



网站资源发布管理的 实践与思考

2022年8月25日



清华大学网站及信息系统情况

- 校级网站及信息系统
 - 范围
 - 为全校提供服务的信息系统
 - 学校主页（新闻网）、院系和部处的部门主页
 - 系统建设：信息办立项，业务负责单位建设，信息化技术中心技术支持
 - 系统运维：信息化技术中心和承建方（中心、公司或校内其他单位）
 - 业务管理：各部处院系
- 非校级信息系统
 - 院系、部处自行建设和运维



清华大学网站及信息系统情况

- 主要存在的问题
 - 数量大
 - 校级信息系统和网站群总计350+个
 - 非校级备案信息系统2000+个，校外访问1000+个
 - 非校级系统管理不善
 - 无专职管理人员，主要依靠学生或公司，甚至无人管理
 - 防护手段缺乏
 - 全校均为公网IP地址
 - 部分非校级系统无基础的防火墙等防护手段
 - 缺乏审计手段
 - 大部分非校级系统日志记录时间不达标，甚至无日志
 - 只管上线不管下线
 - 僵尸网站大量存在



清华大学网站及信息系统情况

- 主要存在的问题
 - 技术问题
 - 不支持HTTPS
 - 不支持IPv6
 - 出现问题无法快速切断
 - 服务器直接对公网，暴露面大



治理方案

• 管理

• 实施强备案机制

- 不备案不能开设服务
- 备案要记录技术架构、开发语言和开发框架等信息

• 备案年审制

- 对备案系统进行定期审核
- 对使用情况要进行跟踪和管理

• 落实二级单位责任

- 网站出现安全问题以OA的方式通知二级单位一把手

清华大学信息系统备案数据											
资产名称		URL		IP地址							
请输入资产名称		请输入URL		请输入IP地址							
资产ID	系统属性	系统名称	URL	IP地址	端口	服务类型	当前状态	存放地点	开通时间	计划下线时间	网站类型
079246	合法	webvpn服务器	https://webvpn.tsing...	166.111.8.214	443	WWW服务	正常运行	李兆基2楼机房	2019-04-15	长期	中文
079245	合法	webvpn服务器	http://webvpn.tsing...	166.111.8.214	80	WWW服务	正常运行	李兆基2楼机房	2019-04-15	长期	中文
079244	合法	统一认证服务运维系统	http://jgyhwa.its.tsing...	166.111.208.50	11010	其他服务	正常运行	6教A600	2019-04-01	长期	中文
079243	合法	MCU互动服务器	http://mcu.its.tsingh...	166.111.208.8	34050	其他服务	正常运行	6教A600	2019-04-01	长期	中文
079242	合法	MCU互动服务器	http://mcu.its.tsingh...	166.111.208.8	4081	其他服务	正常运行	6教A600	2019-04-01	长期	中文
079241	合法	MCU互动服务器	http://mcu.its.tsingh...	166.111.208.8	20000	其他服务	正常运行	6教A600	2019-04-01	长期	中文
079240	合法	MCU互动服务器	http://mcu.its.tsingh...	166.111.208.8	5222	其他服务	正常运行	6教A600	2019-04-01	长期	中文
079239	合法	MCU互动服务器	http://mcu.its.tsingh...	166.111.208.8	5061	其他服务	正常运行	6教A600	2019-04-01	长期	中文
079238	合法	MCU互动服务器	http://mcu.its.tsingh...	166.111.208.8	5060	其他服务	正常运行	6教A600	2019-04-01	长期	中文

清华大学信息系统备案登记及变更申请

信息办制 联系电话：80257/94263

申请方信息						
申请单位	信息技术中心	业务编码	LC284003-2022729			
经办人	刘乃嘉	联系方式	*			
标题	如XX单位（申请单位）XXXX（资产名称）信息系统备案登记/变更申请 *					
保密承诺	☒ 以上（下）内容不包含任何国家秘密和工作秘密。 *					
业务申请						
资产ID	无	* 查询本单位资产ID				
申请事由	*					
申请事项	☐ 备案登记 （模板下载： 备案登记表.xlsx ）注：一次申请只能提交一条信息，不能批量备案。					
	☐ 登记信息变更	字段名称	变更前 变更后			
		--请选择--				
	☐ 系统上线 （需提交 信息系统安全检测登记表.docx 、内容审核意见）					
	☐ 系统注销					
☐ 整改验证						
☐ 其他						



