

BIG DATA | 大数据时代 高校的数据安全

吉林省教育厅 信息办 张雁东



目录

CONTENTS

1

高校网络安全遇到的挑战

2

高校大数据网站安全分析

3

高校大数据的安全策略



01

高校网络安全遇到的挑战

随着信息技术日新月异的快速发展，大数据、云计算、移动互联网和物联网等新技术在高校领域得到大面的普及应用，高等教育行业面临的网络安全威胁和信息安全挑战也越来越严重，高校网络安全存在的许多隐患，已直接影响了教学、科研和管理的健康发展。高校大数据的快速“丰满”吸引着各路“贼人”磨刀霍霍！针对于网络信息安全问题，用大数据分析的角度去对待是一种有效的方式，也将成为必不可换的趋势。



那么针对现阶段都呈现出那些关键问题？

高校各类公共
系统数据的安
全隐患

公共系统的
数据遭到破
坏或泄密

包括图书馆借阅系统、一卡通系统、各类公共查询系统等

保密级别较
高的敏感数
据遭到破坏
或泄密

包括学生个人信息、教师个人信息、人事、财务、科研项目、学生成绩、招考报名系统等





校园网内网环境庞大、复杂、多变，对内网环境的监测做的是否细致到位？

监测设备是否能支撑起庞大的校园网络环境？

通过便携式移动设备或者人为的故意破坏操作、入侵，这些方式能否在第一时间有效的制止或检测到？

外网出口是否做好了充分的保障？

1

2

3

4

防火墙、负载均衡、防病毒扫描这些网络安全设备、硬件、软件对于高校网络起到至关重要的作用。



事件：【时间：2014】

人民大学书报资料中心事件

六四事件二十五周年纪念日来临之际，“反动黑客”攻入人民大学书报资料中心，在网站首页的显眼处挂上“反动”不过，该网站在次日（6月3日）已无法显示。事后反动黑客在其官网展示截图写道：2014年6月2日夜，攻克中共人民大学书报资料中心。



事件2：信息泄露

事件：【时间：2015.4】

美国Metropolitan State大学16万学生信息泄露

美国Metropolitan State大学16万学生个人信息泄露，包括出生日期、家庭住址、电话、个人成绩。

安华金和数据库安全专家点评：随着校园信息化的快速建设，教务、教学系统中存在大量漏洞，国内高校成为信息泄露的重灾区。这些漏洞有的已造成教职员工或学生个人信息泄露，包括大量**学生和教授的隐私信息**；另一方面很多重要院校还承担着**国家众多科研项目**，这都可能成为不法分子的目标。

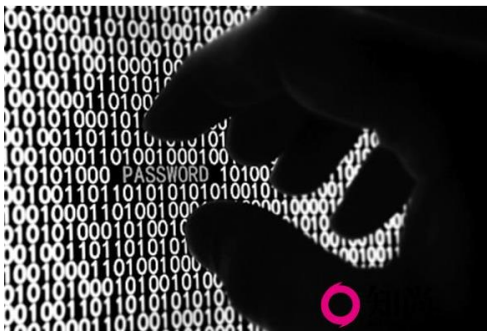
Metropolitan
State University



大都会州立大学

事件：【时间：2015.7】

高校考试成绩被篡改涉及学校十几所，83人改成绩



2015年7月，闫某对所在高校教务处信息管理系统进行扫描时，发现该系统存在漏洞，可以获取管理员列表。闫某随后编制了破译程序，并用管理员账号、密码登录该系统。此后，闫某先后扫描并入侵成都及西安等地10余所高校的教务信息管理系统并下载数据库

中介收钱联系黑客、高校学生编程轻易入侵十几所学校、83名考生成绩“被”合格



事件4：网站被挂马

事件：【时间：2016.9】

斯坦福、纽约大学、等76所大学的官网被挂赌博木马

Stanford The College Puzzle
A college success blog by Dr. Michael W. Kinst

Home » How To Build Your College Website Best Tools And Resources

» Things To Know If You Want To Study Abroad

Federal Data On Distance Education Is Not Accurate

How To Build Your College Website: Best Tools And Resources

December 3rd, 2014

By Jane Hurst

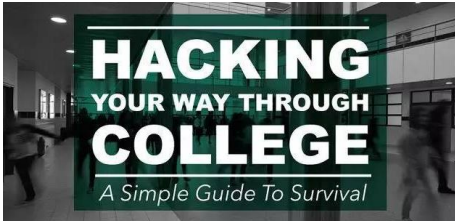
If you are a teacher or a student who wants to create their own website, you have several resources available to you. For starters, if you are already set up on Google, you can use Google Sites to create your website. Or you can choose from one of the following website building tools.

