Ken's Study Journey
Ken的学习之旅

Notice about Rigorous Check and Reminder Board for Massive Website Scanning
Ken's Study Journey Strives to Maintain Internet Security
Say "No" to Massive Website Scanning

Simply Speaking

Please stop your scans for the hidden modules and URLs, like WordPress modules and admin panels (e.g. "/wp-admin").

Ken's Study Journey will rigorously (strictly) check massive website scanning attempts, maintaining a safe environment for the Ken's Study Journey website/ platform and user study plans.

I will invent and add an automated reminder system (may be available on 1 August 2023) to automatically remind scanners.

Any continuous scans after reminders/warnings may be shown publicly on the reminder board.

Dear students, teachers, and visitors,

Thanks for choosing and using Ken's Study Journey services!

No Effect on Previous Reminders

The Ken's Study Journey system continually discovered attempts (including Python programs and servers frequently changing IP addresses) of scanning website hidden modules after noticing/reminding website scanners.

Based on my analysis, the scanners did not open any normal pages (e.g. Ken's Study Journey website home page, "Terms of Service (ToS)", articles, Ken's Study Planner login page, etc.), but instead directly scanned hidden modules (e.g. WordPress). This is why notices took no effect.

Rigorously Checking Scanning Attempts and Reminding Users

Ken's Study Journey will rigorously check massive website scanning attempts, maintaining a safe environment for the Ken's Study Journey website/platform and user study plans.

I have invented and will make and add an automated reminder system (may be available on 1 August 2023) to the security control system and a Reminder Board for continuous violations.

The system will automatically remind users of any continuous attempts of scanning website hidden modules with an HTTP Status Code "429 Too Many Requests".

Please immediately stop scanning once you see the reminder page.

Any continuous scans after reminders/warnings will be automatically reported to Ken's Study Journey headquarter (in Guangzhou, China) by the system, which may hence be displayed on the Reminder Board.

The display will be upheld for 7 days and will mask any sensitive information (e.g. IP addresses).

Please note that my invented system will link and trace any forging attempts (e.g. frequently changing IP addresses and/or server nodes (by changing the system "hosts" file or DNS servers)) using the "Big Data" technology.

User Idea Collection

Since programming and implementation of the new system need several days, I am now collecting user ideas.

You can send your ideas to ken@kenstudyjourney.cn if you have any ideas and/ or reject this policy.

Common Scanning-Prohibited Website Hidden Modules

Please stop your scans for the hidden modules and URLs, which are all non-existent/invalid, including but not limited to:

- Website login pages (massively scan User Names and Passwords)
- WordPress modules, for example:
  - /wp-admin
  - /wp-login.php
  - /wp-comments-post.php
  - Ken's Study Journey website/platform uses its own programming skills without any third-party frameworks (e.g. WordPress)
- Website code backup zip files (including but not limited to "rar", "zip", "7z", "tar.gz"), for example:
  - /kenstudyjourne.zip
  - /kenstudyjourney.zip
  - /www_kenstudyjourney_com.rar
  - /wwwkenstudyjourneycn.zip
  - /planner_kenstudyjourney_cn.tar.gz
- Website administration (admin) panel, for example:
  - /admin/index.php

- /administrator/index.php
- /phpMyAdmin
- /pma
- Non-existent APIs, for example:
  - /api/sonicos/auth/
- Website backend program code files suffix (including but not limited to "php", "jsp", "asp", "aspx", "sql"; "html", "js", "css" are excepted), for example:
  - /phpinfo.php
  - /repeater.php
  - I have disabled these suffixes on all website URLs.

Examples of URLs Cannot be Scanned (from Server Logs):

- 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

Please supervise together and be an Internet security "Volunteer".

Ken's Study Journey strives to maintain Internet security.

Ken's Study Journey

23 July 2023

Guangzhou, China

www.kenstudyjourney.cn, ken@kenstudyjourney.cn

Reminder Board of Threatening Ken's Study Journey Website Security:

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

Why Massive Website Scanning is Not Allowed?

Massively scanning website hidden modules not only meaninglessly occupies server and ISP bandwidth but also wastes your time and threatens Internet security.

Don't negatively impact your and other's daily life by threatening Internet security.

Real Example

Between 2021 and 2023, Twitter, an Internet social media platform, was breached affecting over 200 million users, according to Firefox Monitor.

Website Scanning is an essential attacking stage. Every successful scan means the beginning of an attack process.

Based on further investigation, this was caused by a vulnerability in its website API.

The username is returned when an existent email address or phone number is entered, according to Firewall Times.

Why Ken's Study Journey does not Ban any IP Addresses?

Ken's Study Journey proved that banning user accounts and/or IP addresses can be violent which may have negative impacts.

Attackers immediately change their IP addresses after blocking, which can be achieved using different WiFi networks at different places.

Additionally, some attackers (like students in a school) can abuse the "Coexistence Effect", intentionally preventing other students, under the same IP address, from using the services.

Real Example

My GB-LHR-01 (London, United Kingdom) server detected scanning attempts of WordPress modules from Tor.

Since Ken's Study Journey bans users from using the services via Tor, the requests were dropped by the Web-Application Firewall (WAF), displaying an "Access Denied" page.

The scanner then immediately changed its IP address until an available IP address is found. The scan continued for 11 minutes (all attempts were unsuccessful).

This proved banning IP addresses may have negative impacts.

Did you Know?

Being self-disciplined and elected by our High School's Student Union (as an Inspector of Disciplines), I rigorously checked whether students are following the school rules.

Knowing the importance of rules, I also adopt the same methodology outside our school campus, including Ken's Study Journey website/platform.

Learn More