面向攻防实战的高校网络安全建设思考

上海交通大学

姜开达

2022年6月26日

目录

《网络安全法》明确演练要求

第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

第五十三条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

《教育系统网络安全事件应急预案》具体要求

教 育 部 文 件

教技〔2018〕8号

教育部关于印发《教育系统网络安全事件应急预案》的通知

各省、自治区、直辖市教育厅（教委），新疆生产建设兵团教育局，部属各高等学校，部内各司局、各直属单位，中国教育和科研计算机网网络中心：

根据《中华人民共和国网络安全法》《国家网络安全事件应急预案》的要求，为健全完善教育系统网络安全事件应急工作机制，提高教育系统网络安全应急处置能力，我部制定了《教育系统网络安全事件应急预案》。现印发给你们，请认真贯彻落实。

教 育 部

2018 年 6 月 11 日

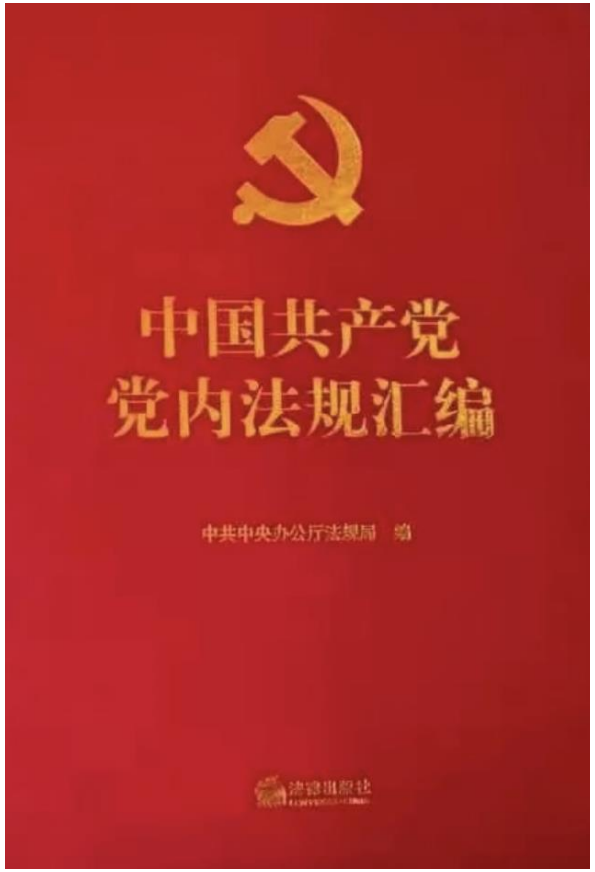
6.3 应急演练

部网络安全应急办每年组织针对特别重大网络安全事件的跨地区、跨层级的应急演练，检验和完善预案，提高实战能力。各单位每年至少组织一次应急演练，每年年底前将本年度演练情况报部网络安全应急办。

7.7 责任与奖惩

各级教育行政部门可对网络安全事件应急管理工作中作出突出贡献的先进集体和个人给予表彰和奖励；对不按照规定制定预案和组织开展演练，迟报、谎报、瞒报和漏报网络安全事件重要情况或者在应急管理工作中有其他失职、渎职行为的，依照相关规定对有关责任人给予处分；构成犯罪的，依法追究刑事责任。

