任子行网站监控预警平台
技术白皮书

目录

1. 网站业务群安全分析

Web 应用的发展，使 Web 系统发挥了越来越重要的作用，与此同时，越来越多的 Web 系统也因为存在安全隐患而频繁遭受到各种攻击，导致 Web 系统敏感数据、页面被篡改、甚至成为传播木马的傀儡，最终会给更多访问者造成伤害，带来严重损失。

1.1 Web 安全攻击形式

由于针对 Web 系统的网络访问控制措施被广泛采用，且一般只开放 HTTP 等必要的服务端口，因此黑客已经难以通过传统网络层攻击方式（查找并攻击操作系统漏洞、数据库漏洞）攻击网站。然而，Web 应用程序漏洞的存在更加普遍，随着 Web 应用技术的深入普及，Web 应用程序漏洞发掘和攻击速度越来越块，基于 Web 漏洞的攻击更容易被利用，已经成为黑客首选。据统计，现在对网站成功的攻击中，超过 7 成都是基于 Web 应用层，而非网络层。前不久 OWASP (Open Web Application Security Project）机构发布了最新的《OWASP Top 10 Application Security Risks》，SQL 注入和 XSS 攻击（Cross Site Scripting，跨站脚本攻击）仍旧排名前两位，是目前存在最为普遍、利用最为广泛、造成危害最为严重的两类 Web 威胁。

攻击者攻击 Web 系统，一般会采取两种手段来达到博名、获利的目的：

1) 网页篡改 Web 系统数据威胁

攻击者通过 SQL 注入等 Web 应用程序漏洞获得 Web 系统权限后，可以进行网页挂马、网页篡改、修改数据等活动。例如：黑客可以通过网页挂马，利用被攻击的 Web 系统作为后续攻击的工具，致使更多人受害；也可以通过网页篡改，丑化 Web 系统所有者的声誉甚至造成政治影响；还也可以通过修改 Web

系统敏感数据，直接达到获取利益的目的。

2）窃取用户信息

利用 Web 应用程序漏洞，构造特殊网页或链接引诱 Web 系统管理员、普通用户点击，以达到窃取用户数据的目的。例如游戏、网银、论坛等账号的窃取，大多是利用了 Web 系统的 XSS 漏洞实现的。

总之，随着攻击技术的不断进步，越来越多的攻击者利用更容易被利用的、普遍存在的 Web 应用程序漏洞对 Web 系统进行攻击并频频得手，目前 Web 系统的生存环境已经日益恶化。部分 Web 系统的所有者已经遭受到攻击，并从攻击造成的损失中深刻认识到 Web 系统安全问题的紧迫性。但大多数 Web 系统的所有者仍然处在已经被攻击而浑然不觉、或者即将被攻击而无应对的巨大风险之中。

3）木马威胁

木马程序是目前比较流行的一类病毒文件，它与一般的病毒不同，它不会自我繁殖，也并不刻意地去感染其他文件。它通过将自身伪装吸引用户执行，或以捆绑在网页中的形式，当用户浏览网页时受害。木马程序向施种木马者提供打开被种者电脑的门户，使施种者可以任意毁坏、窃取被种者的文件和隐私，甚至远程操控被种者的电脑。木马的原理和计算机网络中常常要用到的远程控制软件相似，但由于远程控制软件是“善意”的控制，因此通常不具有隐蔽性;而木马程序则完全相反，木马要达到的是“偷窃”性的远程控制，如果没有很强的隐蔽性的话，那就是毫无价值的。

根据互联网响应中心公布的数据，存在挂马比较严重的情况发生在 2011 年的

11 月份。同时这也是 2011 年年网站挂马率最高的时期。根据数据显示在整个 2011 年期间中国整体互联网网站数量为 5,533,092 其中挂马量为 20,368 由于国家对于互联网安全问题的日益重视并加大了监管的力度。

4) 敏感信息威胁

近年来，电信运营商、各大门户网站的的敏感信息数据泄漏安全事件频繁发生，不仅对运营商自身的核心机密、同行业竞争力和市场声誉造成了严重的影响，也对客户的隐私和个人信息安全构成不同程度的危害。因此，防范敏感信息数据泄漏事件的发生已成为安全工作的重要目标和任务，如何构建敏感信息安全保障体系，保护企业核心数据的安全，保护核心系统安全稳定运行，也一直是学术界和企业共同关注的焦点。

