What is Web Security 2.0?

You must have heard the term “Web 2.0”. The traditional Web of generating content led by websites is called "Web 1.0", while the Web of generating content led by users is called "Web 2.0". This is a new Internet model, such as Twitter, Instagram, We Chat Moments, TikTok etc. So, what is "Web Security 2.0"? Of course, it is also to distinguish the traditional Web security. The traditional Web security is called 1.0, and the upgraded Web security is called 2.0.

To explain what "Web Security 2.0" is, we must first talk about what is Web Security? Then talk about why traditional web security needs to be upgraded to 2.0. Websites have been widely used since the end of the 1990s, and it was the era of http cleartext transmission, because the Internet at that time was only used for information publishing and browsing. With the application of online payment, the http protocol transmitted in cleartext cannot meet the security requirements. The Netscape invented the SSL protocol in 1994, using the SSL certificate to realize https encrypted transmission to ensure automatic encrypted transmission from the browser to the server. In this way, Web security has entered the 1.0 era, so the Web is no longer a cleartext transmission, which can effectively ensure the transmission security of Web information.

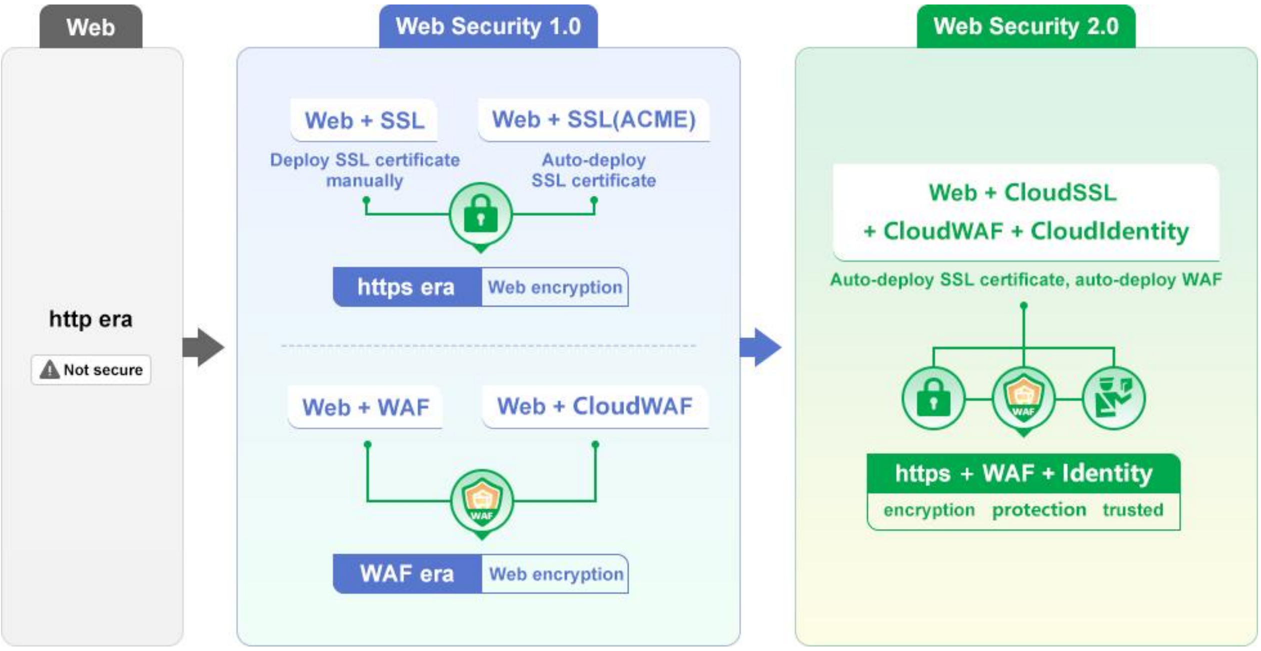
With the popularity of websites, web applications are becoming more and more abundant, and more high-value data in web services have gradually become the main attack targets, more security incidents such as data theft, SQL injection, web page tampering, and web page hacking occur frequently. So, another technical route of web security has emerged - Web Application Firewall (WAF), which is to protect websites from being attacked, and analyzes whether the Web connection is a malicious connection, WAF will allow normal access to website resources and reject the malicious ones. With WAF, web applications are secure, and there is no need to worry about website attacks.

