政府门户网站安全防护解决方案

□

政府门户网站安全现状

□□□ WEB应用是当前业务系统使用最为广泛的形式。根据 Gartner 的调查，信息安全攻击有 75% 都是发生在 Web 应用层而非网络层面上。同时，数据也显示，2/3的WEB网站都相当脆弱，易受攻击。据美国国防部统计，每1000行Web代码中存在5~15个漏洞，而修补一个漏洞通常需要2~9小时。

□□

根据CNCERT的最新统计数据，2007年CNCERT共接到网络安全事件报告4390件。2007年我国大陆被篡改网站总数达到了61228个，同比增长1.5倍;其中政府网站(.gov.cn)被篡改3407个，占大陆被篡改网站的7%。CNCERT统计显示，大陆地区约有4.3万个IP地址主机被植入木马，约有362万个IP地址主机被植入僵尸程序。从以上数据可以看出，提高业务网站的安全防护，是保障业务正常进行的必然前提。

□□

因此，对于影响力强和受众多的门户网站，需要专门的网页(主页)防篡改系统来保护网页和保障网站内容的安全。

□□政府门户网站的潜在风险

□□

政府门户网站因需要被公众访问而暴露于因特网上，容易成为黑客的攻击目标。其中，黑客和不法分子对网站的网页(主页)内容的篡改是时常发生的，而这类事件对公众产生的负面影响又是非常严重的，即：政府形象受损、信息传达失准，甚至可能引发信息泄密等安全事件。。网页篡改者利用操作系统的漏洞和管理的缺陷进行攻击，而目前大量的安全措施(如安装防火墙、入侵检测)集中在网络层上，它们无法有效阻止网页篡改事件发生。目前，政府门户网站常因以下安全漏洞及配置问题，而引发网页信息被篡改、入侵等安全事件：

□□1.

网站数据库账号管理不规范，如：使用默认管理帐号(admin，root，manager等)、弱口令等;

□□2.

门户网站程序设计存在的安全问题，网站程序设计者在编写时，对相关的安全问题没有做适当的处理，存在安全隐患，如SQL注入，上传漏洞，脚本跨站执行等;

□□3.

WEB服务器配置不当，系统本身安全策略设置存在缺陷，可导致门户网站被入侵的问题;

□□4. WEB应用服务权限设置导致系统被入侵的问题;

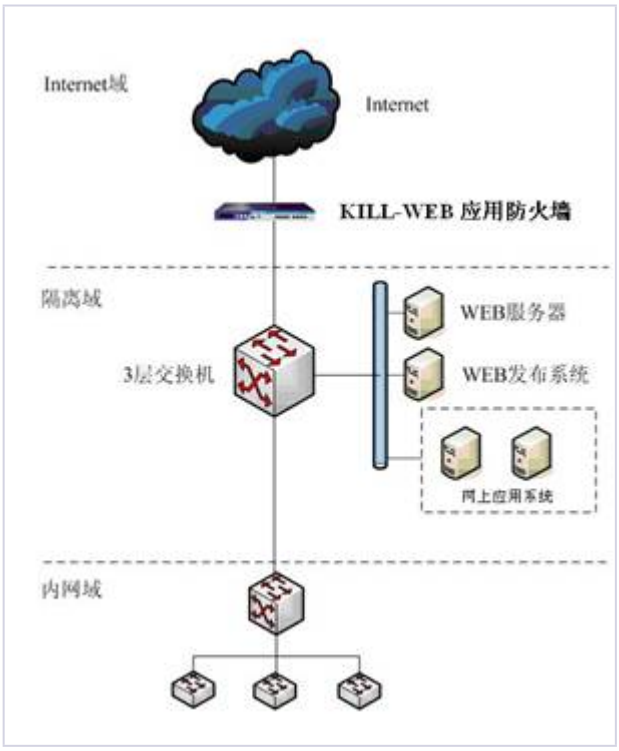
□□5. WEB服务器系统和应用服务的补丁未升级导致门户网站可能被入侵的安全问题等。

□□政府门户网站安全防护解决方案

□□

根据目前政府门户网站可能存在的安全隐患及风险，冠群金辰公司给政府门户网站提出如下安全防护解决方案：

□□在政府门户网站信息系统的Internet边界上或者WEB服务器的前端部署KILL-WEB应用防火墙，并在Web防火墙上实施以下安全策略：



□□

□□I

对政府门户网站及网上系统进行全面的安全防护，过滤如SQL注入、跨站脚本等因传统防火墙不能防护的安全问题;