- **Weebly** – This is an easy website building tool to use, and one of the best things about it is that it is absolutely free to use. It offers plenty of features, so you can create interesting websites that are going to get noticed.
- **Weebly for Education** – Another option is to use Weebly for Education. This website builder has all of the same features as Weebly, as well as features that are made just for those involved in education. It offers the bulk creation of accounts for students, and teachers can manage and moderate these accounts. Students can easily build their own websites and blogs, and you can control the content because you have created the accounts in the first place. Check here to learn more about Weebly for Education.
- **Jimdo** – When you use this tool, you will have a great selection of templates, layouts, backgrounds, and editing options. You can change the template at any time if you want something new, and you can even customize the templates so your website is completely unique to you. Create a blog, and even enjoy email management with Jimdo.
- **School Rack** – This is a free service that teachers can use to create their own websites for their classrooms. This is different than most website builders, because it is not directed towards the masses, but just for teachers and their students. You can use your website to post assignments using an integrated feature so you don't have to create a separate assignment page. Students and parents can also have free accounts, so they can contact the teachers when they need to.
- **Webs** – This is a popular website builder that is free to use, and you can include video and audio content. It also allows you to create calendars and polls, and there are loads of other third-party widgets. You can choose from a huge selection of templates, and page layouts, so you can create a website that is truly unique to you. This is a basic builder, so if you are looking for something that is a lot more advanced, this may not be the tool for you.
- **Web Node** – If you are looking for a website builder that is super-easy to use, look no further than Web Node. In fact, this is a great tool for freelance website builders. You can drag and drop, and change the look of your website at any time. This is a great tool for students, as they can create and share their assignments. One of the biggest benefits is that there is no annoying advertising placed on your website.
- **Snap Pages** – You have the option to use the free service, or pay for the premium service to create your website. There are loads of features on the free service to get you started, and you can set up and maintain a class website. Some of the features include editing and customizing tools, as well as an image resizing tool.
- **Yola** – Here is another free website builder that you can use as much as you like, and add as much content as you wish without having to pay for any extra services. If you are planning on posting a lot of content with audio and video, this is a great website builder to use. You will want to keep this one in mind for future use for both your school and your website.



斯坦福、纽约大学、卡耐基梅隆在内的76所大学的官网基础页面,被植入木马链接导向赌博网站,链接分布在它们官网发布的课程介绍、新闻稿,等多个板块

SEO专家分析指出：大学和政府网站都会被谷歌标记为高信任度信息来源，由此链接到的网站同样也会被视为可信网站，加上每天都有大量的现金流在这些赌博网站滚动，单次光点击就可以产生高达80美元的效益。





