

2009

# HuaTech 网站保护系统 技术白皮书

北京中软华泰信息技术有限责任公司

2009-3-18



## 目 录

1. 公司简介.....	- 1 -
2. 引言.....	- 2 -
3. <b>HuaTech 网站防护系统概述</b> .....	- 3 -
4. <b>HuaTech 网站防护系统主要功能</b> .....	- 4 -
4.1 恶意代码主动防御.....	- 4 -
4.2 网页的文件过滤驱动保护.....	- 4 -
4.3 防 SQL 注入功能 .....	- 5 -
4.4 轻量级 SSL 终止功能 .....	- 5 -
4.5 防跨站攻击.....	- 5 -
4.6 双机热备功能.....	- 5 -
4.7 抗网络攻击能力.....	- 6 -
4.8 采用内核性能优化和安全加固技术.....	- 6 -
5. <b>产品特性</b> .....	- 7 -
5.1 对未知病毒具备免疫能力 .....	- 7 -
5.2 更有效的网页防篡改技术.....	- 7 -
5.3 更简便的布署与管理过程 .....	- 8 -
6. <b>产品能解决的问题</b> .....	- 9 -
7. <b>接口设计说明</b> .....	- 10 -
7.1 型号.....	- 10 -
7.2 系统组成.....	- 10 -
7.3 接口配置.....	- 10 -
7.4 电气性能.....	- 10 -
7.5 参考的安全规范及标准.....	- 11 -
7.6 抗干扰性.....	- 11 -
8. <b>产品典型应用</b> .....	- 12 -
附录 1 常见问题解答 (FAQ) .....	- 13 -
附录 2 产品资质.....	- 16 -

# 1. 公司简介

北京中软华泰信息技术有限责任公司成立于 2000 年，是专业从事信息安全体系研究，信息安全产品研制、生产、销售企业。

公司一直把操作系统安全和信息应用系统安全作为产业方向。

近年来，先后参与国家发改委、科技部、北京市科委等重大产业发展研究项目，并成为国家与微软源代码级合作的技术承担单位。

公司坚持产、学、研相结合的发展方向，与北京交通大学、北京工业大学共同成立研究生培养基地，在为国家输送大批信息安全专业人才的同时也使公司具备了坚实的技术储备。

2008 年初，公安部为制订《等级保护方案设计规范要求》的国家标准，进行等级安全应用技术平台模拟系统搭建工作，公司在众多竞争者中脱颖而出，承接了目前最高等级四级系统的建设任务，并将于 2008 年 11 月底完成项目验收，从而成为等级保护国家标准 863 课题研究参与单位，目前正在配合国家主管单位参与国家重大支持项目的申请工作。

在四级安全应用支持平台模拟系统中公司将“网站应用”作为重点内容，并结合等级保护标准（GB-17859）和正在申报的国标《等级保护方案设计规范要求》研发成功“HuaTech 网站防护系统”。

产品一经推出，就引起国家安全主管单位的高度重视，已经在包括国家发改委、中国人民银行等重要部门进行推广使用，并因此获得“北京市政务信息安全 2008 年度应急处置协作单位”的资格，重点参与奥运保障尤其是网站安全保障工作。

公司的“HuaTechHuaTech 网站防护系统”是软、硬件相结合的产品，实现了从操作系统到应用系统的安全应用“管道式”封装，采用了多因子身份认证、全程访问控制的机制，以自主防御的体系结构作为设计目标，以等级保护国标为设备标准，彻底杜绝了 SQL 注入、跨站攻击和 WEB 服务器的木马、病毒攻击。保证了网站不被攻击、篡改。

