提升网站安全性的 7 个方式

■ 张 格

随着互联网的不断发展，很多企业意识到需要在互联网上建网站来展示自己的企业形象，但对于如何提高网站安全性往往缺少一个正确的认识。

建站很容易，但是做好网站的安全维护却是一件不容易的事情，随着逐年增加的网络攻击，网络黑客通过漏洞对网站进行攻击。为了避免网站遭到攻击，需要提升网站的安全性，同时不影响用户的体验。

在实际的运营管理当中，很多企业对于网站的安全性不够重视，网站存在很多安全隐患。比如服务器崩溃、网站被挂马等，轻则影响用户的使用体验，严重的会导致企业蒙受巨大的经济损失。

企业可以通过以下 7 个方式，提升网站安全性。

1. 选择安全稳定的服务器

网站体验质量的好坏，很大程度上跟服务器有关，网站出现安全问题普遍是因为采用的服务器不稳定，网站快照、DNS 被劫持以及网站页面被挂上各种恶意广告等。

所以在选用服务器的时候千万不能图便宜，要选择知名的、安全性和稳定性高的服务器，现在很多中小型企业都选择云服务器，毕竟云计算大厂商能够提供高防的防火墙和硬件设施。

2. 使用 HTTPS 协议

以前网站采用的是 HTTP传输协议，这种传输协议简单，但是通过明文传输，被截获后很容易将信息泄露。而 HTTPS 是在 HTTP加入 SSL 层，数据通过加密传输，黑客即使攻击了网站，得到的也是加密的信息，使用 HTTPS协议可以保护用户隐私，虽然需要花费一定的费用，但是为了用户账户的安全性，还是很值得的。

3. 限制安装并保持更新插件

为了让用户获得更好的体验，网站所有者会通过下载很多的插件来帮助他们改善网站的用户体验。比如一些炫酷的效果等，然而实际上影响用户真正体验的却是清晰的导航、页面加载的反应速度以及简洁干净的界面。

加载越多的插件，越容易被黑客找到攻击的漏洞。所以为了减少网站被攻击的几率，需要限制安全插件，并且这些插件需要经常检查，保证更新，及时将缺陷进行修补。

4. 屏蔽网站源代码

当我们在浏览银行的网银时，经常会发觉没办法在银行网银的界面里使用鼠标右键。这样的主要目的是阻止客户端通过右键查看网站的源代码，这样可以有效防范网站客户端代码（如：HTML，Js，Css，Img）被拷贝等。

5. 使用 CDN 加速

使用 CDN 加速不仅可以提升用户访问网站的速度，还可以提高网站响应速度，访问量较高的大型网站均使用 CDN 网络加速技术，虽然网站的访问量巨大，但无论在什么地方访问都会感觉速度很快。

更重要的是，因为通过广泛分布的 CDN 节点加上节点之间的智能冗余机制，可以有效地预防黑客入侵以及降低各种 DDoS 攻击对网站的影响，同时保证较好的服务质量 。

6. 使用验证码

验证码的原理很简单，是在服务器生成的一段 Session 储存验证码中生成图片中的文字，而验证码的图片文字经常是通过扭曲渐变的字符串。安全且复杂的验证码使用可以有效防范论坛的注册机，发贴机还有一些密码暴力破解器等对网站有危害的工具。

7. 每日备份

最糟糕的事情就是由于数据丢失导致大量用户无法进行正常的网站访问，这种情况往往由于黑客攻击，导致数据丢失，网页信息不全。前不久发生的寻子公益网站论坛事件就是如此，遭到黑客攻击后，网站数据丢失，影响了很多丢失孩子家庭错失关键信息。

所以需要通过建立每日网站备份，防止数据和内容在安全漏洞事件中丢失，即使遭到攻击，也能够快速恢复数据，用户也能正常访问和使用网站的服务。

现在越来越健全的网络安全体系帮助组织减少攻击面，提高威胁检测、响应能力，帮助降低网络风险。企业建网站可以通过以上几个常规手段来提升网站的安全性，同时也能够提升网站用户的体验满意度。