Three Misunderstandings of Website Security

Recently, I talked with the IT manager of several government websites and several business owners about the insecurity of their websites without SSL certificates. It is generally believed that there is no content on the website that needs to be encrypted, and they cannot understand why all browsers display “Not secure” for website that only have public information for users to browse, they all think that this is browsers or SSL certificate suppliers trying to scare users, the purpose is to promote SSL certificates. Some IT managers even said that my website has passed the security test of a certain authority, so why is it not secure? Why is it still illegal?

From the perspective of users, it seems that what everyone said is very reasonable, but from the perspective of website security professionals, these views are all wrong, but we cannot blame users, this is our popular science work is not enough, so the author writes this blog post, hoping that the IT managers and website owners who really care about their website security can read this article patiently, and they will definitely gain something. Only when the website is secure, can they do their own business with peace of mind.

The first misunderstanding: the website does not have any content that needs to be encrypted, and there is no need to deploy SSL certificate for encryption.

At present, the local government websites generally only display some local information releases and local feature introductions of the city and county. The e-government systems that really require users to log in and enter confidential information have been assigned to the provincial e-government system for unified management, and the local e-government website only needs to be linked to the corresponding provincial e-government service system. As for whether the provincial e-government service website has deployed an SSL certificate to implement https encryption, it is no longer within the jurisdiction of the city or county. This is the reality and the truth, and from this point of view it is not difficult to understand why everyone thinks that https encryption is not needed. However, from a professional website security point of view, there are three reasons why https encryption is still required.

Reason One: Preventing web page tampering and illegal hotlinking.

It is true that the city, county, and district-level e-government websites only have publicly disclosed information, and there is indeed no login page that requires encrypted usernames and passwords, but there are a large number of links to the provincial e-government service system. If the website does not have https encryption, attackers and all Wi-Fi providers can easily tamper with the link on the webpage to lead the user to a fake e-government service website, so that it is very easy to get the username and password of the user on the provincial e-government service system. I believe this is not the result that local e-government websites want to see. These city, county and district e-government websites that do not use https encryption have become a threat to the security of provincial e-government service websites! This is why the author have repeatedly appealed to why the provincial e-government service website should mandatorily require that the local e-government websites of the cities and counties must also implement https encryption.

Reason two: Protecting user privacy of website visitors.

The author saw this reason from Google's official website more than ten years ago. When Google launched the search service, it explained why the search page needs https encryption to protect user privacy. If it is not encrypted, it is very easy for hacker to get the searched keywords illegally, the user may be searching for a very private problem to find a solution. If the search website is not encrypted, other people can get the searching keywords and the searching results he/she click. This will expose the privacy, isn't that scary?

Although city, county and district e-government websites are all information that can be browsed publicly, but users who browse the website do not want irrelevant people to know what content he/she is browsing, which requires https encryption. The city, county, and district e-governments should realize the https encryption of the entire site based on the principle of "People First" to protect the personal privacy of people's online behavior, so that citizens of the city, county, and district can browse the information on the local e-government website with confidence and enhance the people's sense of security and happiness.

Reason three: Eliminate "Not secure" warnings from all browsers.

All browsers prompting "Not secure" warning for websites that do not implement https encryption is definitely not to promote SSL certificates, but because what the author mentioned above is indeed insecure. If the above two reasons are not enough, then for the "face" project, the problem that the browser prompts that the website is not secure should also be solved. When the user sees the browser prompting "Not secure" when surfing the website, the user's first impression for this website must not be good, and he/she must not dare to read more, unless there is really no other way.

The only way to eliminate the browser's "Not secure" warning is to use HTTPS encrypted for the website. HTTPS encryption can be implemented by deploying an SSL certificate on the website or using cloud WAF protection with https encryption. All browsers will display the padlock icon and will not prompt "Not secure". At present, there are free SSL certificates on the market, and there are very cheap paid SSL certificates, both of which can solve the problem. If you don't want to change your website setting, don't want to apply for an SSL certificate and deploy an SSL certificate, you can purchase a Website Security Cloud service. You just need to do 3 domain name resolutions and turn the original website into a WAF/CDN source site to automatically implement https encryption and cloud WAF protection.

The second misunderstanding: my website is a very small enterprise website, there is no information worth attacking.

This misunderstanding is the thinking of many business owners. In the current general environment, it is not easy for small and medium-sized enterprises to survive. Therefore, small and medium-sized enterprises will think that "my website has no information to steal, no need for encryption, no need for protection", "My website is for a so small company that will not attract the attention of hackers." Therefore, many small and medium-sized enterprises' websites do not deploy SSL certificates, they are all accessed through http plaintext, and there are no other security protection measures.

In fact, hackers can use automated tools to find websites without any protection and automatically implant Trojan horses, making your website a "chicken" and a "thug" to attack other systems and passively break the Law. This is the main reason why SME websites are the most vulnerable to cyber-attacks, such as Trojans implanting into websites, web page tampering, SQL injection, database dragging, and email fraud etc. According to a report released by the CNCERT/CC, 53,171 websites in China were implanted with backdoors in 2020, including 256 government websites. These attacks will not only affect the normal access of websites and leak website data, but also face the pressure of compliance with the Cyber Security Law, which may receive an administrative penalty.