治理方案

- 技术
 - 校园网出口管控
 - 对小于1024及8000-8100的端口进行封禁
 - 对校级系统保持严格管控
 - 对非校级系统全部要求使用反向代理
 - 反向代理后前配置WAF，对网站进行防护
 - 建设Web应用前端，统一解决技术问题



治理方案

- 校级系统保持严格管控
 - 上线前严格检查
 - 功能测试、性能测试和安全测试

信息系统安全检测登记表	
一、项目基本信息 (不强制填写)	
以下信息由责任单位填写	
项目名称	清华大学在线教学系统
系统名称	在线教学系统
系统描述	在线教学系统旨在为校内师生提供一个教学视频直播平台，实现线上的课程教学、研讨及考核需求，以适应当下时代的数字化教学场景需求。
所属院系	信息化技术中心
承建单位	广州南方科技股份有限公司
部署域名	tsinghua.edu.cn 和 class.tsinghua.edu.cn
IP地址	166.111.118.151 和 166.111.118.152
端口	80
项目负责人	李博
联系方式	822891
项目管理员	李斌
联系方式	84628
访问范围	☒ 校内 ☐ 校外
访问对象	☒ 匿名 ☐ 教师 ☐ 学生 ☐ 校外用户 ☐ 其他
二、项目安全自查情况	
以下信息由责任单位填写	
1. 手工检查	
检查内容	检查结果
进行代码清理(确保代码中不包含测试、备份、历史等与应用运行无关的文件)	通过
应用管理用户清理(确保上线系统中不存在无用户、不存在弱密码用户)	通过(对接清华统一认证服务)
恶意代码检查(确保代码中不存在已注入的恶意代码)	通过
权限检查(确保程序进行了正确的权限控制)	通过



清华大学信息化建设项目 安全测试报告

项目名称: 学校房屋土地数据管理平台建设

责任单位: 清华大学资产管理处

项目负责人: 李功强

技术负责人: 黄木亮(项目开发单位)