□□I 对政府门户网站进行WEB隐藏，避免利用扫描软件对其进行信息获取分析;

□□I 设置政府门户网站页面防篡改功能及恢复功能，避免恶意篡改页面;

□□I 对门户网站进行应用层控制，限制部分用户上传文件及对敏感页面的访问;

□□I

对访问门户网站信息系统网络进行安全监控以及审计，对可疑IP行为进行全面跟踪分析。

□□WEB应用防火墙的价值体现

□□I 彻底防御因网站篡改带来的负面影响

□□

政府门户网站作为国家行政管理机构发布政策的窗口，其页面一旦被篡改将造成多种严重的后果。部署KILL-WEB应用防火墙，通过其缓存原始网站页面可有效防护其网页不被篡改。

□□I 彻底防御应用层针对WEB的攻击

□□KILL-WEB应用防火墙内置上千种WEB应用攻击特征库，可有效抵御各种已知的、针对WEB服务器的攻击行为，保障政府门户网站系统的安全运行。

□□I WEB应用的审计工具

□□KILL-

WEB应用防火墙不但具有强大的防攻击、防篡改功能，还可通过其审计分析功能对过滤数据进行分析;对异常IP用户进行行为跟踪及对敏感用户进行过滤等。

□□I 即插即用保证业务连续性

□□KILL-

WEB应用防火墙产品的部署十分便捷，无需改变现有的网络拓扑结构。安装后，只需简单的配置安全策略，就可为应用系统提供强大的安全防御，可保障政府门户网站的业务连续性。

我国政府网站存在的安全问题

CNCERT 对近期被Barbaros-DZ

组织篡改的部分我国政府网站进行安全评估，发现这些政府网站均采用了免费开源软件PowerEasy SiteWeaver CMS 的6.6 及6.6

以下的版本作为站点建设和管理软件，而这些软件均存在一个SQL

注入漏洞，而该漏洞的攻击代码早在2009 年2 月20

日就已经被披露。通过该漏洞，黑客可以对数据表执行用户数据新增或编辑等操作，包括变更用户名、邮箱等。

以上评估结果也映射出我国大多数政府网站的安全现状。这些政府单位对网站安全仍然缺乏足够的认识。网站的安全体系十分脆弱，对于安全事件并不具备预警、防护以及恢复的能力。主要表现在以下几个方面：

·缺少对网站系统安全性的整体评估

政府网站建设完成后，

服务商往往只会做一些功能性的测试就马上将其上线运行。缺少整体的安全性测试。也因此不能及时发现网站系统所存在的安全漏洞。这些漏洞如果不及时修补，很容易被黑客所利用，最终对网站造成严重危害。

·对于WEB攻击的防护能力有限

据统计调查，

现阶段政府网站系统的安全措施还多数仅限于购置防火墙等对病毒的防护，但是现行的各

类攻击行为，如SQL注入、XSS等，大多是利用WEB服务软件以及网站程序自身的漏洞和缺陷进行攻击，而政府机构原有的安全措施（如安装防火墙、入侵检测）则主要集中在网络层上，无法对此类攻击事件形成有效的监控和防护。

·被攻击后不能及时恢复

很多政府网站被篡改后，因为系统缺少有效的恢复机制，导致被篡改的页面公布于众，给政府单位造成十分恶劣的影响。还有些网站虽然在接到报告后能够恢复，但由于缺乏必要的经常性维护，并没有根除安全隐患，从而遭到多次篡改。

因此，对于影响力强和受众多的门户网站，需要专门的网页(主页)防篡改系统来保护网页和保障网站内容的安全。

政府门户网站的潜在风险

政府门户网站因需要被公众访问而暴露于因特网上，容易成为黑客的攻击目标。其中，黑客和不法分子对网站的网页(主页)内容的篡改是时常发生的，而这类事件对公众产生的负面影响又是非常严重的，即：政府形象受损、信息传达失准，甚至可能引发信息泄密等安全事件。。网页篡改者利用操作系统的漏洞和管理的缺陷进行攻击，而目前大量的安全措施(如安装防火墙、入侵检测)集中在网络层上，它们无法有效阻止网页篡改事件发生。目前，政府门户网站常因以下安全漏洞及配置问题，而引发网页信息被篡改、入侵等安全事件：

1. 网站数据库账号管理不规范，如：使用默认管理帐号(admin，root，manager等)、弱口令等;

2. 门户网站程序设计存在的安全问题，网站程序设计者在编写时，对相关的安全问题没有做适当的处理，存在安全隐患，如SQL注入，上传漏洞，脚本跨站执行等;

