apr 12 18:39 .
drwxr-xr-x@ 1448 v.vanchuk  staff  46336 Apr 12 18:39 ..
lrwxr-xr-x@    1 v.vanchuk  staff     20 Apr 12 18:39 JSONStream -> ../JSONStream/bin.js
lrwxr-xr-x@    1 v.vanchuk  staff     48 Apr 12 18:39 acorn -> ../@storybook/react/node_modules/acorn/bin/acorn
lrwxr-xr-x@    1 v.vanchuk  staff     42 Apr 12 18:39 addon-styling-setup -> ../@storybook/addon-styling/postinstall.js
lrwxr-xr-x@    1 v.vanchuk  staff     36 Apr 12 18:39 ansi-html -> ../ansi-html-community/bin/ansi-html
lrwxr-xr-x@    1 v.vanchuk  staff     19 Apr 12 18:39 atob -> ../atob/bin/atob.js
lrwxr-xr-x@    1 v.vanchuk  staff     32 Apr 12 18:39 autoprefixer -> ../autoprefixer/bin/autoprefixer
lrwxr-xr-x@    1 v.vanchuk  staff     27 Apr 12 18:39 boast -> ../swagger2openapi/boast.js
lrwxr-xr-x@    1 v.vanchuk  staff     22 Apr 12 18:39 browserslist -> ../browserslist/cli.js
lrwxr-xr-x@    1 v.vanchuk  staff     15 Apr 12 18:39 c8 -> ../c8/bin/c8.js
lrwxr-xr-x@    1 v.vanchuk  staff     48 Apr 12 18:39 can-bind-to-host -> ../can-bind-to-host/dist/bin/can-bind-to-host.js
lrwxr-xr-x@    1 v.vanchuk  staff     52 Apr 12 18:39 check-version -> ../@pwa-ib/eslint-plugin-compat/bin/check-version.js
```

Хорошо, а что все же происходит, при коллизии?

Единственным критерием истины является опыт

Леонардо Пьерович ДаВинчи



Основные гипотезы

Консистентность

Результат повторяется

Имя влияет

Порядок зависит от имен пакетов

Порядок рулит

Очередность определяется упоминанием в package.json

Участники

- @vvscode/evil-dummy-cli 👹
- @vvscode/dummy-cli 👼
- @vvscode/awful-dummy-cli 😈

Участники

@vvscode/awesome-package

- v1.0 👹
- v1.1 👹😈

Участники

- npm
- yarn
- pnpm
- bun

Результаты в картинках

#1

bun	
npm	
pnpm	
yarn	

#2

bun	
npm	
pnpm	
yarn	

#3

bun 

---

npm 

---

pnpm 

---

yarn 

#4

bun	
npm	
pnpm	
yarn	

#5

bun	
npm	
pnpm	
yarn	

И что из этого?

Ладно, понятно, что ничего не понятно, а что там в регистри?

