何为 Web 安全 2.0?

大家一定听说过“Web 2.0”这个名词，传统的由网站主导生成内容的 Web 方式则称之为“Web 1.0”，而由用户主导生成内容的 Web 方式则称之为“Web 2.0”，这是一种新的互联网产品模式，如：推特、微信朋友圈和公众号、抖音等。那什么是“Web 安全 2.0”？当然也是为了区分传统的 Web 安全，把传统的 Web 安全称之为 1.0，升级的 Web 安全就称之为 2.0。

为了解释什么是“Web 安全 2.0”，得先讲讲什么是“Web 安全 1.0”，再讲讲为何传统的 Web 安全需要升级到 2.0。Web 网站从上世纪 90 年底开始普及使用，是 http 明文传输时代，因为当时的互联网仅用于信息发布和浏览。随着网上支付的应用，明文传输的 http 协议就无法满足安全要求了，浏览器厂商 Netscape 公司于 1994 就发明了 SSL 协议，采用 SSL 证书实现 https 加密传输，保障从浏览器到服务器之间的自动加密传输。这样，Web 安全就进入了 1.0 时代，从此 Web 不再是明文传输，能有效保障 Web 信息的传输安全。

而随着网站的普及，各种 Web 应用越来越丰富，Web 服务中各种有较高价值的数据逐渐成为主要攻击目标。数据窃取、SQL 注入、网页篡改、网站挂马等各种安全事件频繁发生。Web 安全的另一支技术路线就出现了-Web 应用防火墙(WAF)，就是为了防护 Web 网站不会被攻击，会分析每一次连接是否是恶意连接，WAF 会放行正常用户访问网站资源而拒绝恶意攻击访问。有了 WAF，Web 应用就安全了，就不用担心各种网站攻击了。

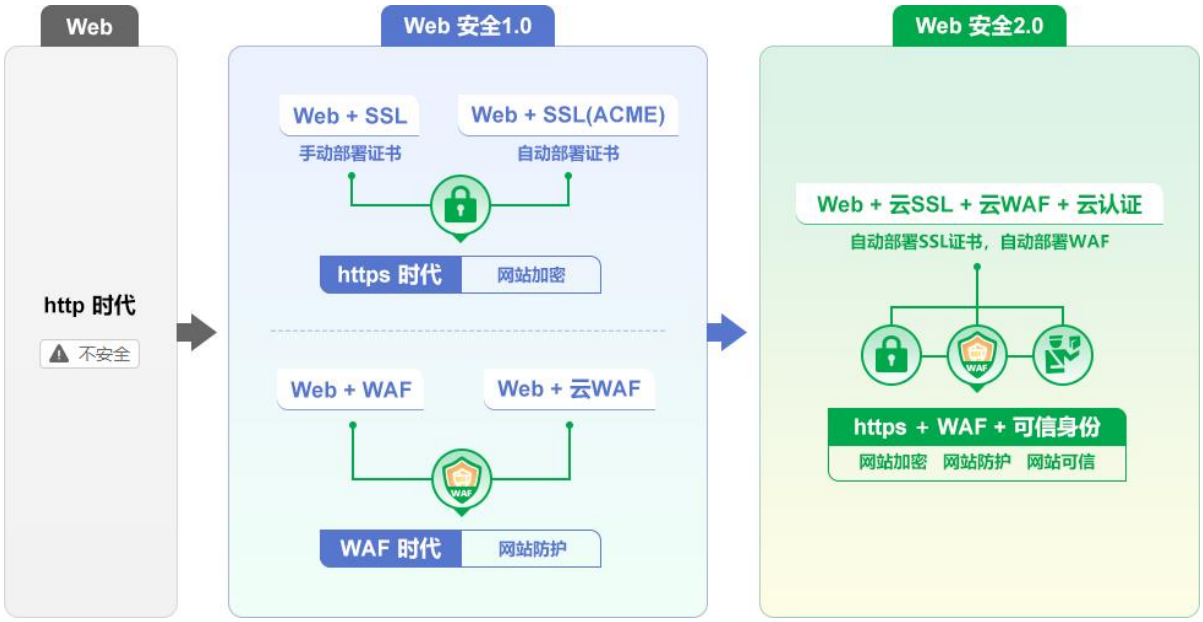
HTTPS 加密是为了保护网站内容的传输安全，而 WAF 则是为了保护网站系统不会遭遇恶意攻击，都是为了网站安全。所以，有些用户为网站部署了 SSL 证书，有些用户为网站部署了 Web 应用防火墙，有些用户则两者都采用了。但是，https 加密只解决了 Web 应用的传输安全，用户必须向 CA 申请 SSL 证书并手动部署 SSL 证书到服务器上，或者在服务器上安装一个 ACME 客户端软件自动申请 SSL 证书和部署 SSL 证书。而 WAF 则只解决了网站的安全防护，并不管用户是否是明文传输访问网站数据这事。即使是支持部署 SSL 证书的 WAF 系统，仍然需要用户人工申请 SSL 证书和部署 SSL 证书到 WAF 上。这两个不同的 Web 安全技术方向都已经无法适应云计算和大数据的发展需要，特别是虚拟主机用户无法安装 SSL 证书，使得大量的采用虚拟主机的网站处于非常不安全的状态！

