Web应用防火墙技术白皮书

BLUE AISEC

关键词：服务器，WAF，网关，HTTP

摘　要：本文介绍了WAF技术的应用背景，描述了WAF技术的实现与运行机制，并简单介绍了WAF技术在实际环境中的应用。

缩略语：

缩略语	英文全名	中文解释
WAF	Web Application Firewall	WEB应用防火墙
HTTP	HyperText Transfer Protocol	超文本传输协议
XSS(CSS)	Cross Site Script	跨站脚本攻击
SQL	Structured Query Language	结构化查询语言

目 录

➢ 概述

➢ Web安全现状

随着环球信息网时代的到来，Web业务平台已经成为企业信息化中流砥柱，大部分企业都在Web平台上架设了自己的业务应用。Web应用平台给企业及用户带来的诸多方便的同时，企业的业务系统也经受着严酷的挑战。业务系统的多元化及互联网的高速发展，引起大量网络爱好者及黑客们的强烈关注，导致Web应用平台潜在威胁也在快速的增长。他们将注意力从以往对传统网络服务器的攻击逐步转移到了对 Web 业务的攻击上。

近几年，众多网络爱好者及黑客出于多种目的，将注意力从传统的网络攻击转变到了Web业务攻击上面来，同时国内爆发了大量由于Web安全漏洞引发的安全事件，大到政府网站，小到贴吧、社区，都受到了黑客的攻击，对企业及个人的经济及生活带来诸多不便。

➢ Web应用防火墙

在Web安全问题急剧增加的催动下，出现了Web应用防火墙。从广义上面讲：Web应用防火墙是一款增加Web应用安全指数产品。现在常见的Web应用防护多为硬件设备，架设在Web应用平台前端，为Web应用平台提供了一个忠实可靠的安全护卫。

总体上说，Web应用防火墙应该具备以下几点功能：

1.审计功能：审核统计经过设备的HTTP报文数量及会话，对出现问题进行分析，提出分析报告；

2.访问控制功能：用来对Web应用平台访问进行控制，包括主动访问空及被动访问控制；

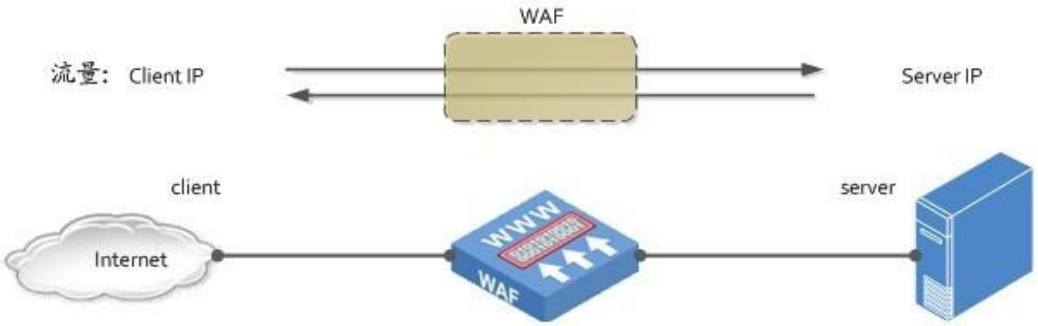
3.网络管理：提供反向代理模式、转发控制、诊断工具等功能；

4.Web攻击防护功能：Web防火墙核心功能，为Web应用平台提供安全防护，阻止攻击对应用平台造成不必要的损失。

➢ 部署方式

➢ 透明模式

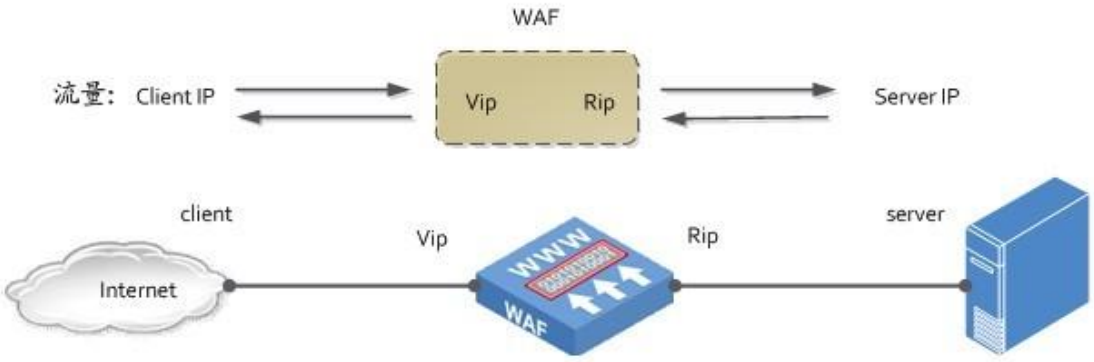
如图所示，透明模式，即WAF设备不改变上下行设备配置，直接部署在两台已运行的设备之间。在透明模式下无需对现有网络结构进行调整，可做到即插即用。