《党委（党组）网络安全工作责任制》贯彻落实

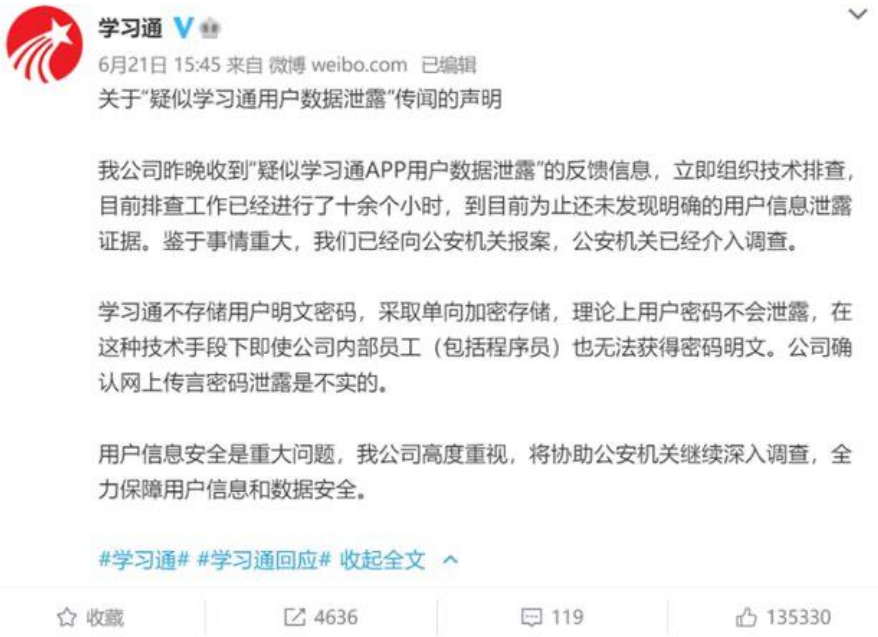


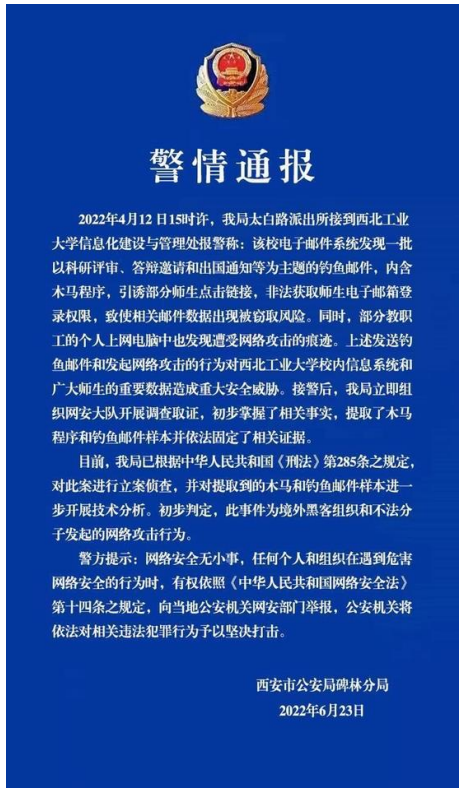
第二条　网络安全工作事关国家安全政权安全和经济社会发展。按照谁主管谁负责、属地管理的原则，各级党委（党组）对本地区本部门网络安全工作负主体责任，领导班子主要负责人是第一责任人，主管网络安全的领导班子成员是直接责任人。

第八条　各级党委（党组）违反或者未能正确履行本办法所列职责，按照有关规定追究其相关责任。

第十条　各级党委（党组）应当建立网络安全责任制检查考核制度，完善健全考核机制。

近期国内外网络安全热点





俄乌战争 网络战　　互联网个人信息保护　　西北工业大学钓鱼邮件

网络安全的本质是对抗，对抗的本质是攻防两端的能力较量。

要提高攻防对抗水平，关键在于看得见、防得住、打得赢。

战怎么打，兵就怎么练

- ✓ 攻防演习，红蓝对抗
  - 不限制攻击路径和攻击方式 的 大型渗透测试行动；
  - 持续1～3周时间，有专业安全人员和安全团队参与；
  - 完全真实环境下的攻防演练，获取一组目标系统权限和数据；
  - 攻击方提前打点，挖掘0Day漏洞，组合利用多种攻击方式绕过防线；
  - 防御方提前整改网络，加固系统，缩小攻击面，但一点突破，全盘皆输。
- ✓ 积极防御，以攻促防
  - 全面排查网络安全风险隐患，360度全身体检；
  - 实际检验各地各校的网络安全防御能力和应急响应机制；
  - 为进一步安全建设明确方向，推动安全防御水平持续提升。

演习中暴露出来的典型问题之一

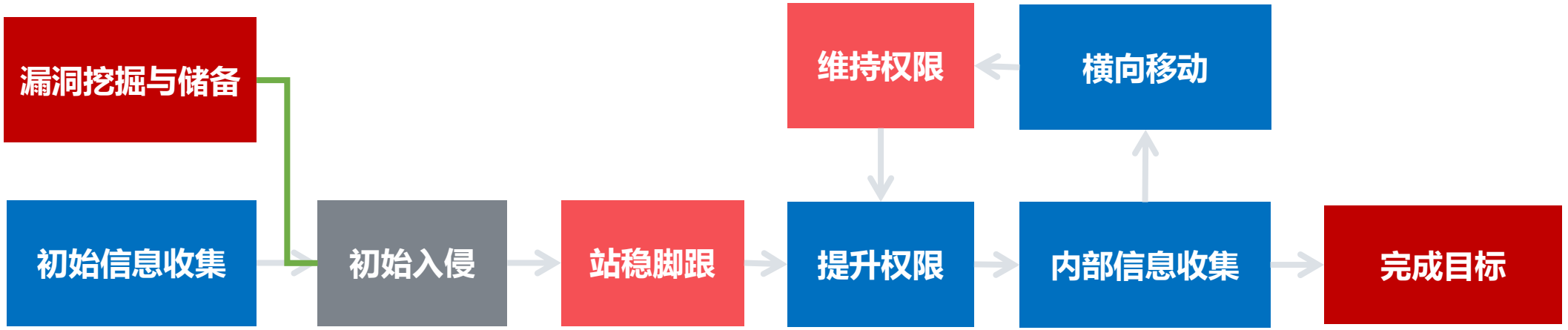
- 管理员弱口令（多年来长期普遍存在）
- 任意文件上传漏洞（可上传后门木马）
- 逻辑漏洞，普通用户可越权访问其他敏感数据
- 未授权访问接口，可匿名直接访问并进一步利用
- SQL注入漏洞，可导致数据库泄漏及进一步利用
- 互联网已公开的历史遗留漏洞，可远程直接利用

演习中暴露出来的典型问题之二

- 高校VPN服务器存在师生弱口令，可利用进入内网
- 统一身份认证帐号存在弱口令或者社工猜解获得密码
- Weblogic、Fastjson、Java反序列化命令执行漏洞等
- 数据中心云管理平台、运维系统存在漏洞，通用口令
- 系统运维配置不当，导致代码文件泄漏，进一步审计出漏洞
- 系统存在厂商默认管理口令或0/N Day漏洞，可远程直接登录

攻击流程与核心要素剖析

攻击流程



核心要素

- ✓ **信息** 是实战攻防的第一生产力，贯穿攻击的整个生命周期，优秀的情报能力可以令准备和攻击事半功倍；
- ✓ **漏洞** 是撕开防线、扩大战果的重要武器，需要依靠信息进行精确制导；
- ✓ **工具** 是潜伏敌线、刺探情报的加速器：主要包括远控，搜集、密码窃取等前后渗透工具。

