Why does ZT Browser provide Website Security Rating Service for free?

Do you know the website you are visiting is secure? Maybe you will answer is "Yes" because all browsers display "Not secure" on the HTTP protocol access to the website. You are right! This is because the information transmitted by HTTP is very easy to be illegally stolen and illegally tampered with. This is the zero trust to the cleartext transmission for all browsers. I ask another question: If the browser displays the security padlock and word "Security", is it really secure? Maybe you will answer: "Yes, because this is prompted by Google Chrome." Sorry, your answer is wrong.

The author has not only continued to promote the popularization of SSL certificates, but also emphasizes the correct deployment of the SSL certificate. Do not think that the website deployment of the SSL certificate is really secure. The unsecured SSL certificate deployment will bring more security risks. Let's draw an analogy for website as house, if an SSL certificate is not deployed, the web server only needs to open one door (port 80), while if an SSL certificate is deployed, another door (port 443) needs to be opened. But we cannot close the door 80, since someone will enter the house from door 80, then should be led to door 443. In other words, in order to build an encrypted passage, the house has to open another door. However, if the security of the door 443 is irresponsible, it means that a new unsafe passage has been added, which may be worse than only open door 80. This must not be the result that the user wants. The user deploys an SSL certificate on the server is for adding an encrypted channel for transmitting confidential information and close the cleartext transmission channel. If someone wants to come in through the cleartext channel, he/she will be guided to the encrypted channel. Therefore, the security measures of this encrypted channel are very important.
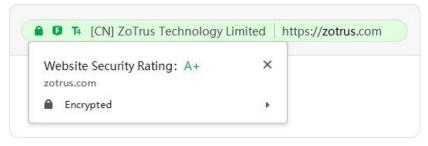
As early as December 6, 2010, the author published the article "There are security vulnerability in the deployment of SSL certificate in Internet banking" as a special writer for "China Computer World", pointing out six major security problems in the deployment of SSL certificates in Internet banking of major banks at that time. Today, 12 years later, not only the Internet banking system, but also the SSL certificate deployment of ecommerce websites, payment websites, and e-government websites still

have many deployment security problems.

Even though the website has correctly deployed the SSL certificate, if the website does not have any security protection, it is very vulnerable to network attacks, and various security incidents such as implanted Trojan horses and tampered web pages occur, so the website is still not secure. In other words, when you see the security padlock, don't believe the word "security" prompted by the browser. Incorrect SSL certificate deployment and no security protection may cause the website to be very insecure. HTTPS encryption is not equal to website security! And because the free SSL certificate is available easily, it makes a counterfeit bank website that can also be very easy to deploy the SSL certificate, which shows that it is absolutely impossible to think that the website is secure when you see a security padlock! Whether the website has passed the trusted third-party identity validation is an indispensable and important element of website security.

Whether a website is secure, there are at least three basic elements, one is HTTPS encryption, the other is WAF protection, and the third is trusted identity validation. The three are indispensable. How to let ordinary netizens simply understand whether a website has the security protection of these three elements? The global exclusive realization of ZT Browser has added an additional two UI icon in the browser address bar to identify whether the website has adopted the above three protective measures, which not only shows the security padlock, but also adds the cloud WAF protection icon and website identity validation level icon.

However, displaying three security icons alone is not enough. It should make websites visitors and website owners very easy to understand the overall security status of the website. This is the original intention of ZT Browser to provide website security rating service for free! ZT Browser is the first in the world innovatively integrating a free website security test and rating service. When users use ZT Browser to access any HTTPS website, just click on the security padlock to display which level of the result of the website security test rating, as shown below.

There are six grades of website security test: A, B, C, D, E, and F, corresponding to 80 or above, 60 or above, 50 or above, 40 or above, 30 or above, and below 30 points. Some rules will increase to A+ or deduce to B+, which is equivalent to 90 or 70 points. Users can also click on the Website Security Rating: rating level to learn more about the test result details, it will be displayed in detail three aspects: SSL Security, WAF Protection, and Trusted Identity.

This SSL security test and rating service parameters and rating guide refer to the SSL Sever Test service of the SSL Labs of QUALYS: https://www.ssllabs.com/ssltest/, which test the website from 4 categories including SSL certificate, protocol support, key exchange, and cipher strength. ZT Browser gets the test results in real time after obtaining the SSL certificate and server configuration parameters, then displays it directly on the browser UI. And user can also click to view the details of each test items, it is very convenient for users to check the security status of the SSL certificate deployment of the website they visited, and to let the website owner can find the SSL deployment security problems in time and fix it in time. This solution will make the SSL certificate to be deployed correctly to truly protect the website security, does not increase the security risk of the website because another encrypted channel is opened.

The second test is cloud WAF protection test that it is relatively simple. If the website uses the cloud WAF protection service trusted by ZT Browser, it will get a full score of 20 points. It is planned to introduce a third-party cloud WAF protection performance rating in the future, then give different service score based on the performance rating. The third test is website identity validation test, the rule is also very simple. The website deploys the EV SSL certificate or passes the EV Certification, then scores 20 points, OV SSL certificate or OV Certification scores 15 points, IV SSL certificate or IV

Certification scores 10 points. The DV SSL certificate that do not validate the website identity scores zero point.

In short, ZoTrus Website Security Rating Service also reflects the concept of zero trust. Never trust the SSL certificate is deployed correctly on the website, but provides users with self-test tools, to let users to discover SSL deployment security vulnerabilities in time and fix vulnerabilities in time. Never trust the website is secure without any security protection on the websites, only trusts the websites with cloud WAF protection. Never trust the website that have not passed identity validation, only trusts the websites with trusted validation icon. ZoTrus Website Security Rating Service follows the zero trust principles, provides users with a tool that intuitively understands the security status of websites. This free service makes the user's website more secure, making the Internet users safer. Everything we do is just for the user's sake.

Richard Wang

June 1, 2022
In Shenzhen, China

(C) 2022 **ZoTrus Technology Limited**