部署特点： 快速，简便，能够做到即插即用，先部署后配置。

➢ 反向代理模式

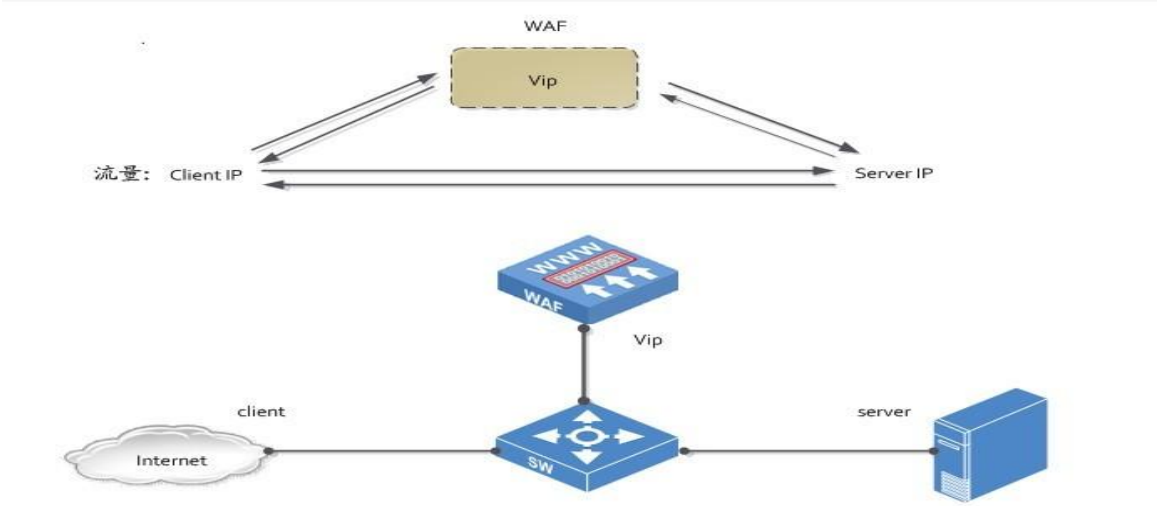
如图所示，反向代理模式是指WAF设备部署网络主干中，客户端通过访问虚拟IP做代理访问后台服务器。



部署特点：需要预先规划好网络部署结构，可以开启负载均衡等功能。

➢ 旁路模式

如图所示，旁路模式指WAF设备不作为后台服务器和客户端之间的路由设备，而是旁挂在 路由设备上。



部署特点：能够不改变原有网络拓扑结构，对原有业务可以无缝接入，可配置负载均衡，

等网络优化业务。

➢ 全方位Web防护功能

➢ 参数攻击防护

OWASP最新的“Web应用十大安全风险”中，前两位分别是注入攻击和XSS(跨站式脚本攻击)，这两种攻击方式均是与HTTP请求参数密切相关的。参数攻击防护的重要性可见一斑。

- Sql 注入攻击防护

Sql注入通常是由于应用程序缺乏对输入数据进行校验所引起的。黑客一般会把一段含有sql语句数据发送给解析器，再经由解释器将数据转恢复成指令执行。Sql注入攻击所造成的后果通常都很大，一般整个数据库的的信息都能被读取或篡改，甚至能够获得包括管理员在内的权限。通常攻击者都会先对SQL注入漏洞的判断，即寻找注入点；然后判断后台数据库类型；最后获取相关权限，进行真正有危险行的攻击。BlueAiSec WAF中SQL注入的特征库中囊括了注入点寻找、猜测数据库类型、猜测权限结构、添加新数据库用户和系统用户、添加权限、猜测数据表结构、备份数据库、目录遍历、上传WEBSHELL、备份日志等特征。实际中攻击净荷可以出现在HTTP请求的任何位置，比如请求字符串、POST数据、cookie、自定义或标准的HTTP头部以及URL路径的部分内容中，BlueAiSec WAF支持上述位置中存在威胁部分进行检测。当攻击者的攻击报文通过设备时，将会对报文中潜在威胁的部分进行特征匹配，如果是我们认为的攻击特征，将针对这一报文进行告警和阻断，防止恶意请求对数据进行篡改。防御工作主要通过以下几个方面进行：