上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

目录

安全密码

- ✓ 设置一个强壮的密码
  - 长度不低于8位，至少包含大写字母、小写字母、数字、特殊字符中的2类
  - 避免出现易猜解字符：姓名拼音or首字母、生日、手机号、学工号、身份证后六位
  - 不能与用户名相同：用户名后添加123、888、123456（简单数字）或2022（年份）
- ✓ 密码不要和他人分享
- ✓ 不重复使用单一密码
  - 不同网站使用不同密码，避免一处泄露、全网皆失
- ✓ 强密码仍需定期修改
- ✓ 避免用明文存储密码
  - 避免明文存储在邮箱、网盘或本地电脑
  - 加密记录密码的文件，可考虑密码管理软件，如KeePass
- ✓ 可以考虑免密码登录
  - 扫码登录、短信验证码、OTP动态口令登录

校园统一身份认证及VPN

现状

✓弱口令极为普遍，攻击者获得师生帐号成为必然

✓VPN拨入校园内网，绕过边界安全防护，长驱直入

解决

✓提前排查弱口令，帐号使用风控

✓VPN访问，按需最小化控制范围

✓WebVPN 增强安全管控，及时发现阻断

钓鱼邮件

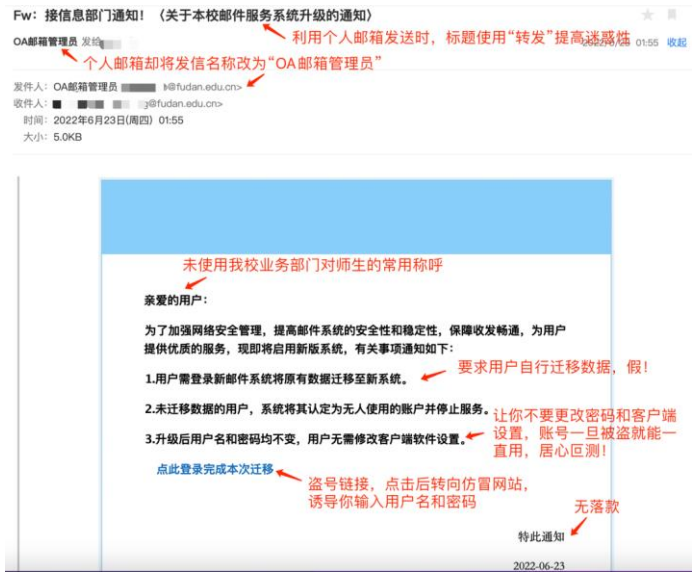
各种攻击入侵和攻防演练中的大杀器

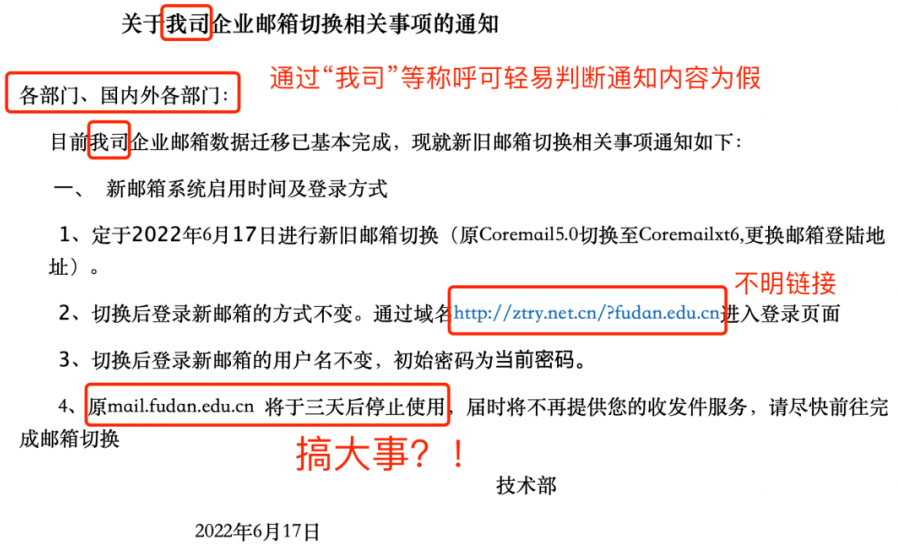
定向投递，精心定制，多轮钓鱼，绕过终端防护

对策：

一轮轮钓鱼演练，安全意识教育

用事实来反复教育师生，狼真的来了





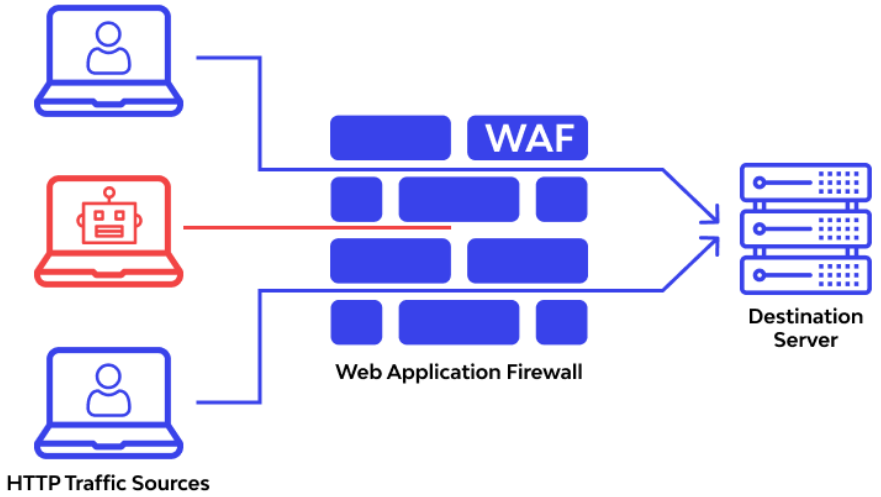
WAF（Web应用防火墙）的绕过

