

教育行业网站应用安全解决方案

根据教育行业网站安全的现状及安全风险分析,智恒联盟应用安全团队通过对教育行业网站安全多年的研究、调研,针对教育行业网站安全提出了全新的安全防护方式,采用 WebGuard 网页防篡改保护系统+WebPecker 网站综合威胁检测系统,完美的解决教育网站安全防护问题免遭黑客攻击篡改,防患于未然。

利用 WebGuard 网页防篡改系统保护网站内容安全

WebGuard 网页防篡改保护系统由北京智恒联盟科技有限公司根据长期对 Web 站点进行安全研究成果自主研发的高可靠性、高安全性以及高易用性的软件系统。主要用于保护站点内容安全,防止黑客非法篡改网页,保护公众形象。该系统也是国内唯一通过国家严格检测的第三代网页防篡改技术。

系统组成

WebGuard 系统包含三个部分:监控代理客户端,管理中心服务器和管理客户端,各部分功能如下:

1. 监控代理客户端 (Monitor Client Setup) 安装在 Web 站点服务器上,根据服务器数量购买客户端数量,主要用于监控站点状态,执行管理中心所配置的策略;
2. 管理中心服务器 (Center Server Setup) 建议部署在独立 pc 服务器上,若所管理的 web 服务器数量较少,也可以同时部署在管理客户端;主要用于用户管理,策略下发,日志监控,以及管理各代理客户端;
3. 管理客户端 (Console Setup) 部署在网管员任意一台计算机,可以由单台 pc 机替代,主要用于登录管理中心服务器进行配置管理 WebGuard 中心服务器;



系统结构示意图

各组建之间通信采取完全加密传输,包括数据传输,用户认证等,确保通信的保密性。

系统主要功能:

- 基于驱动级文件保护技术,支持各类网页格式,包含各类动态页面脚本;
- 完全防护技术,支持大规模连续篡改攻击防护;



- 系统后台自动运行，支持断线状态下篡改监测；
- 驱动技术完全杜绝被篡改内容被外界浏览；
- 支持多站点分布式部署，统一集中管理功能；
- 支持大规模虚拟机、双机热备网站系统部署架构；
- 支持单独文件、文件夹及多级文件夹目录内容篡改保护；
- 支持网页格式类型分类，便于分类管理；
- 支持网页自动上传功能，无需人工干涉；
- 支持异地文件快速同步功能和断点续传功能，极大的增加网站整体安全性和稳定性；
- 支持多用户管理功能，方便操作；
- 支持网页自动同步新增、修改、删除等功能；
- 自动检测文件攻击记录，并实时记入日志，支持导出excel报表；
- 支持服务器多种远程管理功能，如远程接管、远程唤醒、远程关机、远程用户注销等；
- 系统C/S结构，确保高可靠性；
- 支持多个策略管理，策略设置支持即时生效，无需重启；
- 支持服务器冗余双机及负载均衡分布部署；
- 支持多种告警方式，日志告警、声音告警、邮件告警或定制其他告警方式；
- 支持用户认证，采用加密传输，安全可靠；
- 系统全中文界面，操作、配置方便，网络管理人员仅需十分钟即可熟练完成系统初始配置，大大提高工作效率；
- 支持当前所有主流操作系统和web服务器。