项目时间: 2020年3月-2021年12月



治理方案

- 校级系统保持严格管控
 - 定期安全扫描
 - 所有系统均由信息化技术中心负责部署和后期运维
 - 厂商只能按照要求提交版本和说明文档

清华大学网络安全整改通知书

信息办制

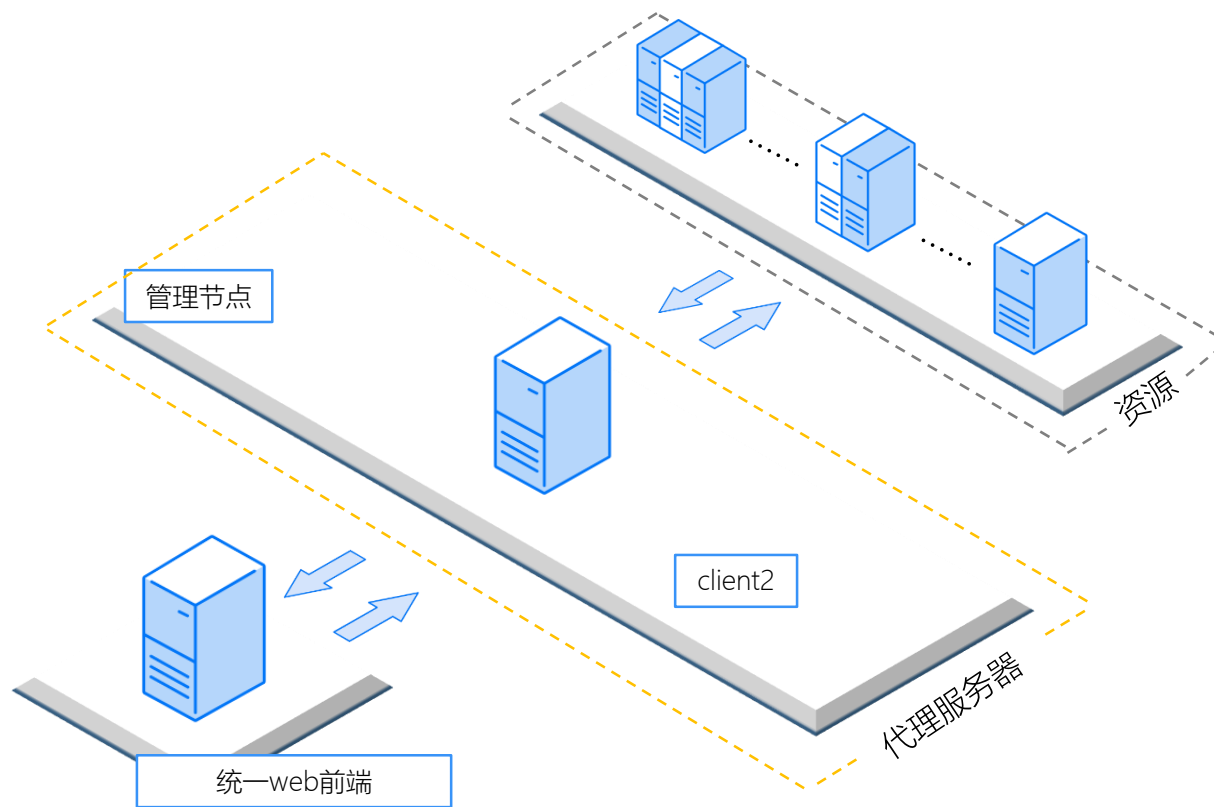
联系电话：80257/94263

漏洞信息			
标题	(整改单位) (整改资产ID) 网络安全整改通知书		
整改通知编号		事件编号	
单位		资产ID	*
IP地址	*	端口号	*
URL	*		
漏洞来源	--请选择--	漏洞类型	*
漏洞等级		漏洞发现时间	2019-09-05
采取措施	--请选择--	限定整改时间	2019-09-05
事件描述			
相关附件	上传文件		
在近期安全检测中发现你单位信息系统存在安全隐患,为避免安全隐患被利用,防止出现网页篡改、挂马、泄露敏感信息等安全事件,请你单位在限定整改时间内修复漏洞完成整改。 学校对存在安全隐患的信息系统处置如下:高危隐患立即限制校内访问,限期(自发出整改通知之日起)5个工作日内完成整改;中危隐患整改时间为10个工作日,低危隐患整改时间为15个工作日,逾期将限制校内访问;整改完毕通过验证后将取消访问限制。 网络安全整改流程: 第一步:签收整改任务。请单位网络安全工作第一责任人签收(院系为党委书记、部处为单位正职)。 第二步:提交整改方案。单位研究制定并提交整改方案(短期内无法完成整改的,方案中应明确整改截止时间)。 第三步:申请整改验证。单位整改完毕后应立即申请验证,如仍存在问题,需进一步整改直至全部完成。 特此通知!			



反向代理——部署方案

- 非校级信息系统实施反向代理
 - 双工作节点，前置负载均衡调度，实现业务双活
 - 前置WAF，加固安全防护





反向代理——运行监控

- 网站发布状态

a.test.com(a.test.com) HTTPS IPv4/IPv6 内外网认证访问

概览 备案 网站备份 基本配置 高级配置

网站状态
一切正常

备案信息
备案信息不完整, 请输入相关信息

HTTPS
一切正常

代理配置
当前为"域名优先"

