

大型Web项目可用性提升 零脚本错误的实战

郭林烁 2017.10



郭林烁 (joeyguo)

@ 腾讯 AlloyTeam



<https://github.com/joeyguo>

1 社区的相关提问



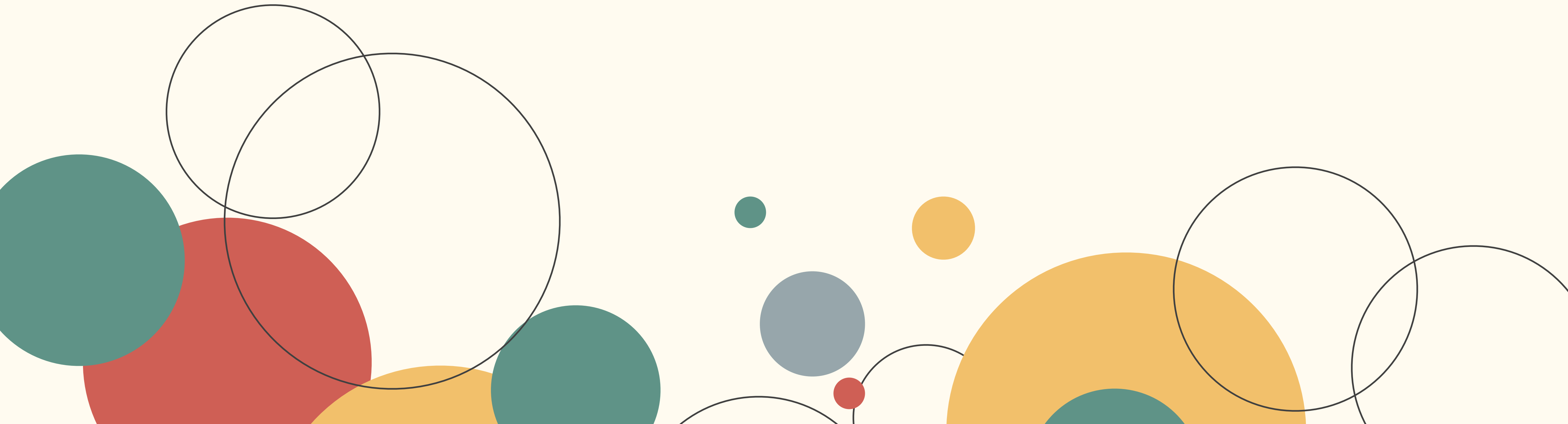
错误信息分析与优化

如何发现代码出了问题？

开发测试与脚本错误

Web 安全与脚本错误

基础的监控体系组成





如何发现线上代码出了问题？

1 不可能有问题！



我的代码**不可能**有问题！

2

不可能 不可能 不可能



不可能，不可能
那是你，那是你



放心吧 不可能的



不可能

那是不可能的



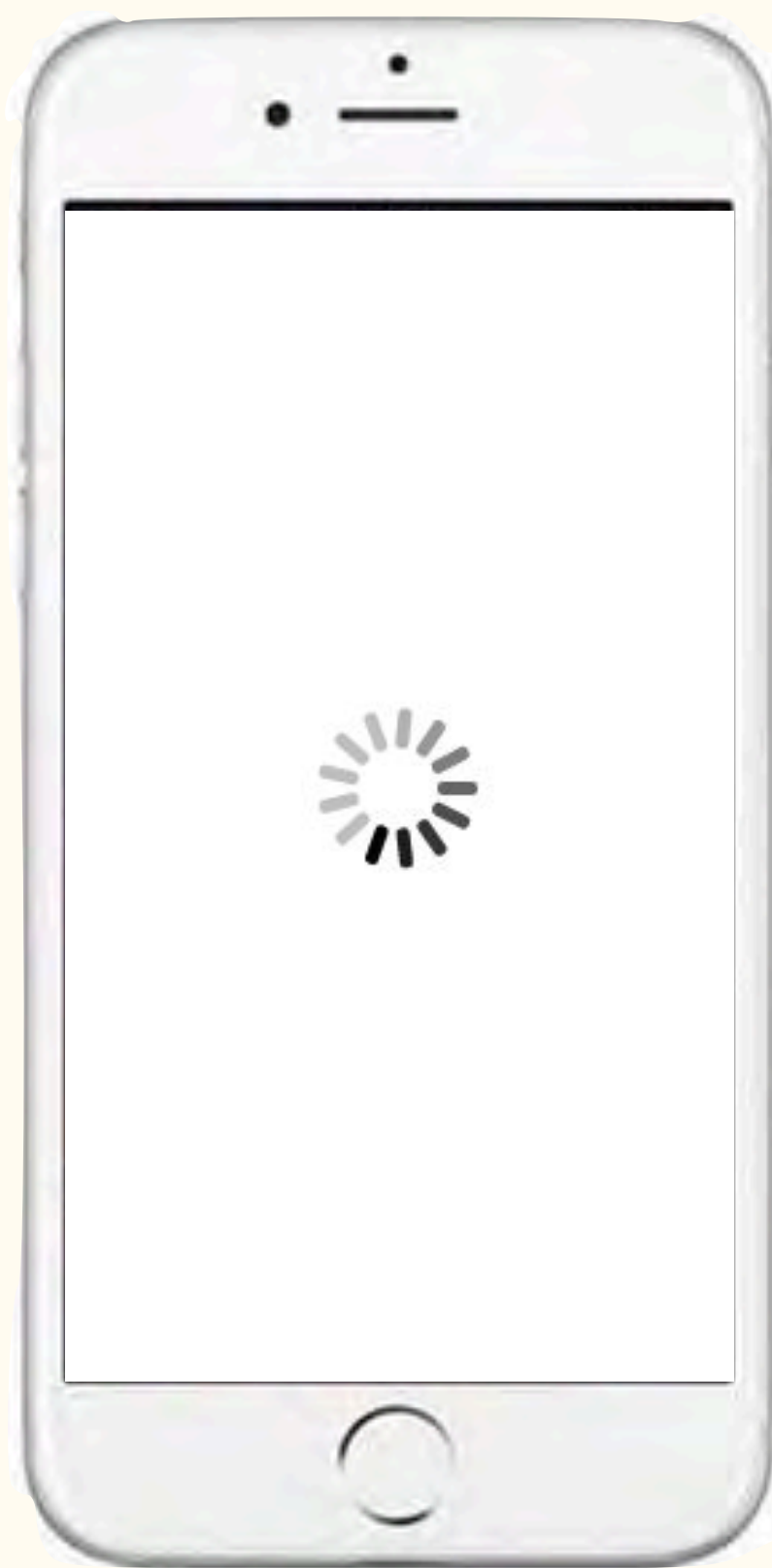
不可能!

3 测试 / 用户反馈



4

遇见问题



我是老板

这页面怎么打不开啊?

前端? 后台? 能否复现?



