厦门大学 信息与网络中心 郑海山
2017/12/01 浙江绍兴

重大活动期间的高校积极信安实践

CONTENTS

目录

THE FIRST PART

相关介绍
ABOUT

THE FIRST PART

相关介绍
ABOUT


网络安全：挑战·策略·应急

厦门大学

重大活动时期网站安全防护手册

静态化处理和安全性检查

静态网站的防护

运维安全的其他注意事项

1

许卓斌11月初在安全工作组会议分享的《重点服务保障期间的安全实践》
http://sec2017.eventdove.com/

2

静态网页安全防护可看《中国教育网络》2017年11月P55页。电子版暂缺。
DNS 安全：
https://dog.xmu.edu.cn/images/paper/dns-query-log-analysis-system-based-on-open-source-software.pdf

3

《DevOps在重大活动网站安全保障中的应用》，具体技术实现
https://dog.xmu.edu.cn/images/slide/devops-security-filtered.pptx

网站传输路径
TRANSFER PATH

上海交通大学姜开达：网络安全的特点是攻防高度不对称，黑客可以一点突破引发目标全线奔溃。作为防护的一方，全局体系任何一处都不能存在短板。

恐怖分子：失败了不要紧，我们只要一次成功，而你们必须每次都成功。

STEP ONE

STEP TWO

STEP THREE

STEP FOUR

用户端浏览器 -> hosts文件 -> DNS -> 浏览器缓存 -> Safe Browsing -> 证书检查 ->网关/无线/路由器 -> 代理 -> CDN -> 防火墙 -> IPS/IDS -> WAF -> 负载均衡 -> 虚拟化宿主机 -> 虚拟机 -> 操作系统 -> HTTP服务器 -> HTTP服务器 WAF -> URL重写 -> 文件载入 -> 脚本解析 -> URL路由分发 -> Cache -> 数据库 -> 渲染结果 -> 压缩 -> HTTPS加密 -> 返回 -> 网络层分包 -> 重组包 -> 浏览器接收 -> 浏览器插件 -> JS渲染 -> 字符集 -> 页面载入完成

纵深防御

通过设置多层重叠的安全防护系统而构成多道防线，使得即使某一防线失效也能被其他防线弥补或纠正，即通过增加系统的防御屏障或将各层之间的漏洞错开的方式防范差错发生的。
https://baike.baidu.com/item/纵深防御