02

高校大数据 网站·安全分析

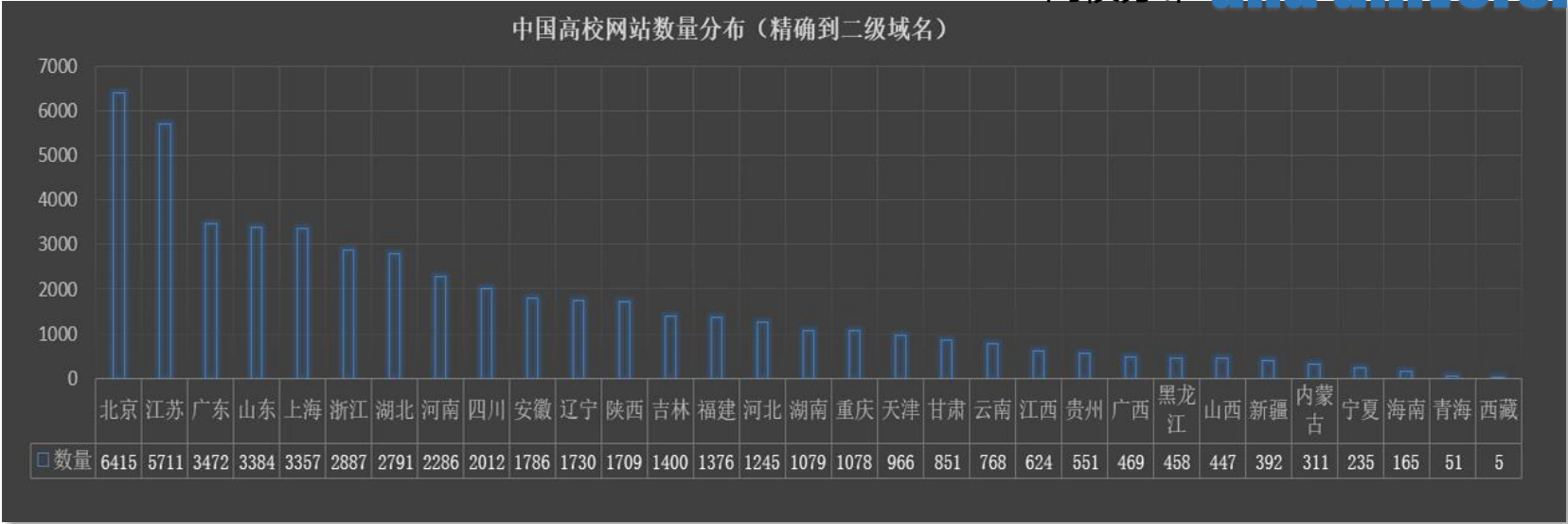
高校网站安全普遍存在“网站建设和管理不统一、网站日常维护缺失、对于网站安全不重视、网站信息保护意识差、软件系统漏洞、服务器漏洞”六大安全隐患。那么通过大数据我们如何解读国内校园安全？



全国高校分布分析

Distribution of colleges and universities

高校分布



目前已收录国内高校网站总计约5万多个（以二级域名计算，统计数据包括院系主页，统计地域不含港澳台），其中，网站数量排名前五位的地区为：北京（6415）、江苏（5711）、广东（3472）、山东（3384）、上海（3357）。高校网站最少的五个地区为：内蒙古（311）、宁夏（235）、海南（165）、青海（51）、西藏（5）。



高校网站安全分析

网站安全 **WEB** **Site Security**

以360网站安全检测平台为检测引擎，高校网站安全平均得分由2012年的37分增长到了58分，平均分仍然不及格。同时，高校网站平均每五个漏洞就有一个高危漏洞，这就意味着中国高校网站依然存在着大量高危漏洞。

各地区高校网站安全平均得分排名（不含港澳台）

- 北京 安徽 西藏 天津 湖北 福建 重庆 广东 江苏 新疆
- 上海 浙江 甘肃 山西 湖南 宁夏 黑龙江 河北 四川 内蒙
- 青海 辽宁 陕西 广西 河南 贵州 山东 云南 吉林 海南