公司今后将致力于等级保护的方案和产品提供。不断推出符合等级保护标准的安全产品，竭尽全力为国家的信息安全事业做出贡献。

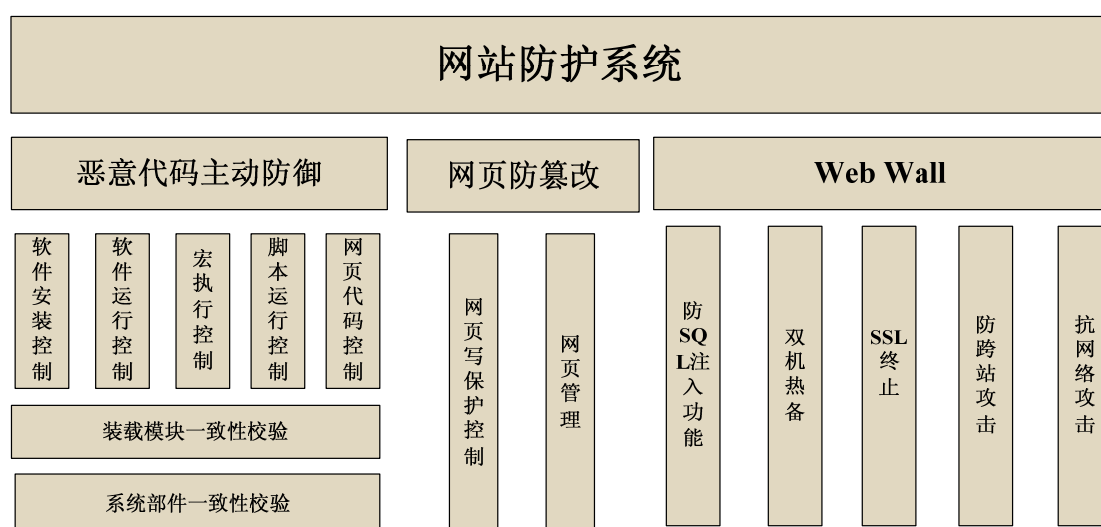
## 2. 引言

随着信息化迅猛发展，互联网已经成为人们工作和生活不可或缺的部分。据《第 20 次中国互联网络发展状况统计报告》显示，中国网民的数量已达到了 1.62 亿，成为了全球第二大网民国家。越来越多的政府机关、企事业等部门为了适应社会的发展，树立自身良好的形象，扩大社会影响，也纷纷建立起自己的网站。《国家信息化领导小组关于我国电子政务建设指导意见》中强调，国家“十五”信息化专项规划已经将电子政务作为国家信息化的重点内容。整个“十五”期间，从中央到地方政府，将有 60% 以上的政府业务和 30% 以上的政府对企业和公众的办公业务上网进行。可见，网站在信息发展中的重要作用，已经渗透至各个角落。然而，由于网站是处于互联网这样一个相对开放的环境中，各类网页应用系统的复杂性和多样性导致系统漏洞层出不穷，病毒木马和恶意代码网上肆虐，黑客入侵和篡改网站的安全事件时有发生。其中，以篡改网站最为恶劣，尤其是政府网站作为一级政府发布重要新闻、重大方针政策以及法规等的重要渠道，一旦被黑客篡改，将严重损害政府的形象，影响社会稳定。根据 CNCERT 调查报告显示，2007 年上半年，中国大陆被篡改网站的数量相比往年处于明显上升趋势，中国大陆被篡改网站总数达到 28367 个，比去年全年增加了近 16%。2007 年 1 月至 6 月期间，中国大陆政府网站被篡改数量各月累计达 1585 个。其中，每月被篡改的 gov.cn 域名网站占整个大陆地区被篡改网站的 6% 左右。网站频遭破坏的主要原因在于网站整体安全性差，缺乏必要的日常维护，有的网站虽然在接到报告后能够恢复，但并没有根除安全隐患，从而遭到多次篡改。

常见的破坏网站的方式主要有以下几种：1) 利用系统漏洞，使用缓冲区溢出方式获得管理员权限，从而任意修改网站内容，窃取信息。2) 利用病毒、蠕虫、木马和间谍软件等恶意代码，破坏系统。3) 利用 DOS、DDOS 等方式，造成服务瘫痪。4) 利用网站漏洞使用 SQL 注入攻击方式，获得系统或数据库管理员权限，从而任意修改数据库。5) 使用弱口令攻击，获得管理员权限，从而任意修改数据库。当前，如何解决黑客的恶意攻击，保证网站页面不被篡改，已经成为信息技术的一个前沿课题。