前端



后台



测试



xx手机，能够复现了

原来是前端兼容问题，
难怪浏览器是正常的



我是老板

老板，问题修复了



修复速度太慢了！



及时发现

方便解决

总结沉淀



打造线上**监控系统**，
及时发现问题，解决问题

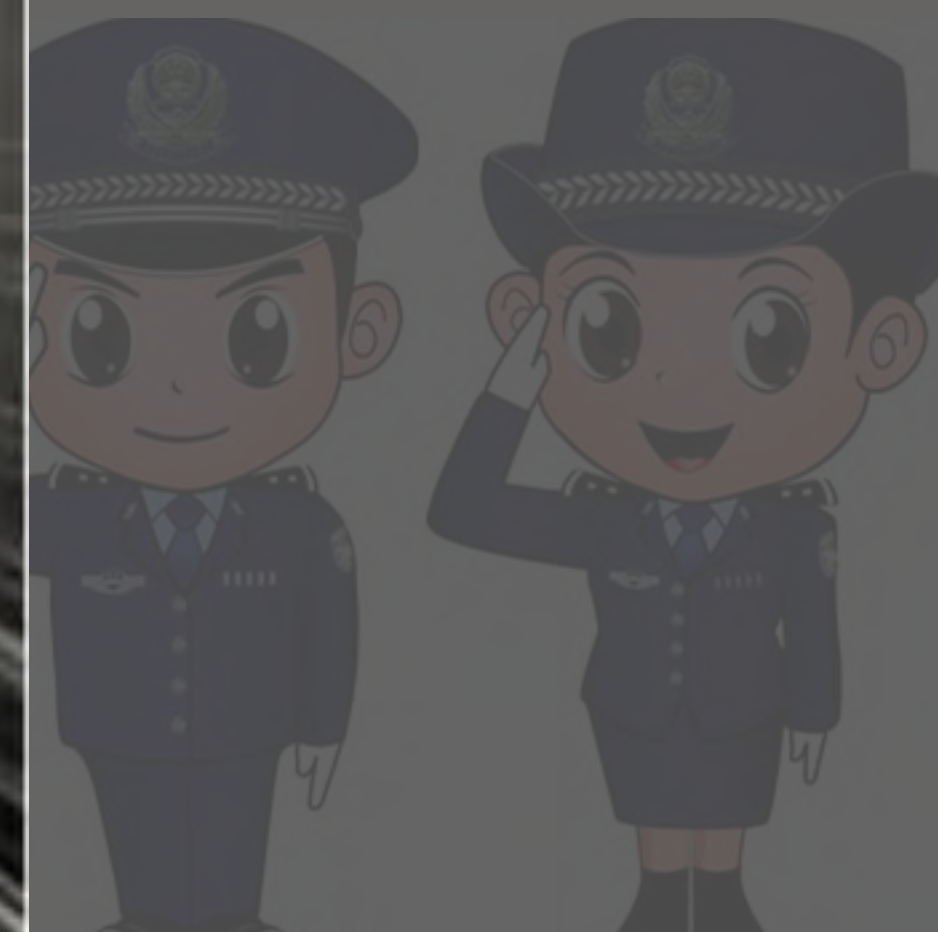


监控系统

监控、上报、信息收集

1

“偷听”(监听)系统基本组成



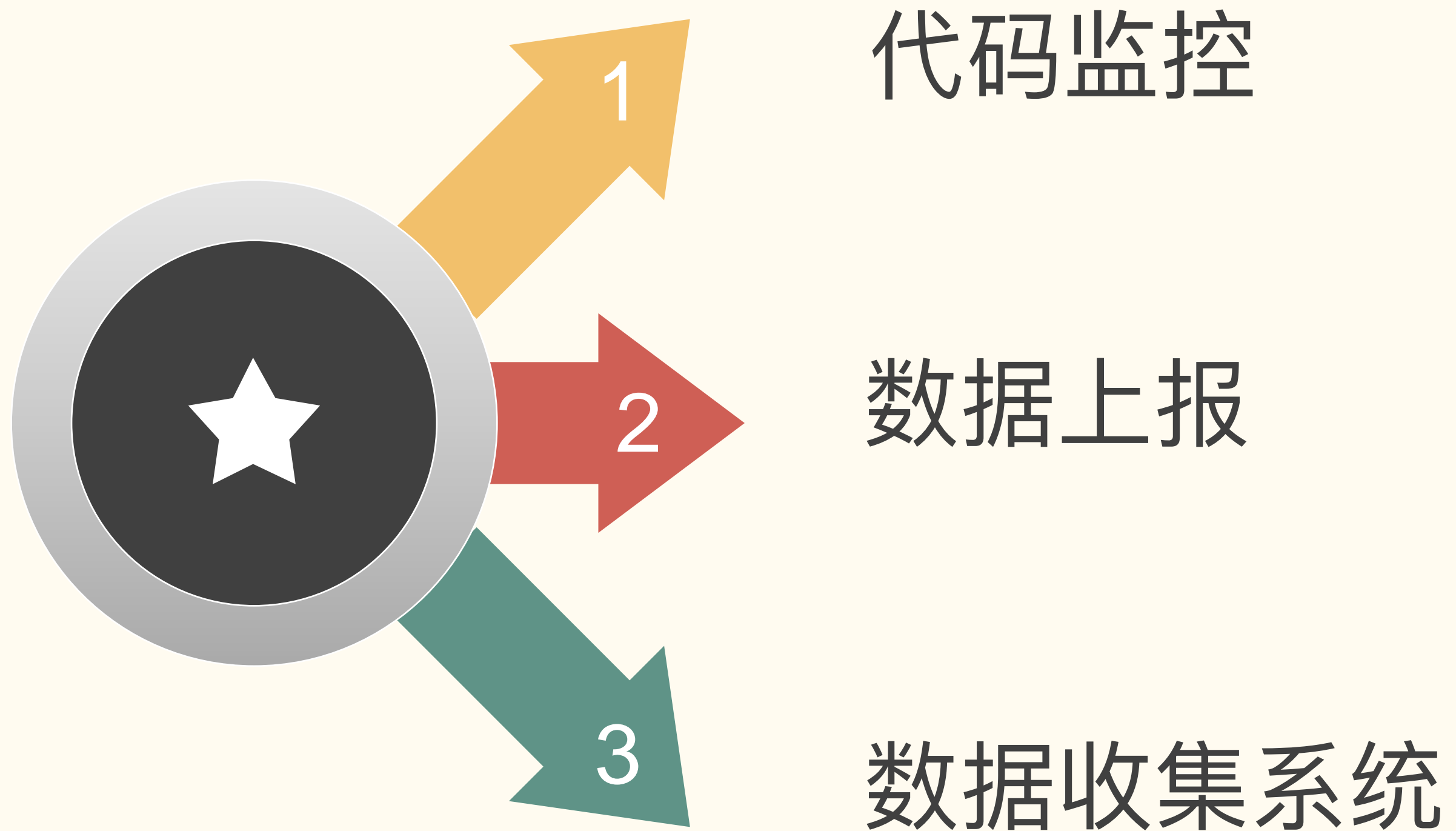
偷听 监控

现场还原 数据呈现

警局 信息收集

2

监控系统基本组成



3 监控方式

监控的方式主要有两种

● try-catch

— — — ▶

预料之内的错误

```
1 try {  
2     test // <- throw error
```

— — — ▶

预料之外的错误

```
1 /**  
2  * @param {String} msg 错误信息  
3  * @param {String} url 出错文件  
4  * @param {Number} row 行号  
5  * @param {Number} col 列号  
6  * @param {Object} error 错误详细信息  
7  */  
8 window.onerror = function(msg, url, row, col, error) {  
9     console.log('onerror 错误信息 ✓');  
10    console.log({  
11        msg, url, row, col, error  
12    })  
13 };  
14  
15 test // <- throw error
```

```
1 try {  
    setTimeout(function() {  
        test // <- throw error 异步错误  
    }, 0)  
    ch(e){  
        console.log('异步错误信息 ✓');  
        console.log(e);  
    }  
}
```

并非此即彼，可结合使用

异步错误无法捕获

4 上报方式

- 通过Ajax发送数据
- 动态创建 img 标签的形式

```
1  function report(msg, level) {  
2      var reportUrl = "http://localhost:8055/report";  
3  
4      new Image().src = reportUrl + '?msg=' + msg;  
5  
6  }
```




● 提供上报接口

● 存储上报数据

● 数据分析展示



错误信息分析与优化

1 错误信息分析 Script error.