5) 网站钓鱼威胁

所谓“钓鱼网站”是一种网络欺诈行为，指不法分子利用各种手段，仿冒真实网站的 URL 地址以及页面内容，或者利用真实网站服务器程序上的漏洞，在站点的某些网页中插入危险的 HTML 代码，以此来骗取用户银行或信用卡账号、密码等私人资料。

“钓鱼网站”近来在全球频繁出现，严重地影响了在线金融服务、电子商务的发展，危害公众利益，影响公众应用互联网的信心。钓鱼网站通常伪装成为银行网站，窃取访问者提交的账号和密码信息。它一般通过电子邮件传播，此类邮件中一个经过伪装的链接将收件人联到钓鱼网站。钓鱼网站的页面与真实网站界面完全一致，要求访问者提交账号和密码。一般来说钓鱼网站结构很简单，只有一个或几个页面，URL 和真实网站有细微差别。

6) 网站断线等威胁

因为某些情况，客户网站不能对外提供访问，造成很坏影响，而常常管理员是事后得知情况，这是困扰管理员的一个重要问题。

另一方面，当网站部署完成后，因为技术等原因，网站所有者无从感知网站的用户体验情况，无法确认不同区域用户的访问网站速度、响应时间、可达情况等，特别是一些公共的门户网站，此问题更为重要。

2. 网站群安全带来巨大损失

那些别有用心的攻击者，正是看中了 Web 应用的价值，为了搏名获利，无时无刻不在对 Web 系统进行着攻击。随着 Web 应用技术的深入普及和大量核心应用使用，Web 系统攻击的技术门槛在不断降低，当攻击跟金钱、名誉甚至政治阴谋联系在一起的时候，我们的 Web 系统很可能已经处于多个攻击者的视线之内。正因为如此，网页挂马、数据篡改、网站钓鱼等 Web 系统安全事件层出不穷，Web 系统被攻击而遭受损失的媒体报道屡见不鲜 Web 系统安全形势日益严峻。而 Web 系统被攻击后造成的巨大损失，也已经成为 Web 系统所有者和访问者不能承受之痛。

2.1 经济损失

虽然没有一个确切的统计数字说明 Web 系统被攻击造成的经济损失有多大，但仅从媒体报道的事件中我们就能体会到，这个经济损失不但不小，并且对某些 Web 系统所有者来说，来说可能是致命的。尤其对与银行、证券以及游戏类网站，攻击成功后黑客可修改敏感数据，实施网页挂马，也可窃取用户的帐户信息，直接划转资金或者虚拟游戏币，不仅给用户带来直接的经济损失，而且会降低用户使用网站服务的信心，这对

金融类企业无疑是巨大打击，可能造成客户流失，形成间接经济损失。

2.2 名誉损失

网站代表着企业、政府机构等组织在互联网用户中的形象，试想一下，如果有一天，当你通过搜索引擎打开网站被提示有恶意代码，或者打开网站就看到防病毒程序报警，首页被篡改，甚至于留有一些侮辱性文字和图片，你会对这个网站的所有者产生什么样的质疑？组织的声誉将因此会受到多大影响？从不断翻新的媒体报道中，我们可以看到这种事件的主角不乏知名企业，甚至是知名的信息安全企业。各种公开的媒体报道举不胜举，但这只是冰山一角，仍有很多组织的网站正遭受着攻击，造成持续的名誉损失而浑然不觉。

2.3 政治风险

尤其对于政府机构的网站，一旦被法轮功、藏独等反动势力入侵并利用网站散播反动言论，不仅将会严重影响政府形象，而且会带来极大的政治风险，产生社会动荡，后果十分严重。2008 年 4 月，红心中国活动的发起网站“我赛网”，不断遭受来自欧洲黑客的攻击。网站的网页一度被篡改，出现藏独旗帜和大量反动语言，造成了非常严重的政治影响，最后工作人员不得不将服务器长时间关闭。2008 年 5 月，正当全国人们都在齐心协力抗震救灾时，有多个地方的地震局网站遭到入侵，攻击者发布虚假的地震消息，致使很多关注地震信息的人获知虚假信息并迅速传播，产生了极大社会恐慌，数十万人露宿街头，有家不敢回，这对已经深受震灾打击的人们来说无疑是雪上加霜。

