中国地质大学（北京）

信息网络中心文件

信息网络中心　　2013.5.15

数字校园应用系统的安全管理

我校数字校园建设于2008年，在统一身份认证、统一平台、统一门户的构架中，其核心是应用系统，主要包括：教务管理系统、研究生管理系统、学生工作管理系统、学生收发费系统、数字迎新系统、协同办公系统、人事管理系统、科研管理系统、财务管理系统、设备资产管理系统、实验室管理系统、后勤管理系统等。

数字校园应用系统成为校内主要部门的业务处理平台，也是广大教职工及学生的信息获取平台，内容涉及到教学、科研、学习、生活等方方面面。因此应用系统的安全管理就显得非常重要，一方面要保障应用系统的正常运行，一方面还要保障业务信息的安全。

1 系统架构

1、部署在校园内网

除了个别有特殊要求的应用，几乎所有的应用系统由校

园网防火墙隔离，部署在校园内网，校园网用户通过统一身份认证授权直接访问数字校园应用系统，校外用户通过VPN获取校内IP地址后再通过统一身份认证授权访问数字校园应用系统。

2、使用Linux操作系统

Linux比Windows操作系统更稳定：Linux更新无需重启，这意味着不需要停止Server，是真正的Server；Linux很少宕机；Linux处理多进程比Windows要好很多。

Linux比Windows操作系统更安全：Linux建立在Unix上，从开始就是为多用户设计的操作系统；几乎没有用户或应用可以访问内核；Linux也会被攻击，但是反应速度明显高于Windows。

3、应用与数据分离

为增强应用系统抗风险能力，将应用系统的应用服务器和数据库服务器分离，应用系统和数据库分别安装部署不同的服务器上，并对应用和数据库分别做数据备份。

4、数据库系统RAC模式

数字校园的核心业务系统都是使用Oracle数据库、并采用RAC双机并行模式。Oracle RAC并行模式与传统的双机热备方式不同。传统的双机热备环境中，始终有一台机器作为备用机，只有当主节点出现问题的时候才换切换到备用机上。而RAC是一种双机并行模式的架构，也就是说，两个节点的

集群节点间是并行运行并具有负载均衡关系，当一台主机出现故障或Oracle 进程宕机，RAC会自动漂移到另一台主机或Oracle 进程，RAC 模式极大地提高了系统的可靠性。

5、应用系统主备模式

对于关键的业务应用系统的应用程序，除了正式运行着的应用服务器，还专门搭建了与正式环境相同的备用应用服务器环境，并且无论是对应用程序升级还是对应用程序备份，主、备两套应用程序都同时处理，以确保正式运行的应用程序出现问题时，随时可以切换到备用应用程序上。

2 系统安全防护

1、操作系统密码策略

应用服务器的操作系统密码安全非常关键，对于操作系统密码的保护至少做到以下几点：

（1）所设置密码的安全强度要比较高，不能简单，如：至少 10 位以上，同时包含数字、大小写字母或特殊字符。

（2） 定期修改密码。

（3）密码不要记下来随手乱放，最好以加密手段来存储和记录密码

2、系统防火墙

防火墙对流经它的网络通信进行扫描，这样能够过滤掉一些攻击，以免其在目标计算机上被执行。防火墙还可以

关闭不使用的端口。而且它还能禁止特定端口的流出通信，封锁特洛伊木马。最后，它可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。防火墙具有很好的保护作用。入侵者必须首先穿越防火墙的安全防线，才能接触目标计算机。你可以将防火墙配置成许多不同保护级别。高级别的保护可能会禁止一些服务，如视频流等，但至少这是你自己的保护选择。

3、系统安全扫描

（1）采用专业化的漏洞扫描软件，定期对操作系统进行安全扫描

支持的操作系统漏洞包括：系统漏洞、WEB应用中间件漏洞、CGI应用漏洞、FTP类漏洞、DNS、后门类、网络设备漏洞类、缓冲区溢出、信息泄露、MAIL类、PRC、NFS、NIS、SNMP、守护进程、PROXY、强力攻击等1000种以上。