#	出现次数	错误内容
1	58648	Script error.
2	1199	ReferenceError: Can't find variable: mqq
3	452	Uncaught TypeError: undefined is not a function
4	408	Uncaught TypeError: Cannot read property 'gid' of null
5	303	Uncaught TypeError: Cannot read property 'sp_id' of null
6	220	TypeError: Cannot read property 'gid' of null @ Object.<anonymous>: (file:///storage/emulated/0/tencent/MobileQQ/qbiz/html5/2146/qun.c (file:///storage/emulated/0/tencent/MobileQQ/qbiz/html5/2146/qun.c file:///storage/emulated/0/tencent/MobileQQ/qbiz/html5/2146/qun.q file:///storage/emulated/0/tencent/MobileQQ/qbiz/html5/2146/qun.q
7	193	TypeError: Cannot read property 'sp_id' of null @ Object.<anonymou result.html:1:13485) @ e (http://qun.qq.com/homework/features/mo http://qun.qq.com/homework/features/model/individual-result.html: result.html:1:13166
8	133	Uncaught TypeError: Cannot read property 'R' of undefined
9	122	[object Event]

2 产生 Script error. 的原因

浏览器安全策略，跨域报错信息无权限获得

```
342 bool ScriptExecutionContext::sanitizeScriptError(String& errorMessage, int& lineNumber,  
343 {  
344     ASSERT(securityOrigin());  
345     if (cachedScript) {  
346         ASSERT(cachedScript->origin());  
347         ASSERT(securityOrigin()->toString() == cachedScript->origin()->toString());  
348         if (cachedScript->isCORSSameOrigin())  
349             return false;  
350     } else if (securityOrigin()->canRequest(completeURL(sourceURL)))  
351         return false;  
352  
353     errorMessage = ASCIILiteral { "Script error." };  
354     sourceURL = { };  
355     lineNumber = 0;  
356     columnNumber = 0;  
357     error = { };  
358     return true;  
359 }
```




3 优化 Script error.

- 同源处理
 - Inline 内联代码
 - 外链同域名
 - 外链灰度同域（ 20% ）

4 优化 Script error.

● 利用跨源资源共享机制(CORS)

● script标签添加crossorigin属性

▼ Request Headers view source

```
Accept: */*
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8,en;q=0.6
Connection: keep-alive
Host: 127.0.0.1:8077
If-Modified-Since: Fri, 10 Mar 2017 02:12:56 GMT
Origin: http://a.com
Referer: http://a.com/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
       rome/49.0.2623.112 Safari/537.36
```

```
<script src="//qq.com/main.js" crossorigin></script>
```

● 响应头增加 Access-Control-Allow-Origin

● 响应头中需带上 Vary: Origin

▼ Response Headers view source

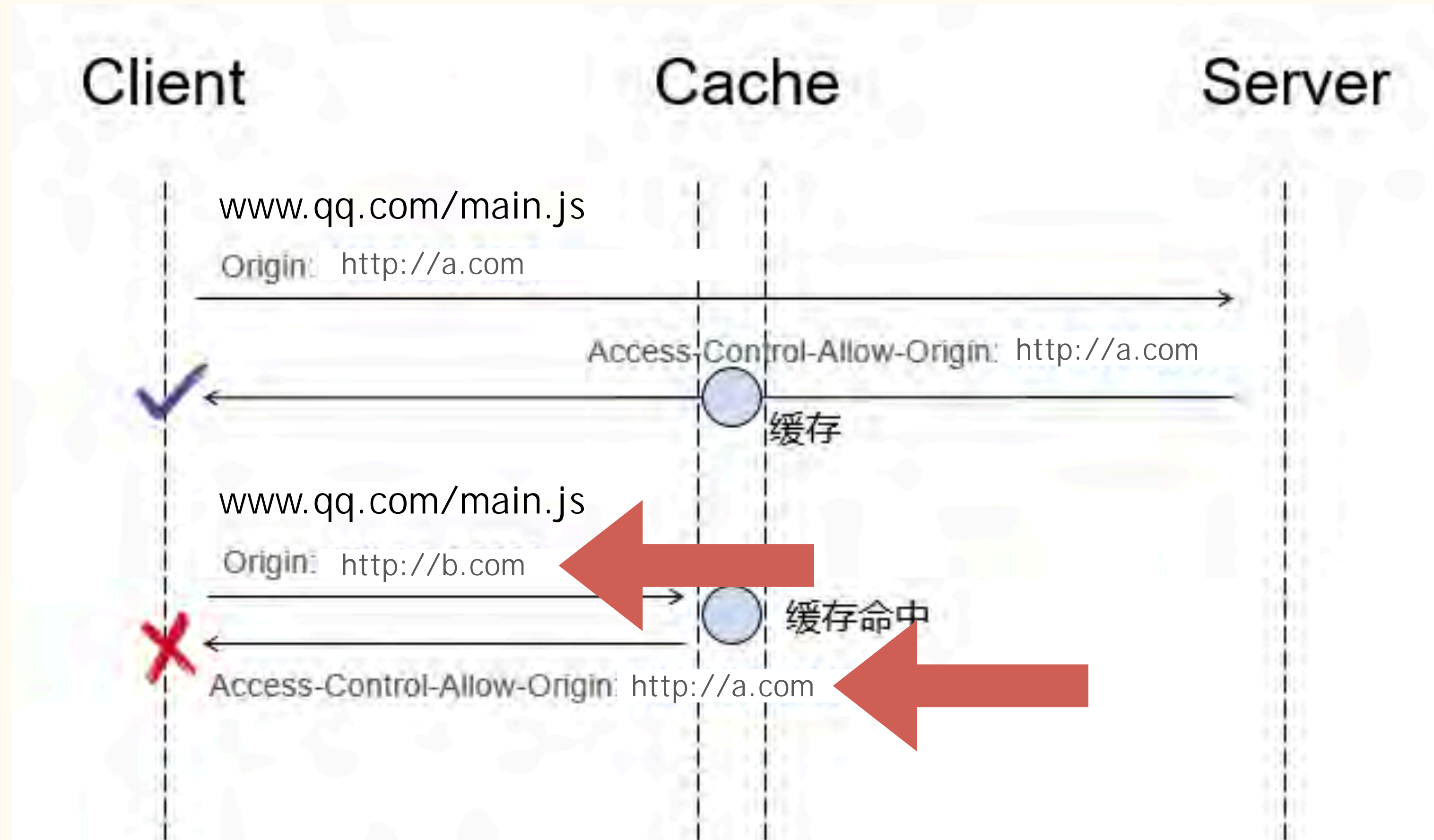
```
Access-Control-Allow-Origin: *
Access-Control-Allow-Origin: http://a.com
Cache-Control: max-age=0
Connection: keep-alive
Content-Length: 1
Content-Type: application/javascript; charset=utf-8
Date: Mon, 13 Mar 2017 02:37:21 GMT
Last-Modified: Fri, 10 Mar 2017 02:12:56 GMT
Vary: Origin
```