### 3. HuaTech 网站防护系统概述

HuaTech 网站防护系统，是华泰公司网络安全研发团队在广泛技术积累和应用实践经验的基础上，对目前国内外相关计算机数据进行详尽搜集、分析、仔细研究，对同类安全产品进行纵横比较分析，自主研制开发的一套针对网站网页保护的防护系统。整个系统由软件和硬件部分共同组成，主要实现了恶意代码主动防御、网页的文件过滤驱动保护、防 SQL 注入、双机热备、抗网络攻击能力等功能。以期防止黑客入侵、网站篡改，从而更有效地对网站网页安全进行保护。



## 4. HuaTech 网站防护系统主要功能

### 4.1 恶意代码主动防御

利用信任链机制，对系统中所有装载的可执行文件代码（例如，EXE、DLL、COM 等）进行控制，所有可执行文件代码在加载运行之间都需要先经过检验，只有通过验证的代码才可以加载。这种方式可以有效阻止恶意代码的运行。验证方法为：首先为系统制定可信白名单，即允许执行代码文件的 hash，在进程装载二进制文件之前首先计算其 hash 值，并与可信白名单进行比较，不在白名单中的一概不允许执行，这样既可以防止恶意代码运行，又可以防止恶意代码依附其他系统或应用程序运行，确保执行代码的真实性和完整性，同时效率上不会有明显影响。

### 4.2 网页的文件过滤驱动保护

利用操作系统漏洞，应用缓冲区溢出等方法可以获得管理员权限，从而可以任意修改网页文件，以达到攻击的目的。

针对这种攻击方式，采用对象相关（Object—Specific）保护方式来保护网页不被篡改。即网站管理员可以自行选择需要保护的网页文件设定为受控对象，对于每一个受保护的對象，管理员为其设定一个对象相关授权码。对象相关保护方式是一种不基于系统用户身份的访问控制技术，对于所有受保护的對象，HuaTech 网站防护系统在操作系统内核对其加以保护，在不知道对象相关授权码的情况下，即使是系统管理员，系统也禁止其对于受保护对象（比如主页）的任何特定操作，比如修改内容、删除、重命名等。

通过对象相关保护方式，即使攻击者拿到系统管理员的权限，由于不知道受控对象的授权码，因而也无法对其进行修改，从而可以有效阻止溢出类攻击对系统网页的篡改。

对于 Web 服务（例如，IIS、APACHE）的相关配置文件也采用同样的方式进行保护，防止通过修改配置文件达到篡改网页的目的。

但是对于受保护对象的读操作没有任何的限制，因而可以保证 Web 正常向外提供服务。只有在提供授权码的情况下才可以对受保护对象进行修改，使得管理员可以方便的更新网页内容。

## 4.3 防 SQL 注入功能

随着 B/S 模式应用开发的发展，使用这种模式编写应用程序的程序员也越来越多。但是由于这个行业的入门门槛不高，程序员的水平及经验也参差不齐，相当大一部分程序员在编写代码的时候，没有对用户输入数据的合法性进行判断，使应用程序存在安全隐患。用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想得知的数据，这就是所谓的 SQL Injection，即 SQL 注入。

HuaTech 网站防护系统可以通过高效的 URL 过滤技术，把 SQL 注入的关键字过滤掉，从而有效的避免网站服务器受到 SQL 注入攻击。

## 4.4 轻量级 SSL 终止功能

如今，几乎所有的安全应用都使用 HTTPS 确保通信的保密性。然而，SSL 数据流采用了端到端加密，因而对被动探测器如入侵检测系统（IDS）产品来说是不透明的。为了阻止恶意流量，HuaTech 网站防护系统可以终止 SSL 安全连接，对数据流进行解码，以便检查明文格式是否含有恶意的流量。

## 4.5 防跨站攻击

跨站攻击（XSS）又叫 CSS（Cross Site Script），跨站脚本攻击。它指的是恶意攻击者往 Web 页面里插入恶意 html 代码，当用户浏览该页之时，嵌入其中 Web 里面的 html 代码会被执行，从而达到恶意用户的特殊目的。HuaTech 网站防护系统通过先进的数据包正则表达式匹配原理，可以准确地过滤数据包中含有的跨站攻击的关键字。从而保护用户的 WEB 服务器安全。