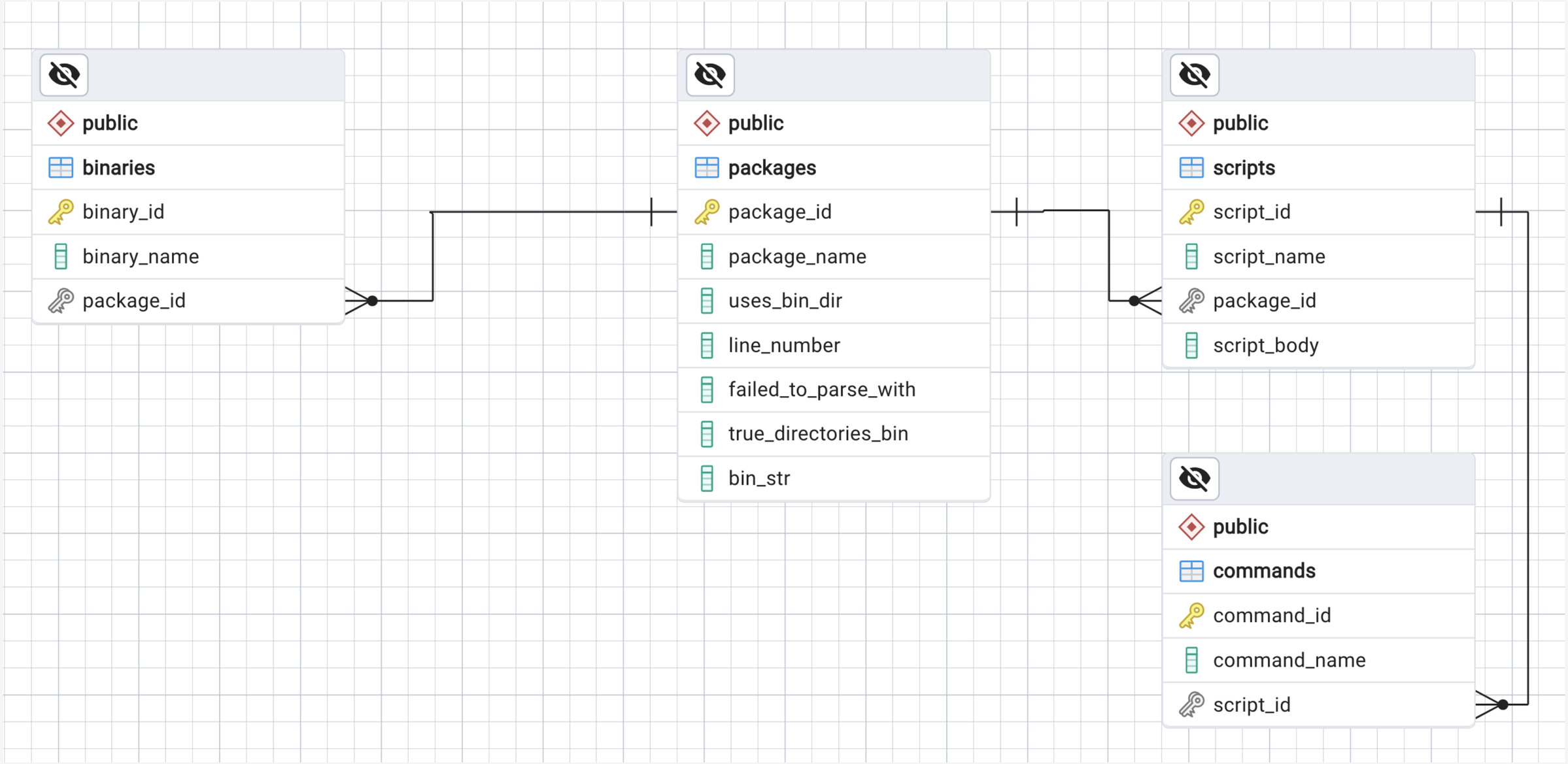
Парсинг базы

Изначально меня интересовал

- Список пакетов
- Список binaries

Позже список расширился

- Список скриптов
- Команды из скриптов


public
binaries
binary_id
binary_name
package_id
public
packages
package_id
package_name
uses_bin_dir
line_number
failed_to_parse_with
true_directories_bin
bin_str
public
scripts
script_id
script_name
package_id
script_body
public
commands
command_id
command_name
script_id

Список binaries

```sql
SELECT
    b.binary_name,
    COUNT(*) AS usage_count,
    STRING_AGG(p.package_name, ', ') AS used_in_packages
FROM binaries b JOIN packages p
ON b.package_id = p.package_id
GROUP BY b.binary_name
ORDER BY usage_count DESC;
```

	binary_name text	usage_count bigint	used_in_packages text
1	react-scripts	2381	codelink-react, @aliangincoding/react-scripts, @dcheng168/react-scripts, vclabs-react-scripts, expl
