**玉溪市第二人民医院**

**网站技术运维方案**

**一. 前言**

网络的迅猛发展为经济和社会发展带来了巨大的影响，不断完善的网络信息化，使政府、科研机构、大型企事业都受益无穷，并有效提高了工作效率。  不过，人们在享受着信息化成果的同时，也同样面临被网络攻击和网络危害的风险。近年来，针对网站的攻击越来越多，利用网站及服务器的漏洞进行网站入侵，入侵成功后进行网页篡改、网页挂马、订单修改、用户欺骗、盗取他人银行账户，甚至有些攻击者非法入侵网站后，进行法轮功宣传、散布台独、藏独反动言论等，这些都为国家和企事业带来了不可估量的损失作为网站管理者，若能主动发现网站服务器漏洞和Web 网站漏洞， 并积极采取补救措施， 就可以很大程度降低网站安全风险， 减少损失。 然而，这一切都需要专业的人员，进行长期的监控，相应的投入会比较大。针对这一情况，网站管理人员，可以将网站的安全维护工作，交由第三方的专业公司或机构，由第三方对网站进行安全维护，从而在最小投资的情况下，将安全隐患拒之门外，保障网站的持续、可靠、安全运行。

因此，在建设网络和网站系统信息安全的基础上，要充分加强日常网站安全预防和运维工作，并能够完善在发生安全事件时的应急响应能力。

**二. 网站安全状况**

目 前 ， 主 流 的 网 站 架 构 是Linux + NGINX + Mysql + PHP 。Linux 是操作系统， NGINX 、Mysql 、PHP 归属于 Web 网站，所以一个网站的安状况，需要同时分析服务器操作系统的安全状况，以及 Web 网站的安全状况。任何一方存在安全漏洞和隐患，都可能为网站带来严重的安全威胁。

通常情况下， Web 网站设计者在设计网站时， 会将绝大多数精力花在考虑满足用户应用，如何实现业务等方面，而很少考虑网站开发过程中所存在的安全漏洞。这些漏洞在不关注网站安全的用户眼里几乎不可见，在正常的网站访问过程中，这些漏洞也不会被察觉。但对于恶意的攻击者而言，这些漏洞很可能会对网站带来致命的危害。同时，如果 NGINX 、Mysql 、PHP 等程序存在安全漏洞，也可能导致网站被攻击

**三. 网站安全维护服务**

一般情况下，攻击者要入侵一个网站，会从以下几个方面入手：

1) 利用网站源代码自身的安全漏洞进行入侵， 如 SQL 注入、XSS 跨站。

2) 利用搭建网站程序的安全漏洞进行入侵，如 NGINX 漏洞， Mysql 漏洞。

3) 利用操作系统的安全漏洞进行入侵，如缓冲区溢出。

所以，对网站进行安全维护，需要同时从服务器、 Web网站、安全应急响应 3 个方面进行。这样既可保证服务器的安全，也可确保网站的安全；既可对服务器和 Web 网站进行全程维护和定期检查，也可在出现安全事件时进行及时的应急响应

3.1 服务器安全维护

对服务器的安全维护工作，包括日常维护和安全检测两个部分，具体如下：

3.1.1 日常维护

1) 操作系统安装、配置、日常维护。

2) 操作系统账户审核， 对账户和密码进行安全性审核， 确定账户的安全性。 3) 操作系统日志分析，确定系统运行的状态。

4) 操作系统上必须开启服务的安装、配置、日常维护，如NGINX 、Sendmail 。具体的服务根据用户的需求而定。

5) 数据库的安装、配置、日常维护。

6) 用户网站的数据备份

3.1.2 安全检测

1) 操作系统漏洞检测。 定期对系统进行漏洞扫描， 并模拟黑客从互联网上对网站服务器进行渗透攻击，以检测系统的安全状况

2) 操作系统安全加固， 禁止不必要开放的端口、 不安全的服务，启用防火墙安全策略，设置安全的并发会话等。

3) 在检测到操作系统的安全漏洞时，及时对其进行修补，以保障服务器的安全。

3.2 WEB 网站安全维护

网站安全维护， 是一项为了防止 web 网站被非法入侵 （如篡改网页、盗取网页数据、网站挂马），对 web 网站进行的授权漏洞检测和安全防御工作。一般采用的方法是，从互联网模拟黑客对 web 网站进行扫描测试，找出 web 网站中可能被黑客利用的弱点，并进行修复。通过对 web 网站上的漏洞进行有效检测和修复，可很大程度上确保网站的安全。

我们的 web 网站扫描测试，可对 web 网站的漏洞进行有效检测。

1) SQL 注入。 检测 web 网站是否存在 SQL 注入漏洞， 如果存在该漏洞，攻击者通过SQL 注入攻击可轻易获得网站的后台管理权限， 甚至网站服务器的管理权限。 2) XSS 跨站。检测 web 网站是否存在XSS 跨站脚本漏洞，如果存在该漏洞，攻击者可进行 Cookie 欺骗、网页挂马等攻击。

