



[case20]聊聊rest api设计

api设计 阅读约 4 分钟

序

本文主要研究下rest api的设计。

设计准则

- easy to use & hard to misuse

易用不易误用，也就是api设计不要太复杂，要简单易用，而且还不能容易用错。

- least astonishment

简单就好，不要试图提供其他花哨、华丽的额外功能，比如对于时间类似的字符串参数，规定好一个输入格式即可，不要试图同时兼容多种格式输入。

- use case & document story

api文档要围绕story或者use case来进行，在一个业务场景下提供完整的闭环操作。

输入规范

- url中的路径

避免驼峰，避免下划线，优先采用横杠

- request method

post表示新增(ur1中没有id)，delete表示删除，get表示查询，put表示全量更新(幂等操作)，post url中携带id也可用于表示更新。

- 分页

比如page及size，或者limit及offset

- 排序

比如sort=+field2,-field2，用逗号分隔多个排序字段，用+表示升序，用-表示降序

- 字段过滤

比如fields=field1,field2,field3

- 复杂查询

简单的比如用eq代表等，lt代表小于，lte代表小于等于，gt代表大于，gte代表大于等于，like代表模糊查询；更复杂的话，可以参考rsql规范。

- 版本

不建议版本化，建议采用新的领域命名才与原有的api区分开来

输出规范

- 返回码

遵循http的返回码规范，4xx表示客户端错误，5xx表示服务端错误。

- 返回jsonObject而不是jsonArray

顶层结构返回jsonArray的话，就不容易扩展了。一般返回jsonObject，通常会携带code，error之类的

- 返回jsonObject的字段

success表示请求是否成功，data表示数据，msg表示消息描述，error描述错误信息详情。

- 错误信息格式

type表示错误异常类型，code表示错误编号用于个性化错误提示，msg用于错误信息描述，link提供该错误信息的具体描述页面

安全相关

- 调用方鉴权

对于api的消费者，要求调用的时候强制提供appId及appKey，用于最基本的调用源的鉴权

- 细粒度鉴权

对于更细粒度的数据权限控制，要细化到url及requestMethod基本

- 参数校验

对于查询、修改等参数要做基本校验，对参数内容进行非法参数过滤。

- 屏蔽错误堆栈

不要暴露后端的错误堆栈，如果是要方便排查问题，可以设置一个开关，来设置是否屏蔽错误堆栈

- 敏感数据脱敏

对于敏感的数据，要适当做一些脱敏处理，比如身份证号，手机号等。在真正需要真实数据的话，需要额外进行请求。

- 账号密码需要加密

登陆接口必须走https，而且必须要有图形验证码，而且还必须防暴力破解，有错误锁定机制，对于密码的传递，必须加密处理

- 防止id遍历问题

对于url的参数，如果id是递增的，则需要处理遍历问题，要么对外暴露经过处理后的id，要么做数据权限控制

- 防止token replay

对于token要有一定的失效机制，另外建议token对url参数进行签名

- 防止文件下载目录遍历

对于提供文件下载的接口，一定要避免目录遍历问题

服务质量保障

- 提供SLA
- 提供流量管理、熔断、限流
- 提供服务扩容机制
- 提供故障演练
- 提供审计功能
- 监控异常流量
- 提供调用方向的隔离


小结


rest api的设计牵扯的方面比较多，本文暂时只是先列了一些，后续有待补充。


doc


- [API设计要点](#)
- [聊聊jpa的动态查询](#)
- [使用RSQL实现端到端的动态查询](#)

阅读 6.6k • 更新于 2018-05-21

 赞 12

 收藏 16

 赞赏

 分享

本作品系 原创 ， 采用《署名-非商业性使用-禁止演绎 4.0 国际》许可协议



codecraft
◆ 10.5k

关注作者

0 条评论

得票 • 时间



撰写评论 ...

提交评论

评论加载中...

推荐阅读

code-craft

用户专栏

spring boot , docker and so on 欢迎关注微信公众号: geek_luandun

626 人关注 1498 篇文章

关注专栏

专栏主页





产品

- 热门问答
- 热门专栏
- 热门课程
- 最新活动
- 技术圈
- 酷工作
- 移动客户端

课程

- Java 开发课程
- PHP 开发课程
- Python 开发课程
- 前端开发课程
- 移动开发课程

资源

- 每周精选
- 用户排行榜
- 徽章
- 帮助中心
- 声望与权限
- 社区服务中心

合作

- 关于我们
- 广告投放
- 职位发布
- 讲师招募
- 联系我们
- 合作伙伴

关注

- 产品技术日志
- 社区运营日志
- 市场运营日志
- 团队日志
- 社区访谈

条款

- 服务条款
- 隐私政策
- 
- 下载 App

Copyright © 2011-2019 SegmentFault. 当前呈现版本 19.02.27



浙ICP备 15005796号-2 浙公网安备 33010602002000号 杭州堆栈科技有限公司版权所有

CDN 存储服务由 又拍云 赞助提供