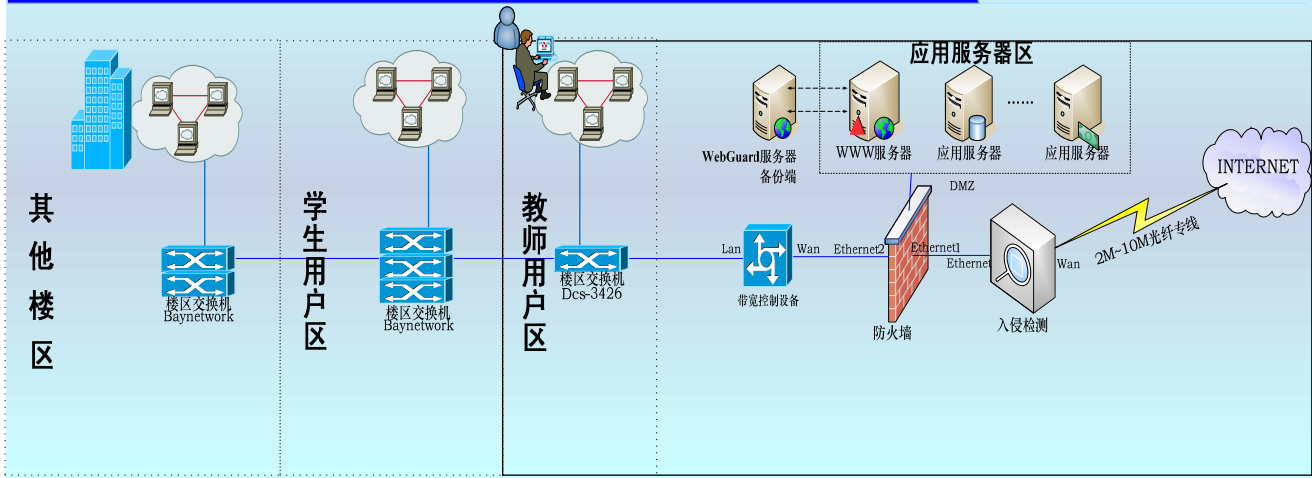
网站动态自适应攻击防护模块主要功能：

- 支持SQL注入攻击防护；
- 支持跨站脚本攻击防护；
- 支持对系统文件的访问防护；
- 支持特殊字符构成的URL利用防护；
- 支持对危险系统路径的访问防护；
- 支持构造危险的Cookie攻击防护；
- 各类攻击的变种防护；
- 支持自定义检测库；
- 规则库支持在线升级功能。

技术特点：

- 完全基于事件触发机制，避免服务器资源额外开支；
- 文件驱动保护技术，确保系统稳定、安全、高效；
- 不限制网站发布服务器类型，实现高可用性和扩展性；
- 文件传输过程加密技术，防窃听和防篡改。

教育系统网页防篡改系统部署拓扑图



图例

| | |
|--|---------------|
| | WebGuard管理服务器 |
| | WebGuard管理客户端 |
| | WebGuard数据同步 |
| | WebGuard监控代理端 |

WebGuard 教育系统应用示意图

针对教育行业网站的具体环境，通过在对外门户网站上部署 WebGuard 网页防篡改监控代理端，用户保护网站内容，防止网页遭到恶意篡改，同时在内容发布服务器或应用服务器上部署 WebGuard 管理服务器及可信代理端，用于网页内容同步、策略指定、日志收集，在中心管理区或教师用户区部署管理客户端 (Console) 用户远程登录管理，以上构架可以完全满足教育系统对网站内容防护的具体需求，保障学校门户网站的安全。

利用 WebPecker 对网站系统进行综合威胁检测

“WebPecker 网站啄木鸟”综合威胁检测系统是北京智恒联盟科技有限公司技术研究团队多年深入研究当前各类流行 Web 攻击手段（如网页挂马攻击、SQL 注入漏洞、跨站脚本攻击等）的经验结晶。通过本地检测技术与远程检测技术相结合，对您的网站进行全面的、深入的、彻底的风险评估，综合性的规则库（本地漏洞库、ActiveX 库、网页木马库、网站代码审计规则库等）以及业界最为领先的智能化爬虫技术及 SQL 注入状态检测技术，使得相比国内外同类产品智能化程度更高，速度更快，结果更准确。

经过数百个用户的实践证明，“网站啄木鸟”是 Web 安全性价比最高的产品，相比国外的 Web 安全扫描产品来说，速度快，具备紧密跟踪国内最新网页木马的快速响应及更新能力。

