Ken's Study Journey
Ken的学习之旅

关于禁止大量扫描网站API接口的提醒

简单来说：

近期，我的其中一台服务器(GB-LHR-01)检测到并上报了在我网站中来自国外的异常行为，例如扫描Ken的学习规划师API接口。

Ken的学习之旅提醒你：大量扫描网站API接口的行为是不对的哦！这样会威胁网站和网络安全。

亲爱的同学、老师和用户们，

感谢您选择和使用Ken的学习之旅服务！

近期，我的其中一台服务器（GB-LHR-01；英国伦敦节点）的安全风控系统检测到并上报了在我服务中威胁网络安全的异常行为（全部来自国外），包括Ken的学习之旅网站和Ken的学习规划师。

根据该服务器上的日志，这些行为包括：

- 扫描不存在的Ken的学习规划师API接口链接，例如：
  https://planner.kenstudyjourney.cn/api/grame/getHomePtLottery/
- 使用Tor上网工具，在Ken的学习之旅网站上扫描WordPress模块(wp-***.php)
  （已被服务器安全风控系统拦截）
  我的网站并没有使用WordPress SDK框架

我的服务目前均已禁止国外用户使用Tor上网工具访问。

但由于这类请求已被英国服务器当地丢弃，没有转发到中国(CN)的服务器，因此没有对服务造成太大影响。

这些行为没有遵守：

- Ken的学习规划师"robots.txt"文件中的规则、
- 我的《服务协议》第四条（爬取非公开信息）

这些行为还违反了部分其它网站上的《服务协议》。

我每天在空闲时间会随机巡查网站上的模块、页面和服务器错误日志，检查：

- 我的网站、服务或部分模块是否宕机/故障（运行不正常）、
- 我的服务中是否出现异常行为

这类似于上课期间老师巡查教室，国际考期间考试局巡查考场。

为了追查不当行为或宕机事故，以及根据中国法律法规，我的服务器都会记录和留存操作日志。

为了同学们学习计划的安全，我的服务器均设有安全风控系统，监控并上报任何异常情况。

Ken的学习之旅提醒你：

- 大量扫描网站API接口的行为是不对的哦！

根据我的《服务协议》，可以做的行为有：

- 仅当你持有API链接和密钥时，使用、爬取和请求对应的API接口
- 爬取和扫描公开显示的网页（如搜索引擎）
- 遵守网站上"robots.txt"文件中的规则
- 正确设置蜘蛛/爬虫HTTP请求头的"User-Agent"值，包括"bot"、"spider"、"crawl"等关键字

不可以做的行为有：

- 大量爬取和扫描非公开的数据（如API接口数据和密钥）
- 使用Tor上网工具/浏览器在网站上进行滥用行为

我目前正在持续在服务器安全风控系统中增加更多安全措施，给予同学们安全的学习环境、氛围和体验。

如果你有任何问题，或不理解《服务协议》等的内容，你可以随时联系我进行解答。

希望同学们能够正确使用网络（包括其它网站和平台）。如发现这类行为，请及时劝阻、制止和举报。

Ken的学习之旅

2023年5月31日

www.kenstudyjourney.cn, ken@kenstudyjourney.cn

你知道吗？

在部分网站中，如果同一个网络IP地址在短时间内向同一个网站（如国外搜索引擎）发送大量请求（网页和API接口），这个IP地址可能会被网站封禁一段时间。

但Ken的学习之旅的目标是教育用户（尤其是学生），而不是惩罚或封禁用户。因此这只是一个提醒。

什么是《服务协议 (ToS)》？

我理解并知悉，部分用户不知道什么是服务协议(ToS, Terms of Service)，因此我在这里将简短解释。

服务协议(ToS)可以在大部分网站底部找到，且大部分平台（网站和APP）会要求用户注册使用前阅读ToS。

它会介绍以下几点，且是具有法律效力的文档。

- 平台提供的服务，
- 在平台中可以做和不可以做的行为，
- 平台的责任（如平台对你造成损失，该平台是否会向你赔偿），
- （等等）

简单来说，网站上常见不允许做的行为有：

- 网络攻击（如(D)DoS/CC攻击、黑客入侵），
- 大量扫描网站API接口和登录页面（账号和密码），
- 发送垃圾邮件，
- 上传或发送（法律法规或平台规范）禁止的内容，
- （等等）

我的另一个Tip：遵守中国法律法规

作为一名国际学校(A Level)学生，我的网站和Ken的学习之旅服务已通过国内ICP和公安备案，并受中国法律管辖。

但我理解并知悉，国外用户可能并不了解我们的规则，因此我在这里将简短介绍。

这同样适用于其它国内网站，甚至是网络运营商ISP的路由器。

根据中国《网络安全法》第二十一条第三款的规定，网站需要记录并留存日志至少6个月，包括：

- 访问者IP地址
- 访问者端口号
- 精确到秒的访问/操作日期和时间
- URL网页链接
- 用户标识符（邮件地址、ID编码等）
- （等等）

因此，服务器和系统都会记录任何访问和操作行为（尤其是黑客入侵或网页扫描的尝试），保存在日志文件中，以便后续调查取证。

当有关部门需要调查网上有害行为或内容时，网站主人需要依法予以配合，提供相应的日志信息。

注：日志还可用于网站平台内部的调查取证，查看是否出现bug和非攻击类宕机（服务器故障）事故。

注意：对于造成服务严重中断的网络攻击（如(D)DoS、CC等攻击），网站主人有权通知网警。