## 4.6 双机热备功能

HuaTech 网站防护系统支持双机热备功能，从而提高系统的稳定性和可靠性。两台 Web Wall 分为主机和从机，在主机工作的同时，从机处于实时监控主机的工作状态，这时所有对内部网络的保护工作由主机完成。当主机因不可抗力而工作异常时，从机能够及时发现问题并立即接替主机的工作，并报警通知网络管理员。待主机故障排除并接入网络后，主机接

管对内网的保护工作，从机则切换为监视状态，继续侦测主机的状态。

## 4.7 抗网络攻击能力

作为一种网络安全防护设备，HuaTech 网站防护系统在网络中自然成为众多攻击者的首要目标，所以抗攻击能力也是 HuaTech 网站防护系统的必备功能。该系统采取多种安全措施，可以防范 Internet 环境中的攻击，如：抗端口扫描、抗 DDOS 攻击等。

## 4.8 采用内核性能优化和安全加固技术

HuaTech 网站防护系统性能的优劣直接影响到它能够被广大客户所接受。对一些用户对响应时间非常敏感的服务必须做好充分的优化工作，否则用户会对 HuaTech 网站防护系统的性能产生疑问。我们借鉴了许多国外的相关资料，针对 HuaTech 网站防护系统中的服务模块，采用多种内核性能优化技术，大大提高了 HuaTech 网站防护系统的工作效率以及系统本身的健壮性。

## 5. 产品特性

### 5.1 对未知病毒具备免疫能力

目前市场上的计算机病毒防杀类产品安全滞后性已经不能满足用户尤其是机构(包括政府和企业)用户的业务安全要求,每一次的大规模病毒爆发都伴随着用户业务和经济上的巨大损失。市场迫切需要一种更加积极主动的安全技术和产品来阻止包括未知恶意代码在内的安全事件的发生,本产品正是满足了这种需求,不仅可以防范已知的病毒、木马、蠕虫,而且对未知恶意代码具备防范能力。

本产品已经过国内某权威机构的上千种病毒样本的攻击测试,能够抵御包括病毒、木马、流氓软件在内的各种恶意代码攻击。

### 5.2 更有效的网页防篡改技术

目前市场上常见的网页防篡改技术有以下三种:

1) 外挂轮询技术: 利用一个网页读取和检测程序, 以轮询方式读出要监控的网页, 与真实网页相比较, 来判断网页内容的完整性, 对于被篡改的网页进行报警和恢复。

2) 核心内嵌技术: 将篡改检测模块内嵌在 Web 服务器软件里, 它在每一个网页流出时都进行完整性检查, 对于篡改网页进行实时访问阻断, 并予以报警和恢复。

3) 事件触发技术: 利用操作系统的文件系统或驱动程序接口, 在网页文件的被修改时进行合法性检查, 对于非法操作进行报警和恢复。

外挂轮询方式以轮询方式检测监控网页, 在两次检测中间就会出现一个时间间隙, 如果攻击发生在这个时间间隙中, 则被篡改的网页内容已经被提供出去, 危害已经造成, 再恢复就没什么意义了。并且由于从外部不断地和独立地扫描 Web 服务器文件, 因此对 Web 服务器形成相当的负载, 并且扫描频度(亦即安全程度)和负载总是矛盾的。

核心内嵌技术需要对每一个流出的网页进行完整性检查, 如果浏览人数众多, 网页需要频繁的被检测, 将会极大的影响系统的性能。

以上三种方法还有一个共同的安全隐患就是都需要备份要监控的网页, 以便在网页被篡

改之后能够恢复。但是其备份服务器也面临着被攻击的风险，一旦备份的网页也被篡改，就没有了恢复的可能。

而我们的保护方式禁止任何非法的网页修改行为，就不存在恢复的问题；同时对于正常的访问行为不做任何的处理，因而对系统性能没有任何的影响。

## 5.3 更简便的布署与管理过程

目前常见的防止 SQL 注入的方式为在网页代码中加入过滤语句，但这种方式是在应用层基础上实现，需要针对不同的网页作不同的处理，不能通用。我们采用网络中间层驱动（NDIS）进行过滤，可以支持所有的网站服务。