1.针对动态字符串构造或动态SQL语句，我们通过参数化语句来替换原有的动态查询语句，这样即实现了防护，又拥有了相对现代数据库而言效率很高的优势；

2.针对输入我们进行输入验证，以保证其符合应用中定义标准的过程；简单到参数值为一种数据类型，也可以复杂到使用正则表达式或业务逻辑进行验证。针对这一种方法我们使用了白名单（正验证）和黑名单（负验证）；对于简单的或已被确认为攻击性语句进行直接黑名单匹配；针对复杂的、潜在威胁的语句，我们将对其进行语法及词法的分析来确认其是否为安全性语句。这里指的语法及词法是针对于新兴的数据及比较老的但依然被沿用的数据库语法及词法；

3.编码输出查询语句；针对这一方法，我们针对不同的数据库进行了不同的编码处理，将潜在威胁的代码变为其他安全代码的一部分，从而有效的组织恶意用户在特定的查询中利用SQL注入漏洞进行攻击；

4.针对输入编码或多重编码的语句，我们将对其进行正规化处理；由于实际中是无法拒绝接收包含编码格式的输入，所以我们寻找到不同编码的的解码方式，对上述语句进行一次或多次解码，由于这个方法比较容易出现错误，我们编写大量函数及算法来针对其进行解码以达到我们需要分析的最终形式来判断其安全性；

- Xss 攻击防护

XSS指的是黑客在Web页面中增添一段恶意html代码，当用户访问该页或触发某项事件时，调用了嵌入在Web页面里面的html代码，从而黑客达到其特殊目的。WAF设备针对这类攻击构建一个特征库，里面包含脚本关键字、标签关键字、事件关键字等特征，同时规约出相关的正则表达式；首先对用户提交的数据进行相应的解码，转换其出现的不规则字符，从而达到我们希望看到的格式，再对这段数据进行检测，匹配特征及正则表达式，阻断含有恶意代码或脚本的请求。同时我们将对输出到页面上的数据进行编码，使得已经存在的恶意代码失去其相应的威胁。

- 命令注入防护

随着web服务器平台的迅速发展，我们已经能够使用内置的API与服务器的操作系统进行几乎任何必须得交互。在正确使用下，这些API可以帮助开发者访问文件系统、连接其他进程、进行安全的网络通信等。但是有时候开发者往往直接向服务器发送操作系统命令，如果向操作系统传入用户提交的输入命令，就很有可能受到命令注入攻击，使得攻击者能够提交专门设计的输入，修改开发者想要执行的命令。BlueAiSec WAF系列产品针对这一问题设计大量函数，通过查找匹配各种操作系统命令及其常见变形规约，严格限制系统参数长度，阻断元字符等方式来有效的阻止黑客进行地各种形势下的命令注入攻击。

- 目录遍历攻击

目前存在很多迫使应用程序执行对文件系统进行读取或写入数据的web功能。为了达到这种潜在威胁方式操作地执行，黑客专门设计并提供此类输入，从而达到访问开发人员设置的具有安全隐私类文件，即目录遍历漏洞。黑客可以利用这些漏洞读取大量安全信息或具有一定价值但又具有隐蔽性的信息，篡改用户或服务器信息等具有威胁的行为。BlueAiSec WAF系列产品具有完备的特征库及精密的算法分析，能够通过对输入的语句进行智能分析，将确认其是否携带危险或潜在威胁，将会通过特征匹配，规约通式匹配来进一步确定其将带来的危险性，如果确定其含有请求目录异常的行为，将对这条恶意访问行为进行阻断防护。

