Ken's Study Journey
Ken的学习之旅

关于Ken的学习之旅严查大量扫描网站隐藏模块及设置曝光台的公告

维护网络安全，Ken的学习之旅在行动

对大量网站扫描说“不”

简单来说

请尽快停止扫描WordPress开源模块、管理后台入口（如/wp-admin）等网站隐藏模块/页面。

Ken的学习之旅将严查大量扫描网站隐藏模块行为，维护Ken的学习之旅网站/平台和用户学习计划的安全。

我将自研并增加“自动劝阻系统”（预计2023年8月1日上线），自动劝阻这些行为。

劝阻无效、持续扫描可能会被显示在“曝光台”中的哦！

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！

公告“劝阻无效”现象

在发布公告提醒禁止国外用户扫描网站后，Ken的学习之旅系统发现仍有部分用户（有Python程序，也有频繁更换IP地址的服务器）在扫描网站隐藏模块（即“劝阻无效”）。

经过进一步分析，扫描者在扫描前并未打开过任何正常网页（如Ken的学习之旅网站首页、《服务协议》、文章、Ken的学习规划师登录页面等），而是直接开始扫描WordPress等隐藏模块，因此公告劝阻并不会起作用。

严查、劝阻扫描行为

接下来，Ken的学习之旅将严查大量扫描网站隐藏模块行为，维护Ken的学习之旅网站/平台和用户学习计划的安全。

在安全风控系统的基础上，我将自研并增加“自动劝阻系统”（预计2023年8月1日上线）和“威胁Ken的学习之旅网站/网络安全曝光台”。

如系统发现持续扫描网站隐藏模块行为，将立即自动劝阻，并返回"429 Too Many Requests"的HTTP响应状态码。

请在显示系统劝阻页面后，立即停止扫描行为。

对劝阻无效、持续扫描的用户和爬虫程序，系统将自动上报Ken的学习之旅中国广州总部。在经过人工核实后，可能会显示在曝光台中。

曝光时间暂定为7天，并部分隐藏/掩盖IP地址等敏感信息。

需要注意的是，我自研的系统将通过“大数据”进行分析。对频繁更换IP地址、通过修改系统hosts文件、DNS服务器等手段频繁更换服务器节点等用户将采取“全链条追踪”措施。

用户意见征集

但不要过度担心。新系统的编写、制作和升级需要几天的时间，目前正在征集用户意见。

如对本措施有异议或有任何意见/建议，欢迎将你的意见/建议发送到ken@kenstudyjourney.cn。

常见禁止扫描的隐藏模块

请尽快停止扫描网站隐藏模块/页面（均为不存在/无效），包括但不限于：

- 网站登录页面（大量扫描用户名和密码）
- WordPress模块，例如：
  - /wp-admin
  - /wp-login.php
  - /wp-comments-post.php
  - Ken的学习之旅网站/平台均为独自编写的代码，不会使用WordPress等第三方建站框架
- 网站代码备份压缩包（包括但不限于rar、zip、7z、tar.gz），例如：
  - /kenstudyjourne.zip
  - /kenstudyjourney.zip
  - /www_kenstudyjourney_com.rar
  - /wwwkenstudyjourneycn.zip
  - /planner_kenstudyjourney_cn.tar.gz
- 网站管理后台入口，例如：
  - /admin/index.php
  - /administrator/index.php
  - /phpMyAdmin
  - /pma
- 不存在的API接口，例如：

    - /api/sonicos/auth/
- 网站后台程序代码文件后缀（包括但不限于php、jsp、asp、aspx、sql，但不包括html、js、css），例如：
    - /phpinfo.php
    - /repeater.php
    - 我已在所有网站URL链接中停止使用上述文件名后缀

部分禁止扫描页面的示例（来自服务器日志）：

- https://www.kenstudyjourney.cn/wp-admin
- https://planner.kenstudyjourney.com/planner_kenstudyjourney_com.tar.gz
- https://www.kenstudyjourney.cn/administrator/index.php
- http://139.180.133.248/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- http://78.141.194.139/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- http://8.134.150.123/phpinfo.php

请大家共同监督，争做网络安全“志愿者”。

维护网络安全，Ken的学习之旅在行动！

Ken的学习之旅

2023年7月23日

中国广州

www.kenstudyjourney.cn, ken@kenstudyjourney.cn

威胁Ken的学习之旅网站/网络安全曝光台：

https://www.kenstudyjourney.cn/zh-cn/internet-security-reminder-board/

为什么不能大量扫描网站隐藏模块？

大量扫描网站隐藏模块，不仅会无意义占用服务器和运营商网络带宽，还会浪费时间、威胁网络安全。

不要因为威胁网络安全，而影响到你和他人的正常生活哦！

真实案例

2021-2023年，国外社交媒体网站Twitter发生数据泄露，影响了2亿多位用户（来自Firefox Monitor）。

漏洞扫描是网络攻击开始的步骤，每一次成功的扫描就意味着攻击的开始。

经过进一步分析，本次入侵主要使用了网站API接口的漏洞。

当输入账号存在的邮件地址或手机号码时，服务器就会返回账号用户名。（来自Firewall Times）。

为什么Ken的学习之旅不会采取“封IP地址”的处置手段？

Ken的学习之旅已将“封账号”和“封IP地址”列为暴力处置手段，拒绝“以暴制暴”。

IP地址被网站/平台封禁后，攻击者第一反应就是更换IP地址。最简单的方法就是到不同的地方连接不同的WiFi网络。

其次，部分攻击者（例如学校学生）会利用“共存效应”，故意影响同IP地址（局域网内）其他同学使用。

真实案例

2023年6月26日，GB-LHR-01（英国伦敦）服务器节点检测到国外来自Tor工具扫描网站WordPress模块行为。

由于Ken的学习之旅已禁止国外用户使用Tor工具访问，该请求已被Web应用防火墙(WAF)拦截，显示“访问被拒绝 (Access Denied)”页面。

但扫描者在看到该页面后，怀疑IP地址已被封禁，第一时间选择更换IP地址，直到找到可用IP地址为止。本次扫描已持续/坚持约11分钟（最终还是失败）。

此事件证明了封禁IP地址可能会有副作用。

你知道吗？

在高中，作为一名自律的学生，我成功当选学校学生会纪检部成员，严查同学们是否在遵守纪律。

同样，在知道规则的重要性后，我还会在校外也采用相同的措施，包括Ken的学习之旅网站/平台。

了解更多