## 6. 产品能解决的问题

- 1) 利用系统漏洞，使用缓冲区/栈溢出等方式的攻击。攻击者即使通过这类攻击获得了系统管理员的权限，但是由于不知道受保护对象的授权码，因此也就无法修改受保护对象。通过将主页及相关配置文件设置成系统保护对象，可以有效保护 Web 内容不会被篡改。
- 2) 恶意代码类攻击。通过信任链机制可以阻止恶意代码被 Web 服务器加载运行，从而确保病毒、蠕虫、木马和间谍软件等恶意代码无法在 Web 服务器上被激活运行，避免系统管理员因为疏忽或者其他途径导致的系统安全隐患。
- 3) SQL 注入攻击。SQL 攻击注入使用的语句在网络驱动层就被过滤，从而无法对数据库造成攻击。

## 7. 接口设计说明

### 7.1 型号

HuaTechHuaTech 网站防护系统（企业级）；

HuaTechHuaTech 网站防护系统（电信级）。

### 7.2 系统组成

HuaTechHuaTech 网站防护系统由恶意代码主动防御子系统、网页防篡改子系统和 Web Wall 子系统等三部分组成。其中恶意代码主动防御子系统、网页防篡改子系统为软件实现，Web Wall 子系统是一个高速稳定的硬件平台和经过安全加固的操作系统的完美结合体。我们采用 B/S 结构，对 HuaTech 网站防护系统利用 WEB 界面统一管理。

### 7.3 接口配置

HuaTechHuaTech 网站防护系统（企业级）的标准配置为：

4 个 10/100 以太网控制器，RJ45 接口（桥接口 1、桥接口 2、桥接口 3、管理口）

2 个 CONSOLE（双机热备、Console）（RJ45）

HuaTechHuaTech 网站防护系统（电信级）的标准配置为：

4 个多模光口模块（桥接口 1、桥接口 2、桥接口 3、桥接口 4），4 个 10/100/1000 以太网控制器，RJ45 接口（桥接口 5、桥接口 6、桥接口 7、管理口）

2 个 CONSOLE（双机热备、Console）（RJ45）

### 7.4 电气性能

电源

220V/50Hz 3.0A（最大） 260W（最大）

环境规范

运行温度：0 - 45 摄氏度

非运行温度：-20 - 65 摄氏度

相对湿度：10 - 90% @40 摄氏度，非冷凝

## 7.5 参考的安全规范及标准

UL 1950

EN 41003

AS/NZS 3260

AS/NZS 3548 Class A

CSA Class A

FCC Class A

EN 60555-2

VCCI (ClassII)

## 7.6 抗干扰性

IEC - 1000 - 4 - 2 (ESD)

IEC - 1000 - 4 - 3 (辐射敏感性)

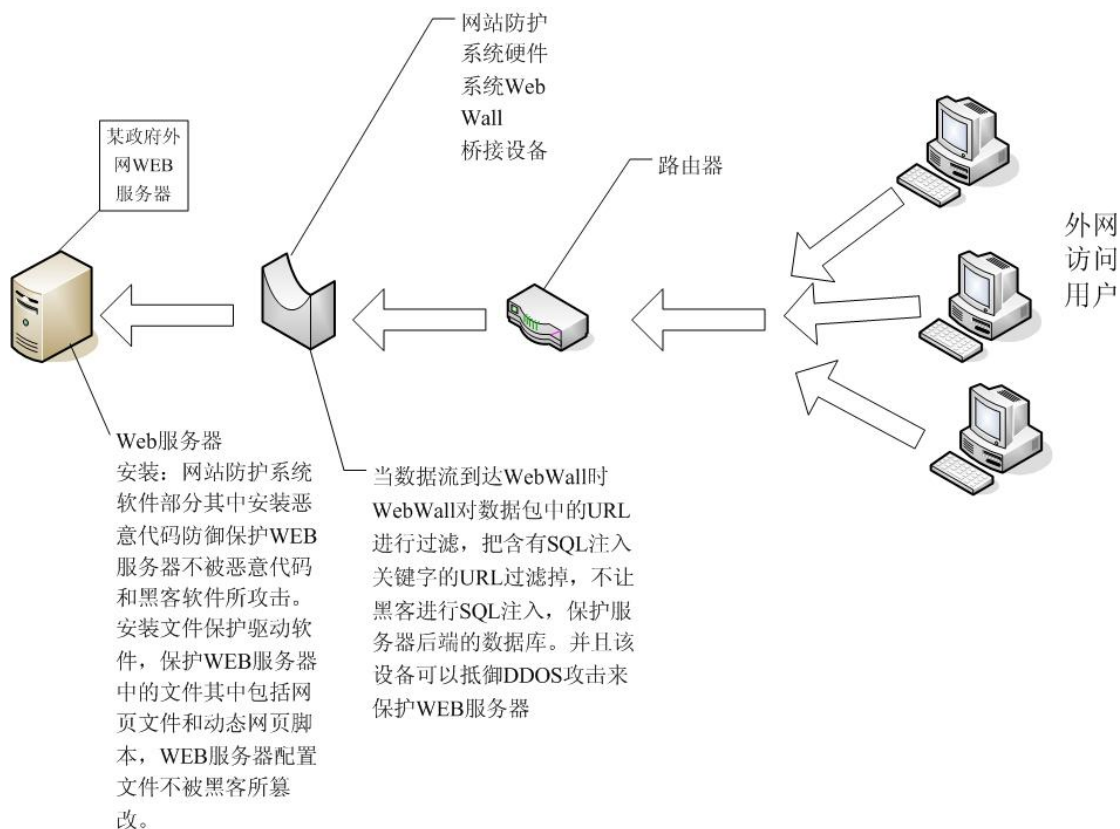
IEC - 1000 - 4 - 4 (电快速瞬变)

