Chrome 新的默认 Referrer-Policy : strict-origin-when-cross-origin

2020-11-19 阅读 14.1K

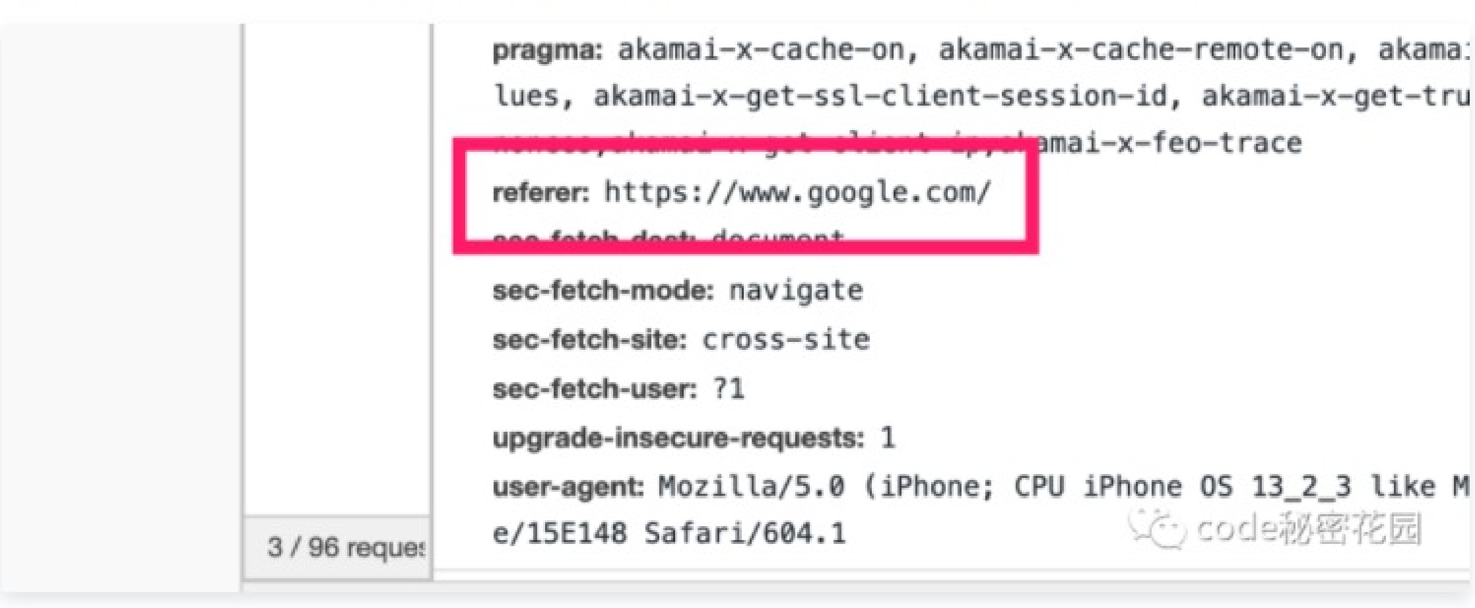
如果你的站点有使用 Referer 标头收集网页的访问来源信息，则此策略变化可能对你的程序造成影响，请仔细阅读。