绕过技巧ABC

a.xxx

b.xxxx

c.xxxxx



对策

✓相信但不要迷信

✓关注被攻击点，防护规则动态调整

✓找到可能被利用点，从源头去解决

RASP 的使用

Runtime Application Self-Protection

应用程序运行时自我防护，相对WAF更深入应用层，各有所长

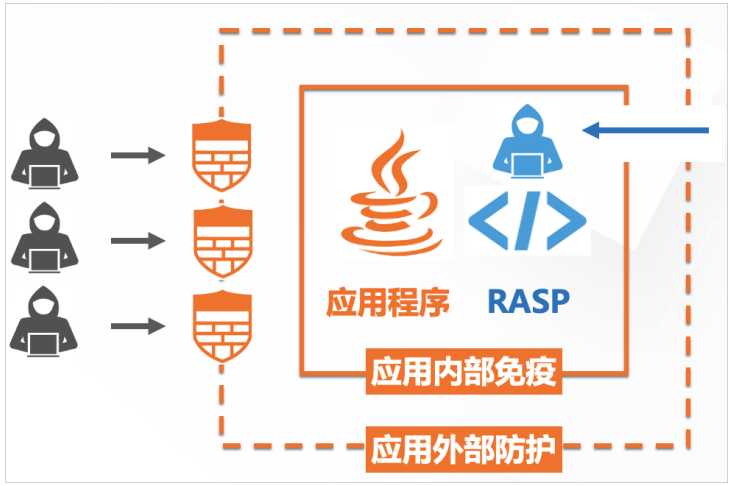
不依赖于请求特征静态规则，主动防御，可对抗未知漏洞利用

效果：

攻击方看到直摇头，NoNoNo

防守方值得来仔细考虑一下，Java/PHP

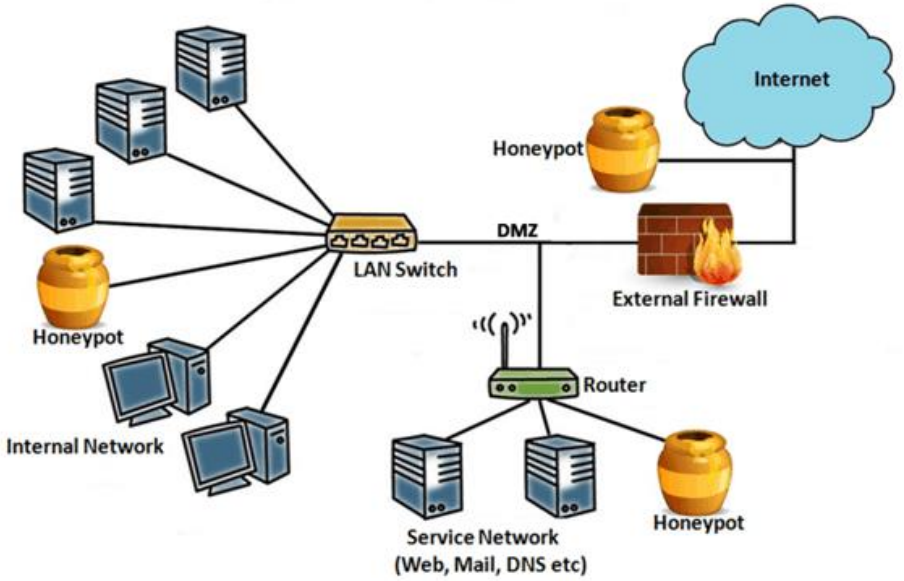
OpenRASP，https://rasp.baidu.com



蜜罐（HoneyPot） 的使用

开放端口和服务，设置诱饵引诱黑客前来攻击
持续分析监测结果，了解最新的攻击动态
精心构造环境，引诱攻击者运行程序或提供虚假情报

效果：
极早期捕获内网的攻击
消耗攻击方时间和精力
追踪攻击方来源，绘制画像成为可能



虚拟化平台的安全管理

vCenter任意文件上传漏洞（CVE-2021-22005）

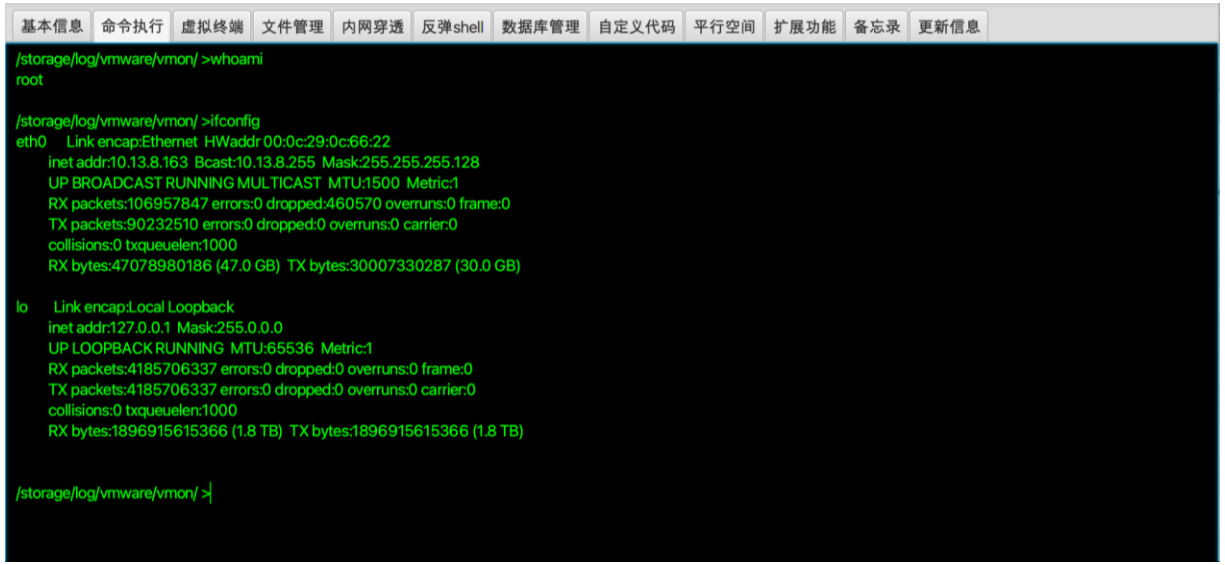
从/storage/db/vmware-vmdir/data.mdb数据库文件中提取cookie

[*] Attempting to log into vCenter with the signed SAML request

[+] Successfuly obtained Administrator cookie for 10.x.x.x!

