Ken's Study Journey
Ken的学习之旅

Ken的学习之旅关于维护网络安全的倡议书

维护网络安全，Ken的学习之旅在行动

科技再发达，安全要严查

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！

2023年1月，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）。Ken的学习之旅对本次网络安全事件高度重视。

近年来，国外网络平台数据泄露事件频发，这敲响了网络安全的警钟。

我随后在春节期间的空闲时间，采取了“远程办公和管理”的方式，紧急对网站代码进行安全更新，再次加强安全性。

经过我的进一步调查，网络平台数据泄露主要通过网站和API漏洞进行。Tor (The Onion Router, 俗称“暗网”)已成为国外入侵及数据泄露的主要作案、逃避追踪工具。

Ken的学习之旅总部与总服务器节点位于中国广州(CN-CAN)。它既作为Ken的学习之旅的网络核心节点，也是全网中最繁忙、服务用户量最多的服务器节点，每天服务成百上千的国内用户，就像市中心图书馆一样。

作为一名国际学校学生和一个国内的网络平台，Ken的学习之旅不仅要遵守中国的法律法规，更要与全世界/国际的学生用户交往和服务。

2023年7月1日，我已完成服务器安全风控和日志系统的升级，为用户学习计划和数据安全提供了进一步的保障。

Ken的学习之旅会尽自己最大努力维护自身系统安全，但用户也可以采取行动，进一步提高安全性。Ken的学习之旅向广大用户提出如下倡议：

一、了解网络安全重要性

网络安全比学习更重要。有了安全，才能保证学习计划不被非法篡改和泄露，提高学习效率、放心学习。

否则，就可能出现忘记课程和任务、迟到、旷课等现象，严重甚至会泄题、影响后续的学习旅程和学业。

二、发现异常情况，及时上报

在使用网络平台时，如发现任何异常情况（见下方附件1）（不仅是Ken的学习之旅服务），请及时向该平台上报。

例如，你可以发邮件到ken@kenstudyjourney.cn上报Ken的学习之旅产品、服务的情况（例如Ken的学习规划师）。

这样既保证了自己的安全，又可以保护其他用户的安全。同时，你还可以上报影响使用的bug哦！

Ken的学习之旅为免费、无偿服务（类似于“志愿者/公益服务”），因此我很抱歉无法对上报做出奖励。但我仍会鼓励及时上报异常情况。

真实案例

2023年6月底，Ken的学习之旅收到用户邮件，上报了Ken的学习规划师无法设置“时间/课程表”的bug。该bug已在12小时内被修复。

三、制止、劝阻非正常使用（滥用）行为

如果扫描登录页面、(D)DoS攻击等非正常使用（滥用）行为（见下方附件2）发生在你身边，请及时劝阻和制止。

如多次劝阻无效、仍屡教不改，可以向平台进行投诉、举报。

四、主动开启多重验证(2FA或MFA)和登录提醒功能

若网站没有做好安全防护，输入密码的登录页面就能被暴力破解。当一个网站被入侵、且账号密码泄露后，其它网站的账号安全也会受到影响。

因此建议开启使用短信/邮件验证码、验证器APP等的双重/多重验证(2FA或MFA)方式。他人知道密码也无法登录账号。

除此之外，还建议开启短信或邮件的登录提醒功能。

五、不要仅为应付检查而维护安全

Ken的学习之旅在学习经验分享讲座中多次强调过，不要仅为应付检查而遵守规则。这只会浪费检查员的辛苦工作，在实际上并不会起任何作用。

要知道网络安全的重要性，自觉提高安全意识，杜绝盗号、数据泄露等危险情况发生。

六、遵守平台规则、法律和法规

在5G、IPv6、人工智能AI、大数据、物联网(IoT)等高新技术的基础上，安全才是最重要的保障。

平台《服务协议》等规则和法律法规的每一条都具有重要性。

例如，中国《网络安全法》规定，网络平台/运营者应当留存网络日志至少六个月。

Ken的学习之旅深刻理解记录日志的重要性。在2023年5-6月，服务器就记录并拦截（抓到）了多起来自国外扫描Ken的学习规划师API接口、网站WordPress模块等非正常行为（见下方附件3）。但多次扫描均不成功，因此没有造成任何影响。