3．任子行 网站统一监管系统解决方案

3.1 网站应用安全监管的需求分析

1) 安全监控需求

随着互联网技术的快速发展，网站攻击的门槛不断降低。各类型网站受到的安全威胁越来越多，为形象、各 Web 应用系统的正常使用。应实现以下基本安全需求：

- 监控网站页面内容完整、不被篡改；
- 监控网站存在的 SQL 注入、XSS、非法访问、信息泄露等应用层漏洞，从而提前解决潜在风险；
- 监控网站服务器可能存在的系统级漏洞，提前杜绝系统威胁；
- 监控网站，防止网站挂马而导致的客户满意度损失；
- 监控网站是否存在敏感信息，对于网站的敏感信息内容自行配制告警功能，方便管理者及时了解到发生的安全事件，可根据量化的标准，对网站的安全事件严重程度进行不同形式的告警，独具可能存在的政治风险和声誉损失；
- 监控网站是否被钓鱼，导致相关的名誉损失。

2) 应用监控需求

- 定期检查服务器健康状态，及时了解服务器状况；
- 及时、准确得到网络运营状态，便于进行紧急响应；
- 要能贯彻自上而下的监控需求，能了解所辖区域的网络营运情况。

3) 管理需求

- 以监控为主，必要时候进行干预，防止意外事情发生；
- 能定期生成每个网站的报表，关联趋势性分析；让管理员及管理者清晰的分析出网站当前的安全状况及趋势，可以作为信息安全建设决策分析依据；
- 对不同的管理员授权相应范围内的管理，大致分为高级管理员、普通管理员及日志审核员。
- 能分级管理管理，从而能”全面感知”应用和服务。

3.2 Web 网站监控预警平台

Web 应用与云计算技术具有天然的联姻关系。基于 SaaS（软件即服务）的云计算技术模型，对 Web 安全监控系统提出好的解决思路。任子行与方正宽带 IDC 合作，搭建 Web 安全监测系统，对用户提供基于云计算（SaaS）模型的 Web 安全监测服务。任子行提供 7×24 小时的实时网站安全监测服务。一旦发现您的网站存在风险状况，任子行安全团队会第一时间通知您，并提供专业的安全解决建议。同时，基于 SaaS 的 Web 安全监测系统结合公司安全专家团队为用户定期提供网站系统评估报告，及时、有效地掌握网站的风险状况及安全趋势，从而提供稳定、安全的 Web 应用环境。