➢ 参数篡改防护

- 对域名对应的 URL 下的特征的参数进行防护

BlueAiSec WAF系列产品通过对特征及其参数进行双重规约，设定其数值范围，检查客

户端请求报文中特定的特征对应的参数是否在规定范围之内，避免客户端输入非法参数值，从而大大减少利用参数传入潜在危险的请求。

➢ HTTP协议攻击防护

- HTTP 请求正规化检查

目前黑客攻击手法层出不穷，很多会利用协议盲点，通过诸如拆分攻击的形式进行恶意攻击。针对这一现象，BlueAiSec WAF系列产品通过对HTTP协议请求方法（GET、POST、PUT、OPTIONS等以及自定义），版本（HTTP/1.1、HTTP/1.0、HTTP/0.9），协议格式等进行正规化校验，将格式不在正规化范围内的报文进行防护，从而达到了避免出现通过协议盲点进行拆分攻击的恶意攻击。

对URL总长度可依据业务类型进行限制，有效的防止畸形的URL对服务器解析造成的压力；对URL部分的请求参数的总个数、总长度、参数名和参数值的长度等协议属性进行限制。

- Cookie 正规化检查

随着Cookie是出现与使用，黑客开始将触手伸至这里，通过Cookie携带异常信息，修改添加其原有的数值，导致服务器无法正常的时候Cookie中的内容，这无疑是给客户带来巨大的麻烦。为解决这一问题，BlueAiSec WAF系列产品将请求中Cookie 部分进行校验，防止通过畸形Cookie窃取服务器中用户私有信息或误导服务器做出错误的判定。

- 请求头正规化

随着信息技术的发展，请求头中的各个字段也逐步被业务系统进行了各种各样的应用，请求头字段也成为了黑客瞄准的一个新的攻击点，例如针对Referer进行攻击，可对统计站点来源的系统进行伪造和其他类型的攻击。针对请求头，BlueAiSec WAF提供9个预定义的常见头域的自定义正规化规则，以及多达32项自定义正规化规则的能力，可灵活的针对请求头域个字段进行正规化控制。针对头域的个数和长度也提供了相应的正规化能力，对一些异常长度的头域字段造成的逃逸尝试也起到了正规化的控制作用。

- Cookie 加密

服务器发送客户端报文中的Cookie值一般存放其内部生成的session值，这个数值就是确定客户端与服务器直接连接的钥匙，不准许被客户端或恶意使用者篡改。如果被恶意篡改将会窃取到用户安全隐私信息，对客户及服务器造成不必要的损失。针对这一问题，BlueAiSec WAF系列产品将通过对应答报文中的set-cookie字段对cookie值进行摘要或者加密，通过httponly的时候禁止用户对cookie进行查看修改，再将加密后的cookie值返回客户端，防止客户端修改cookie信息；同时针对恶意使用者进行的cookie重放，cookie篡改进行了缜密的分析，严格摒弃这类保温通过设备访问服务器。从而达到对此危险进行防护。

➢ HTTPS协议攻击防护

- HTTPS 卸载

HTTP 卸载是指 ASP WAF 在网络中对外提供 HTTPS 的服务，检查完毕攻击后（HTTPS 检测与 HTTP 检测功能基本类似，仅仅是将 HTTPS 的加密协议进行解密处理），将与最终的服务器进行 HTTP 的会话，此种模式可以有效的减轻服务器的负载压力。

同时针对 HTTPS 的一些攻击行为进行过滤，防止利用 HTTPS 协议级别的漏洞对服务器的安全性进行攻击和破坏。

- HTTPS 加载

HTTP 加载与 HTTPS 的卸载相反，是指 ASP WAF 在网络中对外提供 HTTP 的服务，检查完毕攻击后，将与最终的服务器进行 HTTPS 的会话，此种场景主要为了解决客户端到 WAF 之间的链路为可信，但是 WAF 到服务器之间为不可信的链路的情况。

同时针对 HTTPS 的一些攻击行为进行过滤，防止利用 HTTPS 协议级别的漏洞对服务器的安全性进行攻击和破坏。

- HTTPS 双向加载卸载

HTTPS 双向加载卸载即综合两种方式，在网络中 ASP WAF 提供对外的 HTTPS 服务，在设备上进行 HTTPS 协议层面的攻击检测后，解密为 HTTP 协议，继续进行 HTTP 协议级别的攻击检测，最终利用 HTTPS 协议整形能力，将检测过攻击后的 HTTP 协议数据封装成 HTTPS 数据发送到最终的服务器。