2	random-msg	1211	random-messages-test-publish, random-messages-fransalazarco, random-messages-js-npm, rando
3	brain-games	935	project-bg388, brain-games-emk, nodejs-package-inem, dep435-games, maksim1509bgames, front
4	brain-even	888	hexlet-project-sergeimakarovweb, brain-games-orlovmaxxim, brain-games-kav, frontend-project-lvl1
5	weather	837	weather-cli-seliun, weather-cli-terminal, openweather-sdk, af-node-weather, weather-node-cli, cli-wea
6	brain-calc	821	new-dekart-brain-games, brain-games-296, brain-games-strekanov, brain-games-agar88, brain-game
7	brain-gcd	792	brain_games_1202, brain-games_evoly, hexlet_games, project-lvl1-s132, brain_games_s508, bgame
8	brain-progression	746	brain-games-by-jf, project-first-nalanpa, brain-games-rnk, @romanchechel/brain-games-project, proj
9	brain-prime	735	brain-games1505, brain-games-black, brain-games-olga, brain-games-by-botirk, frontend-project-she
10	gendiff	469	cli-gendiff-s225, gen1, gendiff_project_ap, gendiff-nm, gendiff-fomina, gendiff-edu, difference-utility
11	cli	434	@brydget/cli, prereact, z0k0100, hong-cli, d2d, @alephium/cli, @caylonlatte/lerna-test-cli, @uniform
12	md-links	430	mdlinks-effio, md-links-extractor, luzvg-md-links, md-links-leyla, noelia-md-links, md-links-lim015, pa
13	t	383	cv-todo, zhengzekun-node, node-todo-t, node-todo-kinderz, node-memo-1, @corbinhesse/taskline, n
14	brain-balance	382	s320-brain-games, hx168, geh-sp-122, games-for-brain, braingames-dm-abramov, brain-games-hexle
15	myvue-cli	366	webopenyeye-myvue-cli, wyj-cli, xiaowutongxue-vue-cli, jujjzhe-myvue-cli, mistletoejiejie-myvue-cli, w

Самые используемые команды

```sql
SELECT
    command_name,
    COUNT(*) AS usage_count
FROM commands
GROUP BY command_name
ORDER BY usage_count DESC
LIMIT 1000;