为此，Web 安全 1.0 需要升级，在 Web 安全 1.0 的基础上把这两支不同的技术结合在一起，升级为 Web 安全 2.0，并作为一种云服务来为用户提供 Web 安全服务。Web 安全 2.0 为云原

生服务，把云密码服务与云 WAF 服务紧密结合起来，实现全自动为网站安全配置 SSL 证书和配置 Web 应用防火墙服务，全自动为网站提供 Web 安全云服务，而无需人工干预，用户无需向 CA 申请 SSL 证书，也无需在服务器上安装什么软件，只需使用 Web 安全云服务就可全自动实现 https 加密和 WAF 防护，这就是 Web 安全 2.0。

Web 安全 2.0 由于是云原生服务，使得虚拟主机用户也能无缝轻松使用 https 加密和 WAF 服务，轻松实现网站安全防护，使得 Web 安全 2.0 成为了一个划时代的网站安全普惠服务，适用于所有网站的安全防护！Web 安全 2.0 时代彻底结束了需要人工处理的费时费力的旧时代，全自动实现了所有网站的普惠安全，适应了云计算和大数据安全的需要，必将受到所有网站用户的欢迎。

Web 安全 2.0 还有第三个重要元素，那就是网站可信认证。网站实现了 https 加密和 WAF 防护，并不等于网站安全了，并不等于用户就可以信任这个网站，因为欺诈网站也可以实现 https 加密和 WAF 防护。所以，网站的可信身份同 https 加密和 WAF 防护一样重要，而网站身份的展示应该由浏览器来完成，在地址栏显著显示网站的可信身份信息。对于部署了已经认证网站身份的 OV SSL 证书和 EV SSL 证书的网站，浏览器在地址栏直接展示证书主题中的单位名称。而对于部署了没有认证网站身份的 DV SSL 证书的网站，则用户可申请网站可信认证，一样可以在浏览器地址栏展示已认证的网站的单位名称。网站身份可信同 https 加密和 WAF 防护一样重要，为 Web 安全 2.0 时代的三个不可或缺的重要元素。



Web 安全 2.0 是一个典型的零信任安全解决方案，不信任 Web 明文传输，因为明文传输的信息非常容易被非法窃取和非法篡改，全自动使用 SSL 证书实现 https 加密传输；不信任 Web

流量，由 Web 应用防火墙始终验证每次 Web 连接，放行正常连接和拒绝恶意连接。不信任没有通过认证的网站，因为欺诈网站和假冒网站也可以实现 https 加密和 WAF 防护。

根据《密码法》对密码的定义，密码用于信息加密和安全认证，所以，零信任加密码技术，才能完美实现网站安全从 1.0 时代升级到 2.0 时代，完美保障 Web 应用安全。让我们迎接 Web 安全 2.0 时代的到来，让 Web 应用更加安全可信。

王高华

2022 年 4 月 29 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。