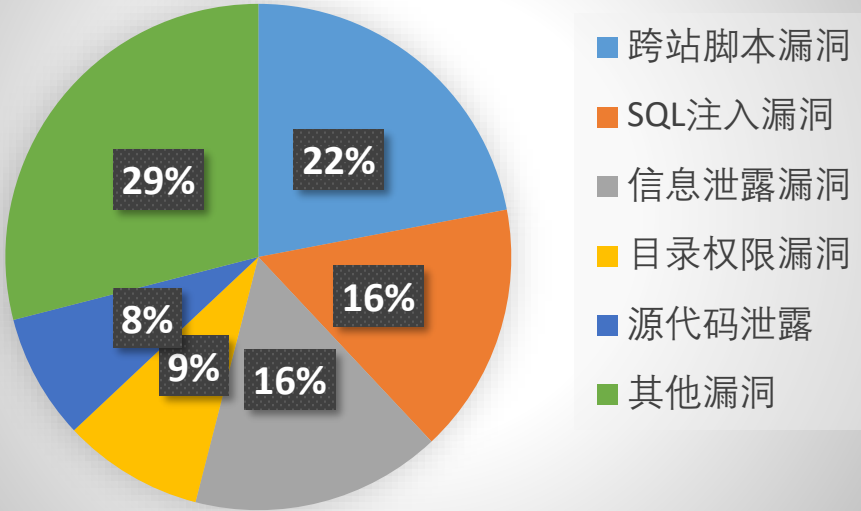




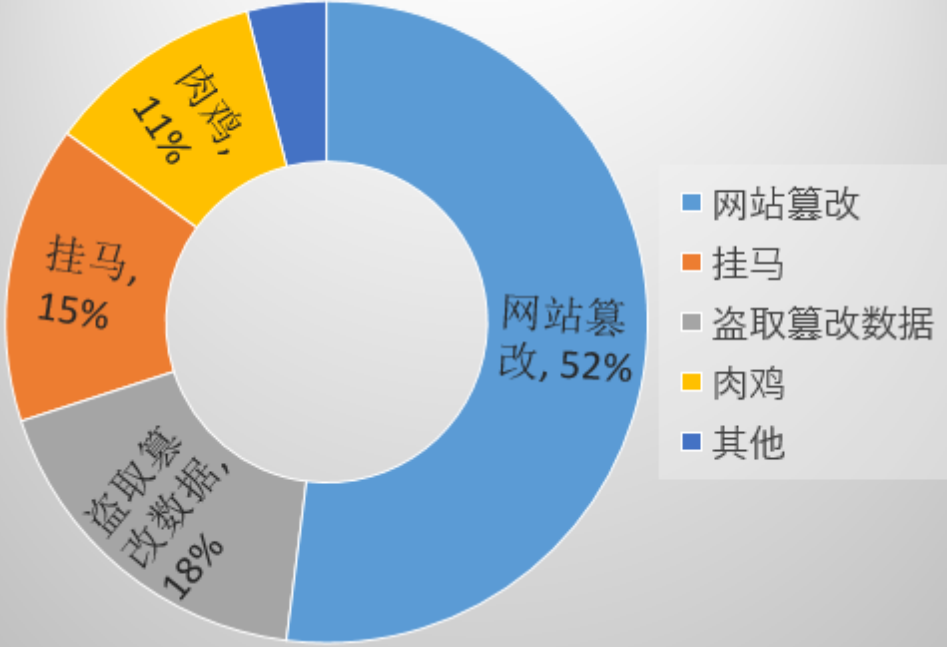
高校漏洞分析与入侵分布情况

漏洞与入侵 Vulnerability analysis and intrusion

中国高校网站安全漏洞分布情况



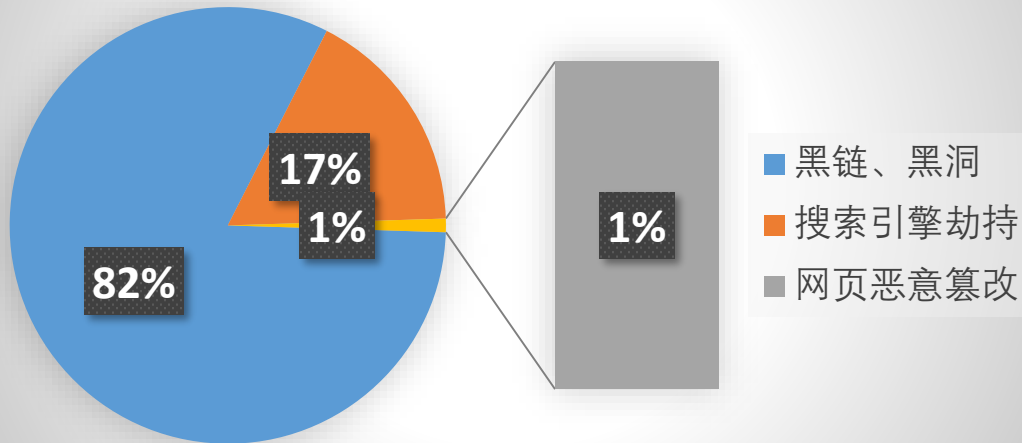
高校网站被侵害类型分布情况



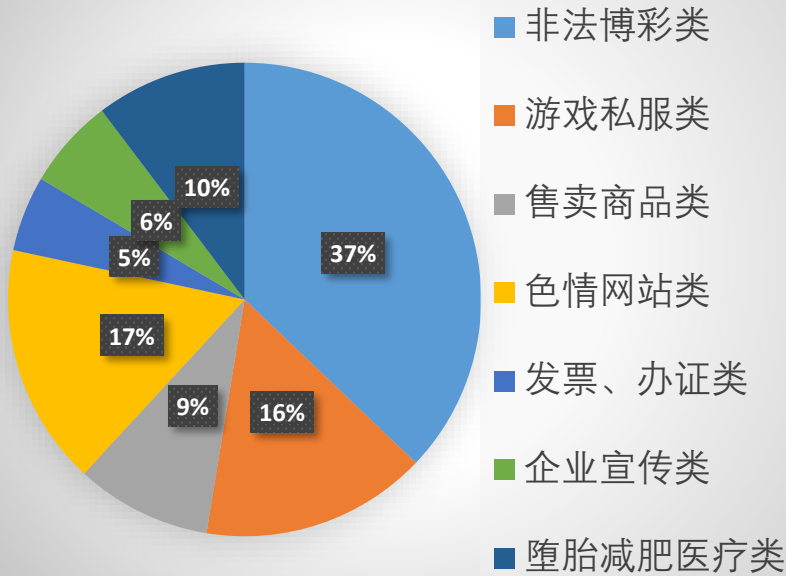


非法篡改与黑链分析

高校网站被篡改类型分布情况



高校网站被篡改内容分布情况



黑色利益链 **Black
interest chain**



03

高校大数据·安全策略

- 1、分析漏洞成果与漏洞原因
- 2、大数据IP定向分析
- 3、校园网络治理与稽查机制
