

为何零信浏览器免费提供网站安全体检评级服务

你知道你正在访问的网站是安全的吗？也许你会回答：“是的”。因为所有浏览器都已经对 http 明文访问网站提示“不安全”。你答对了！这是因为 http 明文传输的信息非常容易被非法窃取和非法篡改，这是所有浏览器对明文信息传输的零信任。笔者再问一个问题：如果浏览器显示安全锁标识，提示“安全”是真的安全吗？也许你会回答：“是真的，因为这是谷歌浏览器提示的”。不好意思，你答错了。

笔者不仅十几年来一直在持续推动 SSL 证书的普及应用，并且也一直在强调正确部署 SSL 证书，千万不要以为网站部署了 SSL 证书，浏览器显示安全锁标识就真的安全了，不安全的 SSL 证书部署会带来更多的安全隐患。打个比方吧，没有部署 SSL 证书，网站服务器只需打开一道门(80 端口)，而部署了 SSL 证书则需要打开另一道门(443 端口)，80 端口还不能关闭，还得开着让用户访问后能自动跳转到 443 端口。也就是说，为了建一个加密通道，房子不得不再开一道门，但是，如果 443 这道门保安不负责任的话，那就等于多增加了一个新的不安全通道，可能比原先只开 80 一道门还糟糕，这一定不是用户想要的结果，用户在服务器部署 SSL 证书就是希望增加一个加密通道用于传输机密信息，而把明文传输通道关闭，如果有人要从明文通道进来就把他/她引导走加密通道。所以，这个加密通道的安全措施非常重要。

笔者早在 2010 年 12 月 6 日作为《计算机世界》报特约撰稿发表了 《网银 SSL 证书部署有漏洞》 的文章，指出了当时的各大银行的网银 SSL 证书部署出现的六大安全问题。12 年后的今天，不仅仅是网银系统，各个电商网站、支付网站、政务网站的 SSL 证书部署仍然还有不少部署安全问题。

即使网站已经正确部署了 SSL 证书，但是如果网站没有任何安全防护，则非常容易遭遇网络攻击，发生被植入木马和网页被篡改等各种安全事故，所以网站仍然是不安全的。也就是说，你看到了安全锁标识，不要轻信浏览器提示的“安全”二字，不正确的 SSL 证书部署和没有安全防护都有可能导致网站很不安全，部署了 SSL 证书实现了 https 加密并不等于网站安全了！而由于免费 SSL 证书随手可得，使得一个假冒银行网站也可以非常容易地做到部署 SSL 证书，这更加说明绝对不能认为看到有安全锁就认为网站是安全的！网站是否通过了可信第三方的身份认证是网站安全的一个不可或缺的重要要素。

一个网站是否安全，至少有三个基本要素，一是 https 加密，二是 WAF 防护，三是可信身

份认证，三者缺一不可。如何让普通网民能简单明了地了解一个网站是否具备了这三个要素的安全防护？零信浏览器全球独家实现创新实现了在浏览器地址栏增加 2 个 UI 标识来标识网站是否采取了以上三个防护措施，不仅显示安全锁标识，而且增加显示云 WAF 防护标识和网站身份认证级别标识。

但是光有三个安全标识还是不够的，应该让网站访问者和网站业主非常容易地了解网站的整体安全状况，这就是零信浏览器免费提供网站安全体检评级服务的初心！零信浏览器全球独家率先创新地集成了完全免费的网站安全体检评级服务，用户使用零信浏览器访问任何 https 网站时，只需点击安全锁标识就能显示网站安全体检评级的结果是哪个等级，如下图所示。



零信浏览器网站安全体检评级共有 A、B、C、D、E、F 六个等级，分别对应百分制的 80 分以上、60 分以上、50 分以上、40 分以上、30 分以上和低于 30 分，其中有些安全规则会评为 A+ 或 B+ 级，相当于 90 分以上或 70 分以上。用户还可以再点击网站安全体检评级：后面的级别了解体检结果详情，会详细展示 SSL 安全部署、WAF 安全防护和网站可信认证等三个方面的打分情况。



其中 SSL 安全部署部分的体检指标和评分标准参考 Qualys 公司 SSL 实验室的 SSL Sever Test 服务：<https://www.ssllabs.com/ssltest/>，分别从 SSL 证书、协议支持、密钥交换和加密套件强度等 4 个维度来检测。零信浏览器在同服务器实现 https 握手时就已经实时获取网站部署的 SSL 证书和服务器配置参数并实时计算出体检结果，不仅直接在浏览器的 SSL 证书 UI 上展示评级结果，而且还可以点击查看各项体检指标的详细情况，非常方便用户查阅正在访问的网站的 SSL 证书部署安全状况，让网站业主能及时发现 SSL 证书部署安全问题并及时修复问题，

让 SSL 证书能正确部署真正保护网站安全，而不是因为另开了一个加密通道反而增加了网站的安全风险。

而第二项体检的云 WAF 防护则比较简单，只要网站使用了零信浏览器信任的云 WAF 防护服务，则得满分 20 分，计划将来引进一个第三方的云 WAF 防护性能评级，并根据这个评级结果给与不同的服务得分。第三项体检的网站可信认证，评分规则也很简单，网站部署了 EV SSL 证书或者通过网站可信 EV 认证，则得满分 20 分，OV 认证则得 15 分，IV 认证则得 10 分。网站部署了未认证网站身份的 DV SSL 证书则为零分。

总之，零信网站安全体检评级服务也体现了零信任理念，不信任网站能正确部署 SSL 证书，但为用户提供自查的工具，让用户能及时发现 SSL 部署安全漏洞，并及时堵住漏洞。不信任网站没有任何防护是安全的，只信任有云 WAF 防护的网站。不信任没有通过身份认证的网站，只信任有可信认证标识的网站。零信网站安全体检服务遵循零信任原则，为用户提供一个直观的了解正在访问的网站安全状况的工具，零信技术这一免费服务使得用户的网站更安全，使得上网用户更安全，一切只为用户着想。

王高华

2022 年 6 月 1 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。