网站日志
点击查看日志

- 后端应用状态

全部等级	全部类型	全部对象	网站可访问状态	未确认未恢复	搜索告警内容	选择日期范围	搜索
批量操作							
☐	告警等级	告警对象	告警内容	触发时间	告警状态	操作	
☐	警告	(网站) [bqgz.bupt.edu.cn]版权工作站	网站可访问状态出现问题, 可能无法正常访问, 原因: 被代理后端URL无法从工作节点访问	2022-07-11 19:31:07	未确认未恢复	确认 恢复 忽略	
☐	警告	(网站) [vse.bupt.edu.cn]网络安全虚拟仿真实验系统	网站可访问状态出现问题, 可能无法正常访问, 原因: 被代理后端URL无法从工作节点访问	2022-07-11 09:51:10	未确认未恢复	确认 恢复 忽略	
☐	警告	(网站) [xb.bupt.edu.cn]北京邮电大学校报电子版	网站可访问状态出现问题, 可能无法正常访问, 原因: 被代理后端URL无法从工作节点访问	2022-07-07 10:01:10	未确认未恢复	确认 恢复 忽略	
☐	警告	(网站) [jysyzx.bupt.edu.cn]国家级语言实验示范中心	网站可访问状态出现问题, 可能无法正常访问, 原因: 被代理后端URL无法从工作节点访问	2022-05-25 17:11:09	未确认未恢复	确认 恢复 忽略	

- 异常日志分析

访问日志

安全日志

2022.08.17 09:43:11 - 2022.08.17 09:58:11

全部网站

访问失败日志

IP

用户名

405

请求方式

访问路径

搜索

时间	网站名	IP	用户名	HTTP协议	状态码	请求方式	访问路径	终端	后端地址	后端响应时
2022-08-17 09:57:22	认证门户 (https)	2001:da8:215:3c02:8bc:5be7:a8e:d745	-	HTTP	405	OPTIONS	/banner/d8f4be37-a3a0-469f-98ef-c83ab8563734	Chrome 104.0.5112/Windows 10	10.3.55.245:8081	0.001s
2022-08-17 09:55:28	一站通3D数字政务大厅	2001:da8:215:6a01::849:fc4	-	HTTP	405	OPTIONS	/js/jquery-3.5.1.min.js	Chrome 104.0.0/Mac OS X 10.15.7	10.3.55.163:80	0.001s
2022-08-17 09:55:28	一站通3D数字政务大厅	2001:da8:215:6a01::849:fc4	-	HTTP	405	OPTIONS	/js/pannellum-1029.js	Chrome 104.0.0/Mac OS X 10.15.7	10.3.55.163:80	0.001s
2022-08-17 09:55:03	认证门户 (https)	2001:da8:215:6a01::849:fc4	-	HTTP	405	OPTIONS	/authserver/cas/img/logo-full.png	Chrome 104.0.0/Mac OS X 10.15.7	10.3.55.243:8081	0.002s



反向代理——使用情况

- 统一发布800+校内网站及系统

资源发布

admin 202

网站资源 反向代理系统 > 资源 > 列表

发布资源 批量操作 自定义列表 运行状态 发布形式 发布协议 访问策略 标签 资源名/域名/URL 搜索

资源发布

资源名	域名	URL	运行状态	访问策略	操作
vcard.sem.tsinghua.edu.cn	http://vcard.sem.tsinghua.edu.cn	http://101.6.8.10	✓	直接访问	编辑 配置 删除
openvpn.cic.tsinghua.edu.cn	http://openvpn.cic.tsinghua.edu.cn	http://166.111.4.20	✓	直接访问	编辑 配置 删除
ccfr.sem.tsinghua.edu.cn	http://ccfr.sem.tsinghua.edu.cn	http://101.6.5.237:4000	✓	直接访问	编辑 配置 删除
cbfr.sem.tsinghua.edu.cn	http://cbfr.sem.tsinghua.edu.cn	http://101.6.5.230:4000	✓	直接访问	编辑 配置 删除
liis.tsinghua.edu.cn	http://liis.tsinghua.edu.cn	http://101.6.5.226	✓	直接访问	编辑 配置 删除
otl.internal.tsinghua.edu.cn	http://otl.internal.tsinghua.edu.cn	http://166.111.4.151	✓	直接访问	编辑 配置 删除
www.sgd.tsinghua.edu.cn	http://www.sgd.tsinghua.edu.cn	http://101.6.5.219	✗	直接访问	编辑 配置 删除
ap.myhome.tsinghua.edu.cn	http://ap.myhome.tsinghua.edu.cn	http://166.111.7.136	✓	直接访问	编辑 配置 删除
newstu.myhome.tsinghua.edu.cn	http://newstu.myhome.tsinghua.edu.cn	http://166.111.7.136	✓	直接访问	编辑 配置 删除
m.myhome.tsinghua.edu.cn	http://m.myhome.tsinghua.edu.cn	http://166.111.7.136	✓	直接访问	编辑 配置 删除
reser.myhome.tsinghua.edu.cn	http://reser.myhome.tsinghua.edu.cn	http://166.111.7.136	✓	直接访问	编辑 配置 删除
hf.myhome.tsinghua.edu.cn	http://hf.myhome.tsinghua.edu.cn	http://166.111.7.136	✓	直接访问	编辑 配置 删除
www.sloa.civil.tsinghua.edu.cn	http://www.sloa.civil.tsinghua.edu.cn	http://166.111.7.242:8080	✓	直接访问	编辑 配置 删除
apply.myhome.tsinghua.edu.cn	http://apply.myhome.tsinghua.edu.cn	http://166.111.7.136	✓	直接访问	编辑 配置 删除
www.hydro30.civil.tsinghua.edu.cn	http://www.hydro30.civil.tsinghua.edu.cn	http://101.6.54.28	✗	直接访问	编辑 配置 删除
lock.myhome.tsinghua.edu.cn:8080	http://lock.myhome.tsinghua.edu.cn:8080	http://101.6.5.63:8080	✓	直接访问	编辑 配置 删除
openings.iis.tsinghua.edu.cn	http://openings.iis.tsinghua.edu.cn	http://101.6.96.3	✓	直接访问	编辑 配置 删除