```

	command_name text	usage_count bigint
1	npm	1635814
2	run	1502818
3	build	777201
4	no	655377
5	specified	653101
6	tsc	599648
7	yarn	469587
8	node	462016
9	eslint	403761
10	jest	351272
11	mocha	239321
12	dist	236709
13	webpack	225381
14	lint	223292
15	rimraf	222302
16	rm	219393
17	rollup	207985

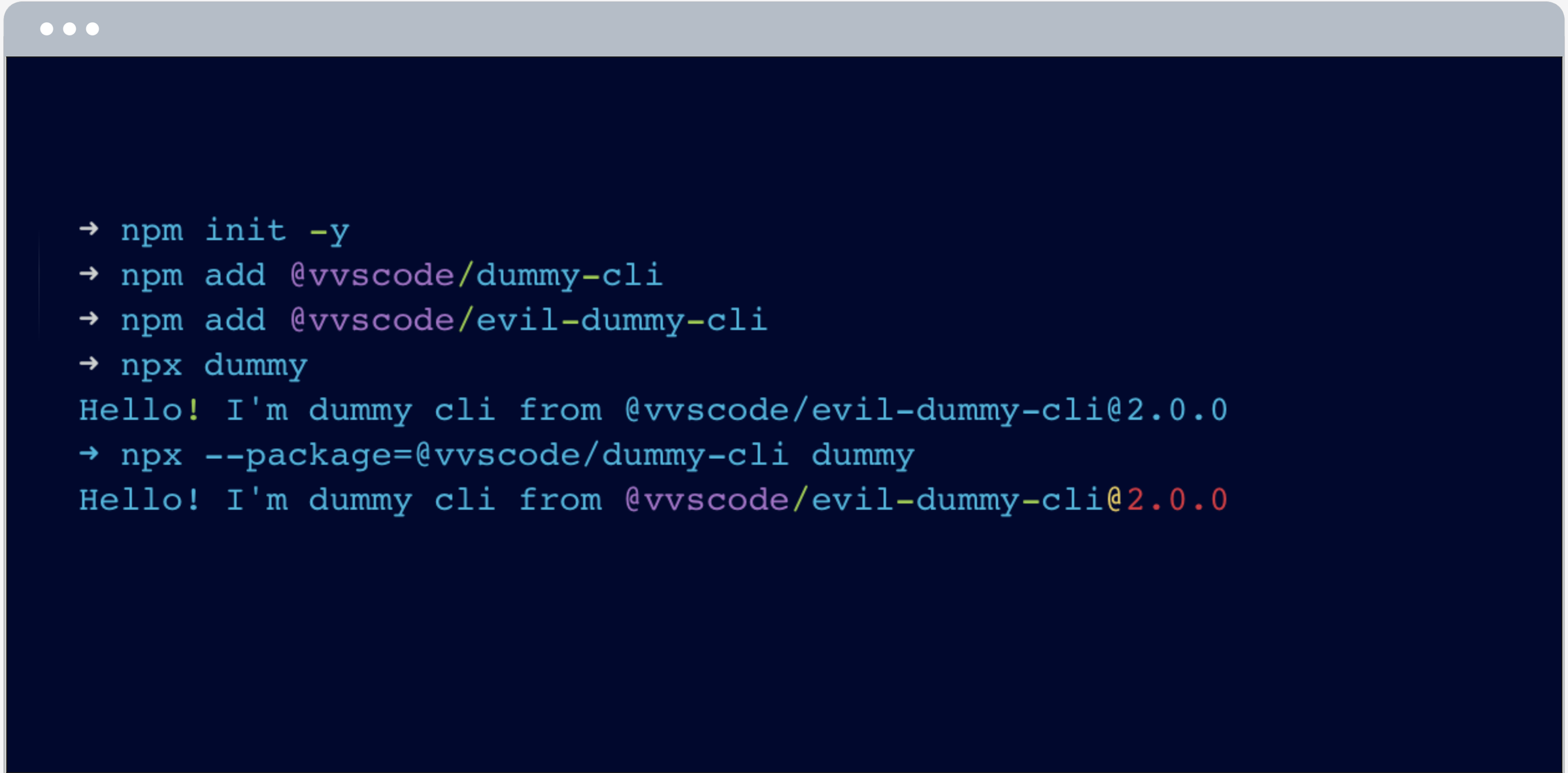
Чем это грозит?

А какое решение?

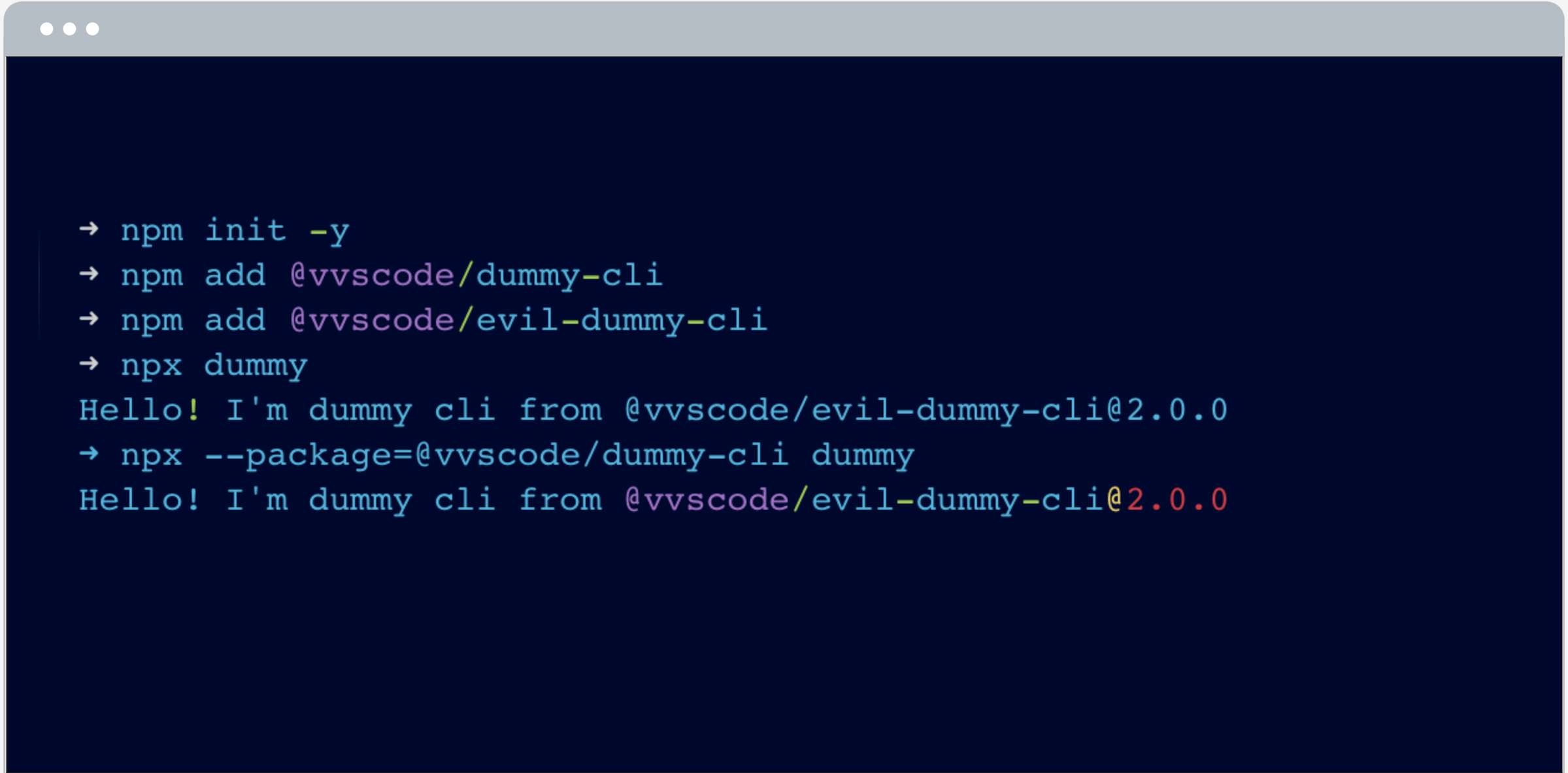
`npm exec --package`

Whatever packages are specified by the --package option will be provided in the PATH of the executed command, along with any locally installed package executables. The --package option may be specified multiple times, to execute the supplied command in an environment where all specified packages are available.

Увы

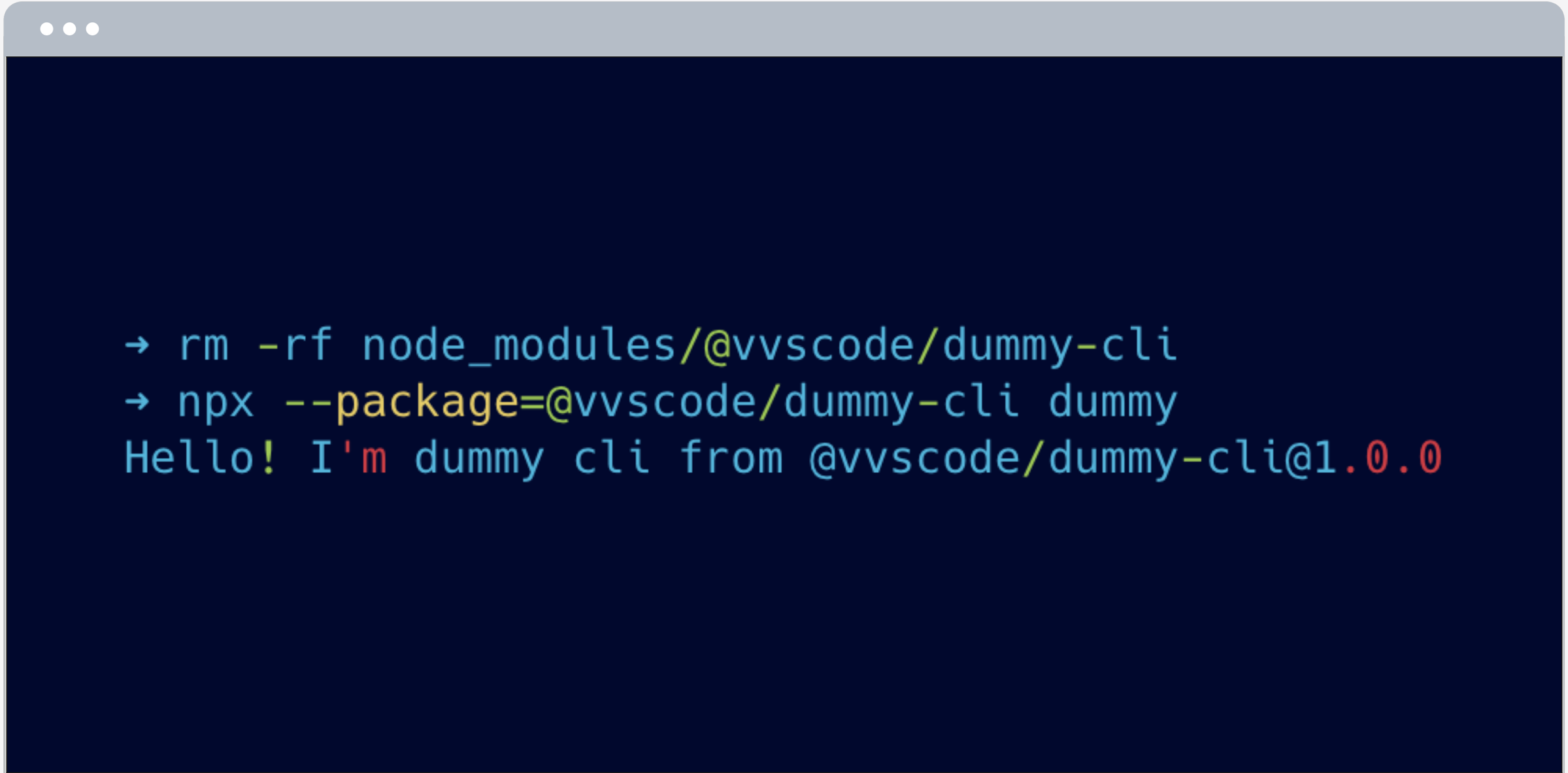

→ npm init -y
→ npm add @vvscode/dummy-cli
→ npm add @vvscode/evil-dummy-cli
→ npx dummy
Hello! I'm dummy cli from @vvscode/evil-dummy-cli@2.0.0
→ npx --package=@vvscode/dummy-cli dummy
Hello! I'm dummy cli from @vvscode/evil-dummy-cli@2.0.0

Увы


→ npm init -y
→ npm add @vvscode/dummy-cli
→ npm add @vvscode/evil-dummy-cli
→ npx dummy
Hello! I'm dummy cli from @vvscode/evil-dummy-cli@2.0.0
→ npx --package=@vvscode/dummy-cli dummy
Hello! I'm dummy cli from @vvscode/evil-dummy-cli@2.0.0

Как
же так?

Нюанс


→ rm -rf node_modules/@vvscode/dummy-cli
→ npx --package=@vvscode/dummy-cli dummy
Hello! I'm dummy cli from @vvscode/dummy-cli@1.0.0

Собираем все вместе

- `install --no-bin-links`
- `npx --package=@pkg/name@version command`

Влияние на DX

К чему это я?

npm bin script confusion: Abusing `bin` to hijack `node` command

	binary_name text	usage_count bigint
1	node	45
2	npm	33

ТИНЬКОФФ

Василий Ванчук

Ведущий эксперт

@ vvscode

ТИНЬКОФФ

Спасибо!