在开始阅读本文之前，如果你不理解 `site` 和 `origin` 之间的关系，请阅读：**同站和同源你理解清楚了么？**

Referer 标头

`Referer` 请求头包含了当前请求页面的来源页面的地址，即表示当前页面是通过此来源页面里的链接进入的。

服务端一般使用 `Referer` 请求头识别访问来源，可能会以此进行统计分析、日志记录以及缓存优化等。

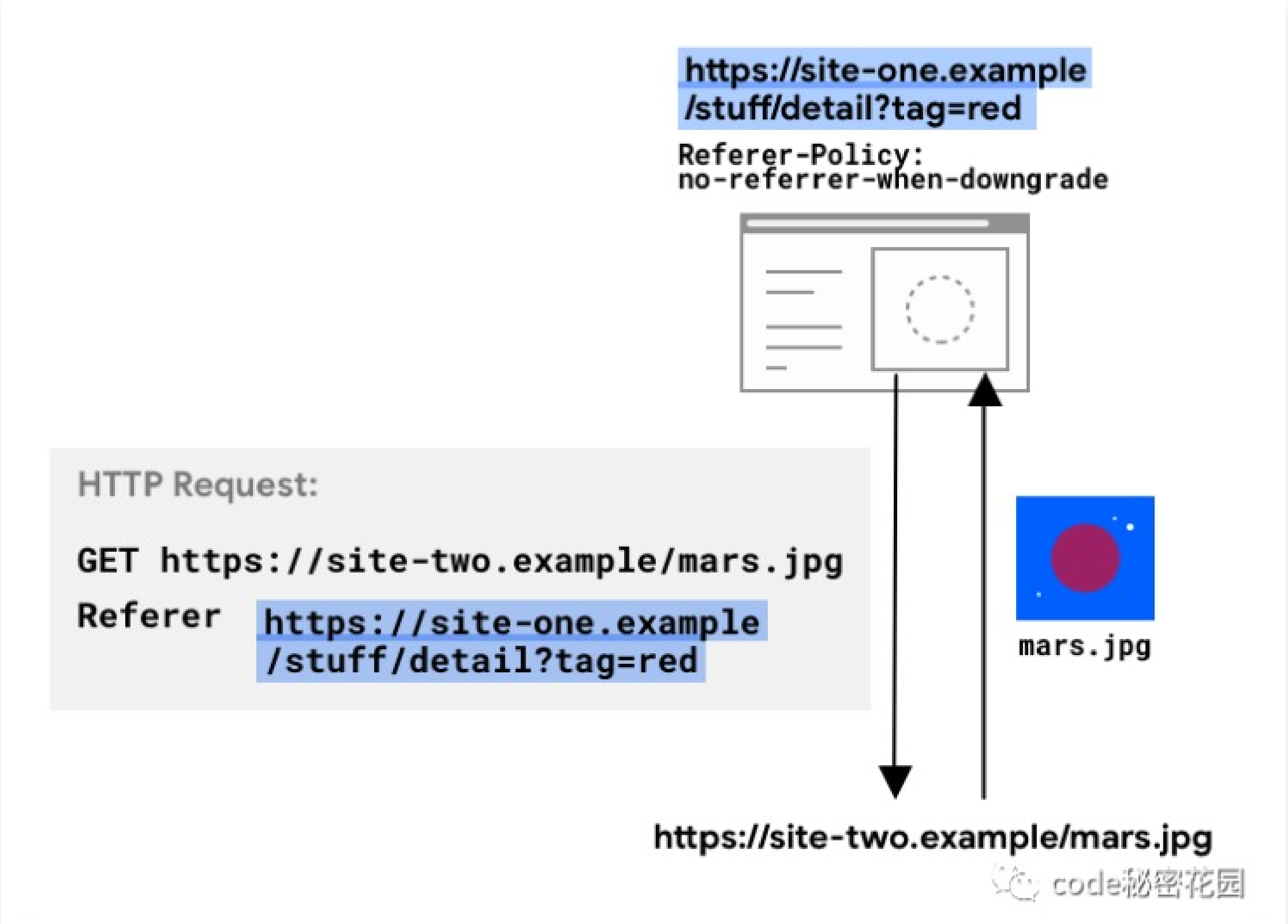


```
pragma: akamai-x-cache-on, akamai-x-cache-remote-on, akama
lues, akamai-x-get-ssl-client-session-id, akamai-x-get-tru
amai-x-feo-trace
referer: https://www.google.com/
sec-fetch-mode: navigate
sec-fetch-site: cross-site
sec-fetch-user: ?1
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (iPhone; CPU iPhone OS 13_2_3 like M
e/15E148 Safari/604.1
```

> 这里有意思的一点：referer 实际上是 "referrer" 误拼写。Referrer-Policy 标头以及 JavaScript 中的 referrer 拼写是没有问题的。

Referer-Policy

`Referer` 请求头可能暴露用户的浏览历史，涉及到用户的隐私问题。所以 HTTP 提供了 `Referrer-Policy` 标头，其用来监管和限制哪些访问来源信息会在 `Referer` 中发送（应该被包含在生成的请求当中）。



`Referer-Policy` 包括以下几个可选项

- `no-referrer`

整个 `Referer` 首部会被移除。访问来源信息不随着请求一起发送。

- `no-referrer-when-downgrade （默认值）`

在同等安全级别的情况下，引用页面的地址会被发送(`HTTPS->HTTPS`)，但是在降级的情况下不会被发送 (`HTTPS->HTTP`)。

- `origin`

在任何情况下，仅发送文件的源作为引用地址。例如 `https://example.com/page.html` 会将 `https://example.com/` 作为引用地址。

- `origin-when-cross-origin`

对于同源的请求，会发送完整的URL作为引用地址，但是对于非同源请求仅发送文件的源。

- `same-origin`

对于同源的请求会发送引用地址，但是对于非同源请求则不发送引用地址信息。

- `strict-origin`

在同等安全级别的情况下，发送文件的源作为引用地址(`HTTPS->HTTPS`)，但是在降级的情况下不会发送 (`HTTPS->HTTP`)。

- `strict-origin-when-cross-origin`

对于同源的请求，会发送完整的URL作为引用地址；在同等安全级别的情况下，发送文件的源作为引用地址(`HTTPS->HTTPS`)；在降级的情况下不发送此首部 (`HTTPS->HTTP`)。

