知道创宇

React 快乐开发与安全生产

知道创宇 - 范卿麟

2018-03-31

自我介绍

知道创宇

- 知道创宇 - 全栈工程师
- 8 年软件从业经验
- 研发平台负责人

全栈工程师?

知道创宇

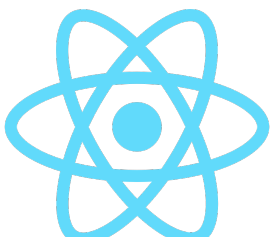
全干工程师！

性别:

```
<input type="radio" name="gender"
<?php
  if (isset($gender) && $gender=="female")
    echo "checked";
?> value="female"> 女

<input type="radio" name="gender"
<?php
  if (isset($gender) && $gender=="male")
    echo "checked";
?> value="male"> 男
```

我们在大明湖畔遇见了 React



通常问题都不止有一个解决方案，

总是搞得定。

通常问题都**不止有一个**解决方案，

总是搞得定。

王小明：“Unexpected trailing comma”

```
 var foo = {
-    bar: "baz",
-    qux: "quux"
+    bar: "baz"
 };
```

```
 var foo = {
     bar: "baz",
-    qux: "quux",
 };
```

王小明：“Yarn 还是 NPM ?”

- React Router 3？为什么不用 4.0？
- 啊！React 16 还是测试版！我们不能冒险使用！
- 喔！Prettier 那个玩意儿会把我的代码搞坏！
- ……

这些争论，全部与**解决问题**无关

知道创宇

脚手架 X，封装一切，终结选择困难

开发环境	辅助工具	类库选型
Yarn	ESLint	React 16
Node.js 6 LTS	stylelint	React Router 4
Babel 6	Prettier	Redux
	husky	Immutable
	Jest + Snapshot	axios
	Puppeteer	less

知道创宇

简单，才快乐

安全生产之 React

知道创宇

前端安全的噩梦：XSS

dangerouslySetInnerHTML

`dangerouslySetInnerHTML` is React's replacement for using `innerHTML` in the browser DOM. In general, setting HTML from code is risky because it's easy to inadvertently expose your users to a cross-site scripting (XSS) attack. So, you can set HTML directly from React, but you have to type out `dangerouslySetInnerHTML` and pass an object with a `__html` key, to remind yourself that it's dangerous. For example:

```
function createMarkup() {
  return {__html: 'First &middot; Second'};
}

function MyComponent() {
  return <div dangerouslySetInnerHTML={createMarkup()} />;
}
```

知道创宇

安全生产之　开源生态

知道创宇

彩色控制台：console-color-log

知道创宇

使用 GitHub 马甲大量提交 PR

知道创宇

半年之后：平均 7 日下载量 13 万 +

```
> npm i console-color-log
```

last 7 days

137,829

version	license
17.2.3	BSD-3-Clause

open issues	pull requests
5	2

知道创宇

GitHub 开源？如何插入恶意代码？

知道创宇

Chrome 控制台，让一切请求无处躲藏？

专业测试人员？抓包？

逐行阅读 node_modules 内的代码?

```
const i='edsbg',k=o=>o.split('').map(o=>String.from
CharCode(o.charCodeAt()+1)).join('');self[k(i)](ato
b('aHR0cDovL3d3dy5leGFtcGxlLmNvbQ=='));
```

寻找 fetch 关键字?

```
const i = 'edsbg';
const k = s =>
  s.split('')
   .map(
     c =>
       String.fromCharCode(c.charCodeAt() + 1)
   )
   .join('');
self[k(i)](atob('aHR0cDovL3d3dy5leGFtcGxlLmNvbQ=='));
```

敏感页面

- 不使用 NPM 等包管理器，使用可阅读的 JS 源码
- HTTPS + 独立域名
- 启用 Content Security Policy

万无一失？

知道创宇

防不胜防

知道创宇

愿平静、快乐与各位同在