在此，我提出一句话“科技再发达，安全要严查”，拒绝滥用高新技术/科技，进行威胁安全的行为。

真实案例

在发现国外异常扫描行为后，Ken的学习之旅在提醒公告的最后还（用英语）对国外用户进行了“普法”，提醒他们中国的网络平台都会记录日志。

七、对大量扫描/漏洞试探说“不”

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。

这包括大量扫描登录页面和API接口，且API接口为一次性调用，无法使用验证码等手段，因此API接口更具有危险性。

因此，Ken的学习之旅系统已为新注册账号默认关闭API接口功能，需要时再手动开启，在登录页面安装防爬取机制，并记录每次登录和API调用情况。

防御攻击，要先从扫描阶段开始，拒绝大量扫描和漏洞试探。

八、文明上网，拒绝滥用，争做网络安全“志愿者”

同学们，网络不是法外之地。上网要做到文明，拒绝滥用行为，发现异常情况及时上报、举报。

Ken的学习之旅一直以来采用“管得严，处置松”的模式，不定期开展提醒和教育，指出并纠正错误，提高意识。拒绝“一刀切”：首次违规直接封账号、封IP地址等暴力处置手段。

部分网络平台为维护网络安全，会对扫描等滥用行为做出封账号、封IP地址、增加验证码等措施。不要因为威胁网络安全而影响到日常学习和生活哦！

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14日

中国广州

www.kenstudyjourney.cn, ken@kenstudyjourney.cn

附件1：网络平台中常见异常情况

1. 账号被异常登录、收到异常登录提醒
2. 在“设置”和“操作日志”中发现异常操作
3. 访问网站后，自动跳转到其它无关网站，或显示其它网站的内容
   （公共WiFi登录认证页面除外）
4. 未经你的许可/操作，非公开数据被无故修改
5. 在你的账号下可查看/修改其他用户的数据

附件2：网络平台中常见非正常使用（滥用）行为

注：这还违反了大部分网站上的《服务协议》文件。

1. 在网站登录页面中，大量扫描用户名和密码（即“暴力破解”）
   注：部分网站设有验证码等防爬机制
2. 大量扫描/试探网站API接口链接、密钥key等信息
3. 大量扫描/试探服务器隐藏端口（如逐一扫描端口1-65535；但TCP/80、TCP/443网站端口和ICMP Ping除外）
4. 扫描网站管理后台入口和WordPress等开源模块（如“/wp-admin”, “/wp-comments-post.php”, “admin.***.com”）
5. 短时间内发送大量、无意义的请求（即(D)DoS或CC攻击）

附件3：服务器中部分可疑页面爬取日志（全部来自Tor工具）

全部由GB-LHR-01（英国伦敦）服务器节点记录、上报：

IP地址	日期和时间 (GMT+8, CST)	访问/爬取URL链接	浏览器/设备类型
185.130.**.** (Tor)	2023-06-12 14:36:**	https:// www.kenstudyjourney.cn/ wp-comments-post.php	Chrome, Windows
104.244.**.** (Tor) 23.154.**.** (Tor)	2023-06-26 04:22:00开始 04:23:00结束	https:// www.kenstudyjourney.cn/ wp-admin/admin-ajax.php	Chrome, 安卓
192.42.**.** (Tor) 107.189.**.** (Tor)	2023-06-26 04:24:15开始 04:25:00结束	https:// www.kenstudyjourney.cn/ wp-content/plugins/**/ download.php	
199.195.**.** (Tor) 185.243.**.** (Tor)	2023-06-26 04:28:15开始 04:28:30结束	https:// www.kenstudyjourney.cn/ wp-content/themes/**/ view-pdf.php	
23.137.**.** (Tor) 91.203.**.** (Tor)	2023-06-26 04:28:00开始 04:33:00结束	https:// www.kenstudyjourney.cn/ wp-content/themes/**/ download.php	