➢ 缓冲区溢出攻击防护

缓冲区溢出攻击指的是利用缓冲区漏洞，对运行程序或系统进行破坏的攻击。正常情况下程序检是不允许输入数据长度超出缓冲区长度,但是绝大多数程序都认为数据长度和我们为其申请的空间大小一致,这就给黑客留下了缓冲区溢出攻击的遍历条件。BlueAiSec WAF系列产品能够对HTTP请求行和请求头双向流进行检测，通过特征检测和阈值阻断来保护Web服务器正常运作。

➢ 网站目录扫描防护

目前存在一些网站目录扫描软件通过将内置或自己填写的常用路径对服务器发起请求链接，分析服务器返回的报文信息，判断该目录是否存在，从而进行下一步危害操作。BlueAiSec WAF系列产品具备完备的目录字典，并定期更新发布新版本；通过内置高精度算法对请求目录字典中内容的频率进行限制，从而有效的防御服务器目录被黑客扫描。

➢ 弱口令、暴力破解防护及二次认证

在管理后台中经常会出现管理员的用户名及密码被攻击者拿到，然后攻击者就光明正大的对服务器进行操作，同时服务器也认为其为正当行为。针对这一问题ASP WAF系列产品通过内置的评分算法对用户的密码进行检测，评分低于阈值时，将判定其为弱口令，提示用户及时修改密码，从而提高攻击者攻击的难度。

BlueAiSec WAF系列产品设备还通过精准算法对登录请求频率进行计算并统计，分析是否存在尝试暴力破解用户名密码的行为发生，从而及时做出正确的防护工作，防止用户密码被暴力破解。

当用户名密码不小心被拿到时，BlueAiSec WAF系列产品还提供了一个二次认证功能，攻击者是无法拿到我们设备中设置的二次认证密码的，这样就可以彻底堵死通过拿到后台管理账号后进行攻击的门。

➢ 应用层DoS攻击防护

DDoS，分布式拒绝服务攻击。很多DoS攻击源同时攻击某台服务器就组成了DDoS攻击.，而应用层DDoS又有其特有的属性，通过对HTTP请求进行限制保护能够有效阻止DoS攻击。BlueAiSec WAF系列产品支持SYN flood， HTTP flood，XML DOS等常见DoS攻击防护。设备通过快速准确的算法计算单位时间内攻击源访问次数，如果超出规定阈值，将对攻击源进行阻断处理；同时我们实现一套专业算法，高效计算阈值的大小。从而对应用层DOS攻击进行实时防护。

➢ 多种策略防护方式

为达到更安全可靠的防护工作，BlueAiSec WAF系列产品支持多种策略防护方式设有多重黑白名单，有效的避免大量攻击。

- url 黑白名单策略防护

通过url黑白名单可以对用户限访问网站服务器路径范围进行严格限制，对重要网页进行有效、可靠的保护。

- usr-agent 黑白名单策略防护

能够通过查找匹配用户信息字段，判定是否为非法用户请求，及时有效地阻断非法用户请求，以确保网站服务器的安全。

- 用户请求细粒化配置防护

BlueAiSec WAF系列产品支持对用户请求方法，协议版本，参数范围及长度，请求报头长度，提交数据长度，还可以通过规约配置正则表达式对请求url参数进行正规化限制。支持对请求头域及实体进行检查，可进行严格限制预定义及自定义头部字段长度，头域最大个数，头部长度及请求及应答实体长度。通过以上细粒化配置可以有效跟踪各种攻击方式，并及时做出有效的防护措施。

- 黑名单联动

BlueAiSec WAF系列产品支持对源ip地址请求被阻断的频率进行统计分析，将超过所设置阈值范围内的源ip地址加入黑名单中，从而实现了黑名单自动更新功能，更加有力的阻断其进一步对web服务器进行攻击。

➢ 敏感关键词过滤及服务器信息防护

●非法关键字过滤

BlueAiSec WAF系列产品通过配置策略，能够有效地隐藏或阻断用户提交信息或网页中包含的敏感关键词，同时可以通过对上述信息进行正则表达式匹配，为用户提供简单方便的是用方法，有效地防止非法内容发布。

●爬虫行为智能过滤

随着web服务的高速发展，网络爬虫数量急剧增加，消耗大量服务器资源，影响服务器访问速度，BlueAiSec WAF系列产品能够对访问服务器的爬虫进行分类阻断，摒弃我们不需要的被访问的爬虫，防止此类消耗巨大服务器资源的事件发生。

