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

文 / 郑海山

在大型活动保障期间，为了提高网站的安全性，较少运维压力，信息部门会选择尽量关闭一些存在安全隐患的网站，缩小需要运维的机器的数量，把保障力量集中于最重要的部分系统和服务器上。门户网站作为学校的第一入口，往往是攻击者的首要目标。如何提高门户网站的安全性成为大型活动保障的重要工作。

将整个网站静态化，可以规避服务端动态脚本语言带来的诸如 SQL 注入、权限绕过、XSS、CSRF 等安全风险，然而静态化并不能完全规避所有风险。通常意义的静态化方法指的是纯 HTML 和图片、JavaScript、CSS 代码，而前端 JavaScript 还是有动态执行的代码。一般现在的网站群也会生成静态网页，网站群系统生成的静态网页与产品高度耦合，中间件不能随意变更，操作系统补丁如果更新到最新可能会对网站功能造成影响。如果能搭建一个纯静态的网站，安全性必将更高。本文将介绍如何打造高安全性的静态网站的方法和静态网站面临的安全问题和防护手段。

一个网站页面，从服务器到浏览者之间会经过非常多步骤，中间任何一个环节都有可能被攻击。防护应当考虑所有环节，包括引入的安全设备是否同时也会引入安全隐患等。一般来说，只要做好静态化，基本上不会被普通的攻击者攻击，本文提到的一些防护措施存在重复和无效的可能，然而基于纵深防御的概念，通过多层重叠的安全防护达到冗余的结果，即使某一个防线由于技术失误造成失效，也可以通过其他防御弥补。

静态化处理和安全性检查

如果网站本身是由网站群系统生成的静态化页面，则可以直接在网站群生成的静态化页面服务器上做好安全防护。通过 URL 重写技术的伪静态与动态页面的安全性一样，这些站点可以使用 wget 开源软件一条命令镜像整个站点。对于静态页面还必须做以下内容方面的检查：

1. 如果网页文本本身带有恶意文本，静态化会将其原封不动的镜像过来。可以通过漏洞扫描工具扫描关键字和隐藏文本来检查。

2.JavaScript 文件是否官方下载，是否已经被植入了恶意代码。可通过重新在官方下载或者使用程序 MD5 检查所有的第三方 JavaScript 代码。

3. 是否引用了其他站点的图片或 JavaScript。如果其他站点图片内容被篡改，会导致网站也被篡改。检查图片是否带有隐藏信息。

4. 是否引用了 IFrame 嵌入第三方网站内容。

网站应当对静态化友好，为了让镜像网站可以在本地或者服务器上直接浏览，wget 会更改页面的 HTML 后缀名，可能导致 JavaScript 脚本运行不正常。wget 也会更改 URL 的相对路径和绝对路径。所以做完静态化后应当多次检查，如果有需要，应当调整原始网站模板，或者在 wget 后使用脚本语言改写内容，使得静态化可以持续自动化执行，使得动态网站的更改可以更快反应到静态网站上。

静态网站的防护

一旦做好了相对安全的静态网站后，针对可能的攻击可以再实现以下纵深防御。

1. 网络层面

网站服务器网络层面的攻击包括可能 DNS 解析被修改导致浏览者访问了攻击者伪造的网站，可能 IP 被同 VLAN 攻击者控制的服务器抢占，或者是同 VLAN 被攻击者控制的服务器发动 ARP 攻击导致网页内被嵌入其他内容。对于网络层面的防护，应当加强 DNS 服务器的管理，保证 DNS 服务器的安全性，同时尽量减少同 VLAN 内服务器的数量，在服务器和交换机上绑定 IP 和 MAC 信息，同时使用 HTTPS 传输减少被篡改的风险。

2. 操作系统和 HTTP 服务器层面

操作系统应当使用最新的版本，最小化安装，所有安全补丁更新到最新。启用严格的防火墙。可以在网络层面限制服务器主动对外发起连接，定期安全更新可采用 HTTP 代理更新。HTTP 服务器应当最小化安装，去除不需要的模块，隐藏 HTTP 服务器版本。