纵深防御只适用于保护核心资产、数据，对于贴标语式的防御无效。整体安全级别由木桶原理最短的那块木板决定。

奥卡姆剃刀原则：若无必要，勿增实体。引入安全设备可能引入安全风险。
KISS（Keep It Simple, Stupid）

相关介绍
工作目标

1

THE FIRST PART

重大活动期间不出网络安全事件，尤其需要确保对外有影响力的网站不被非法篡改

2

THE SECOND PART

重大活动期间维持学校正常运转，维持核心业务系统与主要对外信息发布平台继续运作

3

THE THIRD PART

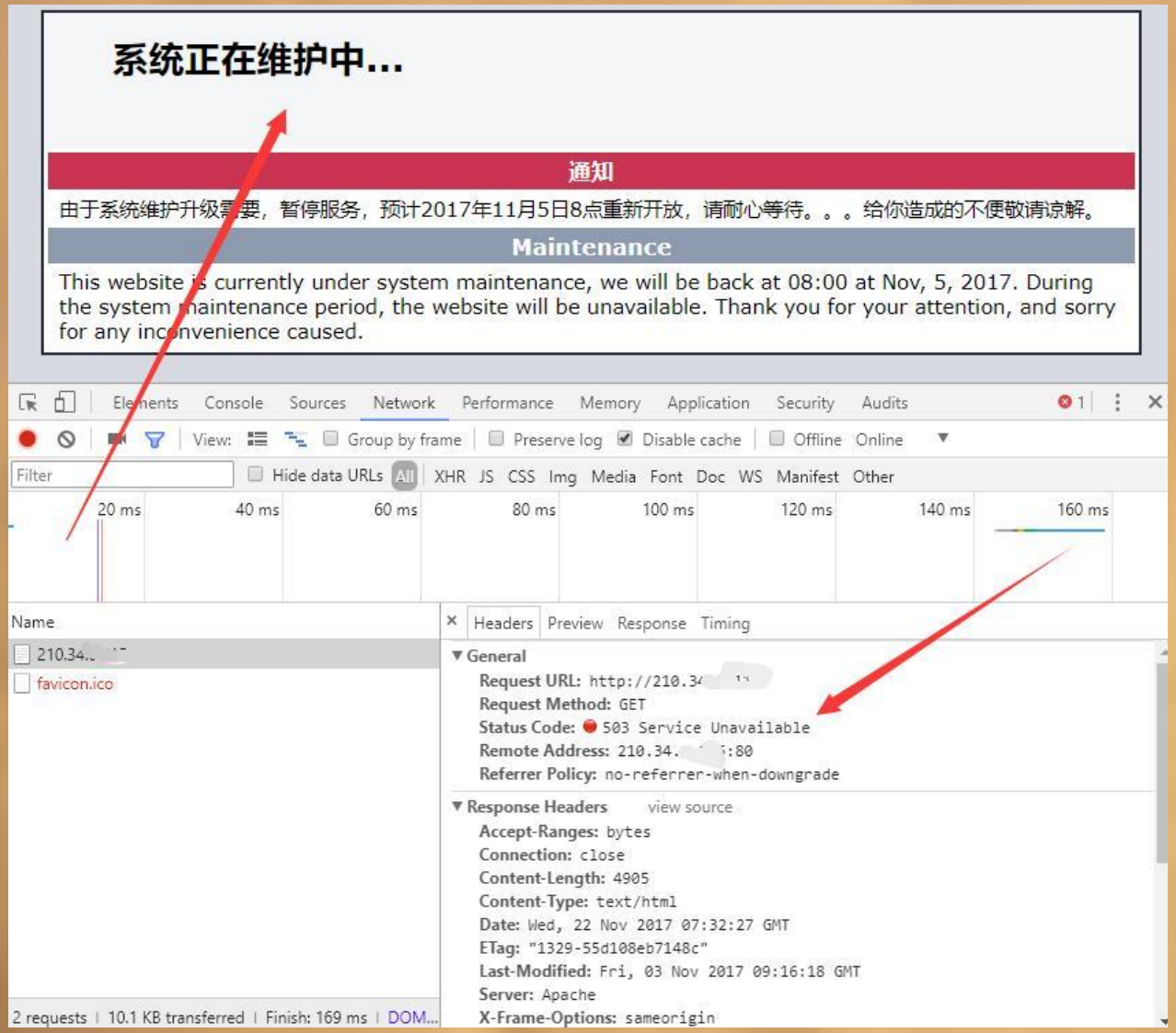
在安全前提下尽可能保障师生的网络应用需求

关

- WIFI认证关闭基于MAC匹配的无感知认证功能
- 关闭边界的大部分端口，限制外网对校园网的SSH/Telnet/FTP及常见远程控制端口。
- 关大部分网站和信息系统，邮件Web端。

开

- WIFI保留安全性较高的802.1x接入认证。
- 厦门大学主页
- 网站群
- DNS
- 邮件，启用SMTPS，POPS，IMAPS
- 利用双因素认证的VPN访问特殊业务系统。



通知页面的技巧

- 对于一些存在安全隐患而被暂时性下线的网站，可使用应用交付设备或者把DNS导入到一个特定的通知页面，以减少突然关闭对网站管理员和浏览者带来的不便。
- 为避免临时性替换网站页面内容导致搜索引擎删除原有网站信息，通知页面应当返回503 HTTP状态码，也可根据恢复时间指定Retry-After返回值。