●服务器敏感信息防护

目前网络中存在大量的嗅探性攻击，这类攻击并不会对服务器产生直接影响，但通过此类攻击可以获得大量服务器内部返回的重要信息，为攻击者下一步攻击提供了遍历条件。BlueAiSec WAF系列产品能够有效地过滤服务器返回给客户端报文中涉及的基本信息，诸如服务器版本号，应用类型等，有效的阻止黑客利用此类信息进行后续的攻击。

●服务器错误信息替换

为防止上文提及的嗅探性攻击，BlueAiSec WAF系列产品对服务器的错误信息返回进行过滤，隐藏或摒弃涉及服务器安全的信息返回至客户端，有效地防止攻击者搜集服务器错误信息，做到对攻击的“事前”防护。

●关键文件防护

在服务器中往往都存放着写有安全隐私性的信息的文件，此类文件是严格保密类文件，但服务器很少会主动对此类文件进行防护，BlueAiSec WAF系列产品能够通过算法对涉及此类

关键文件访问及下载请求进行阻断。防止黑客通过搜集服务器残留的测试脚本，目录文件，残旧数据库等分析服务器漏洞或窃取用户信息。

●恶意文件上传防护

目前大量网站论坛中提供给客户上传文件的功能，这种做法是十分危险的，但又是不得不做的事情，BlueAiSec WAF系列产品通过对上传文件进行缜密地检查，精准的字典匹配，高效率地防止黑客通过绕过认证等限制上传木马，病毒等恶意行为。

●CSRF 攻击防护

CSRF（Cross-Site Request Forgery）即跨站点伪造请求攻击。该攻击以受害者名义伪造请求报文发送给被攻击对象，达到在没有拿到权限的情况下操作在规定权限限制保护下的相关操作，极具危害性。BlueAiSec WAF系列产品通过缜密的算法对访问防护页面的请求报文的特定字段进行分析处理，判定识别出访问者是否通过伪造身份进行黑客攻击，如果确定其为攻击将其阻断，从而达到防护的目的。

➢ 负载均衡功能

BlueAiSec WAF 系列产品支持丰富的负载均衡功能，如下：

- 支持多种负载均衡调度算法
- 支持多样的健康性检查方法
- 支持持续性功能
- 支持 4~7 层负载均衡

➢ 会话管理功能

➢ 会话数限制

BlueAiSec WAF 采用会话识别计数技术，针对特定的目的 ip 进行如下防护：

- 每 ip 连接会话数限制
- 每秒并发会话数限制
- 每秒新建会话数限制

➢ 网页防篡改功能

➢ 网页篡改防护功能

目前有很多企业部门存在一些不需要经常变动，但又是非常重要的网页。针对这类重要网

页ASP WAF系列产品专门为其提供了网页防篡改功能，这一功能通过高效的实现方法，在不对访问产生任何问题的情况下，对重要网页进行篡改防护。如果该防护页面出现被正常或恶意篡改时，设备将会发送上一次原有页面内容至客户端，并产生告警信息。这样用户就可以对本次修改进行有效性检查，确认其是否遭受恶意篡改，如有被恶意篡改现象出现可及时恢复原有内容；若因开发人员需要而进行的修改，可通过设备进行更新此网页。从而安全高效的对网页篡改攻击进行了防护。传统的防篡改都是在设备上开启缓存功能，将请求页面与缓存页面内容进行指纹对比，从而判断网页是否被篡改。对于需要实时更新的页面需要手动刷新。一方面加大了网络管理员的工作量，而刷新操作之间的时间间隔又无法保证用户获取信息的时效性。WAF3000网页防篡改白名单技术，可以将网站允许更改的部分添加到白名单策略中，当Web页面发生更改时，设备会判断更改内容是否在白名单中动态标签内，如果是，则自动刷新设备缓存。

➢ 网站篡改恢复功能

BlueAiSec WAF系列产品支持对网站整体目录进行防护。通过与服务器进行交互后获取网站整体目录结构及内容，采用高效精准的算法进行学习记忆相关内容，根据客户实际需要进行相关防护工作。在网站目录或文件发生异常变化时，产生告警信息，并在规定时间内恢复原目录结构及文件内容。当开发人员进行有必要的修改时，可通对防护对象进行及时更新来解决误认攻击问题。从而对网站目录信息进行了安全可靠的防护。