IEC - 1000 - 4 - 5 (电涌)

IEC - 1000 - 4 - 3 (谐波)

## 8. 产品典型应用

产品典型应用方案图如下



某政府机关 HuaTech 网站防护系统典型应用图

## 附录 1 常见问题解答 (FAQ)

### Q1 本产品的核心是什么？竞争对手的情况？

A: 本产品的核心内容包括：1) 防止恶意代码对网站服务器的破坏；2) 防止黑客通过溢出类攻击破坏网页内容；3) 防止黑客通过 SQL 注入攻击篡改系统网页。

其它主要功能包括：1) SSL 支持；2) 抗 DoS/DDoS 攻击。

目前没有此类技术的竞争对手。市场上的网页防篡改技术都是采用文件指纹比对、然后恢复的方式，这种方式一般都存在性能和安全空档问题，它们的另一个缺点是不支持动态网页的保护，对需要频繁更新的静态网页也十分地不方便。

### Q2 是否能保护动态网页不被篡改？

A: 通过 SQL 注入过滤可以防止动态网页被篡改。如果问题中的动态网页是指论坛内容，那就不叫篡改了，这种情况下，大家都可以提交发言内容，但内容安全需要斑竹控制了，这属于另一个范畴的安全控制了。

### Q3 动态网页如何保护？

A: 首先大家了解下什么是动态网页。动态网页 URL 后缀是以 .asp, .jsp, .php, .cgi 等形式为后缀名的，并且在动态网页网址中有一个标志性的符号“？”，如页面网址为：

[http://www.dangdang.com/product\\_detail/product\\_detail.asp?product\\_id=8915738](http://www.dangdang.com/product_detail/product_detail.asp?product_id=8915738)

这里说的是动态网页，与网页上的各种动画，滚动字幕等视觉上的“动态效果”没有直接关系，动态网页也可以是纯文字内容，也可以是包含各种动画内容，这些只是网页具体内容的表现形式，无论网页是否具有动态效果，采用动态网站技术生成的网页都称为动态网页。

中软华泰 HuaTechHuaTech 网站防护系统是可以保护动态网页的，因为动态网页是通过网站脚本来实现网页的动态显示，而网站脚本是一个一个的文件。HuaTech 网站防护系统通过文件过滤驱动技术对脚本进行保护避免被黑客所修改从而避免网页和网站结构被篡改。另外还有 SQL 注入防护，它可以避免动态网站的数据库被黑客篡改。这样就构成了对网页的整体保护。