校内校外访问提示

对于需要拨VPN访问的信息系统，我们在前端加上Nginx负载均衡，对于校外IP，访问会得到一个提示，告知必须拨双因素认证的VPN，附上详细的说明，而对于校内IP则直接可以访问。

THE SECOND PART

事前
BEFORE

THE SECOND PART

事前
落实信息安全等级保护制度

等保提升了制度、安全设备、网络等整体安全性

工作动员会议

（2017年1月6日）召开全校信息安全等级保护工作动员会。各处级单位须指派具体负责网站管理等技术工作的人员一名参加。

校内网站备案信息更新

（2017年1月15日），在新备案系统登记，信息填写完整后下载《厦门大学网站备案申请表》PDF文档并打印，经加盖单位公章后提交信息与网络中心用户服务部确认。

系统定级及公安备案

（2017年3月31日）。根据我校工作实际，校内网站及信息系统中，厦门大学信息化综合应用平台及厦门大学网站群系统定为三级系统，其余系统均定为二级系统或一级系统。各单位应配合做好系统等级认定工作，提供定级及公安备案所需的各项信息。

安全评估、整改以及等级测评

（2017年5月8日）。各单位应按照信息安全等级保护工作要求，协调、组织信息系统管理人员及开发单位、维护单位配合完成系统的评估、整改及复测工作。针对安全评估过程中发现的问题，各单位应在15个工作日内完成整改工作。

事前
网站治理：定义和定位

1

“僵尸”网站

教育部对僵尸网站给出明确定义和治理要求。其指标为：1）年访问量1000人次以下；2）网站180天以上未更新；3) 系统每年录入的信息在100条以下；4）专题网站使命完成，网站系统无人运维或者运维缺少基本保障。
http://mp.163.com/v2/article/detail/D0L5CCIJ0511CKT4.html