- `unsafe-url`

无论是同源请求还是非同源请求，都发送完整的 URL（移除参数信息之后）作为引用地址。

Referer-Policy 默认值

如果 `Referer-Policy` 未设置任何策略，则使用浏览器的默认值。网站通常会遵循浏览器的默认设置。

> 对于导航和 `iframe` ， `Referer` 头中的数据也可以通过 `JavaScript` 使用 `document.referrer` 访问。

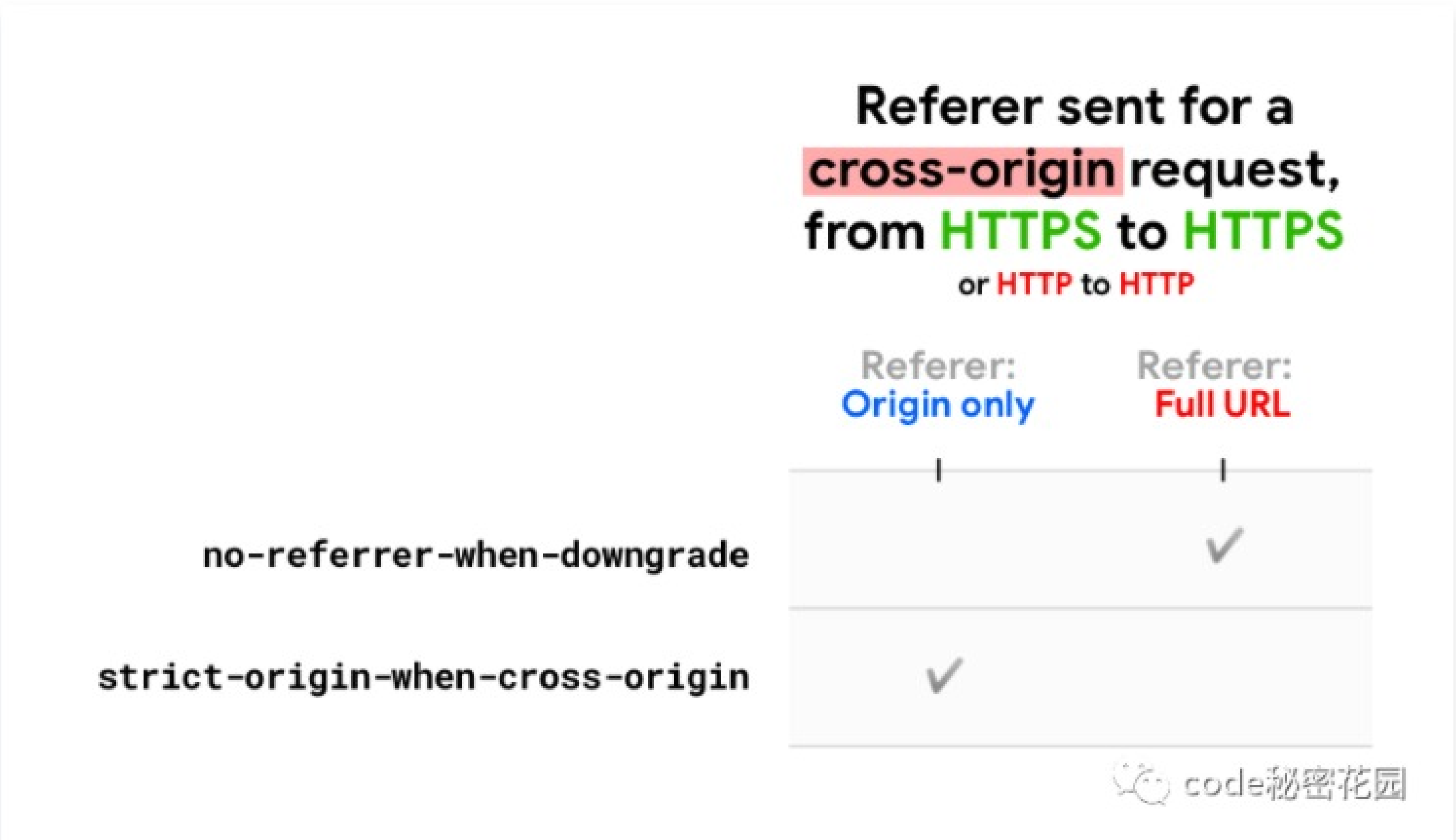
`no-referrer-when-downgrade` 是跨浏览器的一种广泛的默认策略。但是现在，许多浏览器正处于向更多提高隐私的默认设置过渡的阶段。

`Chrome` 计划在85版开始 将其切换默认策略 `no-referrer-when-downgrade` 更换到 `strict-origin-when-cross-origin` 。