- 4、技术联盟·让数据改变未来

A

网站漏洞

定期针对网站漏洞进行检测扫描，对漏洞环节进行分析，并对漏洞进行弥补



B

硬件漏洞

针对校园硬件设备进行定期巡检与网络日志分析，对硬件环节进行定期替换与更新，确保硬件设施安全性

C

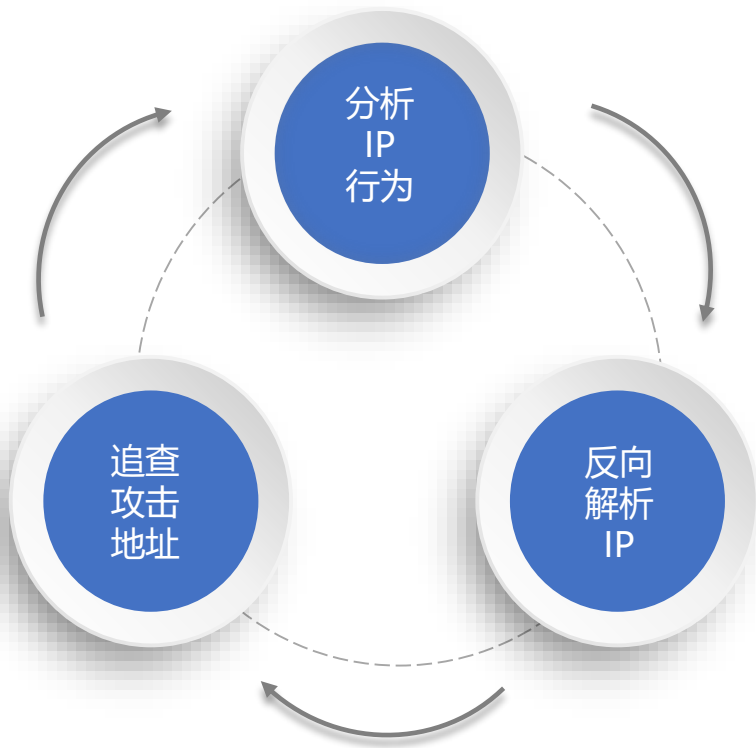
攻击漏洞

针对对于校园网络以及校园网站类扫描或攻击的地址以及时间进行分析，判断常规扫描手段，对扫描的环节进行技术管控





大数据定向IP逆向分析



Analysis

定向IP逆向分析

Directional IP reverse analysis

1. 分析攻击IP的行为与时间段，针对攻击的IP行为方式作为深度解析
2. 通过分析结果进行反向解析，针对攻击地址池进行解读，确保非常规扫描
3. 追查攻击源头，针对攻击IP进行统一上报，分享于其他校园