### Q4 授权码由谁来掌控？

A: 由网页内容的维护人员负责管理, 包括创建、更新、废除。本产品可以支持多网页维护人员模式, 即每个维护人员负责自己管理权限内的内容保护。

**Q5 管理员是否也可以更改网页?**

A: 如果问题中的管理员是指系统管理员, 答案是不可以的, 因为他/她没有可以修改网页的授权码。通过对象相关访问控制机制, 网站的网页维护人员是可以修改更新他/她负责的网页内容部分。

**Q6 黑客如果入侵管理员, 那是否也可以更改其他内容?**

A: 如 Q5, 即使是真正的系统管理员, 他/她也无法更改指定的网页内容。但是为了保证系统的可用性和兼容性, 本产品并不追求对系统其它所有内容实施完全的防护, 因此黑客可能入侵系统并将系统破坏, 导致系统瘫痪, 但是他/她不能改变受保护的网页内容。

**Q7 如果管理员的密码安全级别够强, 能够防止黑客入侵, 那干吗要使用本产品?**

A: 一定要区分系统管理员和网页维护人员这两个角色的区别。黑客攻击并不一定需要系统管理员的密码(口令)。此处的密码级别够强是指网页维护人员维护网页时所需要的授权码。当然, 系统管理员的口令/密码的管理也是信息安全中的一个最基本要求。

**Q8 通常管理员不是制作网页的人, 制作网页的人必然要授权码, 而制作网页的人可能不止一个, 那么如何来维护安全?**

A: 每个维护人员对自己维护的网页都有自己的授权码, 授权码是网页文件所拥有的属性, 而不是某个维护人员的属性。任何人只要知道某个网页文件的授权码, 他/她就可以改动、删除该网页, 因此授权码的安全性很重要。维护人员可以为每个网页文件创建一个不同的授权码, 只要他/她觉得管理这些授权码不是一件多么困难的活。

**Q9 如果服务器被攻击至死机了怎么办? 技术上可能会出现什么样的状况?**

A: 如 Q6, 本产品是一种“宁死不屈”类的产品, 其主要目标是将网页篡改这类恶性事件风险降低为系统故障级别。万一黑客不辞辛苦, 不求任何回报地把网站服务器搞死, 那就最多再重装一遍系统。从攻击分析理论看, 现在的黑客一般也不会这么没有“追求”。

**Q10 如果出现问题, 是否可以远程解决问题?**

A: 本产品的管理支持远程和本地管理两种方式。当然, 如果不幸宕机, 那就只好现场解

决了，比如被黑客弄死了。

**Q11 对于 WEB 容器的保护是如何实现？对于所有的 WEB 容器像：Apache、WebSphere、Tomcat、IIS 如何保护，都应该保护哪些配置文件？**

A: 因为 WEB 容器主要是 WEB 服务的框架它主要也是由文件组成，只要用 HuaTech 网站防护系统将其保护起来就可以。只要文件不被黑客修改 WEB 容器的安全性就可以保障。对于应该保护那些配置文件那就要具体问题具体分析了。这主要由系统管理员根据不同的软件来作出决定。

**Q12 对于数据库本身的保护如何做？**

A: HuaTech 网站防护系统中数据库的防护是从网站入侵的角度来解决数据库的安全问题。而网站入侵中对于数据库的入侵方式最主要的是 SQL 注入。而其他数据库的入侵主要手段不是通过 URL 注入实现的。这类数据库的入侵的防护可由数据库审计类的软件来进行保护。