反向代理——问题与对策

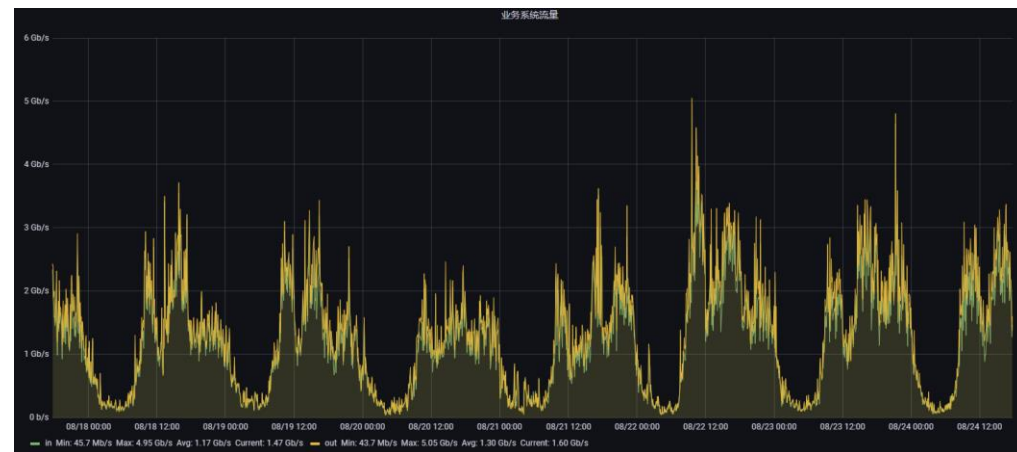
- 实施反向代理过程中的一些问题与解决方案
 - 双活的实现
 - IP地址信息传递
 - 负载均衡与PROXY协议
 - X-Forwarded-For处理
 - Nginx对HTTP协议的处理
 - 上传大文件
 - 服务器响应超时
 - Nginx日志的保留



统一Web前端

• 功能与定位

- 代替原有传统负载均衡，负责HTTP协议整体处理
- 功能
 - 支持HTTP协议基本处理
 - 抗击常规流量攻击
 - 支持HTTPS卸载及SNI
 - IPv4和IPv6地址转换
 - 基于域名的校内外访问控制
 - 缓存与压缩
 - 支持BBR进行网络优化
 - 全网日志收集与后期利用





资源发布思考与探讨

- 后期考虑
 - 完善统一Web前端功能，提高流量防护能力
 - 通过BFD+ECMP实现统一Web前端的多活
 - 网站和信息系统内容的进一步监控与问题发现
 - 反向代理统一策略实施，进一步降低反向代理对网站的影响



谢谢！