系统核心技术

➤ SQL 注入网页抓取

Webpecker 的网页抓取模块采用广度优先爬虫技术以及网站目录还原技术。广度优先的爬虫技术的不会产生爬虫陷入的问题，网站目录还原技术则去除了无关结果，提



高抓取效率。

➤ **SQL 注入状态扫描技术（非错误检测）**

此方法不依赖于特定的数据库类型、设置以及 CGI 语言的种类，对于注入点检测全面，不会产生漏报现象。而常见的 SQL 注入扫描产品均不具备此项技术。

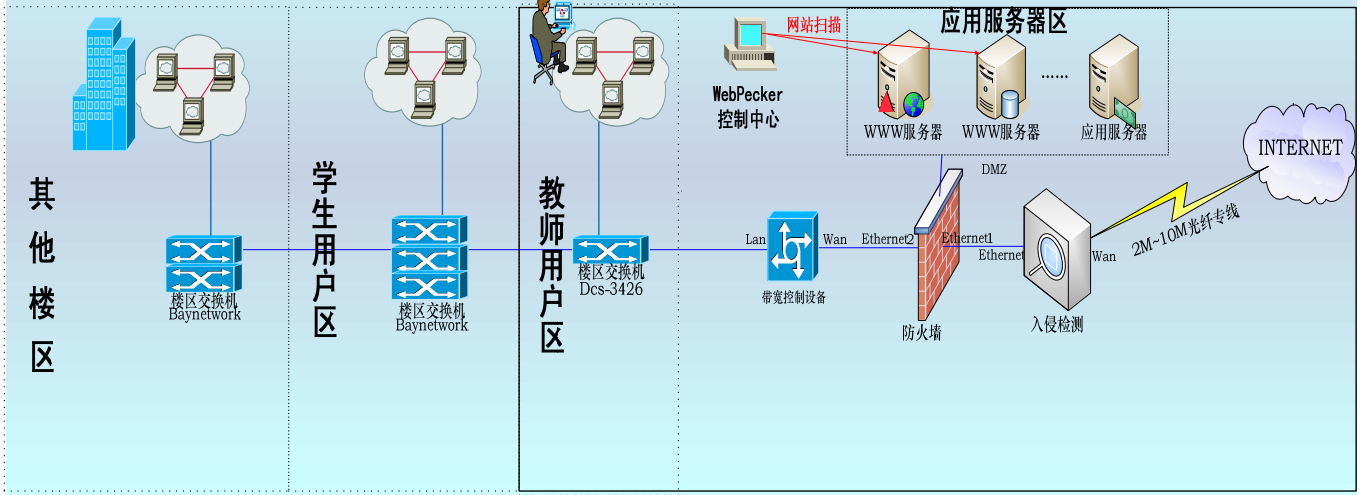
➤ **注入验证基于注入状态**

Webpecker 采用状态检测来对数据库的数据进行猜解，无论网站采用什么 CGI 语言，无论网站是否反馈错误信息，都能进行正常的猜解。

主要功能如下：

| 模块 | 功能 | 说明 |
|--------|---------------|---|
| 漏洞检查 | 本地漏洞检查 | 目的是检查 Web 服务器是否存在常被网页木马利用的漏洞。服务器安全是 Web 安全的基础，所以此检查很重要。 |
| | 危险 ActiveX 检查 | 当前，很多的网页木马都是利用 ActiveX 进行攻击，如果服务器不幸安装了存在漏洞的对应软件，遭受攻击的风险就会很大。业界唯一包含此功能的产品。 |
| | 网站代码审计 | 仅仅保持服务器安全是不够的，还得保证网站代码是安全的。此功能用于检查网站代码的安全性，提示代码中存在的安全问题。此功能是安全研究团队多年实践的结晶。 |
| 木马检测 | 恶意网站判断 | 如果被搜索引擎认定为是恶意网站，对于网站的声誉来说影响很大。此功能用来判断网站是否被搜索引擎收录为恶意网站范围。 |
| | 远程网马扫描 | 业界领先的远程网页木马扫描技术，智能化爬虫技术与检测技术的完美结合，让您及时了解网站是否被挂马，挂在哪个文件，哪一行，让您面对网页挂马的恶劣环境，更有信心。 |
| Web 安全 | SQL 注入扫描 | 此功能用来检查网站是否存在 SQL 注入，使用了状态检测技术，不同于目前国内外产品常用的基于错误的检测技术，加上先进的向量比较算法，使得结果更精确。同比之下，国外的产品很可能会报出上千条漏洞，误报太多。 |
| | 跨站脚本扫描 | 跨站脚本的危害越来越大，攻击者通过跨站攻击可以获得管理员、高级用户的信任关系。此功能用来全面检测网站代码是否容易遭受跨站脚本攻击。 |
| | 管理入口检查 | 目前很多的网站基于内容管理系统(CMS)构建，但是攻击者往往通过寻找管理入口的方式来获得对后台的控制。此功能用来检查网站管理入口设置是否安全，是否容易遭受攻击。 |
| | SQL 注入验证 | 国内外同类产品不具备的功能。采用状态检测来对数据库的数据进行猜解，无论网站采用什么 CGI 语言，无论网站是否反馈错误信息，都能进行正常的猜解，结果更准确。 |
| 敏感信息 | 敏感信息检查 | 商业机密信息对于企业来将最为重要。此项功能用来检查网站是否存在敏感信息，防止重要的信息泄露或非法言论通过网站进行传播。这对于您的企业维稳来说很重要。 |

教育系统WebPecker系统部署拓扑图



WebPecker 教育系统应用拓扑图