3. WEB服务器配置不当，系统本身安全策略设置存在缺陷，可导致门户网站被入侵的问题;

4. WEB应用服务权限设置导致系统被入侵的问题;

5. WEB服务器系统和应用服务的补丁未升级导致门户网站可能被入侵的安全问题等。

政府门户网站安全防护解决方案

根据目前政府门户网站可能存在的安全隐患及风险，给政府门户网站提出如下安全防护解决方案：

在政府门户网站信息系统的Internet边界上或者WEB服务器的前端部署KILL-WEB应用防火墙，并在Web防火墙上实施以下安全策略：

1. 对政府门户网站及网上系统进行全面的安全防护，过滤如SQL注入、跨站脚本等因传统防火墙不能防护的安全问题;

2.对政府门户网站进行WEB隐藏，避免利用扫描软件对其进行信息获取分析;

3.设置政府门户网站页面防篡改功能及恢复功能，避免恶意篡改页面;

4. 对门户网站进行应用层控制，限制部分用户上传文件及对敏感页面的访问;

5. 对访问门户网站信息系统网络进行安全监控以及审计，对可疑IP行为进行全面跟踪分析。

WEB应用防火墙的价值体现

1.彻底防御因网站篡改带来的负面影响

政府门户网站作为国家行政管理机构发布政策的窗口，其页面一旦被篡改将造成多种严重的后果。部署KILL-

WEB应用防火墙，通过其缓存原始网站页面可有效防护其网页不被篡改。

2.彻底防御应用层针对WEB的攻击

KILL-

WEB应用防火墙内置上千种WEB应用攻击特征库，可有效抵御各种已知的、针对WEB服务器的攻击行为，保障政府门户网站系统的安全运行。

3. WEB应用的审计工具

KILL-

WEB应用防火墙不但具有强大的防攻击、防篡改功能，还可通过其审计分析功能对过滤数据进行分析;对异常IP用户进行行为跟踪及对敏感用户进行过滤等。

4.即插即用保证业务连续性

KILL-

WEB应用防火墙产品的部署十分便捷，无需改变现有的网络拓扑结构。安装后，只需简单的配置安全策略，就可为应用系统提供强大的安全防御，可保障政府门户网站的业务连续性。

网站安全检测

一、进行网站安全漏洞扫描

由于现在很多网站都存在sql注入漏洞，上传漏洞等等漏洞，而黑客通过就可以通过网站这些漏洞，进行SQL注入进行攻击，通过上传漏洞进行木马上传等等。所以网站安全检测很重要一步就是网站的漏洞检测。

扫描完后就可以查看网站所存在的漏洞和存在的网页，可以根据报告里面的建议进行漏洞修补，但请注意，在修改网页代码之前要先做好备份工作。　说明：对于发现的网站漏洞要及时修补。

二、网站木马的检测　网站被挂马是非常普遍的事情，同时也是最头疼的一件事。所以网站安全检测中，网站是否被挂马是很重要的一个指标。

其实最简单的检测网站是否有挂马的行为，很简单，直接开个杀毒软件扫描，看看有没有挂马提示就可以啦。当然还有直接去这些杀毒软件建立的网站安全中心，直接提交URL进行木马检测。

说明：网站被挂马是严重影响网站的信誉的，如有被挂马，请速度暂时关闭网站，及时清理木马或木马链接的页面地址。

三、网站环境的检测

网站环境包括网站所在服务器的安全环境和维护网站者的工作环境的安全

很多黑客入侵网站是由于攻击服务器，窃取用户资料。所以在选择服务器时要选择一个有保证的服务商，而且稳定服务器对网站的优化和seo也很有帮助的。

而站长或维护着所处的环境也非常重要，如果本身系统就存在木马，那么盗取帐号就变得很简单了。故要保持系统的安全，可以装瑞星，卡巴这些杀毒软件，还有就是帐号和密码要设置复杂一些。