5 Vary:Origin 的作用

Vary

为缓存服务器提供缓存规则及缓存筛选的依据

Vary:Origin 表示在缓存筛选时，将结合请求的 Origin 进行区分





进行脚本错误分析

6 错误信息分析

具体错误信息

msg[0]	TypeError: e is not a function @ Object.init (http://qun.qq.com/homework/features/js/detail.303c8.js:5:16690) @ Object.o [as init] (http://qun.qq.com/homework/features/js/detail.303c8.js:5:15916) @ http://qun.qq.com/homework/features/js/detail.303c8.js:5:31662 @ u (http://qun.qq.com/homework/features/detail.html:371:31779)
target[0]	http://qun.qq.com/homework/features/js/detail.303c8.js 出错js文件
rowNum[0]	5
colNum[0]	16690 出错行列数

detail.303c8.js

```
1 define("utils",["require","module","exports"],function(e,t,i){var n,o=fun
2 function n(e,t,i){var n={data:i,up:e,top:e._top,namespace:t+""};e[t]="obj
3 },i=(t[e]||"other")+ "_116";return "//pub.idqqimg.com/pc/misc/homework/cour
4 uin:e.uin,nick:e.nick,head:e.head},content:e.content||{},vm:e,direction:t
5 i.exam_msg&&i.exam_msg.kpoint&&i.exam_msg.kpoint.chapterName){var r=i.exa
```

代码压缩后，定错出错代码困难



让脚本错误一目了然

1 让脚本错误一目了然

不压缩代码

```
export default function jsbs(res, opts={}, loc={}) {  
  var dist = beautify(res, opts),  
      sm = generator(res, dist),  
      smConsumer = consumer(sm);  
  
  var line = loc.line,  
      column = loc.column;  
  
  var locRes = line !== undefined && column !== undefined && smConsumer.  
  +
```

代码大小变大很多、源代码泄露

2 让脚本错误一目了然

半压缩

分号换空格 / 保留空格换行

通过特征值快速找到报错代码

```
},  
478: function(t, e, n) {  
    "use strict";  
  
    function r(t) {  
        return t && t.__esModule ? t : {  
            default: t  
        }  
    }  
  
    function o(t, e) {  
        if (!(t instanceof e)) throw new TypeError("Canno  
    }
```

代码大小相对压缩则仍有所变大

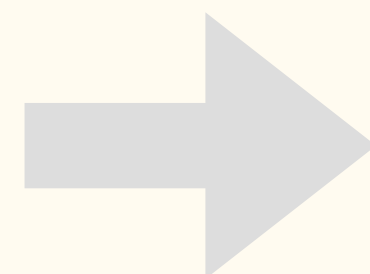
3 让脚本错误一目了然

使用 SourceMap 快速定位

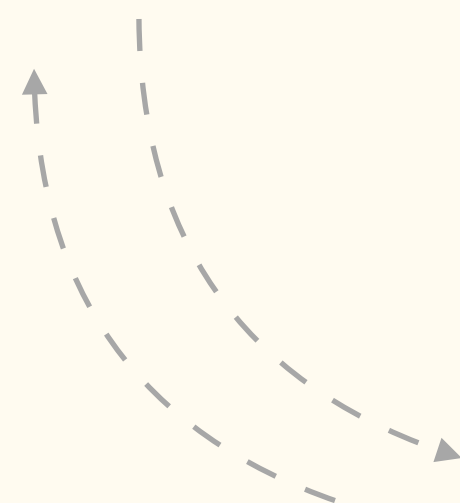
SourceMap

维护源文件盒处理后文件的映射关系
使用VLQ编码来存储映射

源文件



生成文件



SourceMap文件



4 让脚本错误一目了然

利用 SourceMap 结合生成文件的行列 定位 到源文件位置



```
!function(n){function r(e){if(t[e])return t[e].exports;var o=t[e]={i:e,l:!1,exports:{}};return n[e].call(o.exports,o,o.exports,r),o.l=!0,o.exports}var t={};r.m=n,r.c=t,r.i=function(n){return n},r.d=function(n,t,e){r.o(n,t)||Object.defineProperty(n,t,{configurable:!1,enumerable:!0,get:e})},r.n=function(n){var t=n&&n.__esModule?function(){return n.default}:function(){return n};return r.d(t,"a",t),t},r.o=function(n,r){return Object.prototype.hasOwnProperty.call(n,r)},r.p="",r(r.s=0)}([function(n,r){function t(){noerror}t()}]);
```

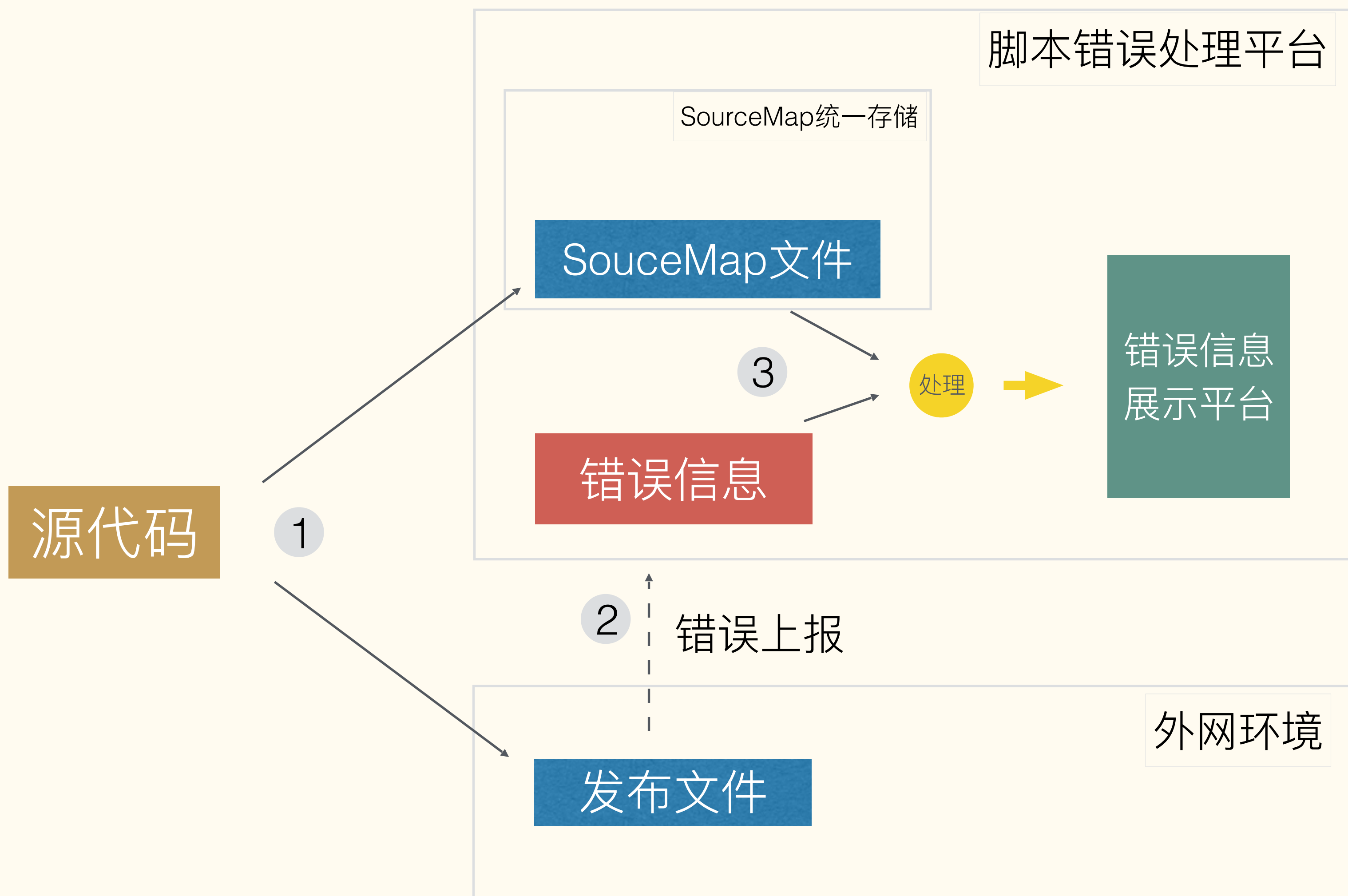
sourcemap + 行列数

```
function init() {  
  noerror;  
  // ...  
}
```