3) 网页挂马。检测 web 网站是否被黑客或恶意攻击者非法植入了木马程序。

4) 上传漏洞。检测 web 网站的上传功能是否存在上传漏洞，如果存在此漏洞，攻击者可直接利用该漏洞上传木马获得 Webshell 。

5) 源代码泄露。 检测 web 网站是否存在源代码泄露漏洞，如果存在此漏洞，攻击者如果存在此漏洞，攻击者可直接下载网站的源代码。

6) 隐藏目录泄露。检测 web 网站的某些隐藏目录是否存在泄露漏洞，如果存在此漏洞，攻击者可了解网站的全部结构。

7) 数据库泄露。 检测 web 网站是否在数据库泄露的漏洞，如果存在此漏洞，攻击者通过暴库等方式，可以非法下载网站数据库。

8) 管理地址泄露。检测 web 网站是否存在管理地址泄露功能，如果存在此漏洞，攻击者可轻易获得网站的后台管理地址。

9) 弱口令。检测 web 网站的后台管理用户，以及前台用户，是否存在使用弱口令的情况。

10) 网站绝对路径泄露。通过该漏洞，攻击者可以知道网站在服务器上的物理位置，如“ 站的后台管理地址”

3.3 网站安全监测

网站安全监测服务，是一款托管式服务，无需安装任何硬件或软件，无需改变目前的网络部署状况，无需专门的人员进行安全设备维护及分析日志。您只需要将监测的网站域名告知我方人员，许可后即可获得 7×24 小时的网站安全监测服务，一旦您的网站遇到风险状况后，鸿信安全监测团队会在第一时间与您确认，并提供专业的解决方案建议。除此之外，鸿信安全专家会定期为您出具周期性的监测报告，让您整体掌握网站的风险状况及安全趋势。

通过专业化的服务产品来实时监测和周期度量网站的风险隐患， 您可以轻松评估您网站的安全状态， 衡量改进情况，能够将网站管理人员从繁重的日常安全维护工作中解放出来，降低投入和管理成本，获得最为专业、有效的服务，并确定对行业和政府法规的遵从情况。

“网站安全监测服务”主要包括以下几方面的内容

1. 远程网站漏洞扫描：网站的风险漏洞是站点被攻击的根源，通过远程的网站应用层漏洞扫描服务，由安徽森淼安全专家定期进行网站结构分析、漏洞分析，用户无需采购任何 Web 应用扫描产品，即可获得网站的漏洞情况，以及修补建议。

2. 远程网页木马监测：基于“云安全”平台，采用业内专业工具及检测技术，可高效、准确识别网站页面中的恶意代码，使网站管理员能够第一时间得知自己网站的安全状态，避免由于网站被挂马给访问者带来的安全隐患。

3. 网页敏感内容监测：实时监测目标站点是否出现一些敏感关键字，如果发现敏感内容，会在第一时间通知用户。用户也可以自定义所关心的敏感关键字。

4. 网站平稳度检测：对服务站点进行实时远程访问平稳度的动态监视，跟踪重点对象的访问平稳度动态变化情况，并根据严重程度及时发出报警信号。

5.网页篡改监测：实时监测目标站点页面状况，发生页面被篡改情况，第一时间通知用户，避免给自身带来的声誉和法律风险

3.4 安全应急响应

安全应急响应是指网站在出现安全事件时，及时对事件进行详细分析、 定位、 排查，以最快速度恢复网站的正常运行，确保网站数据的安全，减小安全事件带来的损失。网站一旦出现安全事件，不论在什么时候，均立即触发安全应急响应服务。这里的安全事件既包括黑客攻击、网页挂马、数据窃取等主动攻击，也包括感染病毒等被动攻击

**四. 服务内容**

我们为您提供的网站的技术及安全维护服务，具体服务内容如下。

1) 每月进行服务器的日常维护工作，检查服务器工作状态。

2) 每月对网站数据进行备份。

3) 每季度对服务器进行1 次漏洞检测， 确定服务器的安全性，并出具相应的漏洞检测报告。

4) 每季度对 web 网站进行 1 次扫描测试， 确定 web 网站的安全性，并出具相应的 web 网站扫描测试报告。

5) 7 ×24 小时的网站安全监测服务。

6) 出现安全事件时， 5×8 的事件响应、处理及恢复， 4 小时内电话响应， 1 个工作日内到达现场，最快时间恢复网站运行，最大程度减少安全事件带来的损失。

7) 在网站日常内容维护中协助完成发布、修改、审核信息中有异常的地方。

8）若有网站功能扩展及新增功能，协商方案解决

**五. 每季度提供相应的检测报告**

**六. 服务报价**

|  |  |  |
| --- | --- | --- |
| **项目** | **内容** | **备注** |
| 云主机维护 | 云服务器日志、补丁、安全扫描 |  |
| 日常维护 | 网站巡查，异常解决 |  |
| 数据备份 | 网站数据及网站文件备份，动态镜像备份 |  |
| 漏洞检测 | 安全检测及协助网安处理异常 |  |
| 网站代码升级 | 网站核心代码更新及升级 |  |
| 技术协助 | 内容运维协助 |  |
| 报价 | 人民币： 元， 报价含税费等其他一切费用 | |