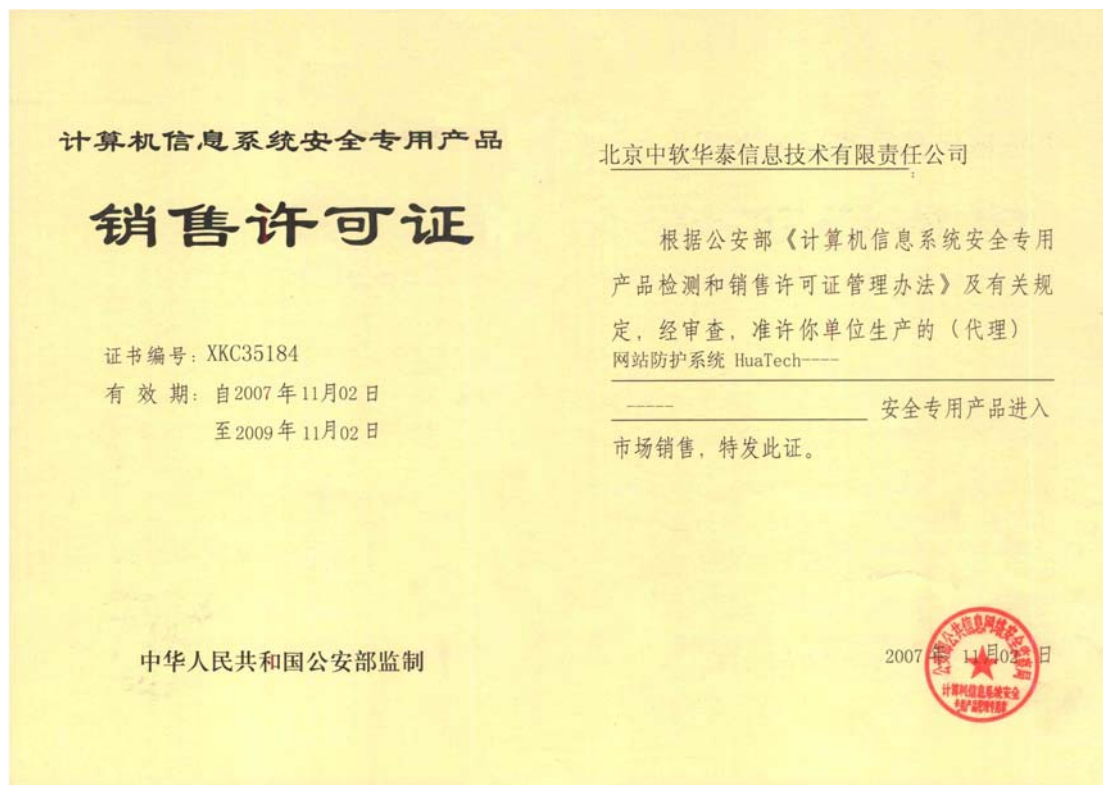
**Q13 现在系统的应用程序管理中有白名单管理，如果在已经运行的网站安装 HuaTech 网站防护系统的时候是如何来制作白名单的？尤其是对于 Windows 里已有的 DLL 文件，这些文件中很有可能就有木马或者是病毒？**

A: 在已经运行的系统中如何来制作白名单的具体方法已经在 HuaTech 网站防护系统的用户手册详细说明了。对于一个已经运行的 Windows 系统中的 DLL 文件有可能是病毒或木马的问题。我们主张在安装 HuaTech 网站防护系统前用户使用不同的杀毒软件来清除病毒或木马。系统清除干净后安装 HuaTech 网站防护系统。我们的软件防护系统属于系统进程管理类，因为他的主要功能是对系统进程进行管理并不具有病毒代码特征识别。所以它可以使病毒和木马等恶意代码的进程不被启动这样就可以保护服务器免受恶意代码的攻击了，而对以前服务器中是否被注入病毒，HuaTech 网站防护系统没有能力识别出来，只能用户使用杀毒软件来清除病毒。

**Q14 如何进行网站操作系统和一些软件的升级？**

A: 网站的操作系统升级时用户会从新安装操作系统只要把 HuaTech 网站防护系统从新安装即可。对于一些软件升级问题我们主张不要频繁升级服务器中的软件，尤其是对一些系统类的软件升级。如用户升级软件 HuaTech 网站防护系统只要手动更新一下白名单即可。

## 附录 2 产品资质





## 国家信息安全认证 产品型号证书

(注册号: CNITSEC2008TYP614)

兹证明:

北京中软华泰信息技术有限责任公司

(北京市海淀区北三环西路32号恒润中心1811室 邮编: 100086)

开发的下列产品:

HuaTech 网站防护系统 (V1.0/百兆)

经中国信息安全产品测评认证中心测试、检验, 符合:

GB/T 18336-2001 《信息技术 安全技术 信息技术安全性评估准则》

标准的要求, 获准国家信息安全产品型号认证。

此证书仅适用于该产品的上述版本或型号

证书签发日期: 2008年1月30日

三年内认证监督符合至2011年1月29日有效

批准人 王贵和



国家认可注册号:  
Registration Number: CNAB081-P