需要支持 sourcemap 生成、不会增加线上代码大小

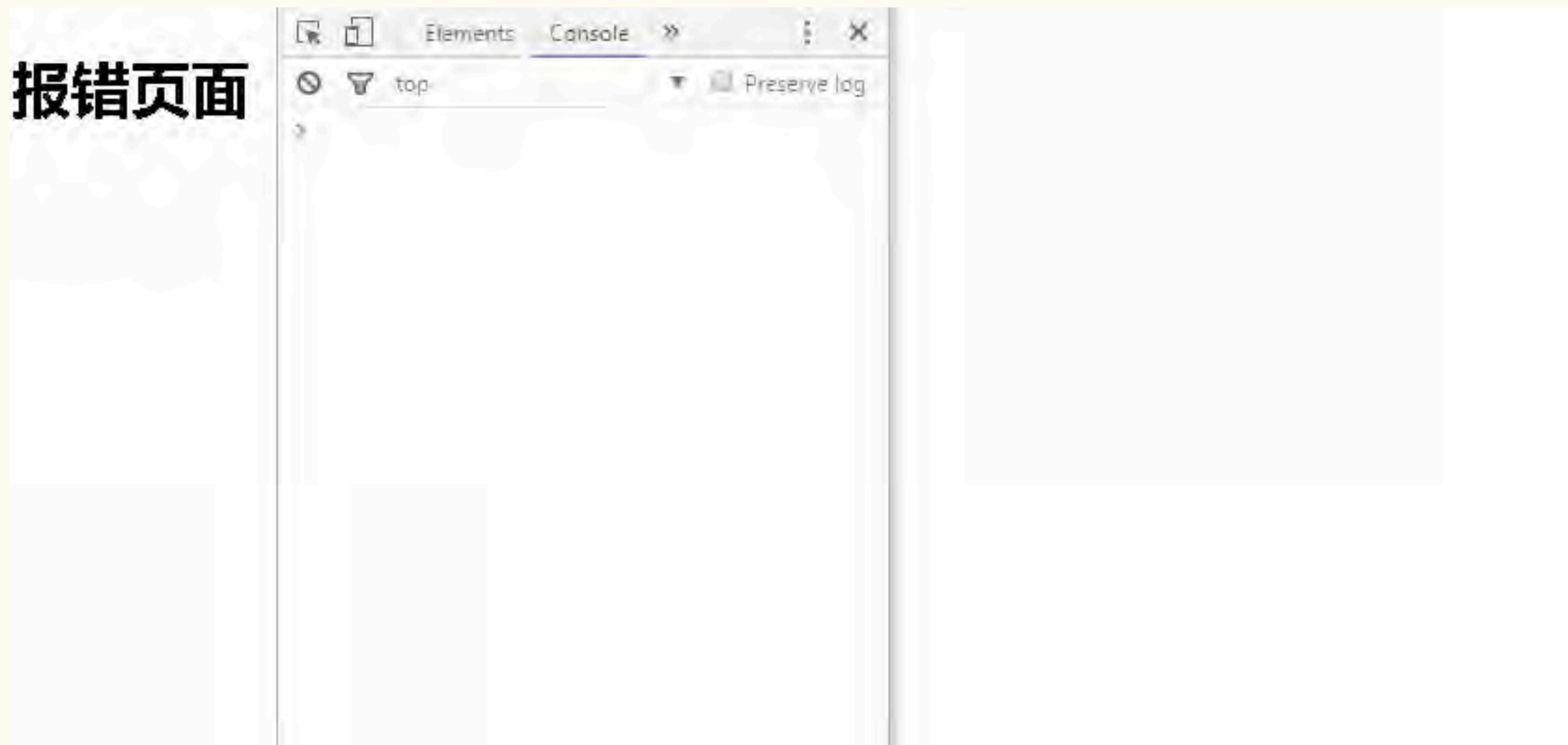
5

基于SourceMap脚本报错监控系统方案



6

基于SourceMap脚本报错监方案示例



7 开源方案 sentry

Captain Planet / Heart

ISSUES EVENTS OVERVIEW USER FEEDBACK RELEASES

Star Subscribe Settings

Unresolved Issues

Sort by: Last Seen

is:unresolved

GRAPH: 24H 14D EVENTS USERS

Error	TypeError	poll(.../sentry/scripts/views.js)	Object [object Object] has no method 'updateFrom'	HEART-1D	6 days ago — 4 months old	1	26	1
Error	★ javax.servlet.ServletException	org.hibernate.jdbc.Util in throwError	Something bad happened	HEART-1G	6 days ago — 4 months old	1	26	1
Error	script-src	example.com	Blocked 'script' from 'example.com'	HEART-1K	6 days ago — 4 months old	1	26	1
Error	ZeroDivisionError	bin/raven in <main>	divided by 0	HEART-1H	6 days ago — 4 months old	1	26	1

Filter people

Chris Jennings

错误列表

错误量告警

项目的团队管理

指定修复负责人

进展与记录

邮件通知

<https://github.com/getsentry/sentry>





8 发现代码不存在的错误信息

```
7      193      TypeError: Cannot read property 'sp_id' of null @ Object.<anonymous>  
              result.html:1:13485) @ e (http://qun.qq.com/homework/features/mo  
              http://qun.qq.com/homework/features/model/individual-result.html:  
              result.html:1:13166
```

这报错信息在代码中不存在!