[+] Cookie: VSPHERE-UI-JSESSIONID=2761xxxxxxxxxxxxxxxxxxxxxx

浏览器替换Cookie获取到vCenter Web权限



不是个别孤立出现

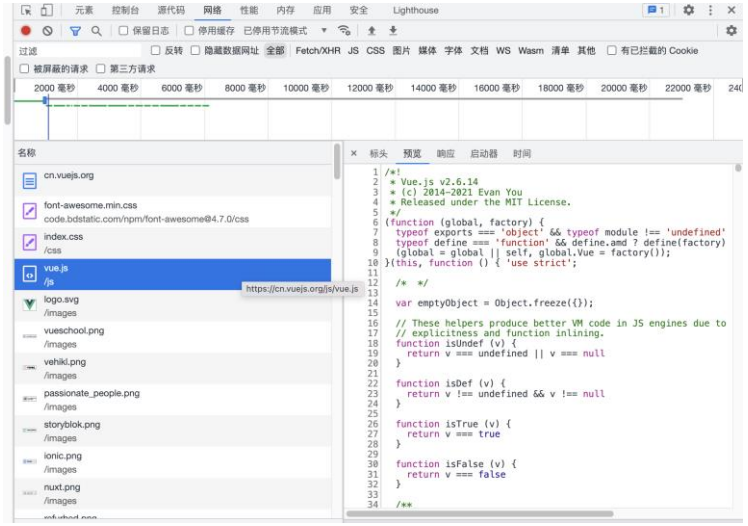
普遍发生于多所高校

数据中心信息系统大面积沦陷

网站前后端分离带来的安全风险

前端：负责交互与展示部分

后端：负责提供数据和处理业务



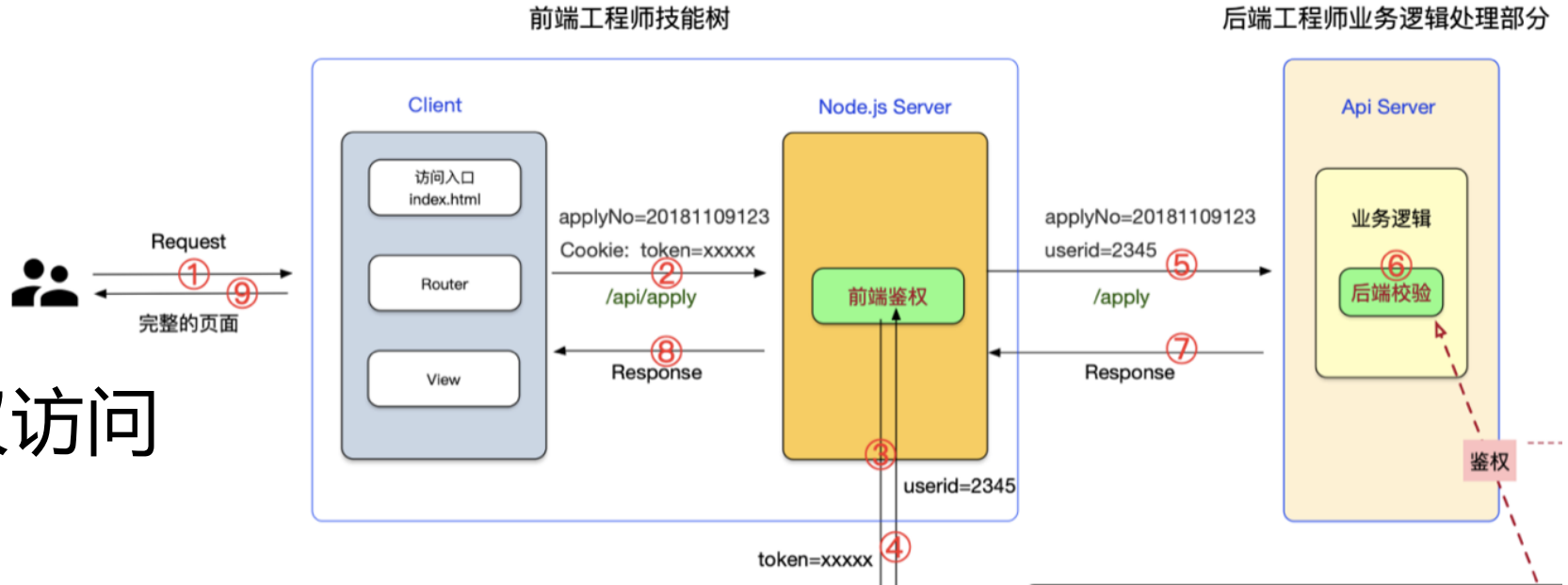
优点：并行开发，调试维护方便

潜在缺点：

暴露全部API接口

暴露全部业务逻辑

后端鉴权失误，越权访问



GitLab / SVN / JIRA 泄漏带来的安全风险

低版本远程代码执行漏洞，直接拿下

社工猜用户名，猜密码，和用户名一样?