3.2.1 监控预警系统模型

如上图所示，云监控中心提供由二大部分组成：

（1） 总控中心

总控中心提供三大功能：

- 用户自助管理

  用户可以注册到系统，进行自我评估和；同时查看当前网站系统运维情况信息汇总；

- 规模监控管理

  导入相关站点进行规模检测和防护处理；可以对垂直管理的下属机构进行评测监控处理，提早防范可能产生的外延威胁；

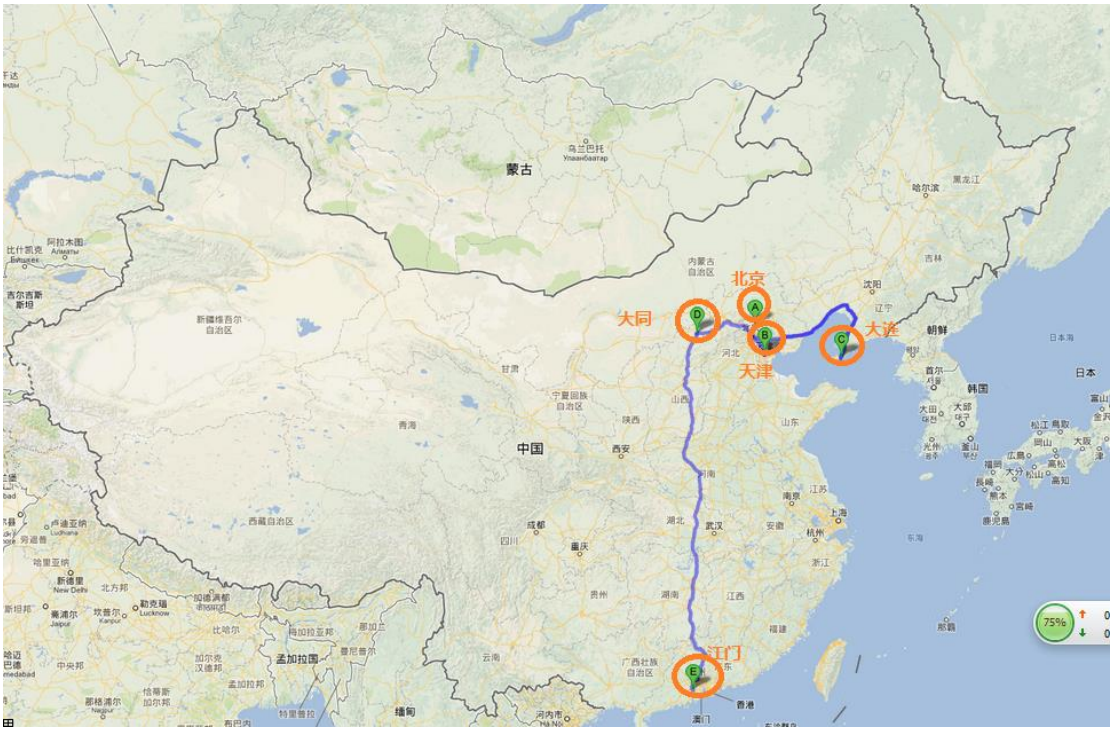
- 趋势分析处理

  针对系统具有的大量数据进行数据挖掘处理，预测、规整可能产生的攻击事前，提前预防。

（2） 监控探针

探针，主要完成信息抓取、分析等工作，探针根据业务情况部署在不同区域，从而尽快感知整个网页态势。当前的主要在全国 5 个节点设置有探头。

3.2.2 任子行云监控中心部署图



目前在北京、天津、大连、大同、江门的五个机房里边设置了探测中心，管理中心设在北京北科大厦机房， 我们将根据业务发展需求，逐步增加相关的监控中心

3.2.3 网站监控功能

任子行 网站安全监测服务涉及以下方面功能，如上图所示：

- Web系统扫描和漏洞扫描监控服务

  目前该系统支持远程OWASP定义的Web威胁和及其相关的漏洞扫描监控服务。通过远程的网站漏洞扫描服务 ,由任子行安全专家定期进行网站结构分析、漏洞分析，即时获得网站的漏洞情况，以及修补建议。

- 网站防钓鱼监控服务

  任子行的防钓鱼系统，只针对Web业务处理进行监控服务。任子行基于云计算技术（SaaS），具有先天的防钓鱼有事。通过构建可信URL数据库、IP信誉和自动化的扫描辅助以人工确认等综合手段，从而构建高效、准确的反钓鱼监控系统。

- 网页木马监测服务

  任子行基于“云安全”平台，采用业内领先的一体化挂马检测技术，高效、准确的识别网站页面中的恶意代码 ,从而使的网站管理员能够第一时间感知网站的安全状态，及时清除网页木马，避免给用户带来安全威胁，继而影响网站信誉。

- 远程网页篡改监测服务

  任子行对页面篡改监控提供二种模式处理：

  (1) 对于网站结构或者属性单一的用户，提供基于防护的篡改监控防护模式。用户可以根据自己情况，从管理中心下载与其服务器相对应的防篡改客户端，安装在自己服务器上，和管理中心互联，完成”监控-防护”的功能；

  (2) 基于扫描的网页篡改监控服务。通过远程实时监测目标网站页面的信息，一旦发现页面被篡改情况，第一时间通知用户。用户可根据任子行提供的安全建议及时修复被篡改页面，避免篡改事件影响扩散，给自身带来声誉和法律风险。