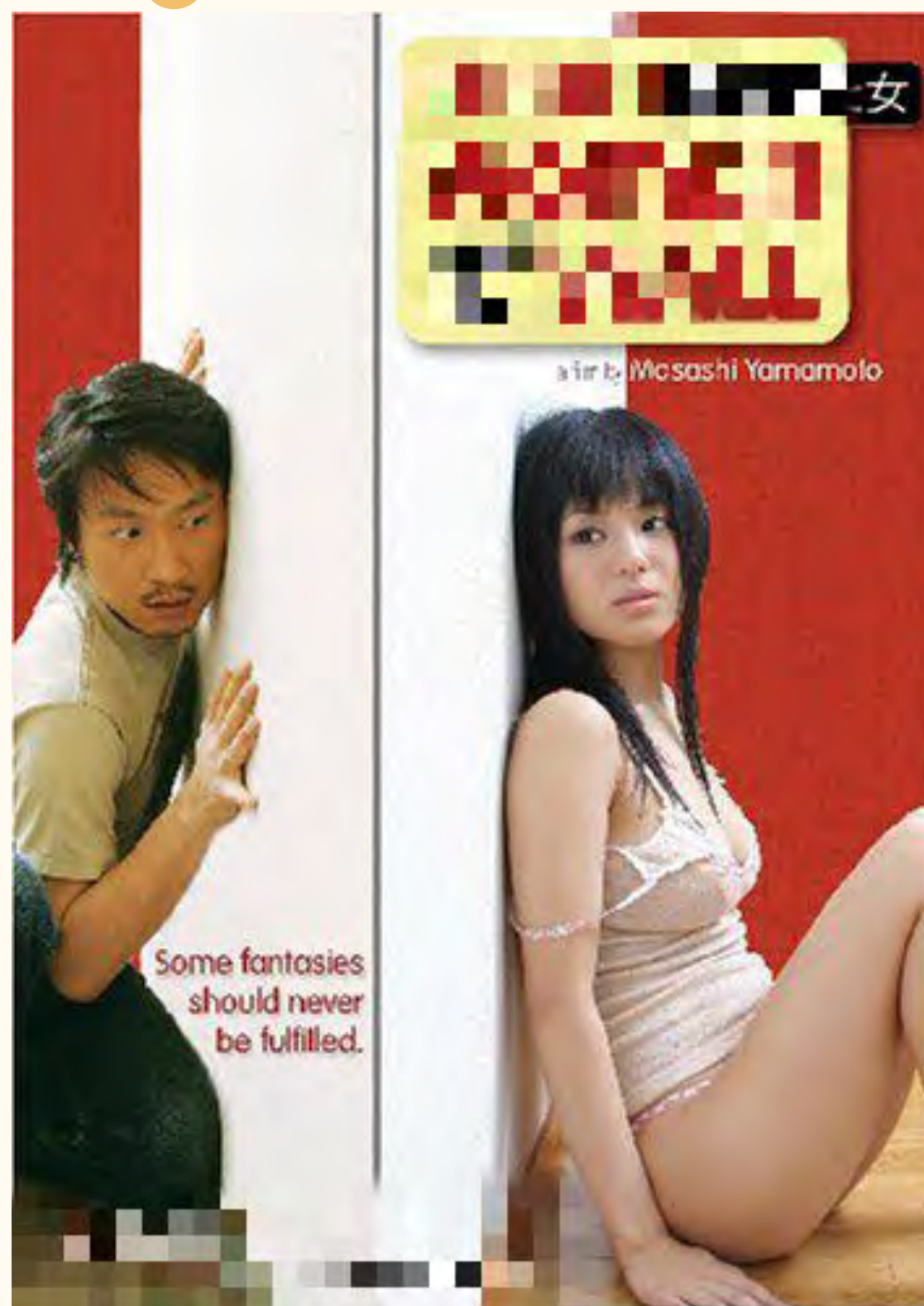


页面被注入了别的代码?



Web 安全 与 脚本错误

1 监控、上报



偷听 监控

● 监控、上报非白名单中的前端资源

监听 document 的 onload 事件，对加载的 src 内容进行上报
只上报非白名单的资源

```
1 document.addEventListener('load', function(e) {  
2     if(..) {  
3         report(e.target)  
4     }  
5 }, true);
```


2 数据分析，场景还原

排名	出现次数	劫持方式的具体类型及地址
1	3113	script-- url:http://wap.zjtoolbar60.10086.cn:8080/www/default/base.js
2	2670	iframe-- url:http://qun.qq.com/homework/features/detail.html?_ww=1027
3	1182	script-- url:l
4	693	script-- url:l



英语作业

joey 2015-08-07 11:31

123123

已查阅 (3)

未查阅 (53)



家校师生群产品

2015-08-07 15:00



桑梓

2015-08-10 17:53



joey

03-17 11:18

关闭



正在加载...

CSP

内容安全策略

白名单

可信任的内容来源

非白名单

无法正常执行

1 CSP (Content Security Policy)

CSP 使用方式

● HTML Meta 标签

```
<meta http-equiv="Content-Security-Policy" content="script-src 'self'">
```

● HTTP Header （ 响应头 带上 CSP 的指令）

▼ Response Headers view source

Connection: keep-alive

Content-Security-Policy: script-src 'self' *.qq.com *.url.cn

2 CSP 配置

两种策略

上报 Content Security Policy
不拦截、

拦截 Content Security Policy
进行拦截

多类参数

指令示例及说明

指令	取值示例	说明
default-src	'self' cdn.example.com	定义针对所有类型（js/image/css/web font/ajax/iframe/多媒体等）资源的默认加载策略，某类型资源如果没有单独定义策略，就使用默认策略

指令值示例及说明

指令	指令值	示例	说明
script-src	'self'	js.example.com	只允许加载来自同源的资源
object-src	'self'		只允许加载来自同源的资源
style-src	'self'	css.example.com	只允许加载来自同源的资源
img-src	'self'	image.example.com	只允许加载来自同源的资源
media-src	'self'	media.example.com	只允许加载来自同源的资源
frame-src	'self'		只允许加载来自同源的资源
connect-src	'self'		只允许加载来自同源的资源
font-src	font.qq.com		只允许加载来自font.qq.com的资源
	*	img-src *	允许任何内容
	'none'	img-src 'none'	不允许任何内容
	'self'	img-src 'self'	允许同源内容
	data:	img-src data:	允许data:协议（如base64编码的图片）
	www.a.com	img-src www.a.com	允许加载指定域名的资源
	*.a.com	img-src *.a.com	允许加载a.com任何子域的资源
	https://img.com	img-src https://img.com	允许加载img.com的https资源
	https:	img-src https:	允许加载https资源
	'unsafe-inline'	script-src 'unsafe-inline'	允许加载inline资源（style属性，onclick，inline js和inline css等等）

https://



3

脚本错误量越来越少

线上的脚本错误量变少了!



开发测试，从“源头”减少错误



开发测试 与 脚本错误

1

测试客户端内嵌页面脚本报错

报错了!

网络问题?

缓存导致?

CCP没返回?