对于服务器的其他防护，以 Linux 为例，安装多个开源安全软件。可在服务器安装 Lynis、OpenScap 等进行配置核

查，使用 nmap 进行扫描，安装 ClamAV 定期检查病毒，安装 chkrookit 或 RootKit Hunter 定期查后门。

对于可能的 DDoS 攻击和慢连接攻击，应当临时性调高静态服务器的 CPU 和内存资源，调大 HTTP 服务器的连接数，减小超时时间，做好缓存，使用 Fail2ban、mod_evasive、mod_reqtimeout、mod_qos 等模块做好资源限制。

对于扫描攻击的防御，可以安装 OSSEC、mod_security 等检测攻击。

3. 文件目录

通常的防篡改软件能防止页面所在的目录不被篡改，但是无法预防通过修改 HTTP 服务器配置文件指向其他目录或者直接写 Python 脚本用 HTTP 服务的情况，所以以上的防护应当交由操作系统来执行。对于文件目录的防篡改，可以安装开源 OSSEC、Tripwire 等软件检查篡改情况，同时可以设置 wwwroot 只读，不可执行，甚至可以为 wwwroot 目录单独分区，在挂载时在 /etc/fstab 内设置只读，或者使用 chattr +i 设置目录只读。

4. 安全设备

即使服务器已经做好了安全防护，也应当在网络层面增加 WAF、IPS、防火墙、防 DDoS 等安全设备增加安全性。应当使用漏洞扫描设备对服务器和网站内容进行漏洞扫描。需要注意的是，由于 WAF 安全设备需要接管客户端和服务器之间的通信并进行阻断等操作，应当保证 WAF 服务器的安全性，注意 WAF 缓存可能带来的影响。

5. 防篡改云服务

购买第三方的远程页面防篡改提醒服务。防篡改提醒服务提供商会从世界各地访问被监控网站，发现篡改行为会通过电话、短信、邮件等多渠道通知。需要注意的是防篡改必须检查所有页面的所有内容（JavaScript、图片、CSS）的修改，并且修改比例应当为 0%。也可自行在互联网云平台搭建防篡改检查程序，通过定期爬虫下载所有内容进行 MD5 比对和修改通知。

6. 管理人员

相关的管理人员应当做好安全培训，保证管理终端的安全性，不使用盗版软件，不安装不必要的浏览器插件，启用强密码规则，管理客户端专用，关闭外网访问，对服务器的管理采用堡垒机。

7. 演练、应急预案和巡检

大型活动保障期间应当定期巡检，安排人员 24 小时值班，并做好事前演练和应急预案。巡检内容包括以上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，备份是否正常查看，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。

运维安全的其他注意事项

1. 使用 Ansible 等自动化配置工具

为确保操作系统、HTTP 服务器的安全配置灵活，方便检查配置和审计，方便系统重建，减少人为失误和变更工作量。应当使用 Ansible、Puppet 等自动化配置工具自动配置整个服务器环境。同时也可以使用 Ansible 等脚本执行自动化巡检任务。

2. 一键断网

为了减少被攻击后传播所造成的不良影响，应当有一键断网措施。一键断网可以从传输的各个层面上执行。比如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；网关使用 ACL 控制、网关关机；网络层面 WAF、IPS、防火墙拦截。在出现疑似攻击后应当尽快将服务器下线，检查无误后方才上线。

3. 应对虚假攻击

由于网络传输的链路过长，各个环节都可能造成网站疑似被攻击，比如云 DNS 投毒、CDN 投毒、客户端本身 ARP 攻击、客户端接入商随意插入广告甚至被人截图后 PS 修改等。如发现应当及时下线，并执行检查，如果确定非自身因素则应当及时上线，并在页面上显著位置公布以消除不良影响。

4. 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，同时收集犯罪证据，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。

5. 网站关闭的通知页面

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，以减少突然给对网站管理员和浏览者带来的不便。同时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。

通过以上的安全防护，可以大大提高门户网站的安全性，减少在大型活动保障期间的运维压力。以上措施也可实施于动态网站，然而动态网站还需要其他包括代码审计等安全措施。由于存在管理人员和 0day 漏洞等的风险，所有的安全措施无法做到百分百安全，只能是提高攻击者攻击的难度，同时，网站还应根据政策法规要求做好备案和信息系统安全等级保护等工作。CEN（责编：王左利）

（作者单位为厦门大学信息与网络中心）