2

“双非”网站

指主体为学校但是IP地址和域名均不是学校的网站和信息系统。
管理手段。技术手段：搜索引擎、http://icp.chinaz.com/conditions

3

“寄生”网站

指依附在已经开放了校外访问权限的服务器上。（萧德洪）
流量分析。

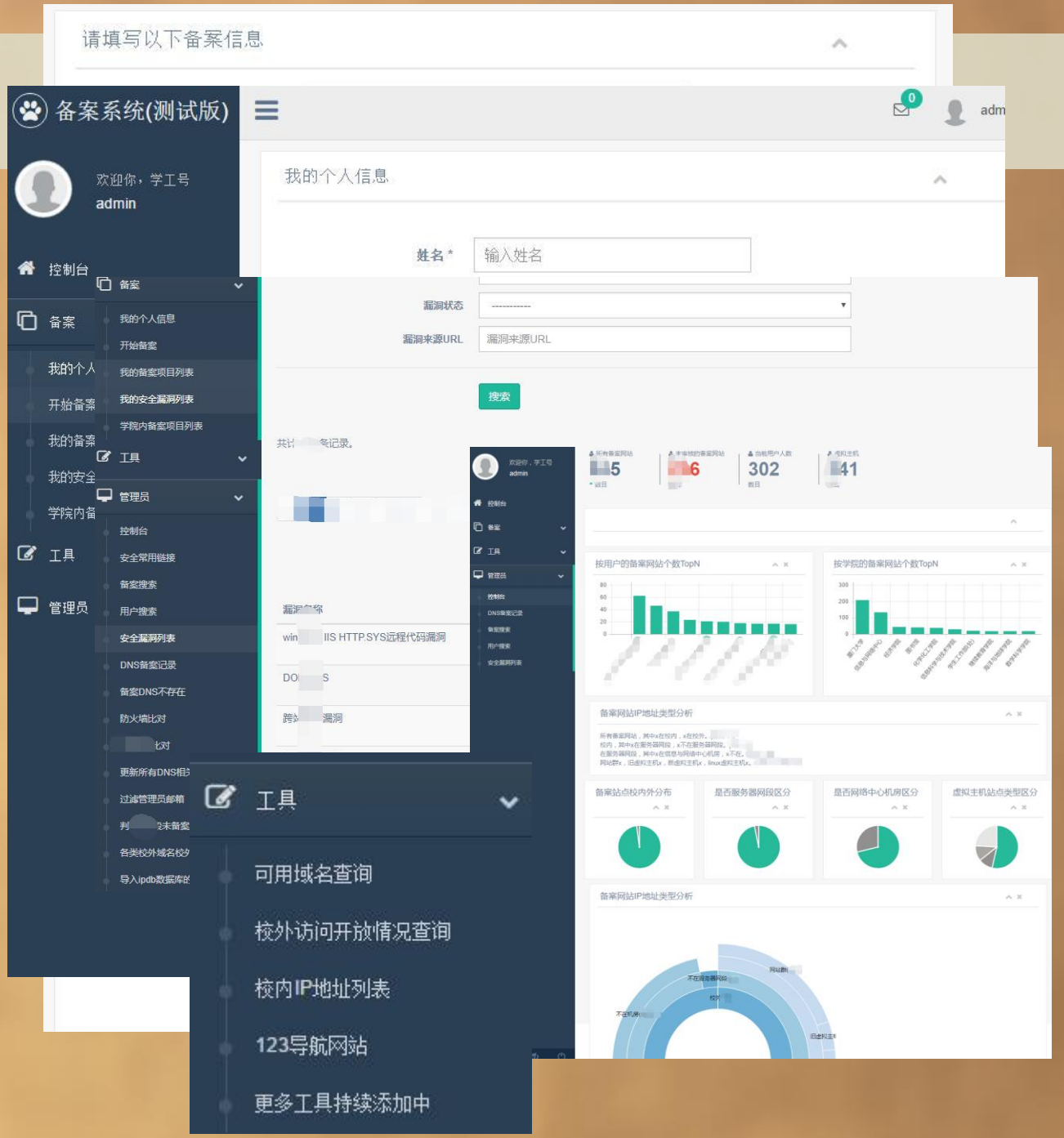
THE SECOND PART

事前
备案系统

所有站点均需在备案系统备案，以便出现安全问题时可以联系到责任人。建立年审机制，杜绝僵尸网站和责任人变换。

SRC平台功能，实现漏洞的全生命周期管理，从各个平台（补天、漏洞盒子、VulTracker、SRC.edu-info、教育部、CNVD、赛尔、福建省、厦门市网安、漏扫工具）过来的漏洞录入到平台，通过邮件跟踪进度，通过技术手段封禁没有修复的站点。实现漏洞从通知，认领，修复，验证，完成的管理。

基于备案记录实现各种扩展：网址导航，截图，DNS记录比对，漏扫，监控，站点分类、导出网站列表到IPDB等。



THE SECOND PART

事前
利用Ticket系统管理台账

- 管理制度评审计划
- 管理制度评审记录
- 安全管理制度收发记录表
- 信息资产登记表
- 重大事件报告表
- 应急预案培训记录表
- 应急预案演练记录表
- 机房人员出入申请表
- 机房设备出入登记簿
- 机房设备出入申请表
- 机房值班记录
- 门禁卡权限申请单
- 病毒事件报告表
- 本地备份登记记录
- 备份恢复测试记录
- 备份介质更换记录
- 业务系统备份数据清单
- 异地备份登记记录
- 重要系统变更记录表
- 重要系统变更申请表
- 介质处置表
- 介质使用清单
- 存储介质清单
- 办公终端安全问题记录单
- 设备审批表
- 设备运行及维护档案
- 安全检查情况汇总表
- 项目终止申请书
- 项目变更申请书
- 信息系统交付清单