泄漏项目源代码，审计挖掘0Day漏洞

泄漏项目文档，明文存储各系统入口和密码

教育软件开发商如果代码库泄漏，对全教育行业威胁巨大

教育通用业务软件的安全风险

统一办事大厅、图书馆系统、教务管理系统等各类通用系统...
版本碎片化，各地不统一，开发商重视程度不够

涉及常见厂商（包括但不限于）：

上海复翼、江苏金智、南京苏迪、江苏汇文、成都思必得、北京易普拉格、西安博达、天津神州浩天、上海树维、浙江正方、北京超星、北京玛格泰克、湖南强智、北京通元、上海泛微、新开普、南京先极、上海万欣、同方知网、北京致远、广东盈世.....

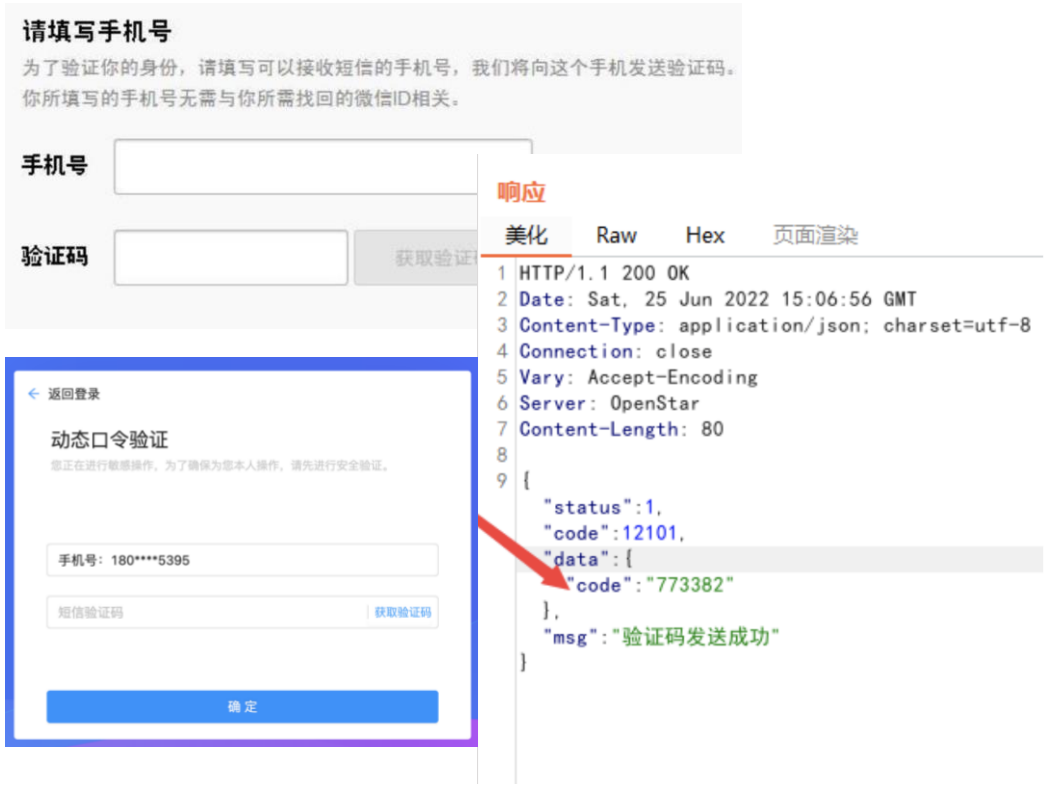
新技术、新应用使用不当带来的安全风险

人脸识别 绕过

活体检测 绕过

手机验证码 绕过

SIM卡验证 绕过

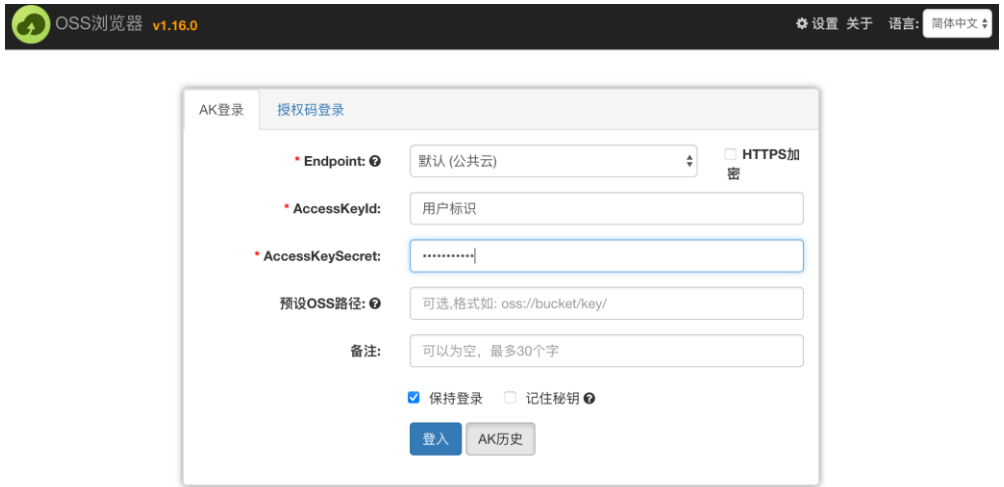


对象存储 OSS 广泛使用带来的安全风险

海量、安全、低成本、高可靠的云存储服务
适合存放任意类型的文件，可弹性扩展

不当使用:

✓密钥AccessKeySecret写入JS代码或源代码，泄漏
✓存储桶Bucket允许公开浏览，泄漏
✓开源 MiniO 低版本漏洞，泄漏



微信公众号、小程序和移动应用的安全风险

传统的Web安全风险继续存在
利用点可能更加隐蔽，但是只要挖，总是会有

- ✓SQL注入漏洞
- ✓各种越权访问
- ✓管理员弱口令
- ✓登录的各种绕过
- ✓APK逆向分析挖掘漏洞

“挖矿”活动综合治理

事前：终端安全防护，域名/IP Blacklist 提前封禁，阻断矿池通讯

事中：持续开展DNS/流量监测，日志分析，极早期发现，通报处置

事后：安全教育，举一反三，长期持续处置，动态清零

数据安全和个人信息保护

当前位置：首页 -> 重要新闻

致歉声明

日期：2020-06-10 编辑：

近日，我校在返校复学准备工作中发生了部分学生个人信息泄露事件，由此给学生和家长带来的不便，我们表示深深的歉意，向社会各界人士、广大网友、媒体的关心和批评表示诚恳的感谢。

我校在积极准备学生返校复学时，按照疫情[illegible]科研处整理了计划返校学生名单，用以核查学生返校来源地及个[illegible]作人员缺乏保密意识，造成部分学生的个人信息泄露，学校[illegible]

事件发生以来，我校在公安机[illegible]帮助下查清了事情原委，及时成立三个工作专班，明确分工，专项排查，第一时间通知师生保护信息安全，不得随意转发，有效地控制了信息的进一步扩散。同时，我校对直接责任人予以解除劳动合同，对相关部门负责人及两名主管校领导予以记过处分，并将配合公安机关对其他涉嫌违法的行为严肃追究。

安全意识淡薄

近两万学生信息遭到泄露，包括姓名、身份证号等20余项信息，泄露文件在微信、QQ等社交平台上广泛流传。事件发生后，多名学生反映接到了骚扰电话和营销电话。

浙江公安机关抓获在暗网兜售浙江中小学生学籍信息黑客
2018年 9月12日

据新华社北京9月7日消息 日前，公安部公布10起打击整治网络违法犯[illegible]“净网2018”专项行动典型案例。

浙[illegible]在暗网兜售浙江中小学生学[illegible]客。今年8月，警方发现，有不法分子在暗网发布帖子出售浙江中小学生学籍信息。浙江公安机关成立专班开展侦查后，于8月10日成功抓获非法侵入浙江省学籍管理系统的王某等3名犯罪嫌疑人。

防护能力不足

主动公示，过度公开

数据使用的原则和管理体制机制

- ✓ 数据收集遵循 最小够用 原则
- ✓ 数据查看遵循 最小授权 原则
- ✓ 数据存储遵循 最短周期 原则
- ✓ 数据共享遵循 用而不存 原则

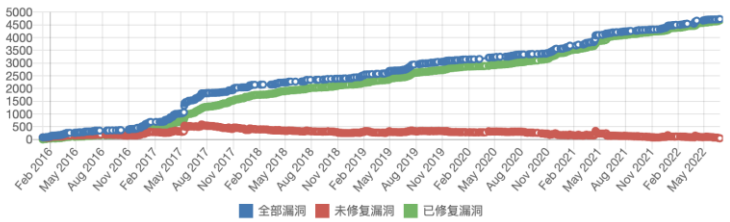
- 明确学校数据生产、管理、责任、使用主体部门
- 制定各类管理办法，系统开发（接口）规范
- 规范数据采集、数据共享标准，要求数据依规使用
- 推进数据应用，提高数据质量，**维护数据安全，**全生命周期管理

安全压力层层传递，二级单位常态化通报

漏洞

总数	未修复	已修复	自动追踪
4727	45	4682	4441

趋势



Vul Tracker 概况 机构 漏洞 地址 网站 HTTPS/IPv6 监测 关于

机构	注入	上传	入侵	口令	执行	授权	泄露	风险	修复	总数
电子信息与电气工程学院	89	28	19	3 265	1 164	3 133	74	7	808	815
农业与生物学院	16	3	3	1 10	4 12		12	5	58	63
生物医学工程学院	2 7			27	2 5	7	1 6	5	52	57
生命科学技术学院	48	10	8	1 27	2 30	14	32	3	172	175
学生工作指导委员会	4	4	4	2 24	1 53	4	32	3	130	133
终身教育学院	21	2	2	54	2 42	32	13	2	170	172
物理与天文学院	15	4	2	2 22	6	8	4	2	62	64
后勤保障中心	10			14	1 16	5	1 3	2	51	53
国际合作与交流处	1 7		1	5	1	3	1	2	19	21
海洋学院				8	1	1		2	8	10

上海交通大学校内公文

xxx〔2022〕15 号　　签发人：xx

上海交通大学关于校园网站 2022 年 5 月内容建设与安全管理情况的通报

各院（系）、部、处、直属单位：

为进一步加强校园网络阵地建设，根据学校网信领导小组和网宣领导小组的安排部署，依据《中共上海交通大学委员会关于网络意识形态工作责任制的实施细则》（沪交委宣〔2021〕78 号）和《上海交通大学校园网站建设与安全管理办法》（沪交委宣〔2018〕187 号），对全校院（系）、部、处、直属单位所属官方网站的内容建设与安全管理情况进行了月度检查。现将有关情况通报如下。