四、其它检测　黑链检测，由于现在黑链的利润很高，故现在更多黑客入侵网站目的就是为挂链接，而被挂黑链会严重影响SEO的优化。

具体检测方法：

可以利用站长工具网里面工具中的“死链接就爱内测/全站PR查询”的选项，　将检测网站分析栏，选择“站外链接”，按“显示链接”按钮，就会列出一堆站外链接，在里

面可以查看有那些链接是PR比较低而且又比较陌生的链接就可能是黑链，将黑链删除就以

。

五、远程连接检测

打开宽带连接，进行宽带的检测和IP地址的检测。以防止恶意的窃取用户资料。

常见的针对Web应用的攻击有：

1、缓冲区溢出——

攻击者利用超出缓冲区大小的请求和构造的二进制代码让服务器执行溢出堆栈中的恶意指

令。

2、Cookie假冒——精心修改cookie数据进行用户假冒。

3、认证逃避——攻击者利用不安全的证书和身份管理。

4、非法输入——在动态网页的输入中使用各种非法数据，获取服务器敏感数据。

5、强制访问——访问未授权的网页。

6、隐藏变量篡改——对网页中的隐藏变量进行修改，欺骗服务器程序。

7、拒绝服务攻击——

构造大量的非法请求，使Web服务器不能响应正常用户的访问。

8、跨站脚本攻击——提交非法脚本，其他用户浏览时盗取用户帐号等信息。

9、SQL注入——构造SQL代码让服务器执行，获取敏感数据。

10、URL 访问限制失效——

黑客可以访问非授权的资源连接强行访问一些登陆网页、历史网页。

11、被破坏的认证和 Session 管理——

Session token 没有被很好的保护 在用户推出系统后，黑客能够盗窃 session。

12、DNS攻击——

黑客利用DNS漏洞进行欺骗DNS服务器，从而达到使DNS解析不正常，IP地址被转向导致网站服务器无法正常打开。

攻击手段举例说明

SQL注入

对于和后台数据库产生交互的网页，如果没有对用户输入数据的合法性进行全面的判断，就会使应用程序存在安全隐患。用户可以在可以提交正常数据的URL或者表单输入框中提交一段精心构造的数据库查询代码，使后台应用执行攻击着的SQL代码，攻击者根据程序返回的结果，获得某些他想得知的敏感数据，如管理员密码，保密商业资料等。

跨站脚本攻击

由于网页可以包含由服务器生成的、并且由客户机浏览器解释的文本和HTML标记。如果不可信的内容被引入到动态页面中，则无论是网站还是客户机都没有足够的信息识别这种情况并采取保护措施。攻击者如果知道某一网站上的应用程序接收跨站点脚本的提交，他就可以在网上上提交可以完成攻击的脚本，如JavaScript、VBScript、ActiveX、HTML 或 Flash 等内容，普通用户一旦点击了网页上这些攻击者提交的脚本，那么就会在用户客户机上执行，完成从截获帐户、更改用户设置、窃取和篡改 cookie 到虚假广告在内的种种攻击行为。

随着攻击向应用层发展，传统网络安全设备不能有效的解决目前的安全威胁，网络中的应用部署面临的安全问题必须通过一种全新设计的高性能防护应用层攻击的安全防火墙——

应用防火墙来解决。应用防火墙通过执行应用会话内部的请求来处理应用层。应用防火墙专门保护Web应用通信流和所有相关的应用资源免受利用Web协议发动的攻击。应用防火

墙可以阻止将应用行为用于恶意目的的浏览器和HTTP攻击。这些攻击包括利用特殊字符或通配符修改数据的数据攻击，设法得到命令串或逻辑语句的逻辑内容攻击，以及以账户、文件或主机为主要目标的目标攻击。

DNS攻击

黑客使用常见的洪水攻击，阻击DNS服务器，导致DNS服务器无法正常工作，从而达到域名解析失败，造成网站无法访问。

网站安全的防御措施

1、FTP密码尽量设置得复杂点，密码里面最好包含大写和小写的英文字母和数字以及特殊字符(如c7b64￥8f63ce687&)，这样黑客用弱口令扫描工具就扫描不到你的FTP用户名和密码了。

2、网站后台不要用默认路径和管理员账号及密码，现在网络上有很多通过默认路径猜解后台帐号密码的工具，如果不修改默认路径和管理员账号和密码，一些怀有不良企图的人很容易猜解到你网站后台账号和密码进入你网站的后台进行非法操作，也就给你网站安全留下了一个隐患，所有务必及时修改网站后台默认路径及管理员账号和密码。

3、更改网站数据库名，文件名也可以多几个特殊符号。

4、网站的注入和跨站漏洞也是黑客经常利用的漏洞。检查一下网站有没有注入漏洞或跨站漏洞，如果有的话就马上打上防注入或防跨站补丁，使黑客无可乘之机。

5、防患于未然，写入一些防挂马代码，让框架代码等挂马无效。

6、最好关闭网站的FSO权限。

7、设置好网站各个文件夹的读写权限。