- 网页敏感信息监测服务

  远程实时监测目标站点页面状况，发现页面出现敏感关键词，第一时间通知用户。用户可参考任子行提供的安全建议及时删除敏感内容，避免事件影响扩散，给自身带来声誉和法律风险。用户也可以自定义所关心的敏感关键词。

- 网站应用监测服务

  应用监控主要涉及以下指标：网站可用性、网站从不同线路来访问得速度情况、网站响应时间，从而判断是否能达到最优、最安全的服务质量。通过任子行的监测系统，从各省运营商网络线路远程实时监测目标站点在多种网络协议下的响应速度、首页加载时间等反映网站性能状况的内容，一旦发现网站无法访问，第一时间通知用户。

- 域名监测(DNS)服务

  从各省运营商网络线路远程实时监测各地主流 ISP 的 DNS 缓存服务器和用户 DNS 授权服务器的可用性，以及它们对被监测域名的解析结果情况。一旦发现用户域名无法解析或解析不正确，第一时间通知用户。用户可参考任子行提供的安全建议恢复域名正常解析，避免域名不可用给访问者带来不好的体验。

- 安全情报分析

  定期提供面向Web的安全漏洞、安全咨询以及Web攻击趋势分析报告，便于掌握并且规避相关安全问题。主要提供

  1) 针对安全漏洞的分析和修复方案；
  2) 重大事件之前的安全预防以及相关通告；
  3) 定期关于网站威胁的分析报告，同时及推送国内的重大安全事件

- 弱密码检测

  定期对目标系统进行密码检测，防止密码导致的泄密事件

4 任子行预警监控服务

项目	服务规格	通用版本	行业版本	定制版本	备注
监测服务	Web扫描	√	√	可选	
	漏洞扫描	√	√	可选	
	木马检测	√	√	可选	
	敏感信息监测	√	可选	可选	
	钓鱼检测	可选	可选	可选	
	Web应用检测	√	√	可选	
	篡改检测	√	√	可选	
监控频率	一周一次	可选	√	可选	
	一月一次	√	可选	可选	
检测报告	一周一次	可选	可选	可选	
	一月一次	√	√	可选	
页面监控	首页	√		可选	
	20页，深度2级		可选	可选	
	100页、深度3级				
管理特性	自查模块	可选	√	可选	

	统一监管模块	√	√	可选	
	分析及其预测报告	可选	√	可选	
	网页防篡改模块	可选	可选	可选	此模块按照每客户端收费
安全情报	漏洞分析预防	可选	√	可选	
	攻击趋势分析	可选	√	可选	
	国内安全事件通报	可选	√	可选	
Web 防护联动	与WAF联动，可以追根溯源	可选	√	可选	
服务	7×24		可选	可选	
	5×8	√	可选	可选	
告警方式	短信	可选	支持4组短信号码	可选	
	邮件	2个邮箱每站点	4个邮箱每站点	可选	
	电话	可选	可选	可选	
支持方式	IM、网络	√	√	可选	
	邮件	√	√	可选	
	电话	可选	√	可选	

5 技术支持

在保修期内，对于任何非人为的原因造成的设备缺陷或损坏，负责及时免费更换。用户报修后 8 小时内赶到现场提供免费服务，并在 24 小时内完成修复工作，未完成提供相同性能的备用设备给用户免费使用，维修好之后换回。

值班服务工程师使用最快的交通工具在 8 小时内赶到现场，紧急情况下项目负责人也必须到达现场进行指挥和协调。尽可能缩短从故障报出到恢复正常运行的时间，保证在甲方提出的提供 7×24 小时的故障服务受理和每周 7 天每天 24 小时在线技术支持；每次维修不超过 2 小时，报修后 24 小时内不能修复故障的，提供备用机。直至故障设备修复，在敏感时期、重大节假日我公司技术服务部门留守有专门的技术服务团队进行技术支持，对于用户或维护人员提出的修改设计的措施。进行快速响应。

提供详细技术资料并免费对用户（由用户方提供名单）进行技术培训（培训内容与采购人共同协商），培训目的和效果采购人能单独操作维护该系统设备，我们承诺培训时间与次数是以采购人能单独操作维护该系统设备为标准。

维修电话：400-700-1218

维修机构：当时办事处或代理公司