深信服 Web 业务安全解决方案

一、Web 安全的挑战

随着互联网技术的高速发展，绝大部分客户都已经将自身业务迁移到互联网上开展，而这当中又主要是以 Web 服务为载体进行相关业务的开展，Web 成为当前互联网应用最为广泛的业务。而针对 Web 业务的安全问题也越来越多。如 2016 年 4 月底的 Struts2 S2-032 让网站的安全问题又引发了业界普遍的关注，很多网站纷纷中招，被黑客入侵造成了严重损失。从历史 Struts2 漏洞爆发数据看，此前每次漏洞公布都深度影响到了政府、金融等行业。网站作为主要的对外门户，已经成为黑客发起攻击的首要目标，网站一旦遭遇攻击，将有可能导致严重的后果：

- 网站被篡改，直接影响对公众树立的社会形象；
- 网站业务被攻击导致瘫痪，影响效率和经济利益；
- 网站敏感数据被窃取，影响单位信誉；
- 网站被攻陷后成为跳板，渗透到内部网络，造成更大面积的破坏；
- 被第三方监管机构，漏洞报告平台通报，带来负面影响；

二、Web 安全的问题

针对 Web 的攻击往往隐藏在正常访问业务行为中，导致传统防火墙、入侵防御系统无法发现和阻止这些攻击。Web 业务系统面临的安全问题是不是单方面的，概括起来主要有以下四个方面：

1）开发时期遗留问题

由于 Web 应用程序的编写人员，在编程的过程中没有考虑到安全的因素，使得黑客能够利用这些漏洞发起对网站的攻击，比如 SQL 注入、跨站脚本攻击等。

2）系统底层漏洞问题

Web 系统包括底层的操作系统和 Web 业务常用的发布系统（如 IIS、Apache），这些系统本身存在诸多的安全漏洞，利用好这些漏洞，可以给入侵者可乘之机。

3）运维管理中的问题

业务系统中由于管理的问题也存在诸多安全隐患，如弱口令、管理员界面等等，导致黑客、病毒可以利用这些缺陷对网站进行攻击。

4）破坏手段多样问题

Web 系统所处的环境的网络安全状况也影响着 Web 系统的安全，比如网络中存在的 DoS 攻击，或者存在感染病毒木马的终端，给黑客提供可利用的跳板等，这些内网自身的安全问题同样会影响到 Web 系统的稳定运行。

三、NGAF 解决之道

深信服 NGAF 提供对 Web 业务系统的三维立体防护解决方案，深入分析黑客攻击的时机和动机。从**事件周期、攻击过程、防护对象**三个维度出发，并可以结合云端安全服务，提供全面的安全防护体系，保护 web 业务系统不受来自各方的侵害。

基于安全事件周期的设计

攻击防护不可能做到 100%安全。Web 系统的安全建设必须贯穿到整个 Web 安全事件周期中，从事前、事中、事后三个维度分阶段进行防护。

NGAF 提供事前策略自检、事中攻击防护、事后防止篡改的整体安全防护。

- 事前风险自检：在配置完安全策略后，NGAF 可以提供 Web 漏洞扫描功能，查看系统还存在哪些安全策略漏洞和隐患，也可通过云端安全服务对网站进行持续的监测；
- 事中攻击防护：2-7 层完整的应用层安全防护，包括：Web 攻击防护、漏洞防护、病毒防护等；
- 事后快速响应：针对网站黑链，网页篡改，网站植入后门等恶意行为进行主动的探测和处置，云端安全服务保持 7*24 在线响应。

基于黑客攻击手段的安全防护

传统的 web 安全防护采用的是防火墙+IPS+WAF 割裂式的安全防护体系，针对各类的攻击总是被动的增补相应功能的安全设备。而对于 Web 安全防护不是单一攻击手段的防护，而需要对黑客攻击动机与时机进行分析，基于黑客的攻击过程的每一个环节进行统一防护。

NGAF 的设计是基于黑客攻击过程的完整 Web 系统安全防护，针对黑客入侵三步曲即扫描、入侵、破坏进行统一的安全防护：

- 扫描：提供网站防扫描、口令暴力破解、关键 URL 防护、应用信息隐藏等；
- 渗透：提供强化的 Web 攻击防护（防 SQL 注入、OS 命令注入、XSS 攻击、CSRF 攻击）、多对象漏洞利用防护等；
- 破坏：提供 Webshell 后门检测、黑链检测、抗 CC 攻击、恶意脚本上传过滤、僵木蠕检测、异常流量清洗等；

提供云端安全服务

对于 Web 业务的防护，除了硬件解决方案以外，深信服还提供一系列的云端安全服务包，帮助用户减轻安全运维的压力。目前提供了专门针对 Web 业务的安全服务包括：

- 网站风险评估服务：网站漏洞扫描，资产风险发现；
- 网站实时监测服务：网站可用性、黑链、网页篡改、后门通信行为监测；
- 安全应急响应服务：威胁处置、0-day 漏洞推送修复、其他应急事件响应；
- 安全运营服务：设备托管服务，每月交付安全运营服务报告；

四、价值体现

通过部署 NGAF 保护 Web 业务系统安全，可以为您提供以下价值：

- ✓ 防止因安全问题造成企业单位形象受损、客户信誉降低等问题
- ✓ 保护机密信息、敏感数据不被泄露
- ✓ 减少因泄露信息而产生法律诉讼的可能性
- ✓ 满足有关法规对 Web 系统安全的规定

五、方案优势

1）Web 业务三维立体防护：

时间：提供事前策略自检、事中攻击防护、事后防止篡改的整体 Web 保护

过程：基于黑客攻击过程的 L2-L7 层完整安全防护，可以有效过滤扫描、入侵、破坏过程中的各种安全威胁

对象：针对终端和服务器的全面防护，防止以终端作为跳板入侵 Web 服务器，以及防止直接针对服务器的攻击

2）更高性价比：

涵盖了 L2-L7 全面的安全功能，可以替代 FW、IPS、WAF，节省投资；

3）提升安全运维效率：

综合业务风险报表结合云端安全服务，让网站安全运维更简单、高效；

六、部分成功案例