- 系统转移、终止或废弃申请表
- 安全设计方案评审表
- 安全培训记录表
- 培训请假单
- 信息安全重要岗位保密协议书
- 人员离岗保密承诺书
- 员工离职（调动）工作交接表
- 员工离职申请表
- 第三方人员保密协议
- 外联单位联系表
- 外部服务人员访问登记表
- 外部服务人员访问申请表
- 重要区域访问申请单
- 安全考核表
- 安全考核记录表
- 信息化建设会议纪要
- 设备变更审批表
- 设备启用审批表
- 设备维修审批表
- 系统配置变更审批表
- 信息安全检查表
- 安全检查记录

事前
网站群

总体原则：将新闻发布为主的宣传性质网站和信息系统分开。

安全级别不同：

新闻发布网站：需要对所有人开放，需要常年开放。

信息系统：可以限制在校内，通过VPN访问。可以在业务期外关闭。

新闻发布性质的大部分迁移到网站群，二级院系无需关注代码和操作系统安全。

管理方面还存在安全隐患：管理员密码泄露，管理员离职，公示与隐私的关系。

开放漏扫工具给二级学院管理员

- 请只对自己的服务器和网站发起漏洞扫描，对未授权的网站发起扫描等尝试攻击也是违法的。请勿对厦门大学IP以外的任何网站发动扫描。
- 漏洞扫描的账户名和密码请勿共享给任何人。系统管理员可能不定期回收账户。
- 为防止对网站正常访问造成影响，请在网站访问量较低时扫描，比如下班后。
- 由于可能有多个用户同时在执行扫描，为减轻漏洞扫描服务器压力，请一次只扫描一个IP或者网站。扫描时间较长，请耐心等待。
- 漏洞扫描有可能对数据造成破坏，请在扫描之前备份自己服务器的数据。
- 漏洞扫描可能被服务器的安全软件拦截，请尝试给安全软件加白名单扫描和不加白名单分别扫描。
- 扫描完请尽快下载HTML或者Word报告保存，系统管理员有可能不定期清理任务。
- 漏洞扫描结果可能误报，扫描结果仅供参考，扫描结果为安全也不一定确实安全。