发现不及时 定位困难





js-error-dialog

脚本错误弹窗组件

<https://github.com/joeyguo/js-error-dialog>

1 测试客户端内嵌页面脚本报错

- 报错自动唤起 (及时、可视化)



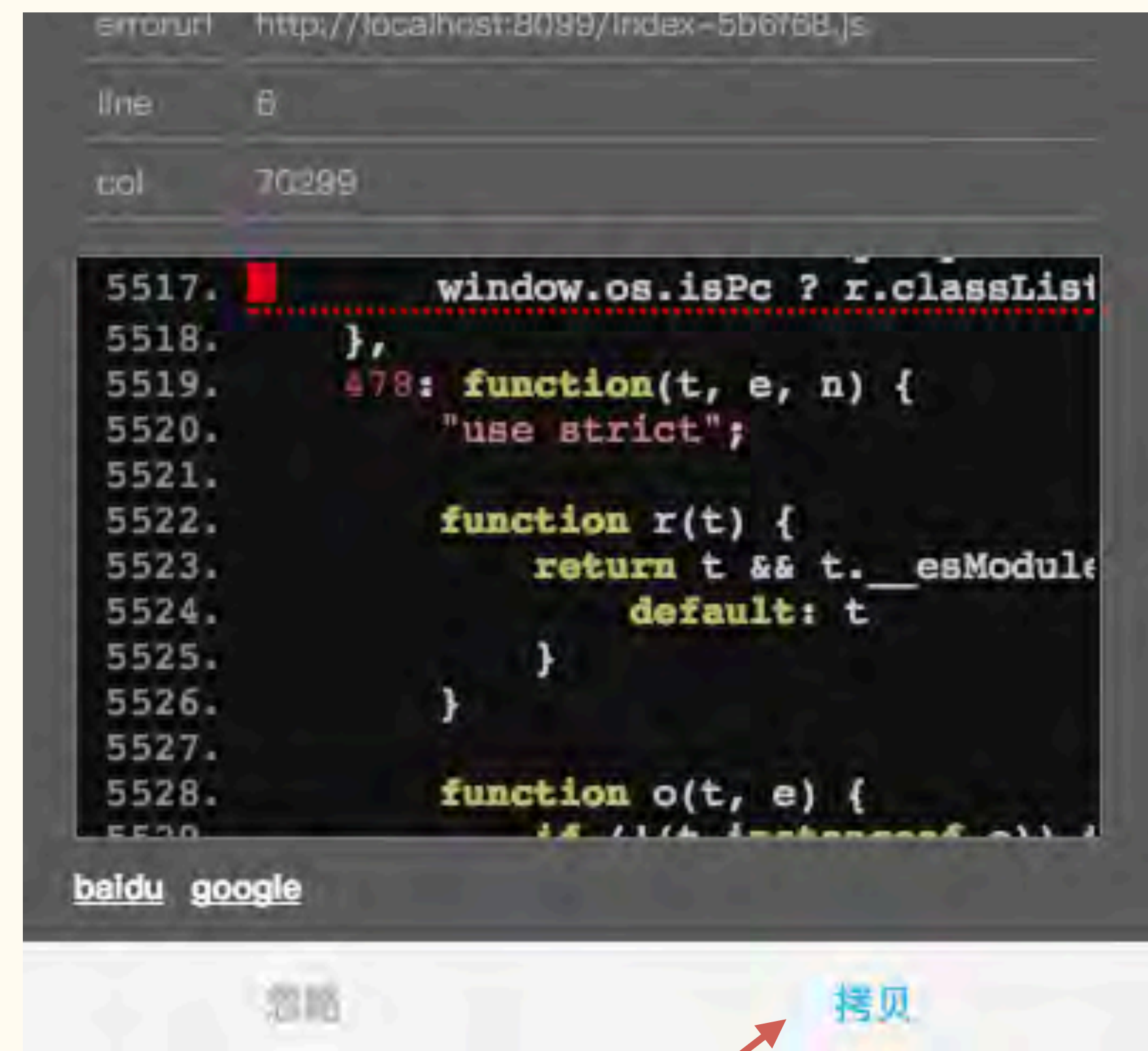
2 js-error-dialog

- 拷贝错误信息(易传播)



弹出错误提示

点击拷贝，发送给我



3 js-error-dialog

● 错误信息还原(可视化)