变化

`strict-origin-when-cross-origin` 提供更多的隐私。有了这个政策， `Referer` 标头只会发送 `origin`

这样可以防止泄漏私人数据，这些数据可以从完整URL的其他部分（例如路径和查询字符串）访问。



例如，在一个跨域请求中：

从 `https://site-one.example/stuff/detail?tag=red` 访问 `https://site-two.example/…`

- 使用 `no-referrer-when-downgrade` : Referer: `https://site-one.example/stuff/detail?tag=red` 。
- 使用 `strict-origin-when-cross-origin` : Referer: `https://site-one.example/` 。

不变的

- 和 `no-referrer-when-downgrade` 一样， `strict-origin-when-cross-origin` 在从 `HTTPS` 来源访问 `HTTP` 站点时，不会携带 `Referer` 头。
- 在相同的来源内， `Referer` 标头值为完整的 `URL` 。

本文分享自微信公众号 - code秘密花园（code_mmhy），作者：ConardLi
原文出处及转载信息见文内详细说明，如有侵权，请联系 yunjia_community@tencent.com 删除。
原始发表时间：2020-11-17
本文参与腾讯云自媒体分享计划，欢迎正在阅读的你也加入，一起分享。

⚠ 举报

点赞 1　分享

0 条评论　我来说两句

登录 后参与评论

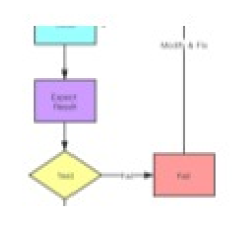
相关文章

迭代器与 for of的使用和原理

看着很简单，但是再回顾这段代码，实际上我们仅仅是需要数组中元素的值，但是却需要提前获取数组长度，声明索引变量等，尤其当多个循环嵌套的时候，更需要使用多个索引变量...

ConardLi

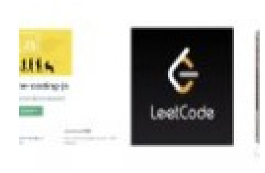
前端自动化测试探索和实践



众所周知的原因，前端作为一种特殊的 GUI 软件，做自动化测试困难重重。在快速迭代，UI 变动大的业务中，自动化测试想要落地更是男上加男？。

ConardLi

前端应该如何准备数据结构和算法？



据我了解，前端程序员有相当一部分不是科班出身，以至于对“数据结构”和“算法”的基础概念都不是很清晰，这直接导致很多人在看到有关这部分的内容就会望而却步。

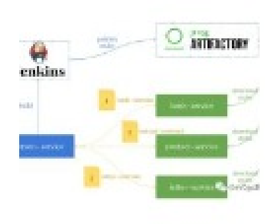
ConardLi

Linux常用命令02 - mv

mv 命令(简称 move)用于将文件和目录从一个位置重命名并移动到另一个位置。 命令的语法如下:

叉叉敌

初识 JFog Artifactory



Artifactory 是 JFrog 的一个产品，用作二进制存储库管理器。二进制存储库可以将所有这些二进制统一托管，从而使团队的管理更加高效和简单。

Peter Shen

用python，生活仍有诗和远方

常听说，现在的代码，就和唐朝的诗一样重要。 可对我们来说，写几行代码没什么，但是，要让我们真正地去写一首唐诗，那可就头大了。。既然如此，为何不干脆用代码写一首唐...

py3study

python技术面试题(八)

答：is是同一性运算符，是判断两个对象的id地址是否相同，是否指向同一块区域；==是比较操作符，用来判断两个对象的数据类型和值是否相同。

小闫同学啊

Java进阶笔记——MySql中的varchar类型

MySQL 数据库的varchar类型在4.1以下的版本中的最大长度限制为255，其数据范围可以是0~255或1~255（根据不同版本数据库来定）。在 MySQ...

慕容千语

使用bash编写Linux shell脚本--调试和版本控制

当我还在布鲁克大学上学的时候， Macquarium 实验室中充满了苹果公司的 Macintosh Plus 电脑。一天，我在为第三年的操作系统课程准备一个程序...

猿人谷

记录一则expdp任务异常处理案例

环境：AIX 6.1 + Oracle 10.2.0.4 现象：在XTTS迁移测试阶段，遇到执行几个expdp的导出任务，迟迟没有返回任何信息，对应日志无任何...

Alfred Zhao

更多文章 >

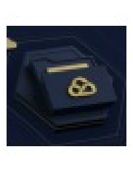
作者介绍

ConardLi

关注　专栏

文章	阅读量	获赞	作者排名
310	105.8K	733	523

精选专题



云计算新趋势

Serverless浪潮已来，如何稳坐潮头领先业界？

活动推荐

【玩转腾讯云】征稿！

一起玩转腾讯云，好礼拿到手软！　立即查看

腾讯云自媒体分享计划

入驻云加社区，共享百万资源包。　立即入驻

目录