（2）从技术层面处理相应漏洞

漏洞扫描之后生成系统安全评估报告，我们对于扫描出的各类漏洞进行针对性地解决。如：进行组件补丁升级。

3 应用安全防护

3.1 应用安全访问控制

数字校园内网应用系统大多数是要面向广大教职工和学生的，对于教职工及学生登录应用系统的账号及初始密码的生成要满足数字校园的统一信息标准及基本的安全规则

要求。

应用系统的用户登录应用系统后在修改本人的密码时，密码的设置要求必须符合一定的规则，如：不能少于8位，必须至少同时包含数字和字母等。

应用系统的用户密码以MD5密文存储。

数字校园内网采用了基于LDAP的统一身份认证技术和基于CAS的单点登录集成，认证传输信息时采用https的双向ssl加密访问技术。

3.2 应用漏洞扫描

采用先进的web应用扫描工具，支持JSP,ASP,.NET,PHP等B/S结构的WEB应用，发现和解决web应用中的漏洞。

1、 定期漏洞扫描

（1）跨站脚本漏洞

"跨站点脚本编制"攻击是一种隐私违例，可让攻击者获取合法用户的凭证，并在与特定Web 站点交互时假冒这位用户。 这个攻击立足于下列事实：Web 站点中所包含的脚本直接将用户在 HTML 页面中的输入（通常是参数值）返回，而不预先加以清理。 如果脚本在响应页面中返回由 JavaScript 代码组成的输入，浏览器便可以执行输入中的代码。 因此，有可能形成指向站点的若干链接，且其中一个参数是由恶意的 JavaScript 代码组成。 该代码将在站点上下文中（由用户浏览器）执行，这授权它通过用户浏览

器访问用户所拥有的站点 Cookie 以及站点的其他窗口。攻击依照下列方式继续进行：攻击者诱惑合法用户单击攻击者生成的链接。 用户单击该链接时，便会生成对于 Web 站点的请求，其中的参数值含有恶意的 JavaScript 代码。 如果Web 站点将这个参数值嵌入在响应的 HTML 页面中（这正是站点问题的本质所在），恶意代码便会在用户浏览器中运行。

（2）注入漏洞

注入漏洞，特别是SQL 注入漏洞，Web 应用程序通常在后端使用数据库，以与企业数据仓库交互。查询数据库事实上的标准语言是 SQL（各大数据库供应商都有自己的不同版本）。Web 应用程序通常会获取用户输入（取自 HTTP 请求），将它并入 SQL 查询中，然后发送到后端数据库。接着应用程序便处理查询结果，有时会向用户显示结果。如果应用程序对用户（攻击者）的输入处理不够小心，攻击者便可以利用这种操作方式。在此情况下，攻击者可以注入恶意的数据，当该数据并入 SQL 查询中时，就将查询的原始语法更改得面目全非。例如，如果应用程序使用用户的输入（如用户名和密码）来查询用户帐户的数据库表，以认证用户，而攻击者能够将恶意数据注入查询的用户名部分（和/或密码部分），查询便可能更改成完全不同的数据复制查询，可能是修改数据库的查询，或在数据库服务器上运行 Shell

命令的查询。

（3）恶意文件执行

目标网站代码存在远程文件包含漏洞，允许攻击者直接上传恶意代码，控制目标网站;受影响的应用，包括PHP 以及XML 。文件上传功能可以让用户将本地文件系统的文件复制到Web 服务器，它提供一种将信息轻松自在添加到站点的方法。 不过，倘若未采取适当措施来确保这个能力不致滥用，攻击者可能会利用这个不安全的文件上载过程。站点有可能因为现有文件遭到覆盖而损坏，甚至有可能上载脚本档或二进制文件，再愚弄服务器运行它们，从而执行任意代码。

（4）直接对象引用隐患

直接对象引用是指开发商将内部执行对象，如文件、目录、数据库记录或关键字以URL链接地址或参数形式暴露给用户，导致敏感信息泄露通过验证用户输入使用，能够有效检测并阻断直接对象引用攻击，防止恶意用户非法访问限定文件或目录等敏感信息。

（5）跨站点请求伪造漏洞

跨站点请求伪造攻击通过强制已登录受害者的浏览器向目标网站发送预认证请求，然后强制受害者浏览器执行有利于攻击者的行为，跨站点请求伪造攻击是一种强大的Web应用攻击方法，通过对来自Web 系统响应的cookies 和参数注入密码校验功能来阻断会话劫持和跨站点请求伪造