打开错误页面, 增加 jed 参数, 自动唤起输入框
粘贴错误信息, 查看生成报告





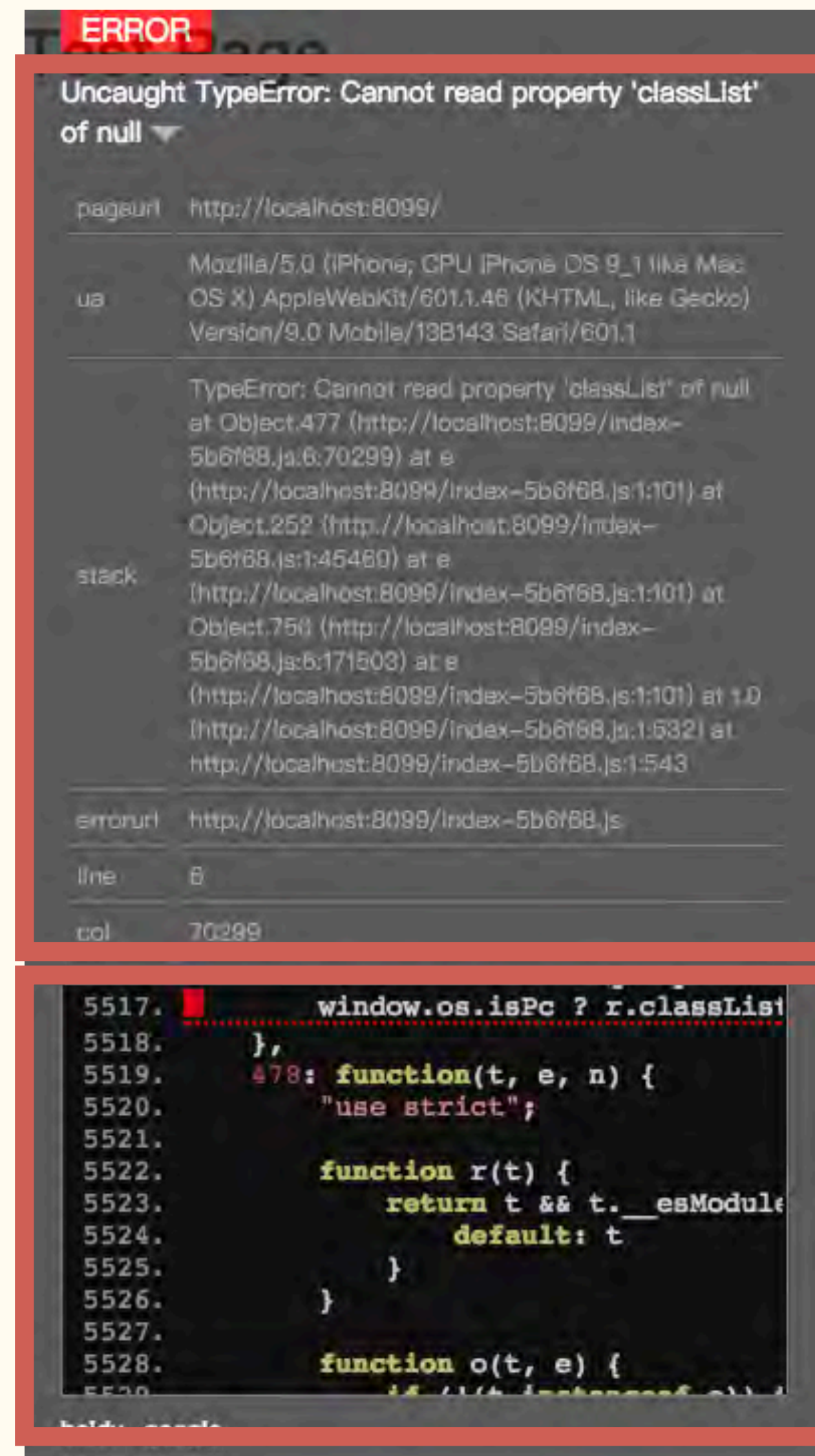
js-error-dialog 原理分析

现场分析

2 js-error-dialog 信息

● 详细的错误信息

- 基础报错信息 与 自定义信息
报错信息、U/A、客户端版本 ...
- 查看压缩代码格式化的位置
精确地看到具体报错代码



3 js-error-dialog 实现核心

● 将压缩代码格式化并找到对应位置

```
!function(n){function r(e){if(t[e])return t[e].exports;var o=t[e]={i:e,l:!1,exports:{}};return n[e].call(o.exports,o,o.exports,r),o.l=!0,o.exports}var t={};r.m=n,r.c=t,r.i=function(n){return n},r.d=function(n,t,e){r.o(n,t)||Object.defineProperty(n,t,{configurable:!1,enumerable:!0,get:e})},r.n=function(n){var t=n&&n.__esModule?function(){return n.default}:function(){return n};return r.o(n,r.p),r.p="",r(r.s=0)}([function(n,r){function t(){noerror}t()}]);
```



```
!function(n) {  
    // ...  
    // ...  
}([ function(n, r) {  
    function t() {  
        noerror;  
    }  
    t();  
} ]);
```



资源体积过大？

5 js-error-dialog 执行流程

js-error-dialog

监控
入口

动态拉取

代码格式化、sourcemap
代码高亮、错误展示

prettyjs

报错更容易发现，线上错误更加少了！



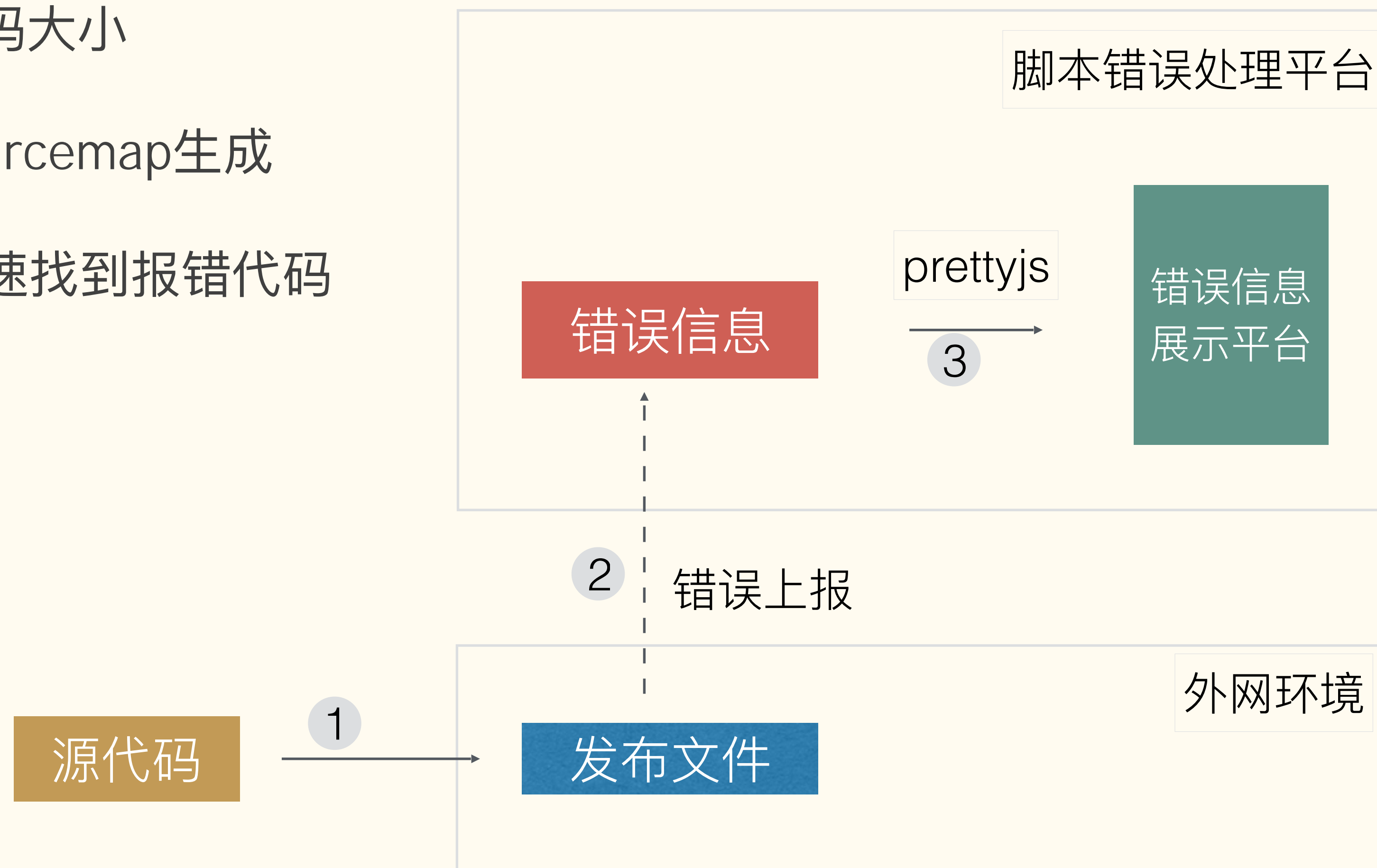
拓展



基于prettyjs脚本报错监控系统方案


1 基于prettyjs脚本报错监控系统方案

- 不增加线上代码大小
- 不需要支持sourcemap生成
- 通过特征值快速找到报错代码





回顾



1 回顾

- 如何发现代码出了问题?
- 监控体系基础组成
- 错误信息分析与优化
- 针对 Web 安全 的脚本错误优化
- 针对 开发测试 的脚本错误优化



joeyguo

- 《脚本错误量极致优化-监控上报与Script error》
<https://github.com/joeyguo/blog/issues/13>
- 《脚本错误量极致优化-让脚本错误一目了然》
<https://github.com/joeyguo/blog/issues/14>
- 《XSS终结者-CSP理论与实践》
<https://github.com/joeyguo/blog/issues/5>
- noerror
<https://github.com/joeyguo/noerror>
- js-beautify-sourcemap
<https://github.com/joeyguo/js-beautify-sourcemap>
- js-error-dialog
<https://github.com/joeyguo/js-error-dialog>
- prettyjs
<https://github.com/joeyguo/prettyjs>

**THANK
YOU**