THE THIRD PART

事中
ING

事中
厦门大学主页的防护

DNS系统4台，3台Log分析服务器。7台测试服务器共14台服务器。

厦门大学主页1台动态服务器，1台静态服务器，1台通知帮助服务器，3台测试服务器。共6台服务器。

基础架构代码化，使用Ansible一键部署。使用自动化脚本快速更新动态服务器变更到静态服务器。

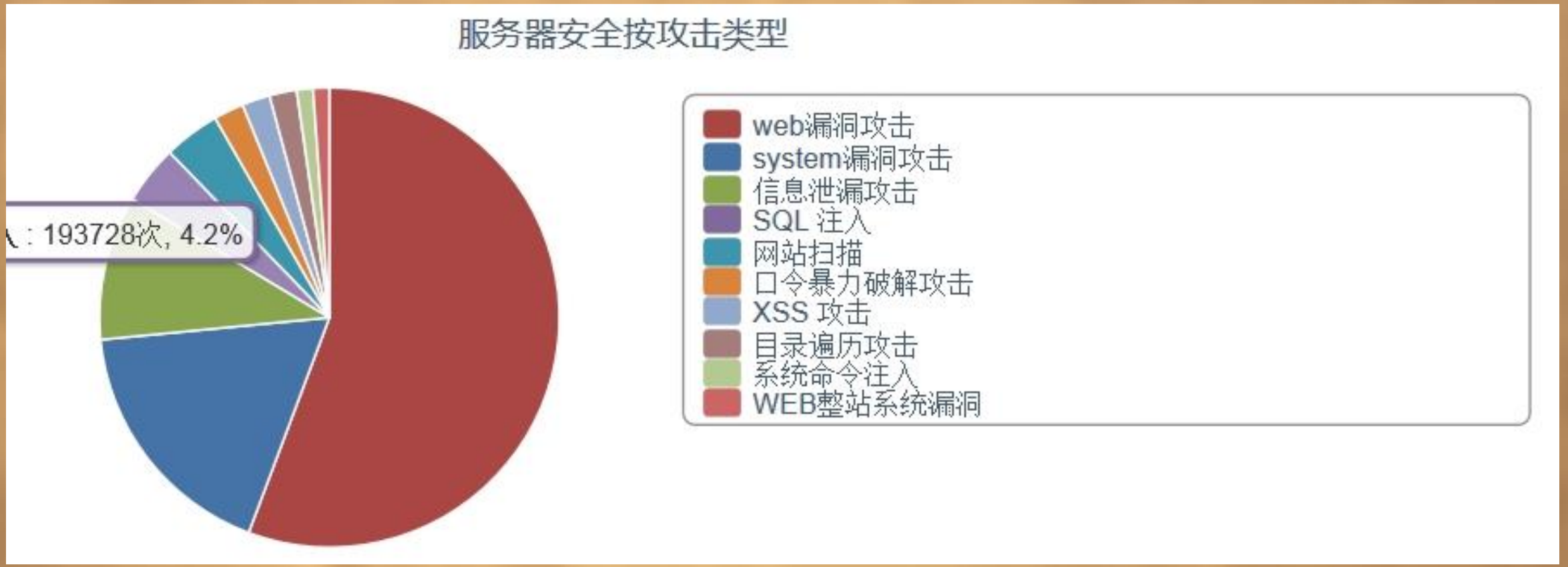
事中
一键断网准备

演练厦门大学主页一键断网，一键断网可以从传输的各个层面上执行。

- 在操作系统增加防火墙、关机、
- 在Web服务器设定访问某个特定页面自动关闭服务器；
- 虚拟机关闭网络；实体机拔掉网线；
- 网络层面WAF、IPS、防火墙拦截。
- 网关使用ACL控制、网关关机；

事中
7*24小时巡检

海恩法则：每一起严重事故的背后，必然有29次轻微事故和300起未遂先兆以及1000起事故隐患。



事中
7*24小时巡检

巡检内容：所有做过的安全防护软件运行情况，系统更新状态。检查各个软件的运行状态和结果分析，检查系统账户、性能、进程、端口、启动项、病毒、后门、漏洞扫描结果、WAF和IPS拦截日志。查看日志传输是否完整，备份是否正常。各个服务器的通常运行状况。检查所有软件和安全设备的软硬件工作状态，配置更改情况。对攻击IP进行封禁等。并做好配置变更和巡检报告。

巡检巡检程序是否正常运行。

应对攻击溯源

安全措施无法做到百分百安全。

在攻击发生后，为了为下一次工作积累经验，同时固定犯罪证据，应当做好攻击溯源准备。应当保存好所有相关日志。比如网络设备日志、安全设备日志、主机日志等。所有的日志应当进入专门的远程日志服务器。服务器做到分钟级别的备份以防止攻击者擦除攻击痕迹。

事中
调整，需求是用来变更的

- 主页新闻临时发布
- 教育部公文接收系统
- 突然的视频会议需求
- 突发的科学计算需求

THE FOURTH PART

事后
AFTER

总结经验，为下次做准备。
保留各种白名单黑名单。

中山大学张永强：抓住机遇上台阶。
网络安全重视程度加大。
建立7*24小时值班制度。
网站治理继续推进。

THE End

总结
SUMARRY

TITLE	TITLE	TITLE	TITLE
1	2	3	4
积极提前做好网站治理等前期准备工作	积极开放必要的信息系统	积极响应用户需求，调整策略	积极安抚用户，提供通知和帮助网站，并做好搜索引擎技术问题

THANK YOU FOR WATCHING

厦门大学信息与网络中心 郑海山 Haishion AT xmu.edu.cn https://dog.xmu.edu.cn

标注

字体使用	英文 Century Gothic
	中文 微软雅黑
行距	正文 1.3
背景图片出处	cn.bing.com
声明	互联网是一个开放共享的平台 OfficePLUS 部分设计灵感与元素来源于网络 如有建议请联系 officeplus@microsoft.com