攻击。Web 应用系统中表单的发布由插入的包含加密令牌的表单验证参数的会话所约束，该加密令牌能证明该配置行为(发布一个含有表单的页面)是Web 应用防御系统的一部分。

（6）认证和会话管理隐患

帐户凭据和会话令牌往往没有得到适当的保护。攻击者通过该隐患获取用户的密码，密钥，认证令牌或假冒其他使用者的身份通过对会话的Cookies 进行客户端IP 地址校验来检测阻断认证和会话管理攻击。

（7）加密存储隐患

应用程序测试过程中，检测到将未加密的登录请求发送到服务器。由于登录过程所用的部分输入字段（例如：用户名、密码、电子邮件地址、社会保险号码，等等）是个人敏感信息，建议通过加密连接（如 SSL）将其发送到服务器。任何以明文传给服务器的信息都可能被窃，稍后可用来电子欺骗身份或伪装用户。 此外，若干隐私权法规指出，用户凭证之类的敏感信息一律以加密方式传给网站。

（8）通信隐患

当有必要为保护某些敏感通信而进行数据传送加密，Web 应用数据传送频繁失败，可以选择HTTPS 协议来访问Web 资源。此外HTTP (明文)请求可以重定向使用HTTPS 。

（9）无限制URL 访问隐患

通常Web 应用敏感信息保护模块通过不显示敏感信息

的URL 链接来防止未经授权的用户访问Web 敏感信息。攻击者利用该隐患可直接访问敏感信息URL，获取Web 敏感信息。访问敏感信息URL 需要有效的用户会话，未经验证的用户(用户没有一个有效的会话)的会话请求，Web 防御系统应将对其进行阻断，来防止此类安全隐患。

2、增加web应用过滤器

针对某些类别的漏洞及安全隐患，在关键的 web 应用中增加过滤器，减少受攻击的机会，提高其安全防护功能。 已经增加的过滤器目前能够防护的安全漏洞及隐患主要有以下几类：

（1） SQL 注入漏洞

（2） HTML 注入

（3） SCRIPT 注入

（4） 跨站脚本攻击（XSS）

（5） CSRF-跨站请求伪造漏洞

4 应用安全监测

web 应用挂马、web 应用篡改等事件通常都是突发性事件，持续时间短，但是挂马事件、篡改事件一旦产生，将会给学校形象、信息网络甚至核心业务造成严重的破坏。而通过定期的安全扫描或安全检查并不能够第一时间发现这些已经产生的严重风险事件并做出相应的处理工作。因此我们

使用专业的网站安全监测系统（WSM）进行安全监测、实时告警，来主动地发现web应用的风险隐患，并及时采取修补措施，达到降低风险、减少损失的目的。

WSM 提供实时的对漏洞、挂马的监测功能，以及提供网页篡改、网页敏感内容和网站平稳度的监测。我们根据 web 应用的关注度，来配置不同的监测策略，再根据web应用中不同页面的重要程度，设置关键页面，并配置对关键页面进行一定频率的监测，可以实现了多维度、不同粒度的风险监测。

5 数据库备份

1、本地备份

数据库每天凌晨以Oracle Dump方式自动备份在本地数据库服务器上。

2、Atempo异机备份

利用数据备份软件 Atempo TimeNavigator 的备份复制功能每天自动将本地数据库备份文件复制到到备份服务器的虚拟磁带库上。

3、Atempo异地备份

利用数据备份软件 Atempo TimeNavigator 的备份复制功能每天自动将本地数据库服务器上备份的dmp文件每天自动复制到教四楼备份服务器上。

4、备份恢复

一旦发生数据库崩溃或数据库遭受攻击，立即向信息中心 DBA 报告，同时暂缓上传数据。DBA 按照下述步骤行数据恢复：

（1）首先从本地数据库服务器上取出最新备份，检查备份文件是否损坏，如果文件完好，则使用此文件进行数据恢复。

（2）如果本地数据库服务器上的备份文件已损坏，则取出备份服务器虚拟带库上的备份文件，检查备份文件是否损坏，如果文件完好，则使用此文件进行数据恢复。

（3）如果备份服务器虚拟磁带库上的备份文件也损坏，则利用异地教四楼备份服务器上的备份文件恢复数据。

（4）如果所有备份均无法恢复，应立即向有关厂商请求紧急支援。