HTTPS encryption is to protect the transmission security of website content, while WAF is to protect the website from malicious attacks, both for website security. So, some users deploy SSL certificates for websites, some users deploy WAF for websites, and some users use both. However, https encryption only solves the transmission security of web applications. Users must apply for an SSL certificate from a CA and manually install the SSL certificate to the Web server or install an ACME client software on the server to automatically apply for an SSL certificate and deploy the SSL certificate. The WAF only solves the security protection of the website and does not care about the cleartext transmission. Even in a WAF system that supports the deployment of SSL certificates, customers still need to manually apply for an SSL certificate and deploy the SSL certificate to the WAF. These two different Web security technology directions have been unable to meet the needs of cloud computing and big data, especially the virtual hosting website don’t support installing SSL certificate, this makes a large number of websites using virtual hosting in a very unsecure state.

So, Web Security 1.0 needs to be upgraded. Based on Web Security 1.0, these two different technology routes are combined, upgraded to Web Security 2.0, and it should be a cloud service to provide Web security services for customers. Web Security 2.0 is a cloud-native service that closely integrates cloud cryptographic services and cloud WAF services to automatically configure SSL certificates and WAF services for website, to automatically provide web security cloud services for websites without manual intervention. Users do not need to apply for an SSL certificate from the CA, nor do they need to install any ACME client software on the server, just use the Website Security Cloud service to automatically realize https encryption and WAF protection, this is web security 2.0.

Because Web Security 2.0 is a cloud-native service, virtual hosting customers can also use https encryption and WAF services easily, and easily realize website security protection, making Web Security 2.0 an epoch-making website security as universal benefit service that suitable for all websites. The Web Security 2.0 era has completely ended the time-consuming and labor-intensive old era of manual processing SSL certificate and WAF service. It fully automatically realizes the universal benefit security for all websites, adapts to the needs of cloud computing and big data security, and will surely be welcomed by all websites.

There is also a third important element of Web Security 2.0, which is the website trusted identity. Because the website implements https encryption and WAF protection, it does not mean that the website is really secure, and it does not mean that users can trust the website because fraudulent websites can also implement https encryption and WAF protection. Therefore, the trusted identity is very important same as https encryption and WAF protection, and the presentation of the website identity should be done by the browser, displaying the trusted identity information of the website in the address bar. For websites that deploy OV SSL certificates and EV SSL certificates that have validated the website identity, the browser directly displays the trusted identity information in the address bar by reading the certificate subject O field. For websites that have deployed a DV SSL certificate that does not validate the identity of the website, users can apply for the Trusted Website Identity Validation service, after passing the validation, the company name can also be displayed in the address bar of the browser. Website trusted identity is as important as https encryption and WAF protection, and they are three indispensable and important elements in the Web Security 2.0 era.



Web Security 2.0 is a typical zero trust security solution. It does not trust Web cleartext transmission, because the information transmitted in cleartext is very easy to be illegally stolen and illegally tampered with, it uses SSL certificate to realize https encrypted transmission automatically. It does not trust all Web traffic, every Web connection is always verified by the WAF, allowing normal connections, and rejecting malicious connections. And it does not trust unvalidated websites, as fraudulent and fake websites can also implement https encryption and WAF protection.

According to the definition of cryptography in the "China Cryptography Law", cryptography is used for data encryption and authentication. Therefore, zero trust plus cryptographic technology can perfectly realize the upgrade of website security from 1.0 era to the 2.0 era, and perfectly guarantee the security of web applications. Let us welcome the arrival of the Web Security 2.0 era and make Web applications more secure and trusted.

Richard Wang

April 29, 2022
In Shenzhen, China