大数据安全治理

校园网络治理与稽查机制

Internet

对于非常规类型网站建立网站池，对于一些非法或与知识无关网站进行屏蔽，有效降低网络风险

Safety

及时更新校园软、硬件设施
确保防御安全有效

01

行为治理

Behavior

通过第三方监控类软件，针对校园上网习惯进行分析，定期针对行为上网进行学习培训

网络治理

02

Safety

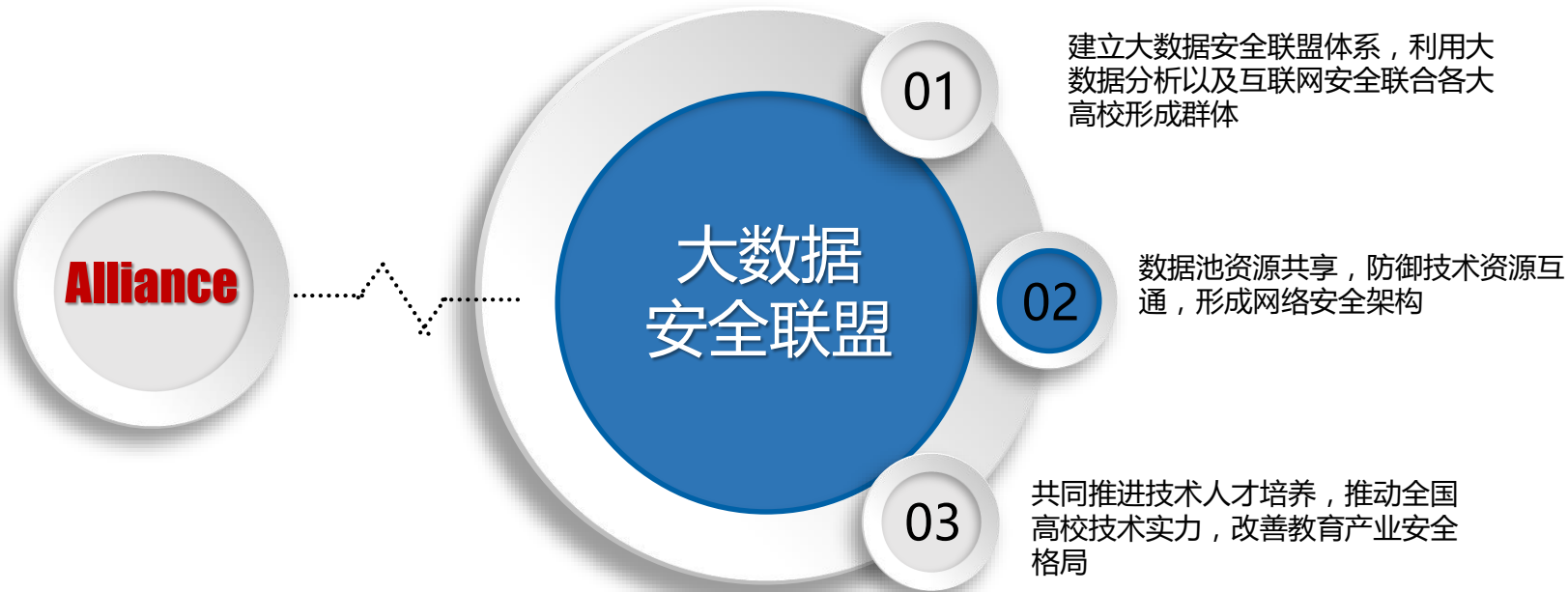
通过舆论信息过滤违规词语，对新型舆论或关键字进行管理屏蔽

03

信息治理

04

安全治理





THANKS

谢 谢 聆 听