How to do? HTTPS encryption and cloud WAF protection are required. HTTPS encryption can prevent illegal modification of codes and illegal implantation of attack links during plaintext transmission, while cloud WAF protection can prevent various attacks in real time, effectively protecting the confidential information security of websites and valuable user data of enterprises and business data security.

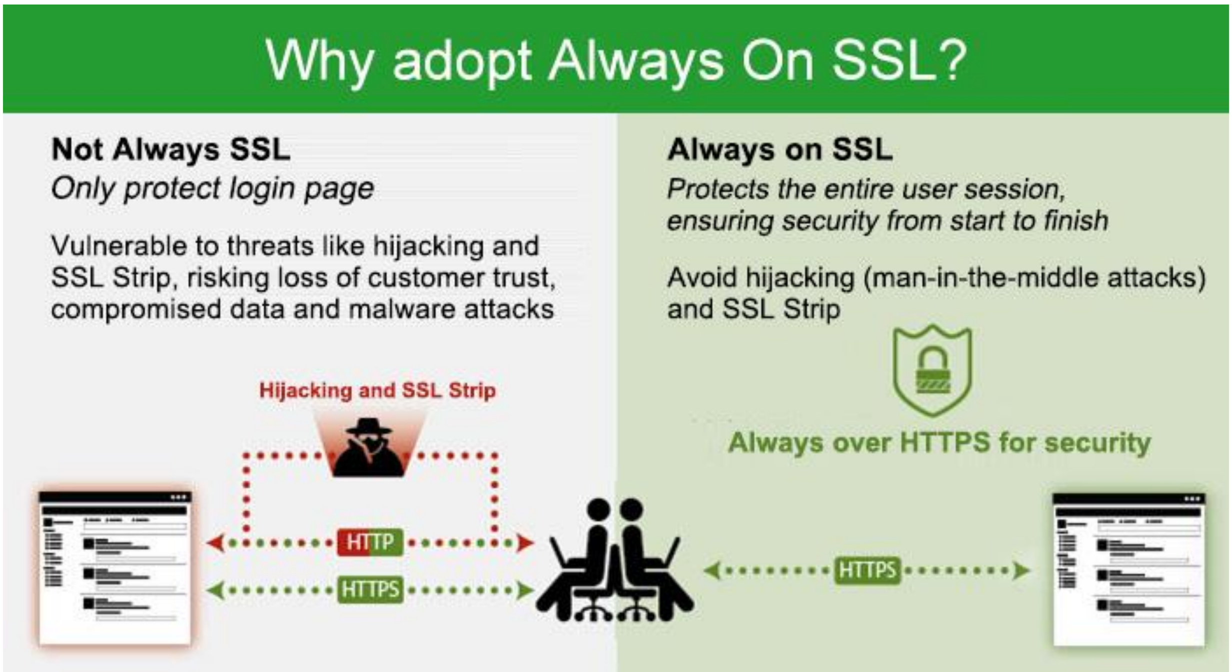
According to Gartner's 2021 report forecast: by 2024, 2 years later, that is 70% of organizations will implement cloud WAF protection for web applications, because website attacks have become the norm now, and it is irrelevant for the size of the website and whether the website has valuable data. To protect the valuable data of the enterprise and the normal and reliable operation of the website, it is recommended to use the Website Security Cloud Service, which can realize https encryption and cloud WAF protection with one click, so that website owners can rest assured and concentrate on doing their own business without worrying about whether the website is normal.

The third misunderstanding: Only the login page needs to be encrypted, and other pages do not need to be encrypted.

Why this problem ranks third is not to say that this problem is not important, but it is necessary to explain clearly why the website needs https encryption first. The user with this problem has implemented HTTPS encryption for the login page, but the whole website after the user authentication passes becomes a plaintext http website, which is also common in many e-government websites, university websites and e-commerce websites.

First, what needs to be affirmed and praised is that the user login authentication page uses https encryption, which can effectively ensure the encrypted transmission security of the username and password entered by the user. However, the website should be encrypted after logging into, because the logged-in system has the most important core data that needs to be protected, including the user's personal privacy information, order information and delivery address, etc. These important data are the core asset of the enterprise, how can it not be protected by encryption? If the pages containing these important data are not encrypted, hackers don’t need to attack the user login authentication system, they can just listen to the data packets after user login and can easily get the important confidential data of e-government websites and corporate websites without attacking at all.

The picture below is the publicity picture of the full-site https encryption that the author used more than ten years ago. It is still applicable now, because there are still many websites that only implement https encryption on the login page. Full-site https encryption can effectively prevent man-in-the-middle attacks, prevent important confidential data leakage and loss of important and valuable customer resource information, and must be highly valued.


Why adopt Always On SSL?
Not Always SSL
Only protect login page
Vulnerable to threats like hijacking and SSL Strip, risking loss of customer trust, compromised data and malware attacks
Hijacking and SSL Strip
HTTP
HTTPS
Always on SSL
Protects the entire user session, ensuring security from start to finish
Avoid hijacking (man-in-the-middle attacks) and SSL Strip
Always over HTTPS for security
HTTPS

Finally, the author summarizes two important points:

(1) All websites must implement https encryption, regardless of the size of the website and the owner of the website.

(2) It is not necessary to change the web server setting by yourself to implement https encryption, you

can choose the cloud services, which can easily realize https encryption and cloud WAF protection with one click. It also meets the compliance requirements of the Cryptography Law and the Cyber Security Law.

Richard Wang

December 06, 2022
In Shenzhen, China