一、总体情况

技术
+
管理

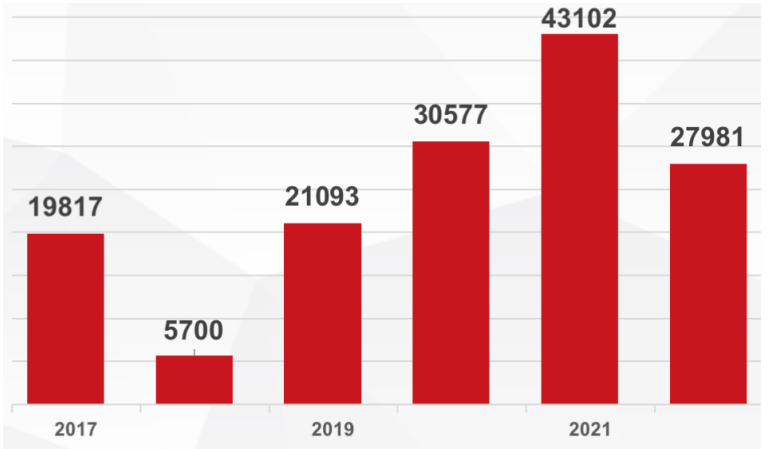
附件三

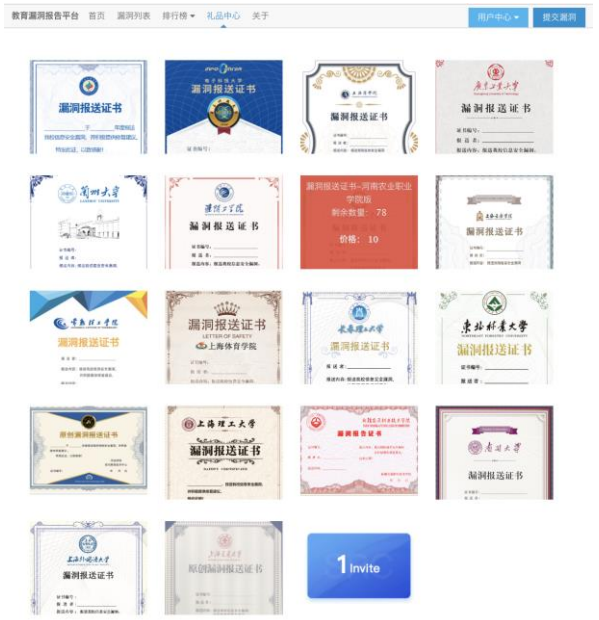
2022 年 5 月全校网站安全与漏洞管理情况

序号	单　位	5 月新增漏洞		尚余未修复漏洞
		新漏洞数	已修复	
1	电子信息与电气工程学院	10	10	10
2	生物医学工程学院	0	0	8
3	学指委	1	1	7
4	农业与生物学院	2	0	6
5	机械与动力工程学院	3	3	4
6	生命科学技术学院	0	0	4
7	上海交通大学出版社	0	0	4
8	物理与天文学院	0	0	3
9	校园管理办公室	0	0	3
10	海洋学院	0	0	2
11	国有资产监督管理委员会办公室	0	0	2
12	后勤保障中心	0	0	2
13	国际合作与交流处	0	0	2
14	终身教育学院	0	0	2
15	李政道研究所	1	0	1
16	航空航天学院	1	0	1
17	药学院	0	0	1
18	化学化工学院	0	0	1
19	档案文博管理中心	0	0	1
20	教务处	0	0	1
21	系统生物医学研究院	0	0	1
22	个性化医学研究院	0	0	1
23	凯原法学院	0	0	1
24	智慧能源创新学院	6	6	0
25	船舶海洋与建筑工程学院	3	3	0
26	规划发展处	1	1	0
27	资产管理与实验室处	1	1	0
28	上海交大-南加州大学文化创意产业学院	1	1	0
29	环境科学与工程学院	1	1	0
30	巴黎高科卓越工程师学院	1	1	0

教育漏洞报告平台(https://src.sjtu.edu.cn)为补充

#	单位	漏洞总数	漏洞威胁值
1	上海交通大学	2434	7311
2	同济大学	1033	2346
3	四川省教育厅	1017	2133
4	江苏省教育厅	1023	2044
5	清华大学	749	1881
6	安徽省教育厅	810	1831
7	浙江省教育厅	783	1813
8	电子科技大学	645	1724
9	浙江大学	710	1680
10	山东省教育厅	676	1608
11	兰州大学	685	1544





你看见或者不看见，漏洞就在那里，不会因为你不关注而消亡

早期发现的越多，后期留存的越少，培养正确的安全漏洞观

漏洞就像海绵里的水，只要挤，总是有的，常态化发现机制

发现，解决，再发现，再解决，举一反三，最终目标是一定程度的动态清零

上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

目 录

安全运营体系建设

安全管理 + 安全技术 + 安全运营

资产安全运营：构建全局视角的多维度资产关联，实现资产动态管理

数据安全运营：以数据保护为核心，实现数据全生命周期动态管理

智能安全运营：监测–响应–预测–防御，自动化闭环智能动态运转

重点保护时期的关注点

- ✓ 管理机制到位、人员团队到位、落实上级要求要到位
- ✓ 清理双非网站、僵尸网站、测试网站，安全隐患动态清零
- ✓ 保障信息系统（网站）的安全运行，访问流畅和业务连续
- ✓ 重点保护数据安全，特别是个人信息安全
- ✓ 多重演练，有应急预案；第一时间发现，第一时间处置
- ✓ 综合评估安全风险，结合业务必要性，分类分级调整互联网访问策略

保**通**不是保**断**

攻防对抗中曲折前行

- ✓ 未知攻焉知防，重金马其诺防线不可取
- ✓ 建立纵深防御体系，守好最后一道防线
- ✓ 人是安全中最薄弱的环节，要意识教育
- ✓ 有限的安全投入，获得匹配的安全能力
- ✓ 平衡管理、技术、运营，一个也不能少

安全实战化
安全专业化
安全常态化

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

谢 谢!